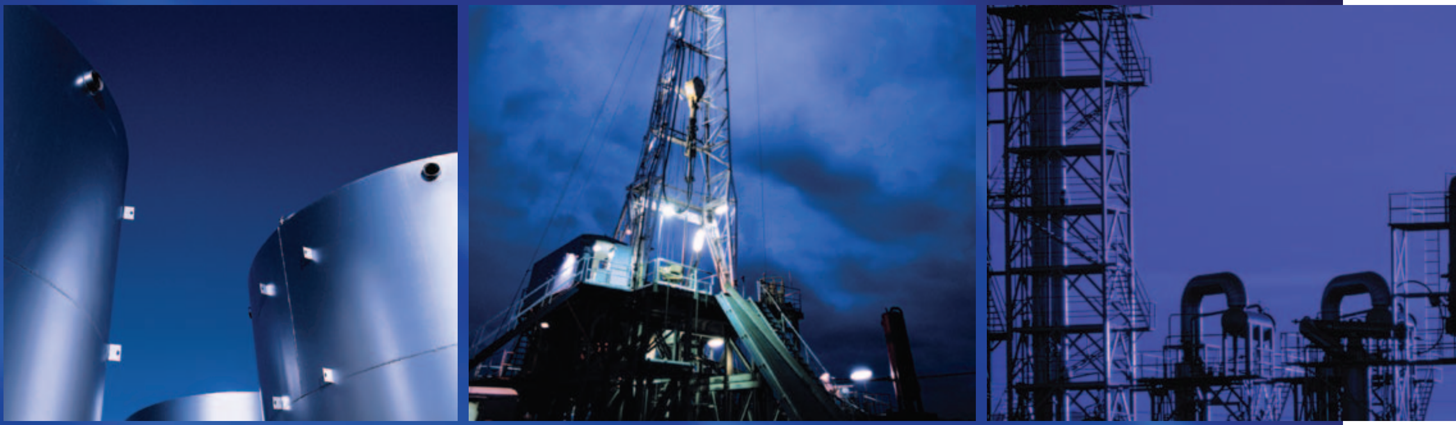


A Reference Security Management Plan for Energy Infrastructure

Prepared by the Harnser Group for the European Commission

Summer 2010

Under Contract TREN/C1/185/2009

A Reference Security Management Plan for Energy Infrastructure

Foreword

The European Union is developing its policy on critical energy infrastructures in relation to the European Programme for Critical Infrastructure Protection (“EPCIP”) which considers measures that will enhance, where necessary, the level of protection of certain infrastructures against external threats.

The integrity of energy infrastructures and their reliable operation are key factors in ensuring the supply in energy, vital for the well-being of the citizens and the functioning of the economy. For this reason energy infrastructure is considered as a priority for the implementation of the EPCIP, hence the policy adopted in December 2008, under Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the need to improve their protection, has the energy sector in its scope. As one of a number of requirements, this Directive included the creation of an Operator Security Plan for all infrastructures designated as European Critical.

The European Commission’s Directorate General for Energy tasked an external contractor to prepare a non-binding Reference Security Management Plan. This is intended to be a useful guidebook for operators of energy infrastructure Assets, systems or parts thereof, independent of its classification as European Critical or under other national category. This concentrates on malicious, human-origin threats, whilst paying attention to all related aspects of an operation.

The Reference Security Management Plan is written from the operator’s perspective, from the need to comply with existing national or international legal and technical frameworks, through to integrating good security risk management within the overall corporate strategic and governance objectives of the company responsible for the infrastructure.

Although this document sets out a complete process useful for creating a robust and enduring Operator Security Plan, operators may decide to use those elements that complement their existing policies and procedures.

Whatever the use made of this document by operators, the process contained therein contributes to a shared objective of improving the security of energy infrastructures.

Introduction

This Reference Security Management Plan is written in the form of a guidebook and has a single goal: To provide a practical methodology to help an owner/operator of an energy infrastructure Asset create and embed a robust and appropriate security framework around an Asset that can be adapted and updated as and when change occurs.

The methodology in the guidebook is presented as a complete process supported by guidance notes and templates to assist a Security Manager in the development and implementation of a Security Management Plan for a specific Asset, that not only fits within the overall risk management framework of the owner/operator, but also reflects best-practice thinking on all aspects of risk identification, assessment, design and implementation.

The process is based on the security risk management methodology developed under PRISM™, a Performance and Risk-based Integrated Security Methodology developed by Harnser Group aimed at delivering practical advice and guidance to companies working in the energy sector. It is based on experience and an understanding of the challenges that many Security Managers face in raising awareness of security and resilience issues within an owner/operator.

Primary ownership of security risk resides with the owners of energy infrastructure, regardless of location. Indeed the energy infrastructure network across the European Union transcends national boundaries in a complex supply chain of interdependent relationships, each with a different perspective and management of security risk.

By implementing the PRISM™ based approach set out in this guidebook, owners and operators of energy infrastructure Assets will have an assurance that there is a consistent approach towards security risk management across the supply chain capable of dealing with changes in a dynamic security environment. Owners and operators of energy infrastructure Assets will be able to invest and develop energy resources across the European Union in full confidence that the critical area of security risk is a) being managed in line with best-practice thinking; b) that corporate governance responsibilities are being met; and c) that by embedding good design principles from the outset of a new investment in an energy Asset will save money.

The methodology is modular, but must be implemented in full. This is so that the owner/operator of an energy infrastructure Asset can derive the full benefits of being seen to have a comprehensive security risk framework, the most important of which is that internal and external Stakeholders have full confidence that the Asset is secure and can therefore continue to operate without interruption.

PRISM™ is based on emerging best-practice in security risk management in relation to security and resilience. It also draws from other disciplines such as strategic planning, project management, technical design work, Stakeholder analysis and risk reporting. It encompasses not only the risk assessment methodology so fundamental to security risk management, but also the environment that the methodology has to operate within.

In the case of Energy Infrastructure, the goal of security is to take prevention, mitigation and responsive measures in order to ensure in relation to a given infrastructure:

The integrity of the Assets

The reliable supply of energy

The health of the workers

The health of the public

The respect for the environment

In common with risk-based models for credit, market and operational risk, there is a recognition amongst risk practitioners and regulators that the environment around the risk model is of equal importance. Without this, the ability of users to understand the model itself, apply it and monitor it, is limited.

Process Overview

The methodology set out in the guidebook is shown in Diagram B. It is comprised of four stages that are modular in nature, yet together define the security risk management framework that need to be addressed in order to produce the Security Management Plan.

Phase A: Strategy & Planning

The first phase relates to the strategy and planning environment around the Security Management Plan. It sets the context and regulatory environment the Security Management Plan has to operate within.

It has four sections:

1. **Rationale:** Why a Security Management Plan is recommended for the Asset and the history of the critical infrastructure protection in the European Union. It also includes a review of key European regulatory initiatives and international standards the author should be aware of.

2. **Stakeholder Analysis:** Provides a series of frameworks and questionnaires to use in order to identify who the key internal and external Stakeholders are, their level of interest and influence over the development and implementation of the Security Management Plan.

3. **Securing the Enterprise:** Explains how to assess the risk management framework within the owner/operator and identify how best to position the Security Management Plan within it.

4. **Planning:** Presents several useful planning tools to oversee the development of the Security Management Plan which require a number of quite complex and time-consuming tasks to be completed. These are included simply as guidance, however, if other planning tools exist then those should be used.

Phase B: Assessment

The Assessment phase is a central feature of a Security Management Plan and encompasses a detailed Security Risk Assessment (SRA), which provides the owner/operator with a framework to identify the range of possible risks facing their business and assess the likelihood of each risk materialising, as well as its potential impact. Each risk is scored using the following:

Risk = Threat x Vulnerability x Impact

Before risk scoring can take place several individual and sequential assessments need to occur:

I. **Asset Criticality:** An identification of Assets at a corporate level and ranking by potential impact in order to provide an overall priority list.

II. **Threat Assessment:** An assessment of the general threat environment around the Asset and the identification of the specific types of threat to the Asset. Rather than simply assessing the risk of ‘terrorism’ the goal is to identify specific threat scenarios within this category that may be faced by the operator.

III. **Vulnerability Assessment:** An assessment of the Asset’s vulnerability to the identified threat scenarios and therefore the likelihood of a successful attack. This will be done by objectively testing existing capability in the key areas of Detection, Delay and Response.

The guidebook provides the Security Manager with information, templates and spreadsheets to help them conduct the above assessments, following on from which the information will be collated in the form of a **Risk Register**. The Risk Register will generate overall scores for each identified risk to allow the Security Manager to decide whether or not specific mitigation actions are necessary. As such it will form the basis for all subsequent decisions regarding security systems deployment, and will provide a tool for ongoing monitoring of risk levels.

The final part of the Assessment stage will be to create a set of formal security system **‘Protection Objectives’**, which can then be signed off by senior management and other Stakeholders. The Protection Objectives will be high-level statements derived directly from the Risk Register, which form the basis for security systems design.

Security in this context is to be understood as “the safety of a state or organisation against criminal activity such as terrorism or espionage” (Source: Oxford English Dictionary)

Phase C: Design

In simple terms there are two elements to effective security systems design. The first element is to ensure that security systems are designed to mitigate specific risks; and the second element is that the security systems must be designed to deliver a level of performance that will mitigate those risks effectively, thus bringing the level of each risk to within the operator's risk appetite. The integration of risk and performance in this manner is the central theme of the PRISM™ approach.

The design phase focuses on the four core functions of a successful security regime – Detection, Delay, Response & Recovery – and consists of two separate levels as discussed below:

Level 1 Design: Risk-based Performance Requirements

The level 1 design process translates each of the established risks and associated protection objectives into a series of performance requirements in the areas of DDRR.

Level 2 Design: Performance-based Security Requirements

The level 2 design process identifies security systems and sub-components which can meet the DDRR performance requirements established under level 1. In order to meet the required level of performance across all DDRR functions it will be necessary to address the requirement for an integrated security system, which will include Physical Security, IT Security, Security Procedures, and Security Personnel. The Security Management Plan will review each of these areas, discussing the capability of various sub-components to meet DDRR performance requirements and providing associated performance criteria and example applications.

By following the design process as outlined above the Security Manager will be able to develop a clear understanding of their requirements without any specialist security systems design knowledge. Subsequently they will be able to use these requirements as the basis for effective engagement with external providers (preferably independent design consultants) – setting clear and focused performance criteria which their detailed systems design must meet and for which they will be held accountable. By embedding good security design into a new build of an energy Asset early on and applying the tendering advice presented in Phase D, the owner of that Asset will have the confidence that the money spent on security will be effective and enduring.

Phase D: Implementation & Review

Once the design phase has been completed and signed off by the operator's management team, the project will move onto the implementation and review phase. The guidebook provides the Security Manager with a set of tools to ensure the work they have proposed in the Security Management Plan is completed and tested on time and in budget. Providing this assurance to the finance department of the owner/operator is a crucial part of securing buy-in to the Security Management Plan.

The first component of this will address security systems implementation, which is likely to be a critical factor in determining overall success of the operator's risk management strategy. Information will be provided with regards to the creation of a robust performance specification, which incorporates the key performance criteria established during the design phase.

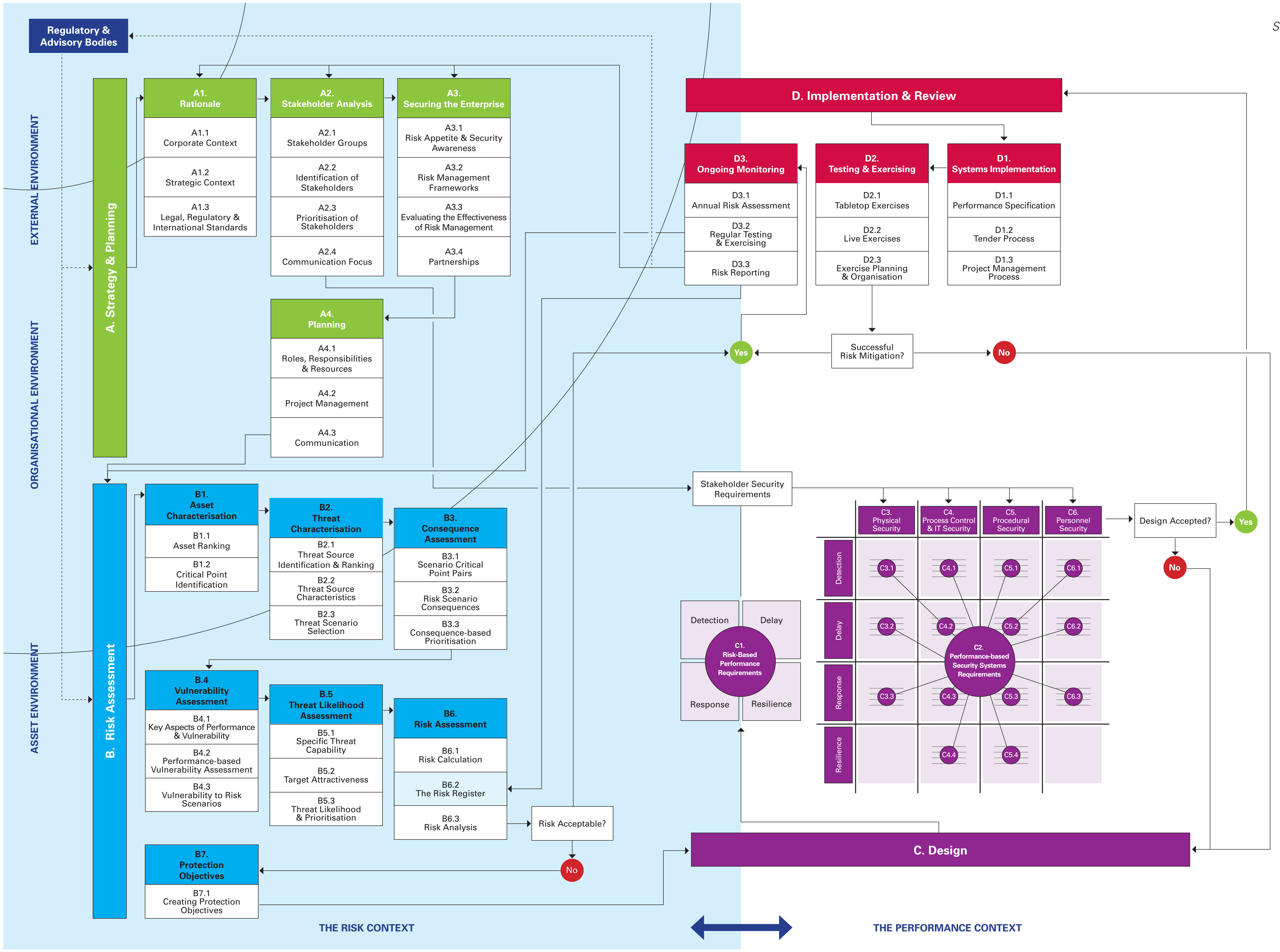
Tools will also be provided to support the tender evaluation process, ensuring that the most suitable contractor is selected to carry out the works. Project management will also be key to successful delivery and the Security Management Plan will include a formal framework which incorporates robust quality assurance, cost control and monitoring methods. Guidance will also be given in relation to independent System Acceptance Testing using the Rotakin standard and/or similar tools.

The next key element of the implementation phase within the Security Management Plan will be a testing and exercising programme that builds organisational capability to use and respond to the various security systems installed. This will take the operator through a structured programme starting with desktop exercising, moving on to live exercising and culminating in multi-agency exercises, therefore enhancing capability in successive and manageable steps.

The Security Management Plan will then explain how monitoring and review will occur to ensure that the security risk management framework implemented by the Security Management Plan remains current. The owner/operator will be provided with a range of tools for ongoing monitoring of security capability through regular security risk assessments and repeat exercises. In conjunction with a risk reporting framework this will ensure that the organisation is aware of any changes in risk levels or security capabilities and that adequate countermeasures are considered.

Stephen Gregory
Chief Executive Officer, Harnser Risk Group

Diagram A


Regulatory & Advisory Bodies
EXTERNAL ENVIRONMENT
ORGANISATIONAL ENVIRONMENT
ASSET ENVIRONMENT
A. Strategy & Planning
A1. Rationale
A1.1 Corporate Context
A1.2 Strategic Context
A1.3 Legal, Regulatory & International Standards
A2. Stakeholder Analysis
A2.1 Stakeholder Groups
A2.2 Identification of Stakeholders
A2.3 Prioritisation of Stakeholders
A2.4 Communication Focus
A3. Securing the Enterprise
A3.1 Risk Appetite & Security Awareness
A3.2 Risk Management Frameworks
A3.3 Evaluating the Effectiveness of Risk Management
A3.4 Partnerships
A4. Planning
A4.1 Roles, Responsibilities & Resources
A4.2 Project Management
A4.3 Communication
B. Risk Assessment
B1. Asset Characterisation
B1.1 Asset Ranking
B1.2 Critical Point Identification
B2. Threat Characterisation
B2.1 Threat Source Identification & Ranking
B2.2 Threat Source Characteristics
B2.3 Threat Scenario Selection
B3. Consequence Assessment
B3.1 Scenario Critical Point Pairs
B3.2 Risk Scenario Consequences
B3.3 Consequence-based Prioritisation
B.4 Vulnerability Assessment
B4.1 Key Aspects of Performance & Vulnerability
B4.2 Performance-based Vulnerability Assessment
B4.3 Vulnerability to Risk Scenarios
B.5 Threat Likelihood Assessment
B5.1 Specific Threat Capability
B5.2 Target Attractiveness
B5.3 Threat Likelihood & Prioritisation
B6. Risk Assessment
B6.1 Risk Calculation
B6.2 The Risk Register
B6.3 Risk Analysis
Risk Acceptable?
No
B7. Protection Objectives
B7.1 Creating Protection Objectives
D. Implementation & Review
D3. Ongoing Monitoring
D3.1 Annual Risk Assessment
D3.2 Regular Testing & Exercising
D3.3 Risk Reporting
D2. Testing & Exercising
D2.1 Tabletop Exercises
D2.2 Live Exercises
D2.3 Exercise Planning & Organisation
D1. Systems Implementation
D1.1 Performance Specification
D1.2 Tender Process
D1.3 Project Management Process
Successful Risk Mitigation?
Yes
No
Stakeholder Security Requirements
C3. Physical Security
C4. Process Control & IT Security
C5. Procedural Security
C6. Personnel Security
Design Accepted?
Yes
No
Detection
Delay
Response
Resilience
C1. Risk-Based Performance Requirements
Detection
Delay
Response
Resilience
C3.1
C4.1
C5.1
C6.1
C3.2
C4.2
C5.2
C6.2
C3.3
C4.3
C5.3
C6.3
C4.4
C5.4
C2. Performance-based Security Systems Requirements
C. Design
THE RISK CONTEXT
THE PERFORMANCE CONTEXT

Source: PRISM™

How to use this Reference Security Management Plan

This Reference Security Management Plan for energy infrastructure owners/operators is a practical guidebook for Security Managers to use in order to prepare and implement a Security Management Plan for a specific Asset(s) and is applicable to any energy infrastructure Asset in any country in the European Union.

It should be read in conjunction with the blank template for the Security Management Plan that can be downloaded from the website **www.prismworld.org**. Each phase of the guidebook refers to a specific section in the template. It explains clearly how to undertake the analysis and reach recommendations that would be presented in the Security Management Plan and submitted for approval and sign-off by the appropriate governing body within the owner/operator.

Energy infrastructure Assets share many similar characteristics although the environment that they operate within, whether external or organisational, can be very different. The Security Management Plan produced as a result of using this guidebook will be for a specific Asset – your Asset.

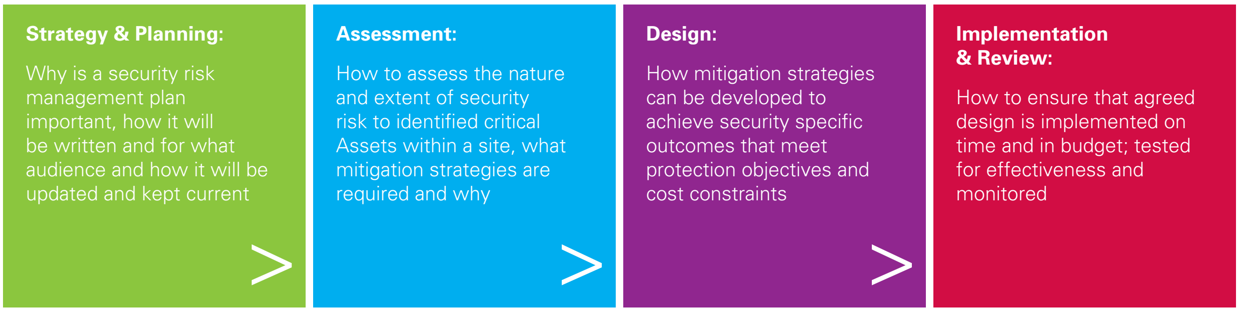
There are several stages involved in focusing on an issue such as security risk and embedding it into the corporate governance framework of the owner/operator. These are similar to any planning activity whether instigated by an external or internal event and are reflected in each part of the process as shown below.

It is acknowledged that the security environment around energy infrastructure Assets across the European Union varies from country to country and access to information on that security environment will also vary. As mentioned in the Introduction, the methodology must be applied in total, even when the gap between what is observed around the Asset, and what is recommended in the guidebook, seem far apart. This is the start of a process and every plan will need to be updated, not only in response to developments within the Asset(s) itself, but also as the security environment changes.

The process set out in this guidebook is based on a methodology called PRISM™ (Performance Risk-based Integrated Security Methodology) developed by the Harnser Group. Further information on PRISM™ is available on **www.prismworld.org**. More detail on this is provided in the Introduction.

If you have any questions or comments on any part of the process set out in the guidebook, please register these on **www.prismworld.org** in the Community area of the website. This is a secure and confidential environment in which to post questions and comments, seek advice, share developments on security risk management and the practical implications of any research or policy initiatives that could affect you and the owner/operator you work for.

Diagram B



Strategy & Planning:
Why is a security risk management plan important, how it will be written and for what audience and how it will be updated and kept current

Assessment:
How to assess the nature and extent of security risk to identified critical Assets within a site, what mitigation strategies are required and why

Design:
How mitigation strategies can be developed to achieve security specific outcomes that meet protection objectives and cost constraints

Implementation & Review:
How to ensure that agreed design is implemented on time and in budget; tested for effectiveness and monitored

Disclaimer

The content of this Study reflect the views and knowledge of the author, Harnser Risk Group Limited, and may not be regarded as stating an official position of the European Commission. In particular, it should be noted that this Study does not intend to establish a model Operator Security Plan as defined in Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

The Study has been prepared with the purpose of providing energy infrastructure operators with a comprehensive methodology for achieving corporate and regulatory requirements as they relate to security risk management.

Harnser Risk Group Limited makes no express or implied representations or warranties regarding these materials or the information contained therein. Without limiting the foregoing, Harnser Risk Group Limited does not warrant that the materials or information contained therein will be error-free or will meet any particular criteria of performance or quality. Harnser Risk Group Limited expressly disclaims all implied warranties, including, without limitation, warranties of merchantability, title, fitness for a particular purpose, non-infringement, compatibility, security, and accuracy.

Your use of these materials and information contained therein is at your own risk, and you assume full responsibility and risk of loss resulting from the use thereof. Harnser Risk Group Limited will not be liable for any special, indirect, incidental, consequential, or punitive damages or any other damages whatsoever, whether in an action of contract, statute, tort (including, without limitation, negligence), or otherwise, relating to the use of these materials or the information contained therein.

If any of the foregoing is not fully enforceable for any reason, the remainder shall nonetheless continue to apply.

Harnser Risk Group Limited, 2010

Contents

A Strategy & Planning

B Risk Assessment

C Design

D Implementation & Review

Bibliography, Glossary and Acronyms

Phase A

Strategy & Planning

Executive Summary – Strategy & Planning

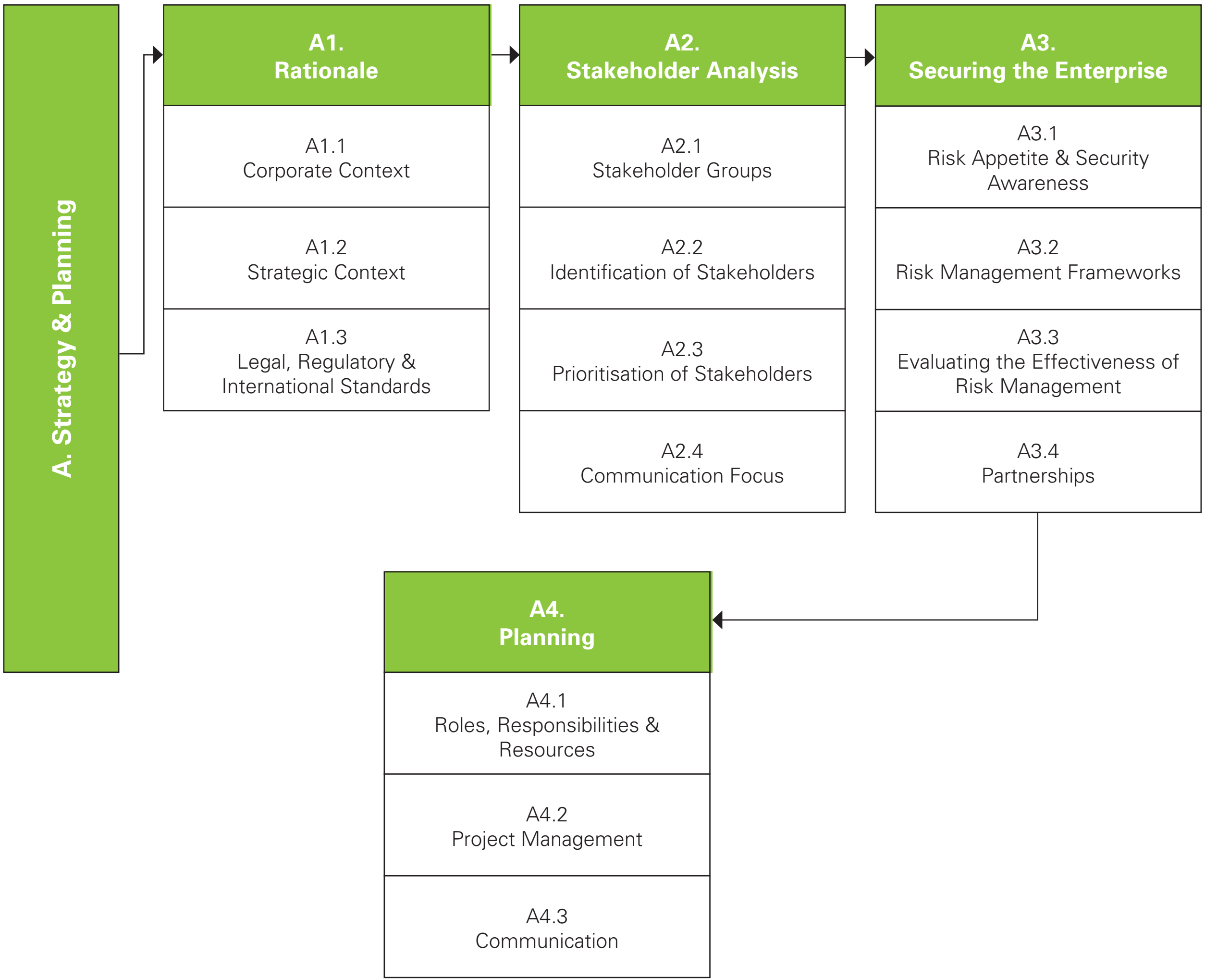
This section defines the external and organisational environment the Security Management Plan has to operate within in order to achieve its objectives.

If this environment is not identified before the Risk Assessment Phase begins, it is probable that the Security Management Plan will not receive the support it needs from key Stakeholders, will not be regarded as a critical area of risk for the owner/operator and will not reflect the important strategic factors that require its preparation or review.

One of the challenges of writing a plan is to make it relevant, interesting and worth the time of those who need to read it and approve it. Phase A provides the Security Manager with a range of tools that will help them explain:

A1 The rationale behind the Security Management Plan, in particular why and how security risk is important and how it impacts on key areas of corporate activity. It considers the strategic drivers that have placed security risk at the forefront of thinking about risk management in the 21st century before summarising the key regulatory and international standards that the Security Management Plan has to function within.

A2 The importance of a good Stakeholder analysis of external and internal parties in the preparation and implementation of the Security Management Plan. In particular, the prioritisation of their interests and influence on the process and outcomes, and how to communicate with them before, during and after the process.



A. Strategy & Planning

A1. Rationale
- A1.1 Corporate Context
- A1.2 Strategic Context
- A1.3 Legal, Regulatory & International Standards

A2. Stakeholder Analysis
- A2.1 Stakeholder Groups
- A2.2 Identification of Stakeholders
- A2.3 Prioritisation of Stakeholders
- A2.4 Communication Focus

A3. Securing the Enterprise
- A3.1 Risk Appetite & Security Awareness
- A3.2 Risk Management Frameworks
- A3.3 Evaluating the Effectiveness of Risk Management
- A3.4 Partnerships

A4. Planning
- A4.1 Roles, Responsibilities & Resources
- A4.2 Project Management
- A4.3 Communication

A3 The importance of placing the Security Management Plan into the core risk management structure adopted by the owner/operator across key risks they are aware of and prioritise. To use a simple analogy: There is no point in throwing a ball, if there is no-one there to catch it. One of the challenges many Security Managers face is raising awareness about the risk they are responsible for within the organisation they work for. This needs to be done if the Security Management Plan is to have any chance of success.

A4 Managing the preparation of the Security Management Plan as a Project helps to raise its profile and ensure the right resources are available to the Security Manager as they undertake the considerable amount of work required to prepare it. A series of simple tools are provided in A4 to assist the Security Manager with this process.

Security Managers are aware of the external and internal environment they work within on a day-to-day basis. Phase A introduces a number of business management concepts that will help the Security Manager position the Security Management Plan within that environment to ensure its successful implementation. By identifying these beforehand, the process of raising awareness and securing buy-in to the Security Management Plan at the right time, will happen as and when you, the Security Manager, need it.

A1 Rationale for a Security Management Plan

Purpose: To explain to the reader how changes at a strategic level have resulted in a complex multi-layered legal, regulatory and best-practice environment that a Security Management Plan needs to operate within.

To provide a justification for the investment that may be required to implement the Security Management Plan.

The Security Manager will need to research their own national or regional framework and add this onto the tables provided in the template for this section.

A1.0 Introduction

One of the challenges many Security Directors and Managers have to deal with is a lack of understanding about what security risk is and why it is of importance to the organisation they work in. This is why the PRISM™ approach places emphasis on understanding the external and internal environment that a Security Management Plan has to operate within. It seeks to align the Security Management Plan alongside and within the internal control framework adopted by the Board of Directors as part of their corporate governance responsibilities. As a consequence the Security Management Plan will have visibility and acceptance within the owner/operator and have a greater chance of implementation. Once this has been achieved, maintaining a high level of awareness and communicating effectively in order to do so, is a key ongoing process once the Security Management Plan has been approved and implemented.

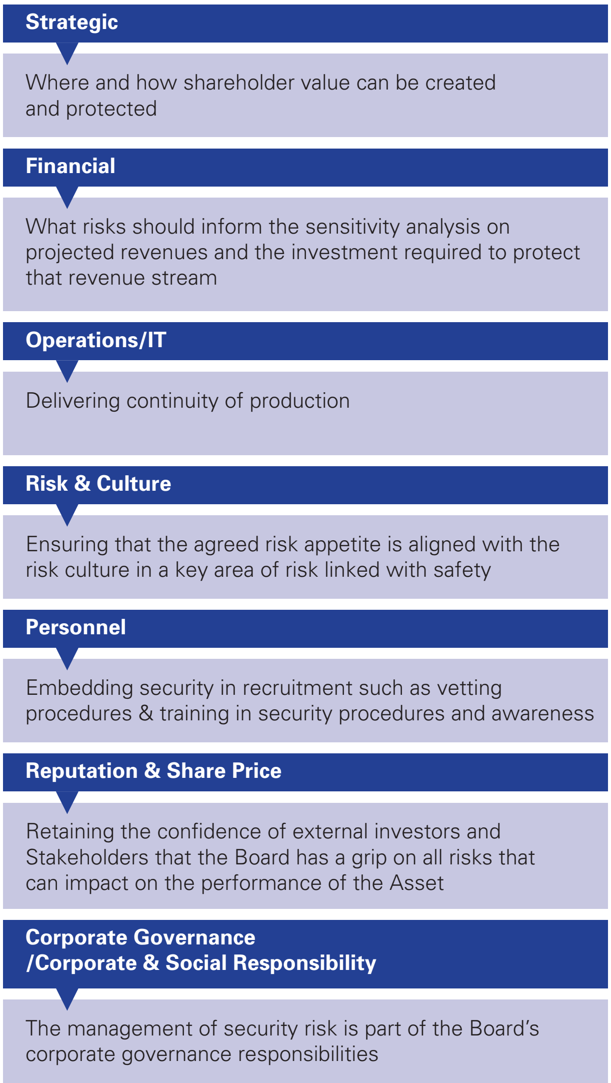
This Section explains how you should set the context for the Security Management Plan and complete the relevant section of the template.

> *One of the challenges many Security Directors and Managers have to deal with is a lack of understanding about what security risk is*

A1.1 Corporate Context

The aim of security risk management is to provide a secure, protective, environment around the Assets of the owner/operator anywhere in the world. Why does this matter? So that other important areas of activity within the organisation can happen without disruption. For example:

Diagram A1a: Corporate Stakeholders



Strategic

Where and how shareholder value can be created and protected

Financial

What risks should inform the sensitivity analysis on projected revenues and the investment required to protect that revenue stream

Operations/IT

Delivering continuity of production

Risk & Culture

Ensuring that the agreed risk appetite is aligned with the risk culture in a key area of risk linked with safety

Personnel

Embedding security in recruitment such as vetting procedures & training in security procedures and awareness

Reputation & Share Price

Retaining the confidence of external investors and Stakeholders that the Board has a grip on all risks that can impact on the performance of the Asset

Corporate Governance /Corporate & Social Responsibility

The management of security risk is part of the Board's corporate governance responsibilities

Source: PRISM™

With security risk having a potential impact on so many important areas of activity within an owner/operator, it is always a surprise to observe that the issue itself is so little understood and rarely discussed amongst the different Stakeholder groups who have an interest in continuity of production. Nevertheless the security environment is dynamic and the Security Management Plan you are going to either write or update, must be reviewed regularly as part of an annual planning process managed by the owner/operator to protect the value of the Assets they are responsible for.

In this section of the Security Management Plan template you need to refer to this challenge and include reference to the areas noted above where a knowledge of security risk is important. The reader of the Security Management Plan should then be aware from the outset why they are reading it and how it is relevant to them.

A1.2 Strategic Context

This section of the Security Management Plan should provide the reader with a view on those key drivers that have positioned the security of energy Assets as a matter of national interest. For example, economic trends and the demand for energy, concerns over health and safety, the environmental agenda, changes in geopolitics etc. The purpose of this section is to explain the strategic context for the Security Management Plan from the owner/operator's perspective which will also contribute to the business and financial justification for a potential investment of resources to implement any recommendations in the Security Management Plan.

The challenge when looking at big picture issues is to answer the question 'why is this important to me?' So it is more than a list of events, but an interpretation of what has changed and why and how this has affected the environment the Asset operates within.

The following table provides an example of a strategic issue that has raised the profile of energy security over the last ten years or so. Complete the blank table in the template with what is relevant to your Asset and the owner/operator. There may be three to six or so key issues you wish to draw to the attention of the reader.

Some of the information you might need to complete the table will be derived from the questionnaires you are going to use later in Phase A.

Table A1a: Drivers of the Security Risk Agenda

Issue	Impact	Comment
Demand for energy supplies	On all countries who rely on energy to fuel economic development	Every operator has a growing demand for its activities, but also faces growing competition as other players seek to benefit from strong demand

A1.3 Legal, Regulatory & International Standards

In many countries across the EU, the strategic drivers you have noted in the previous section have resulted in not only legal and regulatory requirements for operators managing energy infrastructure Assets, but have also helped to influence the following:

- Best-practices set by some participants in the energy sector
- Standards institutes
- Business standards such as in Corporate Governance, Corporate and Social Responsibility, Directors' responsibilities etc.

Table A1b sets out key International standards, best-practice guidelines and Directives that tend to be applicable across all energy infrastructure owners/operators, but it is important that you add to this table those that you are aware of. This provides a critical record of the legal, regulatory, best-practice and international standard framework the Security Management Plan needs to operate within. Whilst many of these are common, there will be those operational at national level to be aware of, in particular those relating to the responsibilities of Boards of Directors.

In many countries across the EU, the strategic drivers you have noted in the previous section have resulted in not only legal and regulatory requirements for operators managing energy infrastructure Assets

Table A1b: Summary of key International Standards, Best-Practice Guidelines and European Commission Directives as at Summer 2010

Area	International Standard/Best-Practice Guidelines	European Commission Directives
Health & Safety	**OHSAS 18001**	**The Seveso II Directive**
	OHSAS 18001 is an international occupational health and safety management system specification which seeks to help organisations in a variety of respects such as minimising risk to employees/etc; improve an existing OH&S management system; demonstrate diligence; gain assurance; etc.	The Seveso Directive is the main piece of EU legislation that deals specifically with the control of onshore major accident hazards involving dangerous substances. The Seveso II Directive includes a revision and extension of the scope, the introduction of new requirements relating to safety management systems, emergency planning and land-use planning and a reinforcement of the provisions on inspections to be carried out by Member States.
Transport of hazardous materials by sea	**The International Maritime Dangerous Goods (IMDG) Code**	**European Community Waste Shipments Regulation**
	The **IMDG Code** was developed as a uniform international code for the transport of dangerous goods by sea covering such matters as packing, container traffic and stowage, with particular reference to the segregation of incompatible substances.	This aims to ensure that waste is properly handled from the time it is shipped to the time it is disposed of or recovered at destination. To achieve its objectives the regulation reinforces and clarifies the current legal framework for waste shipment within the EU and with non-EU countries.
Transport of hazardous materials by other methods	**United Nations Recommendations on the Transport of Dangerous Goods.**	The **European Agreement concerning the International Carriage of Dangerous Goods by Road,** commonly known as **ADR**
	This covers the transport of dangerous goods by all modes of transport except by bulk tanker. They are not obligatory or legally binding on individual countries, but have gained a wide degree of international acceptance: they form the basis of several international agreements and many national laws.	This article states that with the exception of certain exceptionally dangerous materials, hazardous materials may in general be transported internationally in wheeled vehicles, provided that two sets of conditions be met: 1. Annex A regulates the merchandise involved, notably their packaging and labels. 2. Annex B regulates the construction, equipment and use of vehicles for the transport of hazardous materials.
		Directive 2008/68/EC
		Directive 2008/68/EC on the inland transport of dangerous goods[1], adopted in 2008, aims at guaranteeing the safe transport of dangerous goods by road, rail and inland waterways. It is in line with international agreements and ensures harmonised and safe conditions for all land transport of dangerous goods in the EU.
Ship and Port Security	**International Ship and Port Facility Security (ISPS) Code**	**Directive 2005/65/EC(1)**
	The purpose of the **ISPS Code** is to provide a standardised, consistent framework for evaluating risk, enabling Governments to offset changes in threat with changes in vulnerability for ships and port facilities through determination of appropriate security levels and corresponding security measures. The Code is a two-part document describing minimum requirements for security of ships and ports. Part A provides mandatory requirements. Part B provides guidance for implementation.	The main objective of the **Directive 2005/65/EC(1)** is to complement the measures adopted in 2004 by means of Regulation (EC) No 725/2004(2) of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security ('the Regulation'). The main objective of the Regulation was to implement Community measures aimed at enhancing ship and port facility security in the face of the threats posed by intentional unlawful acts. The maritime measures imposed by the Regulation are only some of the measures necessary in order to achieve an adequate level of security across all of the various transport chains linked to maritime transport. The Regulation is limited in scope to security measures onboard vessels and the immediate ship/port interface.

Table A1b: Summary of key International Standards, Best-Practice Guidelines and European Commission Directives as at Summer 2010

Area	International Standard/Best-Practice Guidelines	European Commission Directives
Risk Management	**International Standard, ISO 31000:2009, Risk Management – Principles and Guidelines.**	**Federation of Risk Management Associations (FERMA)**
	ISO 31000:2009 will help organisations of all types and sizes to manage risk effectively.	**FERMA Risk Management Standard** sets out a strategic process, starting with an organisation's overall objectives and aspirations, through to the identification, evaluation and mitigation of risk, and finally the transfer of some of that risk to an insurer.
Environment	**ISO 14001 – International standard for an Environmental Quality Management System (EMS).**	**Directive 2004/35/CE**
	ISO 14001 is an internationally accepted standard that sets out a framework of essential elements for putting an effective Environmental Management System (EMS) in place. The standard is designed to address the delicate balance between maintaining profitability and reducing environmental impact.	**Directive 2004/35/CE** of the European Parliament and of the Council of 21 April 2004 on environmental liability with regard to the prevention and remedying of environmental damage.
		Directive 2008/99/EC
		Directive 2008/99/EC of the European Parliament and of the Council of 19 November 2008 on the protection of the environment through criminal law.
		Directive 2006/12/EC
		Directive 2006/12/EC establishes a legal framework for the treatment of waste within the Community. It aims at protecting the environment and human health through the prevention of the harmful effects of waste generation and waste management.
		Regulation (EC) No 1221/2009
		Regulation (EEC) No 761/2001 of the European Parliament and of the Council of 19 March 2001 allowing voluntary participation by organisations in a Community eco-management and audit scheme (EMAS). The EU EMAS is a management tool for companies and other organisations located inside or outside the Community to evaluate, report and improve their environmental performance. The scheme has been available for participation by companies since 1995 and was originally restricted to companies in industrial sectors. Since 2001 EMAS has been open to all economic sectors including public and private services.
IT Security	**ISO/IEC 27001 – The International Standard for Information Security Management.**	**Directive 2009/140/EC**
		Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.
		Directive 2006/24/EC
	ISO/IEC 27001 is the only auditable international standard which defines the requirements for an Information Security Management System (ISMS). The standard is designed to ensure the selection of adequate and proportionate security controls to help organisations protect information Assets and give confidence to any interested parties, especially customers.	**Directive 2006/24/EC** of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

Table A1b: Summary of key International Standards, Best-Practice Guidelines and European Commission Directives as at Summer 2010

Area	International Standard/Best-Practice Guidelines	European Commission Directives
Security of supply	**International Energy Agency**	**Directive 2005/89/EC**
		Directive 2005/89/EC of the European Parliament and of the Council of 18 January 2006 concerning measures to safeguard security of electricity supply and infrastructure investment.
	The International Energy Agency (IEA) is an intergovernmental organisation which acts as energy policy adviser to 28 member countries in their effort to ensure reliable, affordable and clean energy for their citizens. Its mandate has broadened to incorporate the "Three E's" of balanced energy policy making: energy security, economic development and environmental protection. Current work focuses on climate change policies, market reform, energy technology collaboration and outreach to the rest of the world, especially major consumers and producers of energy like China, India, Russia and the OPEC countries.	**Directive 2006/67/EC**
		Directive 2006/67/EC of 24 July 2006 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products.
	ISO 28000: 2007 Specification for security management systems for the supply chain specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organisations that impact on supply-chain security. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.	
Critical Infrastructure Protection	**Critical Infrastructure Protection**	**EPCIP – European Programme for Critical Infrastructure Protection**
	The USA has had a wide-reaching **Critical Infrastructure Protection** Program in place since 1996. Its Patriot Act of 2001 defined critical infrastructure as those "systems and Assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and Assets would have a debilitation impact on security, national economic security, national public health or safety, or any combination of those matters."	
	Centre for the Protection of National Infrastructure	**Directive 2008/114/EC**
	In the UK the **Centre for the Protection of National Infrastructure** provides information, personnel and physical security advice to the businesses and organisations which make up the UK's national infrastructure, helping to reduce its vulnerability to terrorism and other threats.	**Council Directive 2008/114/EC** of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. European Programme for Critical Infrastructure Protection, EPCIP. **2007/124/EC, Euratom: Council Decision of 12 February 2007** establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks." Seventh Framework Programme for Research (FP7) 2007-2013, Security Research.
	ISO/PAS 22399:2007 Social Security – Guideline for incident preparedness and operational continuity management.	

Table A1b: Summary of key International Standards, Best-Practice Guidelines and European Commission Directives as at Summer 2010

Area	International Standard/Best-Practice Guidelines	European Commission Directives
Emergency Planning & Resilience	**ISO/PAS 22399:2007** provides general guidance for private, governmental, and nongovernmental organisations – to develop their own specific performance criteria for incident preparedness and operational continuity, and design an appropriate management system. It provides a basis for understanding, developing, and implementing continuity of operations and services within an organisation and to provide confidence in business, community, customer, first responder, and organisational interactions. It also enables the organisation to measure its resilience in a consistent and recognised manner.	**2007/124/EC, Euratom: Council Decision of 12 February 2007** establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks. Prevention, preparedness and consequence management of terrorism and other security related risks are essential aspects of the protection of people and critical infrastructure within the area of freedom, security and justice. This programme aims to support Member States' efforts to prevent, to prepare for, and to protect people and critical infrastructure against terrorist attacks. It also aims to ensure protection in the field of terrorism and other security related risks.
	ANSI/ASIS SPC.1-2009 Organisational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use. A management framework for action planning and decision making needed to anticipate, prevent if possible, and prepare for and respond to a disruptive incident (emergency, crisis or disaster).	

A1.4 Summary

This section of the Security Management Plan defines the strategic, legislative and best-practice environment around the Asset and provides the context for the document itself. The reader should have no doubt why having a Security Management Plan is necessary, why the investment that could be required to implement it should be regarded as a priority and why it should be included as part of the risk management framework used by the owner/operator and monitored on an ongoing process.

The reader should have no doubt why having a Security Management Plan is necessary, why the investment that could be required to implement it should be regarded as a priority and why it should be included as part of the risk management framework used by the owner/operator and monitored on an ongoing process.

A2 Stakeholder Analysis

Purpose: To identify and understand the interest and influence that key external and internal Stakeholders have on the preparation and implementation of the Security Management Plan.

The Security Manager can then manage their expectations, secure their input and communicate with them on a timely basis during the entire planning process and on an ongoing basis as appropriate. This is particularly important if the raised level of awareness of security risk issues generated by undertaking the process of developing or updating and implementing the Security Management Plan is to be maintained and embedded in the risk culture of the owner/operator.

A2.0 Introduction

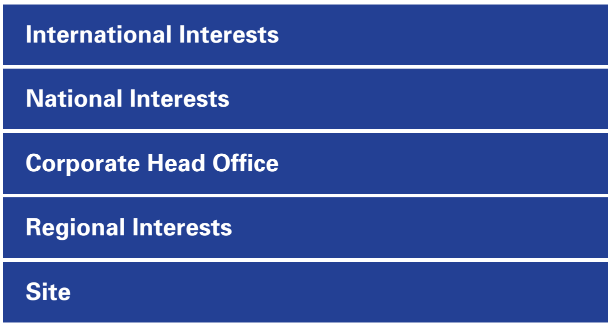
Stakeholders are defined as those parties who have an interest in, and influence on, the work of the Security Manager and the effectiveness of the Security Management Plan. Without the approval and support of all Stakeholders, you will struggle to get the support and resources you need to implement it.

The level of awareness about security risk management issues is covered under Section A3, but by undertaking a Stakeholder analysis and communicating with each group in the right manner, the profile of security risk will be enhanced within each of those Stakeholder groups. So right from the outset of your work to develop a Security Management Plan, you need to know who the key internal and external Stakeholders are and how to engage with them.

A2.1 Stakeholder Groups

The next two diagrams show the various levels of Stakeholder interests and are generic – each Asset and Operator will have slightly different Stakeholder names, so try and obtain the latest organisational structure chart for the environment that you are working within.

Diagram A2a: Stakeholder Groups



International Interests

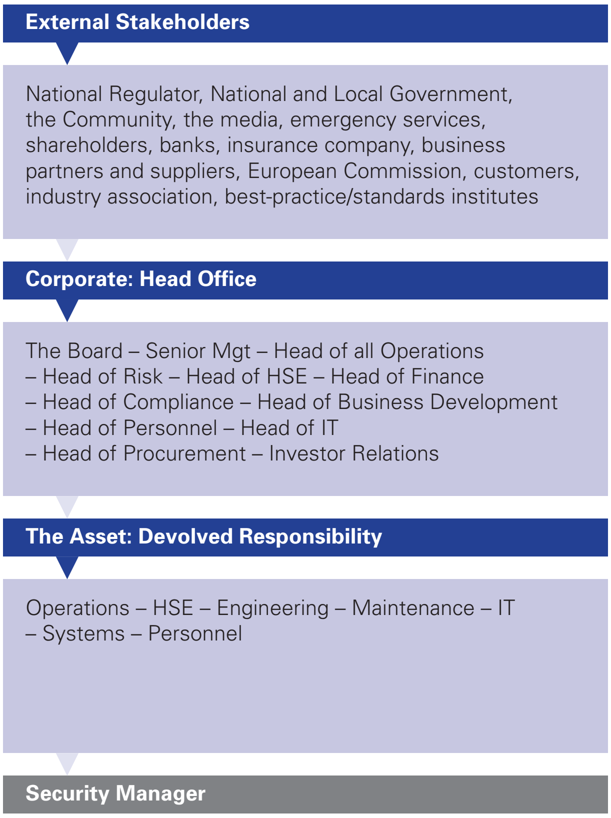
National Interests

Corporate Head Office

Regional Interests

Site

Diagram A2b: Stakeholder Groups



External Stakeholders

National Regulator, National and Local Government, the Community, the media, emergency services, shareholders, banks, insurance company, business partners and suppliers, European Commission, customers, industry association, best-practice/standards institutes

Corporate: Head Office

The Board – Senior Mgt – Head of all Operations – Head of Risk – Head of HSE – Head of Finance – Head of Compliance – Head of Business Development – Head of Personnel – Head of IT – Head of Procurement – Investor Relations

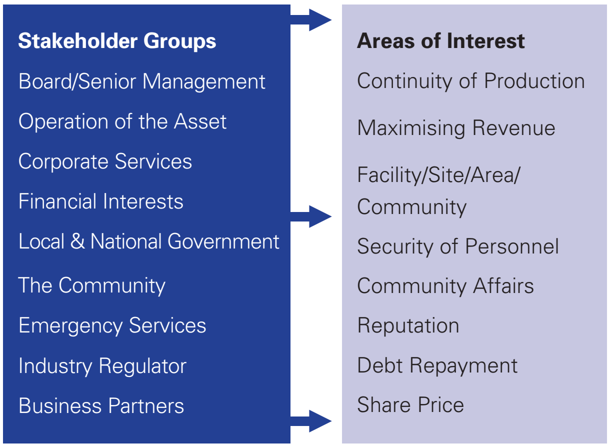
The Asset: Devolved Responsibility

Operations – HSE – Engineering – Maintenance – IT – Systems – Personnel

Security Manager

It is impossible for one person to manage all the expectations of these Stakeholders and not all of them are of equal importance, however, they do share a similar interest in the smooth operation of the Asset, as noted in the diagram A2c:

Diagram A2c: Stakeholder Interests in an Asset



Stakeholder Groups

Board/Senior Management

Operation of the Asset

Corporate Services

Financial Interests

Local & National Government

The Community

Emergency Services

Industry Regulator

Business Partners

Areas of Interest

Continuity of Production

Maximising Revenue

Facility/Site/Area/ Community

Security of Personnel

Community Affairs

Reputation

Debt Repayment

Share Price

All the Stakeholders want to see the Asset delivering those attributes on the right hand side of the diagram and you play a key role in ensuring a secure environment around it to ensure that happens.

A2.2 Identification of Stakeholders

As mentioned earlier, Stakeholders are those individuals and organisations that have an interest in, and impact on, the development and implementation of the Security Management Plan. Those who are able to determine how an enhanced security environment would benefit the Asset will be those working within the operation itself. These will be both internal and external to the operation of the Asset. Once you have identified these, you may end up with a list similar to the one shown in the table below:

Table A2a: External and Internal Stakeholders

External Stakeholder Groups	Impact Stakeholder Groups
Industry Regulator	The Board
Local & National Government	Operations
Emergency Services, including Police, Fire & Ambulance	HSE
Key Suppliers	Personnel/HR
The Community	Maintenance
Interest Groups	Finance/Performance
	Procurement
	IT

Right from the outset of your work to develop a Security Management Plan, you need to know who the key internal and external Stakeholders are and how to engage with them.

In our experience, the following individuals constitute about 90% of the key Stakeholders who have both an interest in and influence on, the outcome of the Security Management Plan. These individuals would contribute to either a) the identification of risk appetite and/or b) the identification of security requirements.

Table A2b: Key Stakeholder Interests

Title/Role	Rationale
Chief Executive or Deputy	To identify the owner/operator strategic security requirements for the Asset
The Security Manager's Manager	Responsible for how the Security Manager spends their time and for agreeing objectives and resources for them
Head of HSE, who might be the above	Responsible for visible risks such as safety and environmental, both of which will have legislative and/or regulatory obligations around them. This person is a key 'champion' of security who will not only establish what the Ops and HSE requirements are from a security perspective, but who will also need to embed reporting on it alongside other reports monitoring HSE risks post implementation.
Head of Operations for the Asset	Responsible for the overall security of the Asset and accountable if something goes wrong. They must understand every aspect of the Security Management Plan and be able to communicate and engage with external Stakeholders about it. They will also hold a budget and report into Head Office.
Head of Personnel for the Asset	Responsible for all hiring, training and dealing with staff issues so a key contributor to the Security Management Plan as regards personnel screening and vetting for employees and contractors.
Financial Controller responsible for the budget of the Asset	Able to sign off on the financial impact of any security risks identified by the Security Management Plan. This will need to be approved, perhaps as exceptional expenditure, and managed as part of a structured programme of investment. The Security Plan provides the rationale for any expenditure and must include any financial cost:benefit analysis in accordance with corporate policy.
Head of Procurement for the Asset	The purchase of any advice, materials etc would need to be undertaken via Procurement so it is important to engage with this department so they are able to become involved at the right stage. They may also be required to sign off any request for financial resources from the Finance department, and deal with any variances if they occur.
Head of Maintenance	Able to establish capability of maintenance department to conduct non-technical aspects of security systems maintenance and any specific requirements.
Head of IT	Able to establish existing IT infrastructure and IT Dept's requirements for integration of security systems with existing applications or networks.
The person responsible for business partners/key suppliers who contribute towards the operation of the Asset	The security of the Asset will depend to some extent on third parties and these will be identified through the Stakeholder analysis work. Once identified, the dependencies and consequent security risks associated with them will be captured as part of the Security Management Plan.
Police Department	Establish their requirements for security systems at the Asset, as well as criminal activity of concern and available Police response times to the Asset site.
Fire & Ambulance Departments	Establish their requirements for emergency access, health and safety procedures and equipment, compliance with building codes and regulations.

The organisation chart should identify the scope of responsibility for key areas at a devolved level. Working out how to gain access to those offsite and gaining their input could require some planning and support from those within the Asset itself.

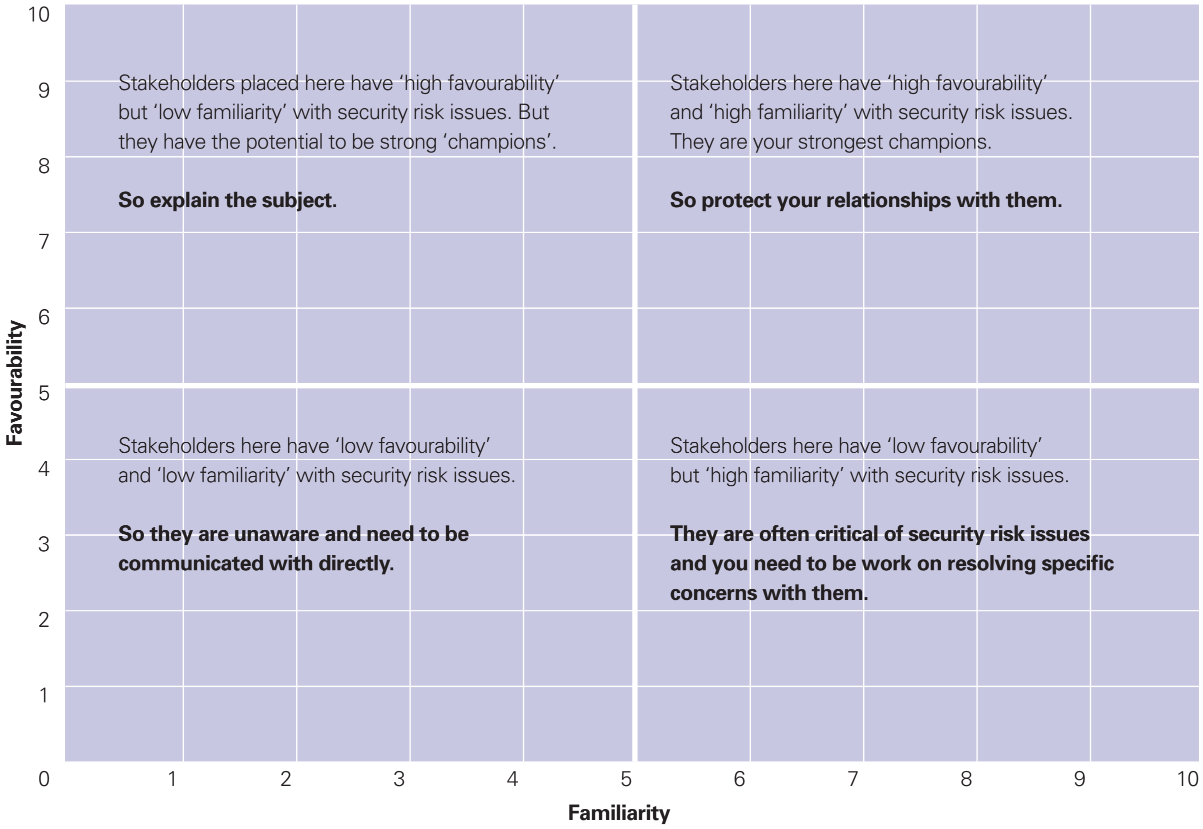
A2.3 Prioritisation of Stakeholders

Not all of the above will have the same level of interest and influence on the Security Management Plan so it is important to prioritise them. The first stage of this process is to use the matrix below to plot where you believe each Stakeholder to be based on the axes of:

Familiarity	How well does each Stakeholder understand security risk and what the Security Management Plan is seeking to achieve?
Favourability	How well disposed is each Stakeholder towards the development and, crucially, the implementation of the Security Management Plan?

By going through this process you will have identified who is of most value to you in developing and implementing the Security Management Plan, how you need to communicate and engage with them and also how ongoing communication needs to occur thereafter.

Table A2c: Stakeholder Familiarity and Favourability Matrix



Stakeholders placed here have ‘high favourability’ but ‘low familiarity’ with security risk issues. But they have the potential to be strong ‘champions’.

So explain the subject.

Stakeholders here have ‘high favourability’ and ‘high familiarity’ with security risk issues. They are your strongest champions.

So protect your relationships with them.

Stakeholders here have ‘low favourability’ and ‘low familiarity’ with security risk issues.

So they are unaware and need to be communicated with directly.

Stakeholders here have ‘low favourability’ but ‘high familiarity’ with security risk issues.

They are often critical of security risk issues and you need to be work on resolving specific concerns with them.

A2.4 Communication Focus

Once you have identified where each Stakeholder group is positioned on the matrix, you can then determine when and how you need to engage with them. We suggest that you add the actions arising from that assessment onto your Project Plan, a template of which is provided in Section A4, so that communicating with Stakeholders at the right time and in the right way, is fundamental to the development of the Security Management Plan.

The point has been made about using the opportunity you have created for yourself by developing or updating a Security Management Plan for the Asset to maintain the raised level of interest and awareness of security risk you have generated amongst all Stakeholders. This is a key benefit from undertaking this planning process. Whilst you will be compiling a report on security risks as part of the Implementation & Review phase of the guidebook, do take advice from those in the owner/operator who deal with internal communication about how to keep security issues at the forefront of those who work in the Asset. Your aim is to make all those who work in the Asset to think of security in the same way they do safety, and that is an ongoing process. Use the resources you have in the organisation to help you get and keep your security messages in the high favourability/high familiarity box on the matrix.

A2.5 Summary

As a result of this Section, you will have been able to identify key external and internal Stakeholders, prioritised them according to how important they are, their impact on your Security Management and identified who and where you need to focus your communication on thereafter.

Further on in Phase B you are going to interview a number of key internal Stakeholders to identify their protection objectives, but having worked through your Stakeholder analysis at this stage the process of engaging with them will be faster and more effective.

Once you have identified where each Stakeholder group is positioned on the matrix, you can then determine when and how you need to engage with them.

A3 Securing the Enterprise

Purpose: The environment the Security Management Plan has to operate in will determine whether it is implemented or not. So it is important for the Security Manager to understand what that environment looks like and how their Security Management Plan needs to fit into it.

If the Security Management Plan is not aligned alongside the risk management framework adopted by the owner/operator – it will not been seen as relevant and important. These are challenges already faced by Security Managers trying to raise the profile of security risks within their own organisations, and secure funds to invest in the management of those risks.

This can be avoided. In this section the Security Manager will be given several tools to help them identify a) the risk appetite and culture of the owner/operator as a means of assessing how aware Management are of security risks; b) what the risk management framework is and how to position their Security Management Plan within it to ensure that it is seen as relevant and accessible.

The process of developing or updating a Security Management Plan will have a positive impact on how security is perceived within the owner/operator. A heightened awareness of security risk will be a key outcome from the ongoing monitoring and reporting of progress against the Security Management Plan.

A3.0 Introduction

In Section A1 you will have explained the rationale for writing or updating the Security Management Plan for the Asset you are responsible for and in Section A2 you will have identified the key external and internal Stakeholders you need to engage with as part of that process. This Section looks at the level of awareness in the organisation of security risk issues and how the Security Management Plan needs to be positioned with the risk management framework run by the owner/operator to make sure it is adopted and implemented.

By ensuring the Security Management Plan fits into the existing risk management framework, it will have visibility and this is critical to its adoption. It is important for key personnel in the organisation to understand how decisions at a strategic, financial and operational level can increase or decrease security risk. For example, strategic decisions to expand an Asset or build a new Asset in a new location; financial pressures to cut costs can make an Asset less secure; operational pressures on performance can encourage people to bypass procedures and processes etc, resulting in a culture which does not prioritise security as a key risk to the Asset. It is important for you to note these for the reader so they understand why embedding security risk is so important. This is looked at under the section on Risk Appetite.

A3.1 Risk Appetite & Security Risk Awareness

The risk management infrastructure in an organisation is designed to manage risks within the agreed 'risk appetite' of the Board of Directors. So it is important to understand where an owner/operator lies on the spectrum shown below.

Diagram A3a: Risk Appetite

Willingness to take or accept Risk
Unwillingness or aversion to take Risk

The Board of an owner/operator will usually have an aversion to some risks and an appetite for others. It depends on what type of business activity they are responsible for and the risks that arise as a result of those activities. For example, in the energy sector safety risk is of paramount importance and managed as a key priority in the business, whereas in the finance sector safety is not a priority, but the credit risk it takes in dealing with those who borrow from them is because they eventually need to be repaid.

Risk appetite also has a direct impact on the risk culture and risk awareness in an organisation and this is not specific to any one risk. For example, financial pressures in many organisations can result in shortcuts being taken without the risk consequences being properly understood. This can be very subtle, but very dangerous. Having a strong risk culture where risk appetite is apparent and embedded in the risk management infrastructure is critical.

Security risk rarely has a high profile and is often managed outside the risk management framework applied to more visible risks. In this Section you are going to get a feel for what the risk appetite is in the owner/operator of the Asset and the level of awareness there is about security risk. To do this, there are a number of questions that you can ask key internal Stakeholders and these are set out in Annex A3(i).

Once a risk has been identified an organisation has several options; it can be:

1. Tolerated: Without any further action
2. Treated: Action is taken to constrain the risk to an acceptable level
3. Transferred: To a third party either by insurance or outsourcing who 'manages' the risk
4. Terminated: The activity is no longer undertaken and no risk exposure occurs

Organisations need to decide what option best suits the risk concerned bearing in mind that:

a) The Risk: Reward trade-off needs to be considered. Companies in the energy and finance sectors actively manage risk to generate rewards for their shareholders.

b) Whilst many risks can be identified, not every risk can be quantified and therefore managed down to an acceptable level, so contingency plans are important. 'Expect the Unexpected'

Before you complete the Stakeholder questionnaires in Annex A3(i), find out if there is an organisational structure chart that explains who is responsible for what in risk management. If this exists within the organisation, it will help you to identify the right people to approach. If not, it may be apparent from the titles people have or from what you know about how risk tends to be managed. The questionnaires in Annex A3(i) are addressed to the following internal Stakeholders and provide a basis for your own questions:

Diagram A3b: Internal Stakeholders

Strategic

The Management team of the owner/operator

Financial

The Financial Controller for the owner/operator or Asset

Operations/IT

Head of Operations/Production

Risk & Culture

Head of HSE & Head of Operations/Production

Personnel

Head of Personnel for the Asset

Please use these templates to record the responses you receive, and also to note down whether the response represented, in your opinion, the following:

H = High or Positive

M = Medium or Neutral

L = Low or Negative

Either score will demonstrate where on the spectrum the responses fall and what they tell you about the risk appetite and security risk awareness of the interviewee. By collating scores in this way, you can summarise the outcome of your interviews in the form of feedback which might be requested by those you have interviewed. Also, it will be important to use the overall results as a means of making the financial case for an investment in security risk, where appropriate.

Questionnaires appear in several parts of the guidebook to find out information on different subjects. For example, questionnaires to assess risk appetite, to assess the quality of the risk management undertaken in an owner/operator; to evaluate the awareness of security risk within the owner/operator; to identify security requirements and to test assumptions about Asset criticality and performance measures. As many of these are directed at the same individuals, it makes sense to hold one 'interview' with a Stakeholder and use the time as effectively as possible.

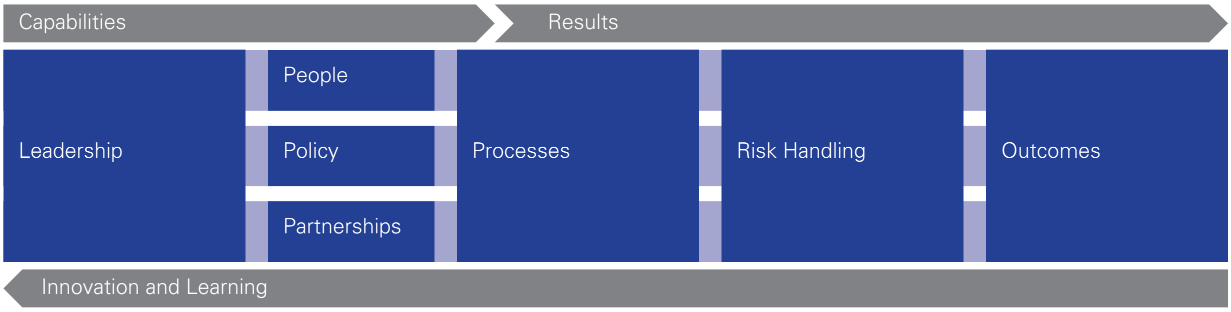
A3.2 Risk Management Frameworks

Having got some idea of risk appetite, you then need to understand how well the owner/operator manages the risks they are aware of, and avoids those they are not. There is a lot of discussion about risk appetite and risk culture and both are, of course, difficult to measure. However, you can see how both are manifested in the internal controls implemented by the owner/operator to manage risk. Remember that a company's set of internal controls define how risk is managed and how the energy infrastructure Assets of an owner are safeguarded.

It is probable that the owner/operator has a system of internal controls that manage quality assurance (QA) to cover risks such as HSE and operational issues around integrity. If you can identify what those controls are and how they are implemented you will then know how to integrate your Security Plan alongside them. This will raise awareness that good security risk management has a key role to play in safeguarding the Assets for which the owner/operator is responsible for and is not just an ancillary 'tick-box' exercise.

Remember that although there are many different risk management frameworks, they tend to include the same elements. One such model is the European Model for Business Excellence – now called the EQFM Model, which sets out the key elements of an overall risk management framework as a series of interlinked elements that build on capabilities to deliver a series of results or outcomes – essentially inputs and outputs. Almost every risk management has these same elements, they may be presented differently but the purpose and intent of each is the same.

Diagram A3c: EQFM



In security terms, this risk management model touches on many elements of the process defined in this guidebook and shows in particular how each part of the model works together to achieve a series of Outcomes that need to be delivered to a certain standard. In Phase C these outcomes are captured under the 'Design' phase as Detection, Delay, Response and Resilience.

Risk management is a subject that has been written about extensively and in many countries across the EU there are institutes and academic institutions dedicated to its study.

It is possible to access good reading material from a range of sources. If you would like advice as to where to find those of most use to you, please contact the authors who will be able to provide you with guidance as to the most beneficial documents and research material.

A3.3 Evaluating the Effectiveness of Risk Management

So this framework has the right elements and addresses the right questions, but how do you know if it works? Where is the evidence that it is being used, that people understand it, and that the outcomes are being delivered?

It is important that you know how effective the current risk management framework is for the Asset because the Security Management Plan is going to form part of it. If the existing framework is regarded by those responsible for the Asset as having a value in delivering effective internal controls, the Security Management Plan has a greater chance of being implemented.

By finding out the answers to the questions posed in Annex A3(ii) you will be able to assess how well risk is managed and how to position security risk accordingly. The questions focus on three key aspects of any risk management framework which have their genesis in the EQFM framework shown above.

Capabilities	1. Leadership: Do senior management support and promote risk management?
	2. Are people equipped and supported to manage risk well?
	3. Is there a clear risk strategy and risk policies?
	4. Are there effective arrangements for managing risks with partners?
	5. Do the organisation's processes incorporate effective risk management?
Risk Handling	6. Are risks handled well?
Outcomes	7. Does risk management contribute to achieving outcomes as noted above?

Source: Risk Management Assessment Framework, HM Government

Each question is evaluated against five levels, each of which reflects different levels of 'maturity' in how an organisation manages risk. For example:

(1) Awareness and understanding

(2) Implementation planned and in progress

(3) Implemented in all key areas

(4) Embedded and improving

(5) Excellent capability established

Other words that have been used to describe varying levels of evolved risk management similar to the above are: Initial/Adhoc – Fragmented – Comprehensive – Integrated – Strategic.

You need to establish where the owner/operator sits on this spectrum because it has an impact on how well received the Security Plan will be and the ability of the owner/operator to implement it. You may feel that security risk management itself is not well established and is perhaps, 'ad hoc' in nature. This may, or may not, reflect how risk is managed across the organisation. However, there is no doubt that the trend in risk management – irrespective of which risk – is towards a greater maturity. The operating environment in the energy sector is becoming more complex and requires the best possible risk management to be evident in an owner/operator in order to satisfy the risk:reward expectations of an increasingly complex and interwoven Stakeholder environment.

It is worth noting that good risk management is difficult to implement and research shows that there are seven reasons why many companies that take risk every day, get the management of risk wrong:

Summary of what goes wrong in risk management:

1. The potential interaction of multiple risks was underestimated or disregarded
2. Probabilistic modelling was overemphasised; shortcuts were taken; scenario planning was underused; transparency into potential issues was absent
3. Risk managers were isolated in silos
4. Warnings were ignored; those who delivered them were dismissed as negative or criticised for not being team players
5. A short-term perspective with a single-minded focus on making the quarterly financials
6. Companies lacked a comprehensive approach to firm wide risk management; authority and responsibility were poorly controlled and defined
7. Risk management often focused on compliance rather than performance, leading to inadequate assessments and responses

Source: Deloittes 'Putting Risk in the Comfort Zone: Nine Principles for Building the Risk Intelligent Enterprise' 2009

Many of these are understandable and you will probably recognise some of attributes in the Asset(s) you are responsible for, however, given the impact of security risk on many of an organisation's key functions, we want to make sure that your Security Management Plan avoids them.

The operating environment in the energy sector is becoming more complex and requires the best possible risk management.

A3.4 Partnerships

The scope of the Security Management Plan you are preparing is for the site of the Asset you are responsible for. However, it is impossible to ignore the interdependencies the Asset has in terms of its suppliers and business partnerships. From a resilience perspective alone it is incumbent upon the owner/operator to ensure that business continuity plans are tested and effective, but for the purposes of the Security Management Plan, this section poses the important question: 'Has someone asked about the extent and effectiveness of security risk management in the business partner/supplier on whom the Asset depends?' You need to ask this question and satisfy yourself about the answer. If not, the Security Management Plan must be clear about what assurances it can, and cannot, provide about the security arrangements of the Asset's key partners.

A3.5 Summary

As a result of this section you should have a feel for risk appetite and the awareness of security risk in the organisation and also be able to identify who needs to read, approve and 'own' the Security Management Plan for security around the Asset. This person will also champion the performance risk indicators that should be incorporated onto a Risk Report that monitors all risks managed by the senior management team of the owner/operator, who may be responsible for more than one site.

Regardless of how well you believe the existing risk management structure operates within your organisation, this must not dictate the quality of the Security Management Plan you prepare for the management of security risk around the Asset for which you are responsible.

Even if it is not easy to apply all aspects of the guidebook as much as you would like, as long as you work your way through each section in a sequential manner, you will have the confidence of knowing that every key aspect of the issue has been brought to the attention of your key Stakeholders, and you have done the groundwork for good security risk management. The environment around any Asset is dynamic and writing a Security Management Plan is the start of a process that will ensure the Plan is updated regularly to reflect changes as and when they occur. At each review point, you will have an opportunity to raise the profile of security risk management and strengthen the quality of the framework that underpins it. If once you have completed the Security Management Plan you feel that some areas require further development you could seek the support of an independent specialist to review and update the plan as required.

A3 Annex A3(i): Risk Appetite and Security Risk Awareness Templates

Annex A3(i): Risk Appetite and Security Risk Awareness

Phase A: Strategy & Planning

Template 1: Management Team: Risk Appetite

Ref.	Strategy: Future Proofing the Asset for Development and Growth	Responses	H-M-L
RA1	Is there a statement of risk appetite approved by the Board?		
RA2	How would you describe the risk appetite of the organisation? Is there a common definition of risk used in the organisation or is it more often associated with one particular risk such as financial or safety or environmental?		
RA3	Are there roles, responsibilities and authorities relating to risk management in the organisation?		
RA4	Is Risk Management a designated function in the organisation and at what level in the organisation is it represented?		
RA5	At what point in the strategic planning process are all risks aggregated and looked at on a consolidated basis?		
RA6	What keeps you awake at night?		
RA7	Do the company's corporate values mention risk?		
RA8	Is there a performance culture in the company that focuses on more than just delivering results?		
RA9	What would they describe as the most important risks they face?		

Template 2: Management Team: Security Risk Awareness

Ref.	Strategy: Future Proofing the Asset for Development and Growth	Responses	H-M-L
SRA1	How would you describe the nature and extent of the security risks that threaten the operation of this Asset?		
SRA2	Which external Stakeholders have a keen interest in security at this Asset? How often do you communicate to them about security issues?		
SRA3	What information do you receive from external sources and what do you think of it?		
SRA4	How important is security as a strategic priority? i.e. Does it influence in any way Board decisions about the future direction and growth of the organisation?		
SRA5	How often does the Board discuss security as an Agenda item?		
SRA6	How well do you think this Asset is managed compared with others in this country and region?		
SRA7	What due diligence do you undertake when choosing business partners to work with?		
SRA8	What information would you like to have to feel comfortable that security risks are being properly monitored and managed?		

Annex A3(i): Risk Appetite and Security Risk Awareness

Phase A: Strategy & Planning

Template 1: Financial Controller: Risk Appetite

Ref.	Finance: Planning for the Investment Required to Secure Revenues from the Asset	Responses	H-M-L
RA1	What measures of return on investment do you use to identify value?		
RA2	What amount of sensitivity analysis is undertaken when preparing projected returns on Assets and new investments?		
RA3	What is the acceptable range of variance?		
RA4	What is the most important risk the Asset faces?		
RA5	How often are you asked by banks and other external Stakeholders about risk in relation to what they expect to see from your activities?		
RA6	What are the Key Performance Indicators looked at most by the Board and senior management?		

Template 2: Financial Controller: Security Risk Awareness

Ref.	Finance: Planning for the Investment Required to Secure Revenues from the Asset	Responses	H-M-L
SRA1	Do you take account of security risk when reviewing the stability of the revenue generated by the Asset?		
SRA2	Do you think your bank(s) understand all the risks managed by the Board? If so, which ones are more important to them?		
SRA3	How does the budgetary process take account of expenditure on security?		
SRA4	What is the CAPEX security budget for the forthcoming financial year?		
SRA5	What is the OPEX budget for the forthcoming year in relation to additional personnel (guards, operators, security manager etc), ongoing maintenance costs etc		
SRA6	The Security Management Plan may recommend an investment in security that could fall outside the agreed budget for CAPEX in the forthcoming financial year. What would be the approval process to secure the finance required for this exceptional spend?		
SRA7	Do you know what the financial cost of security risk breaches is? i.e. One Key Performance Indicator is the cost of outage (per hour/day/week)		
SRA8	What level of insurance cover do you have in place to cover security losses and what exclusions are there? i.e. Terrorism, environmental etc How often is this reviewed and the level of cover reaffirmed?		
SRA9	When financial forecasts are prepared for the Board and/or the bank do you run sensitivities that result from breaches in security?		

Annex A3(i): Risk Appetite and Security Risk Awareness

Phase A: Strategy & Planning

Template 1: Head of Operations/Production: Risk Appetite

Ref.	Operations: Ensuring Continuity of Production	Responses	H-M-L
RA1	What are the key operational risks that have to be managed every day?		
RA2	Who is responsible for doing so and reporting on any exceptions?		
RA3	Do you think those risks are taken account of by those responsible for developing the Assets and managing the finances of the owner/operator?		
RA4	What is the most important risk you manage?		

Template 2: Head of Operations/Production: Security Risk Awareness

Ref.	Operations: Ensuring Continuity of Production	Responses	H-M-L
SRA1	What concerns do you want to be sure your security risk management team addresses?		
SRA2	Are these all of equal importance? (they may answer reputation, share price, environment, employees etc)		
SRA3	What part of your operation do you want to be secure?		

Annex A3(i): Risk Appetite and Security Risk Awareness **Phase A: Strategy & Planning**

Template 1: Head of HSE and Head of Operations/Production: Risk Appetite

Ref.	Risk and Culture: Aligning Security with Risk Appetite and Risk Management	Responses	H-M-L
RA1	How do you think someone would describe the culture of risk in this organisation?		
RA2	How often do you ask staff about their awareness of risk in the organisation?		
RA3	What risks do you think are at the forefront of staff minds when they come to work?		
RA4	What information is available on risk incidents and how often is it communicated?		

Template 2: Head of HSE and Head of Operations/Production: Security Risk Awareness

Ref.	Risk and Culture: Aligning Security with Risk Appetite and Risk Management	Responses	H-M-L
SRA1	Can you define what the term 'security' means to you? i.e. Theft, vandalism, outages, terrorism		
SRA2	Who is responsible for managing security risk in the organisation and who do they report to?		
SRA3	What would you describe as being the most serious security risks to the Asset as being?		
SRA4	How would you describe your appetite for security risks? i.e. What level of losses are you prepared to bear as part of the normal course of business?		
SRA5	Do you think external Stakeholder such as the Regulator, Government, bank and shareholders share your risk appetite in this area?		
SRA6	Does the Board receive regular reports on security issues?		
SRA7	What information would you like to have to feel comfortable that security risks are being properly monitored and managed?		
SRA8	How does the reporting you receive (or do not receive) on security risk compare with the reporting the Board gets on other risks such as operational risks, safety, finance etc?		
SRA9	Who is responsible for testing your security and how often do you do so?		

Annex A3(i): Risk Appetite and Security Risk Awareness **Phase A: Strategy & Planning**

Template 1: Head of Personnel: Risk Appetite

Ref.	Personnel: Embedding a Risk Awareness in Recruitment and Training	Responses	H-M-L
RA1	What do you think of the risk culture in the Operator and how is it evident in the working environment around the Asset?		
RA2	Do you think there is good leadership on risk awareness? Do managers 'walk the talk'?		
RA3	Has anyone been disciplined for failing to adhere to a risk requirement?		

Template 2: Head of Personnel: Security Risk Awareness

Ref.	Personnel: Embedding a Risk Awareness in Recruitment and Training	Responses	H-M-L
SRA1	Who is responsible for the security vetting of employees and contractors? How often is this updated?		
SRA2	How often does someone from Personnel meet the Security department to discuss this aspect of security?		
SRA3	What role does Personnel play in access control procedures? Writing them, testing them etc.		
SRA4	What do you want assurance on, regarding the security of personnel you are responsible for on site?		

A3 Annex A3(ii): Risk Management Assessment Questionnaires

Annex A3(ii): Risk Management Assessment Questionnaires **Phase A: Strategy & Planning**

1. Leadership: Do Senior Management support and promote risk management?				
Level 1: □ Awareness and understanding	Level 2: □ Implementation planned and in progress	Level 3: □ Implemented in all key areas	Level 4: □ Embedded and improving	Level 5: □ Excellent capability established
Top management are aware of the need to manage uncertainty and risk and have made resources available to do so	Senior Managers take the lead to ensure that approaches for addressing risk are being developed and implemented	Senior Managers act as role models to apply risk management consistently and thoroughly across the organisation	Senior Management are proactive in driving and maintaining the embedding and integration of risk management; in setting criteria and arrangements for risk management and in providing top down commitment to well managed risk and the seizing of opportunities where that risk is acceptable	Senior Managers reinforce and sustain risk capability, organisational and business resilience and commitment to excellence. Leaders are regarded as exemplars
Evidence:				

Date: Signed:

2. Risk Strategy and Policies: Is there a clear strategy supported by risk policies?				
Level 1: □ Awareness and understanding	Level 2: □ Implementation planned and in progress	Level 3: □ Implemented in all key areas	Level 4: □ Embedded and improving	Level 5: □ Excellent capability established
The need for a risk strategy and related policies has been identified and accepted	A risk management strategy and policies have been drawn up and communicated and are being acted upon	Risk strategy and policies are communicated effectively and made to work through a framework of processes	An effective risk strategy and policies are an inherent feature of department policies and processes	Risk management aspects of strategy and policymaking help to drive the risk agenda and are reviewed and improved. Regarded as a role model
Evidence:				

Date: Signed:

3. People: Are people equipped and supported to manage risk well?				
Level 1: □ Awareness and understanding	Level 2: □ Implementation planned and in progress	Level 3: □ Implemented in all key areas	Level 4: □ Embedded and improving	Level 5: □ Excellent capability established
Key people are aware of the need to assess and manage risks and they understand risk concepts and principles	Suitable guidance is available and a training programme has been implemented to develop risk capability	A core group of people have the skills and knowledge to manage risk effectively	People are encouraged and supported to be innovative and are generally empowered to take well-managed risks. Most people have relevant skills and knowledge to manage risks effectively and regular training is available for people to enhance their risk skills and fill any 'gaps'	All staff are empowered to be responsible for risk management and see it as an inherent part of the business. They have a good record of proactively managing risks
Evidence:				

Date:

Signed:

4. Partnerships: Are there effective arrangements for managing risks with partners?				
Level 1: □ Awareness and understanding	Level 2: □ Implementation planned and in progress	Level 3: □ Implemented in all key areas	Level 4: □ Embedded and improving	Level 5: □ Excellent capability established
Key people are aware of areas of potential risk with partnerships and understand the need to agree approaches to manage these risks	Approaches for addressing risk with partners are being developed and implemented	Risk with partners is managed consistently for key areas and across organisational boundaries	Sound risk management arrangements have been established with partners and suppliers chosen in full knowledge of their risk management capabilities	Excellent arrangements in place to identify and manage risks with all partners and to monitor and improve performance. Organisation regarded as a role model
Evidence:				

Date:

Signed:

5. Processes: Do the operator's processes incorporate effective risk management?				
Level 1: □ Awareness and understanding	Level 2: □ Implementation planned and in progress	Level 3: □ Implemented in all key areas	Level 4: □ Embedded and improving	Level 5: □ Excellent capability established
Some stand-alone risk processes have been identified	Recommended risk management processes are being developed	Risk management processes implemented in key areas. Risk capability self-assessment tools used in some areas	Risk management is an integral part of the organisation's core processes (policy, planning, delivery etc) and data are collected to monitor and improve risk management performance	Management of risk and uncertainty is an integrated part of all business processes. Best-practice approaches are used and developed. Selected as a benchmark site by other organisations
Evidence:				

Date: Signed:

6. Risk Handling: Are risks handled well?				
Level 1: □ Awareness and understanding	Level 2: □ Implementation planned and in progress	Level 3: □ Implemented in all key areas	Level 4: □ Embedded and improving	Level 5: □ Excellent capability established
No clear evidence that risk management is being effective	Limited evidence that risk management is being effective in at least most relevant areas	Clear evidence that risk management is being effective in all relevant areas	Clear evidence that risk management is being effective in all relevant areas	Very clear evidence of excellent risk handling in all areas and that improvement is being pursued
Evidence:				

Date: Signed:

7. Results: Does risk management contribute to achieving outcomes?				
Level 1: □ Awareness and understanding	Level 2: □ Implementation planned and in progress	Level 3: □ Implemented in all key areas	Level 4: □ Embedded and improving	Level 5: □ Excellent capability established
No clear evidence of improved outcomes	Limited evidence of improved outcome performance consistent with improved risk management	Clear evidence of significant improvements in outcome performance demonstrated by measures including, where relevant, Stakeholders' perceptions	Clear evidence of very significantly improved delivery of outcomes and showing positive and sustained improvement	Excellent evidence of markedly improved delivery of outcomes which compares favourably with other organisations employing best-practice
Evidence:				

Date: Signed:

A4 Planning

Purpose: To provide some project management tools for the Security Manager to use to complete their Security Management Plan.

A4.0 Introduction

Putting together a Security Management Plan will require the use of some basic Project Management tools to ensure the creation of the document has visibility and the approval it requires.

This is not about the Project Management required to implement the Security Management Plan especially the engagement of contractors, which is explained in Phase D.

A4.1 Roles, Responsibilities and Resources

Although you may be the overall owner of the Security Management Plan, you will not be able to deliver it alone. Working your way through the PRISM™ is a challenging project and we suggest you secure help and establish a small Project Team to assist you as you work through the Guidebook.

A4.2 Project Management

The tools of most value to the Security Manager are as follows:

I. Project Charter

II. Project Plan

A Project Charter that sets out the scope of the project and who is involved. An example is shown below:

OPERATOR NAME			
RISK MANAGEMENT : Security Management Planning			
Project Name	Security Management Plan	Project Sponsor	Head of Risk or HSE
Originating Area	Risk or HSE	Project Manager	Security Manager
Date of Initiation	TBC	Date of Completion	TBA
Project Purpose Statement			
This section is a short overview about why the Security Plan is being put together from a strategic and operational perspective, and what it hopes to achieve			
Deliverable			
A hard copy (i.e.) of a Security Management Plan to be distributed amongst all Stakeholders			
Resourcing			
A list of those who need to input into the preparation of the Security Management Plan			
Potential time and any financial spend			
Significant Risks and Dependencies			
A clear statement reiterating the importance of having a robust and effective Security Plan in place and the interest from external Stakeholders. The need for the Project to have visibility and the full support of key internal Stakeholders if it is to succeed. Communication about the Project will need to be evident and ownership of the Plan should be made explicit. Really answering the question: 'What has to happen for the Security Plan to become a central part of corporate governance within the Operator?'			
Benefits			
These need to cited and reflect both the benefits to the Security Manager and the Operator itself. They would include ensuring that security around the Asset meets international standards and gives assurance to key external Stakeholders including current and future business partners. That it acts as a single point of reference for the specific risk of security, but is part of the overall risk management framework endorsed as part of the corporate governance responsibilities of the Board.			

A Project Plan is also useful although this should not become too onerous. A simple Tactical Plan template will suffice, for example as shown below. Both are on Excel and can be created into a generic format that can be adapted for each Operator.

Security Management Plan: Project Plan							
Project Objective		Area Objective	Target	Owner	Target Date	Deliverable	Status
Phase A: Strategy & Planning							
A1							
	Milestone – Add in key ones						
Phase B: Assessment							
B1							
	Milestone – Add in key ones						
Phase C: Design							
C1							
	Milestone – Add in key ones						
Phase D: Implementation & Review							
D1							
	Milestone – Add in key ones						

Key:	
Red box – incomplete	
Green box – complete	
Blue box – milestone	

A Planning Workshop is a useful kick-off to the Project enabling all Stakeholders to be identified and communicated with about the Project Charter and to buy into the work and its eventual outcome.

A4.3 Communication

You need to be able to communicate the Security Management Plan and its resultant actions to all the key Stakeholders you have identified according to the needs you identified in A2. Communication can take many formats and we recommend you use internal experts within the organisation. It is critical that the Security Management Plan is communicated effectively as part of the process of ensuring its adoption and acceptance as an important risk to be managed.

A4.4 Summary

Undertaking the work to put together a Security Management Plan requires planning. It is a Project in its own right and requires the time and commitment from a number of individuals to do well. Keeping Stakeholders informed of progress and engaging with them at the right time in the process also requires forethought, so by spending time initially planning how, who and when you intend to undertake each phase of the work set out in this guidebook, will reap benefits later on in the process.

You need to be able to communicate the Security Management Plan and its resultant actions to all the key Stakeholders you have identified

Phase B

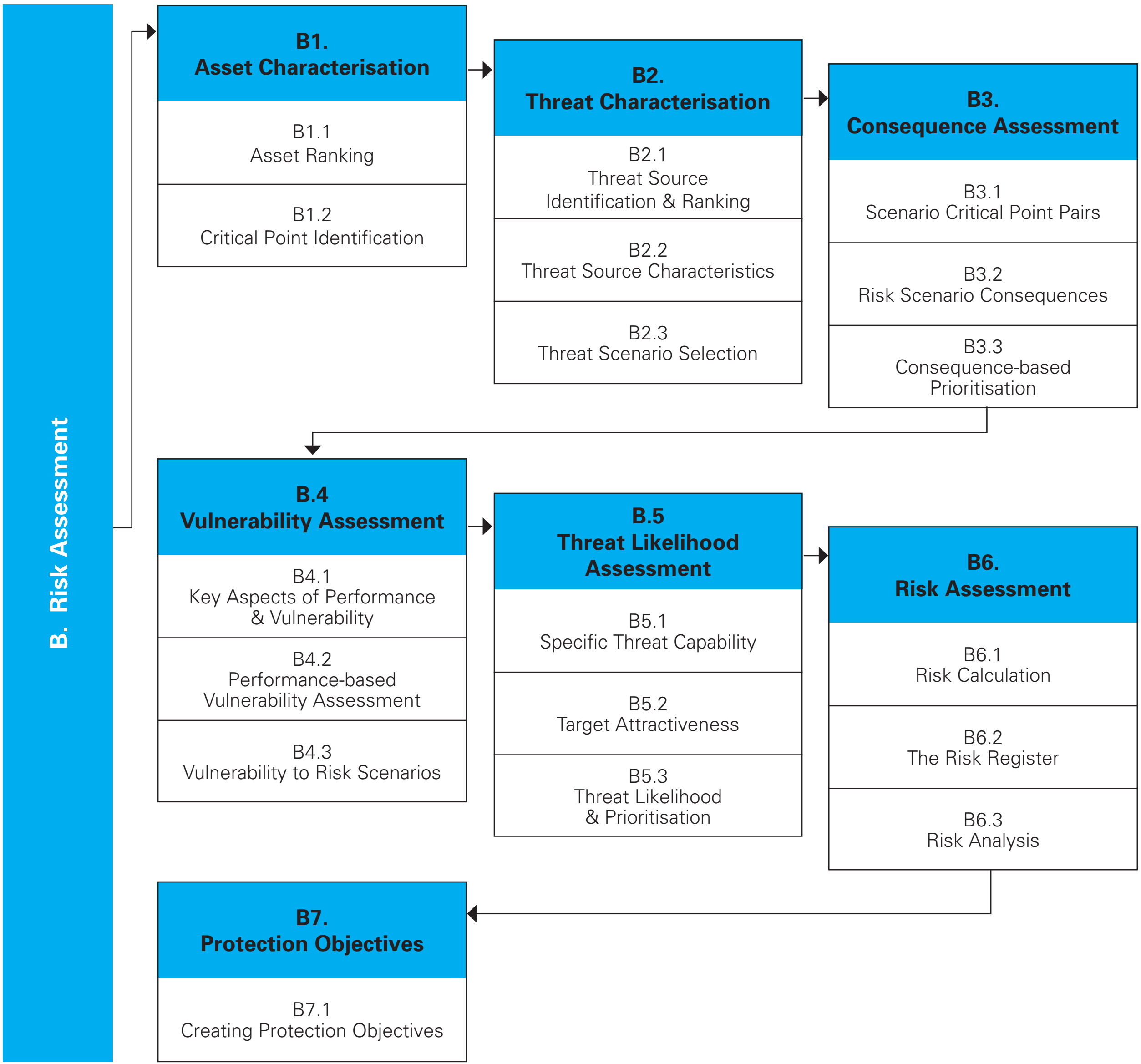
Risk Assessment

PHASE B

Executive Summary – Risk Assessment

The Risk Assessment Phase is of central importance to the Security Management Plan, providing the basis on which to determine the type, nature and severity of risks facing the owner/operator's Assets and the wider European Energy Network. It provides the basis for all subsequent Risk Management decision-making, and in particular a sophisticated tool in the delivery of focused and cost-effective risk mitigation measures to the organisation.

The Risk Assessment process that you will conduct as part of the Security Management Plan is shown in the following diagram and explained further below:



B. Risk Assessment

B1. Asset Characterisation
B1.1 Asset Ranking
B1.2 Critical Point Identification

B2. Threat Characterisation
B2.1 Threat Source Identification & Ranking
B2.2 Threat Source Characteristics
B2.3 Threat Scenario Selection

B3. Consequence Assessment
B3.1 Scenario Critical Point Pairs
B3.2 Risk Scenario Consequences
B3.3 Consequence-based Prioritisation

B.4 Vulnerability Assessment
B4.1 Key Aspects of Performance & Vulnerability
B4.2 Performance-based Vulnerability Assessment
B4.3 Vulnerability to Risk Scenarios

B.5 Threat Likelihood Assessment
B5.1 Specific Threat Capability
B5.2 Target Attractiveness
B5.3 Threat Likelihood & Prioritisation

B6. Risk Assessment
B6.1 Risk Calculation
B6.2 The Risk Register
B6.3 Risk Analysis

B7. Protection Objectives
B7.1 Creating Protection Objectives

The Risk Assessment process analyses risk at both the Asset Level and the Component Level in order to provide specific and usable outputs. Although criminal security risks including terrorism are the primary focus for the Security Management Plan, the Risk Assessment process also addresses non-criminal risks including natural, accidental and consequential hazards. As such it provides the flexibility to support an 'All-Risks' approach.

The first stage in the Risk Assessment process (B1) is to identify which Assets are of greatest importance to the organisation, subsequently selecting these in turn for application of the full Security Management Plan process. Once an Asset has been selected you will then be shown how to identify the processes, components and dependencies that are critical to its functioning and therefore require specific consideration.

Threat Characterisation (B2) forms the second stage of the Risk Assessment and will guide you through the identification of potential sources of Threat and the collection and assessment of Threat information. Following on from this it will be possible to characterise each Threat source and create a number of relevant Threat Scenarios that will be used as the basis for assessing specific risks to the Asset.

Section B3 assesses the 'Potential Worst-Case Consequences' of each Threat Scenario by considering the type and severity of impact that may be faced by both the Asset's owner/ operator, as well as the wider community, given that many Assets benefiting from this process will be considered Critical European Infrastructure. Consequences are considered at both the Asset Level and the Component Level, with each Threat Scenario – Component Pair being considered as a separate 'Risk Scenario'.

The next stage (B4) will be to assess the Vulnerability of each critical component in relation to each scenario. To do this you will be provided with a framework for assessing existing performance in the key functional areas of Detection, Delay, Response and Resilience, and using this to identify the Likelihood that each Risk Scenario, if materialising, will lead to the potential worst-case consequences identified previously.

Section B5 assesses the Likelihood that each Criminal Threat will occur specifically in relation to the Asset in question. Criminal Threats differ from non-criminal Threats due to the element of human intent, and as such it is necessary to gauge 'Target Attractiveness' as well as the Threat source's specific capability to conduct each attack, in order to assess Threat Likelihood. Utilising information from the Consequence and Vulnerability assessments this section will provide you with a framework to identify whether the ratio between risk and reward is likely to meet with the Threat source's objectives and whether they have the means to conduct the attack.

Following on from individual assessments in sections B1-B5 you will be able to calculate overall risk scores for each Risk Scenario (B6). These will be input into a Risk Register, which will be used as a key tool in the analysis, monitoring and reporting of all risks facing the organisation. Subsequently you will be asked to create a series of specific 'Protection Objectives' (B7) in relation to those risks that fall outside of the organisation's risk appetite as established in Phase A of the Security Management Plan. Once signed off by risk owners these Protection Objectives will be used as the basis for Risk Mitigation activity as addressed in Phases C and D of the Security Management Plan.

It will be evident from the above Introduction that the Risk Assessment process you are about to embark upon is quite detailed and will in most cases take a reasonable amount of time to conduct. However, once completed this will provide a thorough understanding of risks facing the organisation and also an excellent basis upon which to formulate the remainder of the Security Management Plan. It will also provide a key tool for ongoing risk management activity in the form of the Risk Register, which can be updated on a regular basis to ensure that you are always in control of the risks facing your organisation and its Assets.

B1 Asset Characterisation

Purpose: To provide a framework for ranking all corporate Assets on the basis of criticality to the organisation or community and using this to identify and prioritise Assets that require the full risk management process to be implemented. Once an Asset has been selected to determine the Critical Points within the Asset that may require specific protection as well as the critical dependencies external to the Asset which it relies upon for continued operation.

B1.0 Introduction

Energy owners/operators will often have a diverse portfolio of infrastructure Assets under their control, each playing a different role within the overall business process. Whilst some Assets may be critical to the continuing operation of the business, represent substantial investment in technology, people or processes, and be of national or regional economic significance, other Assets may be of peripheral importance or easily replaceable.

Therefore the **first** part of the Asset Characterisation process is to identify and rank all corporate Assets on the basis of their overall importance to the organisation and the wider community. This will ensure that the requirements of critical Assets are addressed first and foremost, thereby supporting the cost-effective and targeted allocation of resources.

Once an Asset has been identified as being critical to the organisation and the wider energy network, the full risk management process should be conducted in order to identify and quantify the various types of risk faced by the Asset and its component parts, as well as the type of countermeasures that could reduce these risks to an acceptable level. At this point the Security Management Plan methodology moves from the organisational environment to that of the Asset itself.

The **second** part of the Asset Characterisation process is to understand the characteristics and functions of the Asset in more detail in order to identify factors that will be relevant to subsequent phases of the assessment process, and determine which parts of the Asset are critical to its core role or function and may therefore require specific attention.

The following sections of the guidebook take the Project Team through the recommended Asset Ranking and Asset Criticality assessments.

B1.1 Asset Ranking

Asset Ranking forms the first stage of the Asset Characterisation process and consists of a framework to identify relevant corporate Assets and rank them according to their criticality, forming an overall list of prioritised Assets. Assets can then be selected from this list in order of priority to take forward to the next stage.

The process can be conducted as a ‘desktop’ exercise since the objective is to make an initial assessment of Asset criticality to inform priorities rather than determine precisely how Assets and components function, the latter being addressed later once an Asset has been selected.

In some sectors or countries government or regulatory agencies may have already set Asset criticality levels or provided specific guidance to operators, and in this case such guidance must take precedence over this process. Of particular relevance in this respect is ‘EU Directive 2008/114/EC – Identification of European Critical Infrastructure’, and it is recommended that your Project Team familiarise themselves with this guidance before embarking on the Asset Ranking process, which consists of the following steps.

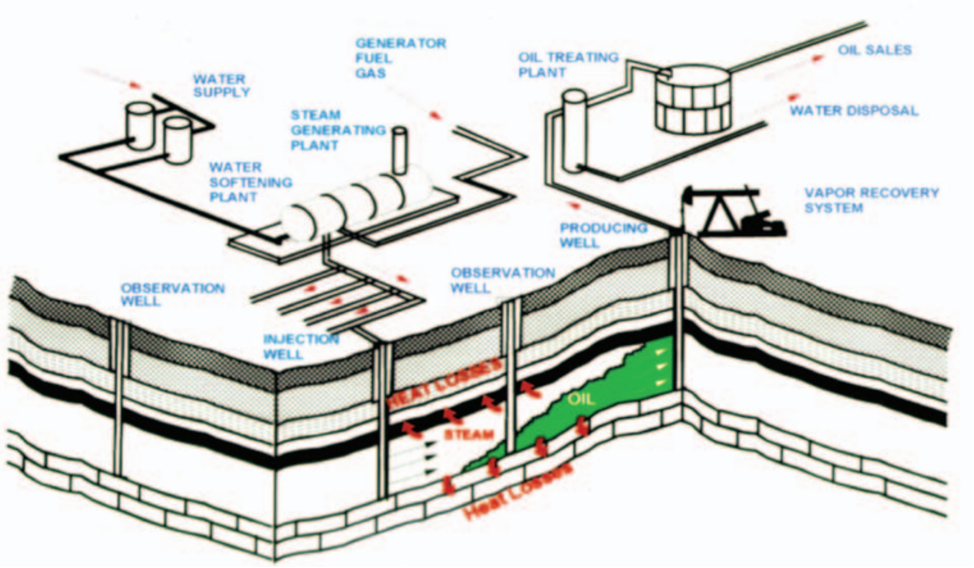
Step 1: Understand the Role of the Assets

The first step in the Asset ranking process is to understand the role of each Asset in the context of the organisation’s overall service delivery and mission, as well as in relation to the wider energy network of which it forms a part. Without a good understanding of the organisational and network context it is not possible to assess the criticality of individual Assets – what appears to be a relatively minor low-value Asset could in fact be critical to other Assets within the network that may depend upon its output.

In order to develop this understanding the Project Team should refer to (and preferably include) someone with detailed operational knowledge of all infrastructure that falls within the responsibility of the organisation, as well as related infrastructure within the wider energy network.

The second step will be to draw up a list of corporate Assets and then map these on a schematic drawing which shows the relationships and dependencies of these various Assets (for many organisations this will already be available within the business). A simple example for an oilfield operation is shown in the following diagram:

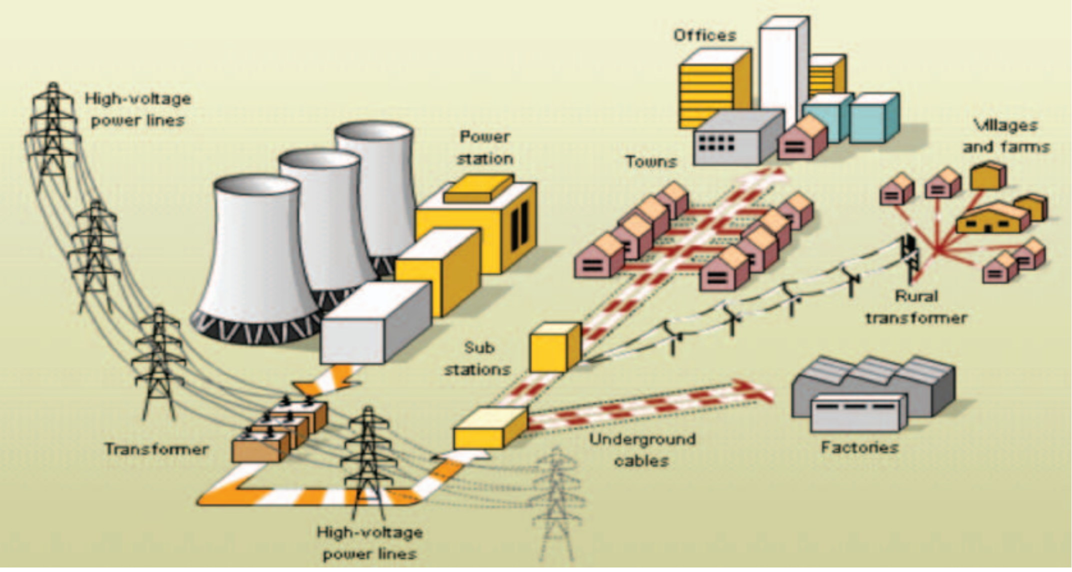
Diagram B1a (i): Oilfield Operations Schematic



However, the creation of a more detailed schematic will be required, showing all of the various dependencies for each Asset (both upstream and downstream), as well the level of service production, redundant or diverse supply routes and interconnections with other networks.

A second schematic drawing should subsequently be produced for the network level, showing where the organisation's Assets fall within the overall energy chain. For example, if the organisation was responsible for electricity transmission within a particular region this diagram would also include power generation (upstream network) and electricity distribution (downstream network). An example is shown in the following diagram:

Diagram B1a (ii): Power Generation, Transmission and Distribution Schematic



This process will help the Project Team to understand in more detail the overall role and importance of each Asset, as well as the various dependencies and relationships between Assets. Further information should also be gathered for each Asset including the volume of production, percentage of overall service delivery, and the number and type of personnel at the facility. This information should be entered into a summary table, an example of which is shown below:

Table B1a Asset Log

Asset Ref and Name	A1. Grid Substation
Number and Type of Workforce	2 Management, 5 Technical, 3 Administrative. Occasional contractors.
Role of Asset	To transform network electricity voltage from 415kV to 133kV.
Key Dependencies – Inputs	1. Supply from Power Station (externally owned Asset) 2. Switching by Load Distribution Centre (company Asset ref x).
Key Dependencies – Outputs	3. Onward supply to distribution grid.
Level of Service Delivery	Maximum load of 2,800MW, equating to 30% of the company's supply across all transmission networks.
Further Considerations	The company has legal obligations to meet minimum supply and therefore the Asset is central to the business mission.

Source: PRISM™

Additional information can be added as required, although at this stage the objective is not to complete a detailed process analysis for each Asset (this will be done in the next section), but to identify in broad terms the role and potential importance of each Asset to allow subsequent ranking and prioritisation.

Step 2: Rank Assets Based on Criticality

Once the role and functioning of all corporate Assets has been understood in broad terms you can rank them based upon their overall criticality to the owner/operator. The recommended process uses four criteria to assess the criticality of Assets, which are:

1. Workforce – number and type of workforce located onsite.
2. Service Delivery – % of overall service delivery that the Asset is responsible for.
3. Dependencies – importance of the Asset to other Assets within the organisation or energy network.
4. Mission/Objectives – overall importance of the Asset to the business mission or objectives taking into account all factors combined.

Although there are potential consequences that could be associated with each of the above criteria, the focus at this stage is purely on criticality factors – consequence assessments require a more detailed understanding of the Asset's processes, components and external environment, as well as the incidents that could create these consequences. As such they come later on in the risk assessment process once this information has been gathered.

A common approach to this type of Asset Ranking process is to assign a score to each of the above criteria and add them together to give a total criticality score. However, it will become apparent during the Asset Ranking process that some Assets are highly critical based upon only one or two of the above criteria. For example the operator may have a gas-fired power station that is critical to their oil processing facility, but which is unmanned and not directly responsible for any service delivery. Therefore, if assigning scores of 1-5 for each of the above categories the cumulative score may only amount to 10 out of 20 – a moderate level only. For this reason the recommended Asset Ranking process centres around a flexible set of scoring criteria which allows criticality levels to be awarded on the basis of any of the core criteria (Workforce/Service Delivery/ Dependencies) or as a result of the overall importance to the organisation's Mission, which could be determined by a combination of these three criteria or other factors specific to the Asset in question.

The recommended scoring criteria and guidance notes are provided in the following table:

Diagram B1b: Asset Ranking Scoring Matrix

Criticality Scoring Criteria								
Score	**Level**	**Workforce**		**Service Delivery**		**Dependencies**		**Overall Mission/ Objectives**
5	Very High	A very high percentage of the workforce or specialist staff or management is located at this facility	OR	The Asset is responsible for >75% of total service delivery	OR	The Asset is critical to the functioning of other key Assets within the organisation/ network	OR	The Asset is critical to the central mission or objectives of the organisation
4	High	A high percentage of the workforce or specialist staff or management is located at this facility	OR	The Asset is responsible for >50% of total service delivery	OR	The Asset is very important to the functioning of other key Assets within the organisation/ network	OR	The Asset is very important to the central mission or objectives of the organisation
3	Moderate	A moderate percentage of the workforce or specialist staff or management is located at this facility	OR	The Asset is responsible for >25% of total service delivery	OR	The Asset is moderately important to the functioning of other key Assets within the organisation/ network	OR	The Asset is moderately important to the central mission or objectives of the organisation
2	Low	A low percentage of the workforce or specialist staff or management is located at this facility	OR	The Asset is responsible for >10% of total service delivery	OR	The Asset is of low importance to the functioning of other key Assets within the organisation/ network	OR	The Asset is of low importance to the central mission or objectives of the organisation
1	Very Low	A very low percentage of the workforce or specialist staff or management is located at this facility	OR	The Asset is responsible for <10% of total service delivery	OR	The Asset is of very low importance to the functioning of other key Assets within the organisation/ network	OR	The Asset is of very low importance to the central mission or objectives of the organisation

Source: PRISM™

For each corporate Asset the Project Team should agree on a criticality score of 1-5 based upon the above factors. This information can be entered into a spreadsheet and used to rank Assets and determine the order of priority for application of the full risk management process as outlined in the remainder of this guidance document. Organisations with a large number of Assets may want to set a minimum criticality threshold for taking them forward to the next stage, such as a criticality score of >2.

B1.2 Critical Point Identification

Once an Asset has been selected for assessment and enhancement the next stage is to determine which parts of the Asset and related external infrastructure are critical to its service delivery, integrity or core functions. This can be done through the following steps:

Step 1: Establish General Characteristics

Data Collection

In order to help establish the general characteristics of the Asset the Project Team should collect relevant information, which may include the following:

- GIS or aerial mapping of the facility and surrounding area
- General site layout drawing showing boundaries and all key buildings and infrastructure
- Topographical map and Environmental records
- Operating Procedures
- Asset and Equipment Inventory
- Visitor and Contractor Logbooks
- Health, Safety and Security Manuals

Along with any other information relevant to the general characteristics and operation of the facility.

Method

Building upon the information gathered for the Asset Ranking process, the Project Team should create a profile of the Asset, outlining physical, environmental and operational characteristics, as well as those of the surrounding environment. This information will be used as the starting point for subsequent assessments in the areas of criticality, consequence, vulnerability and Threat.

The following table provides an overview of the key information that should be documented when building up the profile of the site:

Table B1c: Key Information Acquisition

Area	Information Required
Role of the Asset	Description of general role of Asset, including: – Position within the organisation and energy network – Main inputs and outputs, including maximum production levels
Physical Description	Details of geographical location, boundaries (marked on map), buildings, infrastructure, vehicle and pedestrian access points etc
Environment	Environmental conditions including: – Prevailing winds – Approximate frequency and type of severe weather – Terrain – Surrounding area – population levels, adjacent hazards, environmental concerns etc – Adjacent or co-located infrastructure, companies, facilities
People onsite	Number and location of people typically onsite including: – Employees – managers, technical staff, administrative staff – Contractors (routine and during shutdown) – Visitors
Operating states	– Shift patterns – Continuous operation – Occupancy times for each building or area of the plant – Planned shutdown periods
Procedures	Summary of key procedures related to: – Operation and management of main facility processes. – Health & safety – Evacuation and emergency – Security
Security Systems	Overview of existing security systems deployed at the site, including: – Perimeter fencing – CCTV – Intruder detection systems – Physical and electronic access control systems – Security guarding – SCADA and IT security
Safety Systems	Details of existing safety systems deployed at the site, including: – Fire and gas detection – Physical bunds/spill protection – Emergency shutdown systems – Over-pressure protection
Buildings and Infrastructure	Create a list of all significant buildings and infrastructure within the site and provide details of: – Physical construction – Building management – IT systems
Equipment	List main equipment held onsite and location
Information	Provide details of all significant corporate information held onsite, including: – Paper files – Electronic data – Proprietary/confidential information – Government classified information

Source: PRISM™

Step 2: Conduct an Asset Process Analysis

The majority of energy infrastructure Assets consist of a number of key processes, for example oil production, gas compression, electricity distribution, plant control, business administration and so forth. Each of these processes are implemented via a collection of physical or logical sub-components and may also be reliant upon a number of external dependencies in order to perform the process (for example essential services such as electricity supply, gas supply or communications, as well as downstream Assets that provide an output route for service delivery, such as grid sub-stations, gas compressor stations or shipping/export terminals). **Although physical components are often the most obvious or visible it is worth remembering that logical components such as SCADA systems and other electronic/software infrastructure can be just as critical to service delivery and asset integrity, and therefore need to be considered within the Asset Process Analysis.**

The objective of the Asset Process Analysis is to identify the processes, components and dependencies that together make up the Asset as a whole, as well as various factors that determine how critical each of these elements are to the Asset and the organisation. In this way those that are deemed critical can be prioritised for further assessment, whilst those that are absolutely non-critical can be ignored.

What will become apparent in later stages of the guidebook is that the majority of risks faced by a given energy infrastructure Asset would actually be manifested in the form of a physical or logical impact upon one or more of these critical processes, sub-components or dependencies, which in turn affects the service delivery or integrity of the Asset, resulting in undesirable consequences for the operator or external environment or both. For the purposes of the risk assessment process and the wider Security Management Plan, the Asset's critical processes, sub-components and external dependencies will be referred to as 'Critical Points' ('CPs'). It is these CPs that constitute the 'physical risk elements' that could be impacted upon by any given risk materialising.

For any given type of Threat only a discrete number of physical risk elements may actually be at risk – some of these will not be impacted upon by the Threat, whilst others may not be vulnerable to the Threat. Therefore, once all of the Critical Points have been identified they can be mapped against relevant Risk Scenarios. By analysing risk at this level of granularity you will be able to identify precisely what parts of the Asset are critical, what specific risks these CPs face and how they should be protected. This results in a very targeted, efficient and cost-effective use of resources, which will ultimately ensure that all significant risks can be mitigated to an acceptable level.

Data Collection

In addition to the information gathered in step 3 the Project Team should assemble the following, where available:

- Building floor and elevation plans
- Process Hazard Analysis Map showing hazardous zones
- Piping & Instrumentation Drawing (P&ID)
- SCADA and IT network diagrams
- Process Flow Diagrams (PFDs) and process descriptions
- Inventories – Types and classifications of all hazardous inventories together with the size and location of the inventories
- Layouts – Process locations, buildings, control centres, equipment locations, incomer locations (water, electricity, gas, etc) and roads
- Supply & Production statistics, including volumes and historical or anticipated outages

Method

Many facilities will already have some form of process analysis typically conducted from an operations or process safety perspective. Although these can be a good source of information it is necessary to conduct a separate Asset Process Analysis, which considers issues that may be relevant to security risks and not just health, safety or operational risks.

The Asset Process Analysis should be conducted via a site survey guided by the process/production manager or senior engineer, as well as via reference to the documentation outlined above. You can then use the output to identify the following:

1. Processes

All of the main processes present within the Asset. There are five main types of process to consider as shown in the following table:

Table: B1d: Process Type

Types of Process	
Name	**Description**
Administration	Processes supporting the function of the Asset and/or operation of the business
Control	Processes directly involved in the control of the plant
Production	Processes responsible for the Asset's output
Storage	Processes involved in the storage of product or related chemicals
Utilities and Supply	Processes related to utilities or supplies required by the Asset

Source: PRISM™

For each process identified the following information should be established and recorded:

1a. How Critical is the Process to the overall role and function of the Asset?

Guidance – Try to estimate the percentage of production/service delivery that would be affected if the process ceased to continue. This may be directly, or indirectly via the loss of other dependent processes. Consider any other impacts that the loss of this process may have and how significant these would be to the overall functioning of the Asset.

1b. How easy/difficult would it be to restart this process if disrupted?

Guidance – some processes take significant time and effort to re-initiate, even when all physical components are operational. This can be exacerbated if the process did not shutdown properly. Discuss the steps required to restart each process with the relevant technical personnel.

For those processes that are deemed important or critical to the Asset it will be necessary to identify their sub-components and external dependencies using the following guidance:

2. Sub-Components

The collection of physical or logical components that together perform each of the processes that have been identified above. There are five main types of component to consider as shown in the following table:

Table B1e: Types of Sub-Asset

Types of Sub-Asset	
Name	**Description**
Infrastructure	Pipes, valves, storage tanks, cables, switchgear and other plant components
Buildings	Control rooms, sub-stations, warehouses, laboratories, administrative offices, canteens, training facilities etc
People	Managers, specialists, administrators, visitors, contractors and others onsite
Equipment	Control equipment, tools, medical supplies, SCADA and IT systems
Information	Electronic data, paper files, intellectual property

Source: PRISM™

For each component identified the following information should be established and recorded:

2a. Could this Component pose a hazard to people or the environment?

Guidance – Identify the location and size of all large inventories of hazardous materials and ensure that these are included in the list of components. Plants containing large inventories of hazardous materials are subject to the EU SEVESO directive as well as any national directives such as the UK's Control Of Major Accidents and Hazards (COMAH) Regulations. These regulations require each owner/operator to produce a safety report in relation to their holding of hazardous materials, and this information will be useful in completing this task. But also consider hazardous materials or quantities that fall below minimum legislative thresholds, however, could still pose a significant hazard.

Example – A small amount of hazardous Chemical, Biological or Radiological material could be used to contaminate the water supply, process or HVAC system. It could also be stolen and used in an attack elsewhere.

The above information will also be useful in assessing the possible domino effects, see paragraph 2c below.

2b. What would be the magnitude of impact on the process if this component was damaged?

Guidance – Try to estimate the level of disruption to the process if this component was damaged or lost.

2c. Is there a 'Domino' Risk to other Components or processes?

Guidance – A 'Domino Risk' relates to where the loss or damage to a part of the facility may have a severe adverse affect on an adjacent or dependent part of the facility.

Example – A diesel tank which supplies fuel to an emergency power generator may fail resulting in a fire and bleve. On its own this tank is not normally critical to the ongoing process. However, should this tank be located next to the main plant electricity switchroom, then its failure may result in damage to critical switchgear without which the plant cannot function.

Example – A high-pressure gas feeder pipeline supplying gas to a grid distribution centre may fail. On its own the loss of one feeder may not have critical consequences for the national infrastructure. However, a jet fire emanating from the damage to the feeder may cause severe damage or restrict access to the gas distribution plant for an extended period.

2d. Is there any redundancy if the Component is lost?

Guidance – Plants may have inbuilt redundancy allowing the loss of one or more Components, whilst still retaining the ability to deliver the full extent of the service. Examine whether or not the process can still operate without the Component and for what period of time. Where redundancy is in place note down whether or not it is physically redundant (i.e. in a separate location), or in the context of dependencies whether or not there is a diverse supply route. If redundant components are co-located with primary ones they may also be damaged or destroyed by the same incident, therefore offering no additional benefit.

Example – A gas processing plant will have a number of pressure let-down trains with at least one train being spare capacity above what is required for the full service delivery. This will allow for essential maintenance, filter changes etc. The loss of one train would have no immediate process impact.

2e. What is the anticipated outage time if the Component was damaged/destroyed?

Guidance – The loss of a component or piece of equipment should be evaluated in terms of the potential outage time, i.e. the time that it would take to repair or replace the item following damage or total loss. Specialist components such as high-voltage transformers or non-standard valves may have significant lead times and this should be highlighted.

Also identify any holding of critical spares/replacements for each Component. This will reduce the potential outage time. Some owners/operators may have sharing agreements with other operators of similar facilities where common spares holdings are shared in the event of damage resulting from an incident.

2f. How resilient is the Component to different types of incident?

Guidance – Assess how resilient each component or process is to various forms of attack, natural hazards, improper use etc.

Example – A pipe or pressure vessel manufactured from thick-wall high-strength steel is reasonably resilient to attack whereas electrical switchgear can be rendered inoperable with a large hammer.

3. Dependencies

External Assets that are relied upon by a process and/or specific component. These may provide an input to the process or take an output from the process, and may be owned by the same company or a different company. There are five main types of dependency to consider as shown in the following table:

Table B1f: Types of Dependencies

Types of Dependencies	
Name	**Description**
Fuel/Feedstock	Gas, electricity, coal, chemicals
Utilities	Gas, electricity, water, telecommunications
Network	Transmission grid, sub-stations, pipes, compressor stations
Supply Routes	Road, rail, seaport, overhead cables
Supply Chain	Suppliers, customers

Source: PRISM™

3a. How critical is this dependency to the process/ Component?

Guidance – Examine whether the process or component can function without each dependency. Are diverse supply routes available, could alternative supplies be sourced at short notice? If the loss of the dependency would not result in a complete failure/outage, estimate the percentage impact it would have on the process or component.

As well as essential inputs to the process also consider the downstream infrastructure such as transmission grids/grid sub-stations and the supporting services such as transport, logistics and supply chains.

Example – A gas-fired power station will be dependent upon the ability to transmit electricity to a grid sub-station. If there is an outage at the grid sub-station electricity production would have to cease. Similarly an oil processing facility may be dependent upon an export line, however, onsite storage tanks may allow production to continue for several days even if they could not ship offsite.

3b. Are these dependencies company-owned Assets?

Guidance – For each dependency, state whether they are owned by the same company or a different company. In later stages of the process it may be necessary to visit these external Assets and decide whether or not they are adequately protected or pose any specific risks.

3c. Has there been any historical outages or supply-chain failures associated with each dependency?

Guidance – Historical data such as this will help to assess the Likelihood of future incidents in later stages of the risk assessment process.

Output

All of the above information should be recorded as part of the Asset Process Analysis, along with any further comments or concerns from the Project Team or site representatives. A process diagram should then be created to represent this information in graphical form and ensure that the relationship and interconnections between processes, components and dependencies is fully understood.

Step 3: Identify 'Critical Points'

The next step will be to assess the criticality of each of the components and dependencies identified during the process analysis, in order to determine which of these can be considered as a 'Critical Point'. In some cases the Project Team may also choose to designate a process as a CP, for example where it consists of a number of discrete, co-located components which would all be effected by a given risk in the same manner, hence there would be no advantage in considering each component individually. This can be useful for very large/complex infrastructure as it will ensure that the list of Critical Points remains fairly concise and manageable.

The process for scoring components and dependencies is similar to that used previously for Asset Ranking – a number of criteria used to determine criticality either independently or in conjunction with each other.

1. Hazard Level – the level of potential hazard to people or the environment posed by the component
2. Magnitude – the amount of overall service delivery that the component/dependency contributes toward
3. Replacement Time/Effort – the length of potential outage and difficulty of replacement, taking into account any redundancy
4. Operational Importance – the level of overall importance to the operation taking into account the above criteria as well as any additional factors relevant to specific Assets

The recommended scoring criteria and guidance notes are provided in the table on the following page.

Guidance – historical data such as this will help to assess the Likelihood of future incidents in later stages of the risk assessment process.

Diagram B1g: Criticality Scoring Criteria

Criticality Scoring Criteria								
Score	**Level**	**Hazard Level**		**Magnitude**		**Replacement Time/Effort**		**Operational Importance**
5	Very High	The component could pose a very serious hazard to people or the environment	OR	The component/ dependency affects >75% of service delivery	OR	Loss of the component would lead to an outage time of >6 months, or be extremely difficult to replace	OR	The component/ dependency is essential to the overall operation, which could not continue without it
4	High	The component could pose a significant hazard to people or the environment	OR	The component/ dependency affects >50% of service delivery	OR	Loss of the component would lead to an outage time of >1 month, or be difficult to replace	OR	The component/ dependency is very important to the overall operation, which would be significantly compromised without it
3	Moderate	The component could pose a moderate hazard to people or the environment	OR	The component affects >25% of service delivery	OR	Loss of the component would lead to an outage time of >1 week or be quite difficult to replace	OR	The component/ dependency is important to the overall operation, which would be adversely affected without it
2	Low	The component poses a minor hazard to people or the environment	OR	The component affects >10% of service delivery	OR	Loss of the component would lead to a minor outage quickly rectified with an easy replacement	OR	The component/ dependency is only of partial importance to the overall operation, which would not be significantly affected without it
1	Very Low	The component does not provide any significant hazard to people or the environment	OR	The component affects <10% of service delivery	OR	Loss of the component would not cause an outage – the Asset is not dependent upon it or full redundancy is in place	OR	The component/ dependency is not important to the overall operation, which would not be at all affected without it

Source: PRISM™

The criteria detailed on the last page should be used to assign criticality scores to each significant component or dependency identified during the Asset Process Analysis. Once this has been completed they should then be ranked in order of importance. Those components and dependencies with a score of 3, 4 or 5 should be formally designated within the Security Management Plan as 'Critical Points' and taken forward to subsequent stages of the risk assessment. Those with scores of 1 or 2 are not considered critical to the Asset and can be disregarded at this stage, unless the Project Team have a specific requirement to include them in further analysis (these non-critical Assets will benefit from general security enhancements that result from the risk management process, but not specific countermeasures).

This is shown in the following example whereby 12 components have been assigned scores of 3-5 and designated as Critical Points, whilst three components have been assigned scores of 1-2 and will not be taken forward to the next stage.

B1.3 Summary

The Asset Characterisation process consisted of two main components – firstly Asset Ranking and secondly Critical Point Identification. The Asset Ranking process will have provided an overview of the role and importance of all corporate Assets and assisted the Project Team in prioritising these Assets and selecting the most important to be taken forward for further assessment.

Following on from this the Critical Point Identification process will have helped the Project Team to understand the characteristics of the Asset in more detail, including the processes, components and dependencies that are integral to its operation. This will have allowed criticality scores to be applied to all significant elements resulting in the formal designation of Critical Points, which will be taken forward to subsequent stages of the risk assessment process for further analysis.

Table B1h: Criticality Point Designation

Ref	Name	Criticality Score	Comments
CP1	Import Manifold	4	
CP2	Dehydration Tank	5	
CP3	Gas Station	5	
CP4	Sub-station	5	
CP5	Oil Storage Tanks	4	
CP6	Chemical Storage Tank A	5	
CP7	Chemical Storage Tank B	4	
CP8	Paper Files	3	
CP9	Electronic Data	3	
CP10	Control Room	5	
CP11	Production Hall	5	
CP12	Employees	5	
C1	Training Room	1	
C2	Workshop	2	
C3	Office Stores Facility	1	

Source: PRISM™

Asset Criticality Analysis will have helped the Project Team to understand the characteristics of the Asset in more detail

B2 Threat Characterisation

Purpose: To assist the owner/operator in identifying possible sources of Threat to the Asset, both criminal and non-criminal, and to provide a method of screening and prioritising these potential Threat Sources based on the inherent level of Threat posed by each one.

To then explore the characteristics of each Threat Source identified previously and develop a range of potential Threat Scenarios to be used as the basis for subsequent consequence, vulnerability and Likelihood analysis, as well as to inform risk mitigation measures.

B2.0 Introduction

The Security Management Plan Threat Assessment process is split into two separate phases. First, Section B2 identifies the potential types of criminal and non-criminal Threats that may pose a risk to the Asset, both in terms of Threat Sources and Threat Scenarios. Secondly Section B5 assesses the Likelihood of those Threats materialising. The Likelihood Assessment is conducted separately as it is first necessary in the context of criminal Threats to understand the potential consequences of a particular act upon an Asset (Section B3) and the existing level of vulnerability around the Asset (Section B4) – or, looking at it from the criminal's perspective, the level of reward versus the required resources/risk of failure.

In this respect the majority of criminals are logical actors who look to achieve a favourable risk:reward ratio and select targets accordingly. Along with capability and intent of the Threat actor, 'target attractiveness' is therefore key in determining Likelihood of an attack against a specific Asset, and requires an appreciation of both consequences and vulnerability. Where the consequences/reward are equal the Likelihood of an attack will increase when the required means decrease, as demonstrated by the recent popularity of 'soft targets' (eg. crowded public places) by certain terrorist groups. It is also worth bearing in mind that some criminal groups will conduct just as detailed vulnerability and consequence assessments as that done by the owner/operator when selecting their targets and methods of attack!

The starting point in the above process is to identify and prioritise the possible Threat Sources and Scenarios relevant to the Asset and location in question. The process for doing this is described in the following sections.

B2.1 Threat Source Identification and Ranking

The first stage of the Threat Characterisation process is to identify the possible sources of Threat to the Asset and subsequently rank them by Threat score to allow those of greatest significance to be taken forward for further analysis. There are three steps to this process.

Step 1: Identify Potential Threat Sources

For the purpose of the Security Management Plan potential Threats are sub-divided into two primary groups – criminal Threats and non-criminal Threats. Within each of these groups there are a number of further classifications which will help to identify the range of Threat Sources that could pose a risk to the Asset under consideration. Each group is considered below.

Criminal Threat Sources

A criminal Threat is distinguished by the element of human intent to commit the act in question, whether it be causing harm to the Assets (including people), organisation or environment, or removing or altering the Assets in some way. When looking to identify the range of possible criminal Threat Sources relevant to the Asset it may help to use the following five categories of criminal:

A. Terrorists
B. Economic Criminals
C. Violent Criminals
D. Subversives
E. Petty Criminals

This will cover the vast majority of criminal Threats although more groups can be added as required. Within each of these groups a number of specific types of criminal can be identified as shown in Table 2a.

Table B2a: Criminal Threat Classification

Ref	Category/Sub-Category	Ref	Category/Sub-Category
A: Terrorists		**B: Economic Criminals**	
A1	State Sponsored Terrorists	B1	Transnational Criminal Organisation
A2	Religious Extremists	B2	Organised Crime Groups
A3	Radical Revolutionaries	B3	Sophisticated Individuals
A4	Guerrillas	B4	Opportunistic Individuals
A5	Amateur Terrorists	B5	Other – Specify
C: Violent Criminals		**D: Subversives**	
C1	Workforce	D1	Political and Industrial Spies
C2	Contractors, Visitors	D2	Activist Groups
C3	Deranged Persons	D3	Disgruntled Persons
C4	Sexual Attackers	D4	Hackers
C5	Muggers	D5	Others
C6	Other – Specify		
E: Petty Criminals			
E1	Vandals		
E2	Petty Thieves		
E3	Other – Specify		

Source: PRISM^{TM}

When criminal acts are classified in the above manner the range of possible Threats and related criminal intentions becomes apparent. Whilst not all of these will be relevant to each Asset or location it is important to start the assessment process with a broad view of Threat Sources and narrow this down through focused research and analysis.

Non-Criminal Threat Sources

All Threats without the element of human intent can be classified as non-criminal. For the purpose of the Security Management Plan non-criminal Threats are broken down into the following three groups:

F. Natural Hazards
G. Accidental Hazards
H. Consequential Hazards

Again these groups can be further separated into a range of specific Threat Sources, for example:

Table B2b: Specific Threat Sources

Ref	Category/Sub-Category	Ref	Category/Sub-Category	Ref	Category/Sub-Category
A: Natural Hazards		B: Accidental Hazards		C: Consequential Hazards	
A1	Flood	B1	Fire	C1	Loss of Suppliers
A2	Cyclonic Storms	B2	Explosion	C2	Loss of Customers
A3	Tornados	B3	Containment Failure	C3	Loss of Employees
A4	Earthquake	B4	Structural Collapse	C4	Outage – Essential Services
A5	Tsunami	B5	Electrocution	C5	Loss of Transportation
A6	Wildfire			C6	Proximity Hazards
A7	Blizzard/Ice Storm				

Source: PRISM™

Step 2: Collect Threat information

In order to identify which of the above Threat Sources is relevant to a particular Asset, sector, country or region, it is first necessary to collect and analyse Threat information from a range of sources. This information will also be used to identify particular characteristics of individual Threat Sources in later sections of the assessment process.

The Project Team or Security Manager should develop a formal resource list which could include the following:

National Level

- Threat assessments provided by Member State governments
- National security and intelligence agencies
- Government Directives and Legislation

Local Level

- Local government assessments where available
- Liaison with local law enforcement and military
- Liaison with civic elements such as local government authorities

Media

- Open-source reporting – internet, printed press, TV, radio
- Use of commercial/business intelligence companies – commissioned reports or subscription publications
- Trade journals

Owner/Operator Assets

- Subject to legal provisions, the owner/operator's own Human Resources department and line managers for information on potential Threats from employees
- Owner/Operator's procurement and legal departments for information on possible supply chain Threats
- Reporting from owner/operator's own security personnel especially for information on immediate local environment, suspicious persons/vehicles/possible hostile reconnaissance/journalists etc
- Encouragement of employees to report possible security Threats/breaches
- Liaison with owner/operators of similar Assets for information sharing
- Analysis of site CCTV, Access Control and IDS systems to identify attempts at unauthorised entry

In addition the Project Team should review previous Threat assessments, security logs, safety reports and related analysis. A Process Hazard Analysis will have already been completed for the majority of energy facilities and will provide a good source of information about potential non-criminal hazards (as well as possible consequences). In many cases this will include detailed and quantifiable risk assessments and it is worth reiterating that the aim of the Security Management Plan is not to replace this work but rather to utilise it in building a holistic picture of possible risks facing the energy network as well as each Asset. Capturing both criminal and non-criminal risks within a single framework is also important since some countermeasures will be effective against both types of risk and therefore more easily justifiable in terms of required expenditure.

When gathering and assessing information on Threat Sources there are a number of additional considerations:

Relevance: A high proportion of Threat reporting is imprecise and often generic in nature i.e. not specific to the industry sector or geographical location within which the Asset sits. For example the country Threat level from terrorism could be graded as high, whilst the Threat to a specific sector such as energy could be low. Therefore, Threat reporting should be considered in relation to the specific Asset and geographical location in question.

Reliability: When dealing with Threat information it is important to note that there will be varying degrees of **Reliability (of source)** and **Credibility (of the information)** and it may be useful to grade the Threat information, for example:

Table B2c: Threat Information Classification

Reliability of source	Credibility of info
A Completely reliable	1 Confirmed by other sources
B Usually reliable	2 Probably true
C Fairly reliable	3 Possibly true
D Not usually reliable	4 Doubtful
E Unknown	5 Untrue

Source: PRISM™

Example: Grading B1 = a usually reliable source has supplied confirmed information

Where possible the assessment should not rely upon a single source but should seek corroboration from as many sources as possible. It is particularly important when evaluating information to consider how objective the reporting is and whether the source may have any biases or personal/corporate/political agendas.

Precedence: The assessment team will need to establish which sources will take precedence in the event of differing reporting or from which agencies they will take their lead in terms of changing Threat levels or reacting to information. This is particularly so for foreign-owned companies who may receive different reporting from their own government as opposed to the government whose territory the Asset sits within. This is likely to vary depending on the country of operation, any legal requirements imposed by government, and the level of information that they typically share with owner/operators.

Volume: The internet has dramatically increased the volume and availability of open-source reporting and whilst it can be a very useful tool in gathering Threat information, it can also overwhelm the assessment team. In order to manage this it is necessary to record and prioritise the various sources of Threat information utilised – and over time create a more focused approach to research.

Step 3: Rank and Prioritise Threat Sources

The next stage in the process is to use the Threat information gathered in the previous step to draw up a list of potential Threat Sources and score them based upon the general level of Threat that they may pose. This will subsequently allow these Threat Sources to be prioritised with relevant ones being taken forward to the next stage.

The scoring process for criminal and non-criminal Threat Sources differs slightly.

Criminal Threats

Once a list of possible Threat Sources has been produced the following information and analysis should be assembled (Information highlighted in bold will be used to score Threat levels):

Table B2d: Criminal Threats: Information and Analysis

Information required	Guidance
1. Type and Category of Threat	This can be taken from the classifications outlined previously – for example 'Terrorist/Religious Extremist'
2. Name of Threat Source	The name of the Threat Source should be stated if known – for example 'GSPCC'.
3. Main Objectives	State the main objectives of the Threat Source such as mass casualty attacks, economic damage, psychological damage or financial gain.
4. Threat Level to Sector (Government Advised)	If a government agency has provided a Threat level specific to this type of Threat and sector it should be recorded and can be used as an alternative to the scoring process that follows. If the Threat level is not sector-specific it should be taken into account in the scoring process but should not replace it.
5. Degree of Presence within the Geographical Area of Concern?	Not all Threats are relevant to all geographical locations. It is therefore necessary to assess how well established the Threat is in the area of concern – is there frequent press reporting, public statements by the group, financing activity etc, and are they in a period of growth or decline? Although some Threats are international in nature a lack of local support base will make attacks more difficult to mount and may indicate that the area is of lesser priority.
6. Inherent Capability to Achieve Objectives	Assess the general level of capability that the Threat Source may have – are attacks purely aspirational or have they demonstrated that they have the capability to achieve their objectives?
7. Intention to Carry out the Threat	Assess the level of intention to carry out the Threat – how well motivated do they appear to be, is an attack in this location a priority for them or do they have other priorities elsewhere?
8. Known History of Attacks	Summarise any known history of attacks by this Threat Source – have they been carried out against this Asset/sector/country/region or only further afield? How regular are the attacks and what type of Assets have been targeted in the past?

Source: PRISM™

When the above information has been gathered and analysed in qualitative terms a scoring table should be created to allow Threats to be compared and prioritised for further assessment. An example of the scoring table showing all Threat Source categories is shown on the following page.

Table B2e: Criminal Threat Source Scoring Matrix

Possible Threat Sources				Threat Level to Sector (Govt. Advised)	-OR-	Is the Threat Present?	Does Threat have inherent capability to achieve Objectives?	Does Threat have intention to act?	Has Threat Targeted Facility/Sector /Country/Region Before?	Threat Score
Ref	Category/Sub-Category	Name if Known	Main Objectives			Threat Assessment				
A: Terrorists										
A1	State-Sponsored Terrorists									0
A2	Religious Extremists									0
A3	Radical Revolutionaries									0
A4	Guerrillas									0
A5	Amateur Terrorists									0
B: Economic Criminals										
B1	Transnational Criminal Organisation									0
B2	Organised Crime Groups									0
B3	Sophisticated Individuals									0
B4	Opportunistic Individuals									0
B5	Other – Specify									0
C: Violent Criminals										
C1	Workforce									0
C2	Contractors, Visitors									0
C3	Deranged Persons									0
C4	Sexual Attackers									0
C5	Muggers									0
C6	Other – Specify									0
D: Subversives										
D1	Political and Industrial Spies									0
D2	Activist Groups									0
D3	Disgruntled Persons									0
D4	Hackers									0
D5	Other – Specify									0
E: Petty Criminals										
E1	Vandals									0
E2	Petty Thieves									0
E3	Other – Specify									0

Source: PRISM^{TM}

It is important to note at this stage this is not intended to cover every aspect of the Threat assessment process but rather to allow Threat Sources to be prioritised. In particular the methods of attack used by various groups will be addressed in the following section, whilst the Likelihood of various attack scenarios being carried out specifically against the Asset in question will be addressed in section B5.

The B2e matrix uses scores from 1-5 for each of the four scoring criteria and uses this to calculate an overall score each identified Threat Source. The individual scoring criteria are provided in the following tables:

Table B2f: Scoring Criteria – Criminal Threats

1. Is the Threat Present?		
Score	**Criteria**	**Category**
5	The Threat is endemic in the area/country/region	Very High
4	The Threat is well-established in the area/country/region	High
3	The Threat has some presence in the area/country/region	Moderate
2	The Threat has very limited presence in the area/country/region	Low
1	The Threat is not known to be present in the area/country/region	Very Low
2. Does the Threat Have Inherent Capability to Achieve Objectives?		
Score	**Criteria**	**Category**
5	The Threat is currently judged to have a very high level of capability to achieve objectives	Very High
4	The Threat is currently judged to have a high level of capability to achieve objectives	High
3	The Threat is currently judged to have a moderate level of capability to achieve objectives	Moderate
2	The Threat is currently judged to have limited capability to achieve objectives	Low
1	The Threat is not currently judged to have any capability to achieve objectives	Very Low
3. Does the Threat Have Intention to Act?		
Score	**Criteria**	**Category**
5	The Threat is currently judged to have a very high level of intention to act	Very High
4	The Threat is currently judged to have a high level of intention to act	High
3	The Threat is currently judged to have a moderate intention to act	Moderate
2	The Threat is currently judged to have limited intention to act	Low
1	The Threat is not currently judged to have any intention to carry out an attack	Very Low
4. Has Threat Targeted Asset/Sector/Country/Region Before?		
Score	**Criteria**	**Category**
5	The Threat has targeted the Asset before	Very High
4	The Threat has targeted the sector within this country before	High
3	The Threat has targeted a different sector within this country before, or the same sector within the region	Moderate
2	The Threat has targeted a different sector within the region before	Low
1	The Threat has not carried out attacks in the region before.	Very Low

Source: PRISM™

Non-Criminal Threats

For non-criminal Threats it is possible to determine a Threat Likelihood Score without having first completed the consequence and vulnerability assessment section, since human intent and therefore Target Attractiveness do not play a role in determining Likelihood of the Threat materialising. Instead Likelihood can be determined via consideration of historical incidents, as well as relevant information about the geographical and socio-economic context within which the Asset resides.

In order to determine the Likelihood of Non-Criminal Threats the Project Team should review the information collected during the previous step with regards to potential Threat Sources and consider the areas set out in the following table (information highlighted in bold will be used to score Threat levels):

Table B2g: Non-Criminal Threats Information and Guidance

Information required	Guidance
1. Type and Category of Threat	This can be taken from the classifications outlined previously – for example 'Natural Hazard/ Flood'
2. Name of Threat Source	In some case such as 'loss of supplier' the name of the Threat Source should also be stated, for example 'Company X' or 'Chemical Supply from Company Y'.
3. Threat Characteristics	What characterises this type of Threat and how might it occur?
4. Relevance to Asset	Does the Asset have specific characteristics that make it relevant to the Threat, either in terms of geographical location, prevalence of adverse meteorological conditions, single-point dependencies within the supply chain, or infrastructure/ processes that could be subjected to accidental damage?
5. Historical Incidents	For non-criminal hazards the main indicator of Threat level is history of similar incidents, whether that is natural hazards, accident records or supply-chain failures.
6. Anticipated Frequency	A secondary factor is the anticipated frequency of incidents – this should take into account both historical data but also future predictions based upon changes in environmental conditions, Asset characteristics, number of workforce, and known supply-chain issues.

Source: PRISM™

When the above information has been gathered and analysed in qualitative terms a scoring table should be created to allow Non-Criminal Threats to be compared and prioritised for further assessment. An example of the scoring table showing all Threat Source categories is shown below.

In order to determine the Likelihood of Non-Criminal Threats the Project Team should review the information collected during the previous step with regards to potential Threat Sources.

Table B2h: Non-Criminal Threat Source Scoring Matrix

Possible Threat Sources

				Relevance to Asset	Historical Incidents	Anticipated Frequency	Threat Score
Ref	**Category/Sub-Category**	**Name of Threat Source (if known)**	**Main Objectives**	**Threat Assessment**			
A: Natural Hazards							
A1	Flood						0
A2	Cyclonic Storms						0
A3	Tornados						0
A4	Earthquakes						0
A5	Tsunami						0
A6	Wildfire						0
A7	Blizzard/Ice Storm						0
A8	Other – Specify						
B: Accidental Hazards							
B1	Fire						0
B2	Explosion						0
B3	Containment Failure						0
B4	Structural Collapse						0
B5	Electrocution						0
B6	Other – Specify						
C: Consequential Hazards							
C1	Loss of Suppliers						0
C2	Loss of Customers						0
C3	Loss of Employees						0
C4	Outage – Essential Services						0
C5	Loss of Transportation						0
C6	Proximity Hazards						0
C7	Other – Specify						0

Source: PRISM™

The above Table B2h uses scores from 1-5 for each of the three criteria and utilises this to calculate an overall score for each identified Threat Source. The individual scoring criteria are provided in the following tables:

Table B2i: Scoring Criteria – Non-Criminal Threats

1. Relevance to Asset		
Score	**Criteria**	**Category**
5	The Threat is extremely relevant to the Asset, geographical area or supply chain	Very High
4	The Threat is very relevant to the Asset, geographical area or supply chain	High
3	The Threat is of moderate relevance to the Asset, geographical area or supply chain	Moderate
2	The Threat is of limited relevance to the Asset, geographical area or supply chain	Low
1	The Threat is of very little relevance to the Asset, geographical area or supply chain	Very Low
2. Historical Incidents		
Score	**Criteria**	**Category**
5	This Threat has occurred and specifically affected the Asset, local area or supply chain in question	Very High
4	This Threat has occurred and affected other Assets or the local area or the wider sector supply chain	High
3	This Threat has occurred in the region or within other sectors	Moderate
2	This Threat has not occurred but it is quite possible that it may in future	Low
1	This Threat has not occurred and it is very unlikely to in future	Very Low
3. Anticipated Frequency		
Score	**Criteria**	**Category**
5	The Threat is likely to occur at least once a month	Very High
4	The Threat is likely to occur at least once a year	High
3	The Threat is likely to occur at least once every 10 years	Moderate
2	The Threat is likely to occur at least once every 100 years	Low
1	The Threat is likely to occur less than once in 100 years	Very Low

Source: PRISM™

Since no further steps are necessary to calculate Non-Criminal Likelihood these scores will be taken directly to the Threat Likelihood section of the Risk Register. However, where owner/operators are using an alternative method to assess Non-Criminal Risks, existing Likelihood scores can be used instead as discussed in Section B6.

Threat Source Ranking and Prioritisation

Once both criminal and non-criminal Threat Sources have been assessed they can be ranked and prioritised according to overall Threat score as shown in table B2j.

Table B2j: Overall Threat Source Scores

Threat Sources					
Risk Ref	**Category**	**Sub-Category**	**Name (if known)**	**Main Objectives/Characteristics**	**Threat Score**
A: CRIMINAL THREATS					
A1	Terrorist	Religious Extremist	Al-Qaeda	Mass Casualty Attacks, Damage to Critical Infrastructure, Psychological damage to host nation, theft of precursor CBRNE materials	4
A2	Economic Criminal	Sophisticated Individual	Employee	Material gain through misuse of access	5
A3	Subversive	Activist Group	-	Disruption to target infrastructure, media attention, gain public support	3
B: NON-CRIMINAL THREATS					
B1	Natural Hazard	Flooding	-	Can cause widespread disruption and damage to vulnerable infrastructure	6
B2	Accidental Hazard	Explosion	-	Potential for significant damage to Asset through human error	8
B3	Consequential Hazard	Outage – Essential Services	-	Loss of essential services as a result of supplier failure	6

Source: PRISM™

Depending upon the number of relevant Threat sources identified the Project Team may wish to filter out those that score very low, for example less than 2, however it is important that this assessment is revisited on a regular basis and any changes in associated Threat levels captured.

The selected Threat Sources will then be taken forward to the next stage which examines their likely characteristics in more detail and develops a range of possible scenarios in which the Threat could manifest itself.

B2.2 Threat Source Characteristics

Threat Scenarios are an important tool in the risk management process as they transform general Threats into specific incidents and as such allow for a more detailed analysis of consequences, Asset vulnerability and Likelihood. As a result the owner/operator can decide specifically what parts of the Asset need to be protected from which type of Threats, which subsequently provides the basis for the design of cost-effective and focused mitigation measures.

The potential disadvantage of using scenarios as the basis for risk analysis is that it is impossible to cover all eventualities and as such there is the possibility that mitigation measures may not provide complete protection. However, this is always a possibility and typically far more likely to occur when trying to protect against a Threat in general rather than a specific type of incident. In order to further reduce this risk and ensure scenarios are as representative of real-life incidents as possible, the Security Management Plan takes the following approach:

- Starts with a wide range of scenarios based upon careful analysis of Threat characteristics, and subsequently filters out those scenarios which are less relevant due to a lack of significant consequences, inherent vulnerability or Likelihood. As a result a wide range of possibilities can be considered, but only the most relevant scenarios are captured in the Risk Register (section B6), which subsequently provides the basis for very focused mitigation options

- Uses the scenario as the highest point of analysis, thus allowing each scenario to be considered in terms of the risk posed to all parts of the Asset deemed critical rather than just the Asset as a whole or a single component (when others may be also be at risk). In effect this creates a number of sub-scenarios for each primary Threat Scenario

The following section provides guidance on the manner in which Threat Scenarios can be developed and as such is key to the overall process. It should be given due time and attention by the Project Team and revisited on a regular basis. Prior to developing these scenarios it is necessary to understand the possible characteristics of each Threat Source identified previously. Guidance on doing so is provided below.

Criminal Threat Characteristics

Criminal Threat characteristics, often referred to as Modus Operandi (MO) or Methods of Attack, can be identified by conducting an analysis of past attacks to identify common patterns amongst different Threat actors or groups. This is evident when considering the MO of terrorist groups such as Al-Qaeda, who are renowned for careful planning, extensive hostile reconnaissance, radicalisation and recruitment of people to form the attack cell and a desire to create a ‘spectacular’ often via multiple, near-simultaneous attacks on people and infrastructure. However, other terrorist groups, even those aligned with Al-Qaeda, may have significantly different MOs, either as a result of differences in strategic objectives, available resources or ideology. In this respect it is very useful to be as specific as possible about the Threat actor – rather than assess the Threat from ‘Terrorism’ consideration should be given to specific groups and their individual characteristics.

Another important consideration in the current context is that attack methods are constantly evolving, sometimes as a result of experience from past attacks, influence from other groups or simply to meet the demands of a specific target. Since the attack on the World Trade Center in 2001, Al-Qaeda have become synonymous with ‘novel’ attacks, but the same goes for economic crime – for example the use of kidnapping tactics to gain entry into a high-security cash storage facility (commonly referred to as ‘Tiger Kidnap’) as has occurred in the UK, Northern Ireland and Belgium in recent years.

Therefore, it is also important at this stage to consider methods which could be used to fulfil the objectives of each Threat Source. In some cases these methods may be improbable but this is considered in Section B5 (which examines the Likelihood of attack) and therefore the Project Team should keep an open mind at this stage. In addition it is vital that this part of the Security Management Plan is updated at least annually as part of a formal review process, and also in response to events or changes in the security environment during the year.

When defining the characteristics of a particular criminal Threat Source it is useful to consider five aspects of their attack: Professionalism; Means of Access; Weapons; Method of Delivery/Initiation; and Potential Targets. In each of these areas there are a range of possible considerations relating to the type of attack that could be conducted as shown in the table on the following page:

Table B2k: Criminal Threat Characteristics

Area	Possible Characteristics/MO/Method of Attack	
Level of Professionalism	– Planning – Training – Hostile Reconnaissance	– Recruitment – Radicalisation – Determination
Means of Access	– Improvised Tools – Specialist Tools – Overwhelm Guards or Staff – Stealth/Bypass – Vehicle Penetration – Stolen Vehicle – Insider Access	– Collusion with Insider – False Credentials – Social Engineering – Tiger Kidnap – Utilise Public Areas – Remote Attack
Use of Weapons	– Blunt Objects – Blades – Firearms – Grenades – RPGs, Mortars, MANPADS – Explosives – Incendiary Devices – Chemical Agents	– Biological Agents – Radioactive Agents – Fuel Tankers – Electronic Devices – Malicious Software – Handcuffs, lock-on devices, human blockades – None
Method of Delivery and Initiation (IED/Incendiary/CBR)	**– IEDs and Incendiaries** – Vehicle-borne – Person-borne – By Post/Courier – Hand-placed – Suicide – Remote detonation – Timer – Trip-wire	**– CBR Agents** – By Post/Courier – Aerosolised – Hidden Onsite – External Release – Internal Release – Use of HVAC System – Contamination (Food, Water, Fuel) – Human Carrier – Enhanced IED – Deliberate Release from Site
Possible Targets	– Groups of People – Individuals – Infrastructure Critical Points – Infrastructure Hazardous Points	– Remote Dependencies – Supply Chain – Valuable Physical Property – Information

Source: PRISM™

For each Threat Source identified in the previous section the Project Team should compile a list of relevant characteristics using the five areas highlighted. These characteristics will be used not only to create scenarios but also to inform subsequent stages of the risk assessments and risk mitigation process.

Some operators may find it helpful to score each of the above characteristics in terms of relevance to the Threat Source, for example using the following scale:

Score	Scoring Criteria	Category
5	The Threat Source has used this MO extensively in the past	Very High
4	The Threat Source has used this MO on several occasions or indicated that they intend to in future	High
3	The Threat Source has not used this MO but it would be suitable for meeting their objectives	Moderate
2	The Threat has not used this MO, it is possible but unlikely that they would do so	Low
1	The Threat is very unlikely to use this MO	Very Low

However, since this is not an exhaustive list it is important that whatever approach is used to define the characteristics of each Threat Source, it offers the flexibility to incorporate additional possibilities rather than just a pre-defined list. It is also worthwhile including further notes and explanation of each characteristic as these will be useful in subsequent countermeasure design.

Non-criminal Threat Characteristics

Non-criminal Threat characteristics are often easier to identify based primarily upon past events as well as local environmental factors. The following table provides a number of considerations and should be completed for each non-criminal Threat identified previously:

Table B2l: Non-criminal Threat Characteristics

Area	Possible Characteristics
Anticipated Intensity	What level of intensity has been associated with similar events in this area? For example if a natural hazard how severe is it likely to be?
Anticipated Scale	Will the event affect the Asset as a whole or just individual components, processes or business functions?
Anticipated Duration	From previous events similar in character how long is it likely to last – will the Asset be subjected to sustained impact for a significant period of time or will it be over relatively quickly?
Advance Warning	Is there likely to be any advanced warning of the Threat? This may come from a supplier, a meteorology organisation or more discreetly from safety reports and other indicators.

Source: PRISM™

B2.3: Threat Scenario Selection

The next stage in the Threat Characterisation process is to use the key characteristics associated with each Threat Source to create one or more potential Threat Scenarios – for Threat Sources who are known to have used a variety of different attack methods it may be necessary to create several different scenarios that reflect this, whilst for others who have a specific MO one may be sufficient.

Threat Scenarios need to be flexible enough to cover slight variations in the method of attack that may actually be employed, but not so flexible that they do not provide a useful analysis tool. Some examples of this are now provided.

Table B2m: Threat Scenarios

Threat Source 1/Terrorist/Religious Extremist/'GSPCC' – Scenario 1: IED Attack	
Not Specific Enough	An IED Attack
About Right	A hand-placed IED attack on a critical component
Too Specific	A six-man assault team attack the facility at night, cut through the perimeter fence using a blowtorch and placed an IED with timing device on Transformer 1. They are interrupted on the way out of the facility and shoot two security guards
Threat Source 1/Terrorist/Religious Extremist/'GSPCC' – Scenario 2: CBRN Attack	
Not Specific Enough	CBRN attack on the Asset
About Right	A CBRN agent is introduced into the HVAC System
Too Specific	Entry is gained into the site by use of false credentials and hydrogen cyanide is aerosolised and released into the HVAC system of the Administration Building during peak occupancy

Source: PRISM™

Other characteristics such as method of entry are also important and could be included in the scenario; however, it is often better to use this information in the vulnerability assessment stage as a wider range of possibilities can be considered without the need for endless scenarios. For example in the context of the above scenarios the vulnerability assessment could consider all of the ways in which the attacker could gain access to the site, particularly those that they have used in the past.

The scenarios should however cover the main types of attack and possible targets associated with each Threat Source, since this is necessary to identify possible consequences of the Threat materialising, which is addressed in Section B3.

In order to provide further assistance with the creation of Threat Scenarios table B2n outlines some common scenarios associated with each type of Threat Source. However, it should not be taken as a definitive list – as highlighted earlier attack methods vary between groups and specific analysis is necessary.

Table B2n: Examples of Common Scenarios

Threat Source	Generic Scenarios	Considerations
Terrorist	**Vehicle-Borne Improvised Explosive Device (VBIED)** • Car, Truck, Motorcycle, Bicycle, Aircraft • Suicide attack at gatehouse or perimeter • Vehicle left near Asset or as attempt to gain access before detonation at vulnerable point • By proxy – innocent person forced to drive vehicle or device placed on employee or delivery vehicle	VBIED attack against gatehouse or perimeter used to facilitate entry to wider site. Use of 'false flag' vehicles Vehicle used as a hoax
	Person-Borne IED • Suicide rucksack, briefcase, handbag, vest • Detonation at gatehouse or attempt to gain entry before detonation near vulnerable point • By proxy – innocent person forced to carry device	Detonation of smaller device used to tie up/distract first responders before follow-up with larger attack
	Delivered IED • Parcel, packet, letter bomb • Device delivered to gatehouse by courier • Device delivered via normal mail channels	Detonation of smaller device used to tie up/distract first responders before follow-up with larger attack Package used as a hoax
	Small Arms Attack • CQA against gatehouse • CQA against employees arriving/departing • CQA against delivery vehicles • Drive-by attack against gatehouse or perimeter • Standoff attack from perimeter against personnel or vulnerable points – sniper	SAA at gate house may be used to facilitate entry to wider site or as precursor to follow-up attack such as VBIED Reconnaissance by fire – standoff SAA used to gauge reaction of security elements onsite
	Indirect Fire Attack • Against gatehouse • Against critical points, cafeterias, staff car parks	Precursor to follow-up attacks – VBIED, SAA
	Chemical, Biological, Radiological Attack (CBR) • CBR materials delivered in letters or parcels • Attempts to add CBR materials to water, air-handling systems • Food and drink supplies adulterated with CBR materials	Exact nature of a CBR attack may not be immediately obvious. Effects on people may not be immediate Hoaxes/false alarms
	Physical and Logical/Electronic Sabotage • Physical Sabotage of Critical Points and process controls • Electronic interference with Process Control Systems • Introduction of non-CBR contaminant such as metal filings to damage plant	Electronic interference of Process Control/SCADA systems with the intent to compromise containment is an increasing concern as necessary IT skills are become more accessible to terrorist groups and process control systems have increasing connections with corporate data networks and the web.

Source: PRISM™

Table B2n: Examples of Common Scenarios (cont.)

Threat Source	Generic Scenarios	Considerations
Economic Criminal	**Theft** • Information • Property – vehicles, tools, IT equipment, clothing • Site-specific components • Cash • Crime elements, competitors, local populace, contractors, employees • Major fraud	May also be perpetrated as opportunity arises during other attack types Articles stolen may be used in other attacks – i.e. use of vehicles and uniforms to gain access to other sites
	Kidnapping • Including high-value staff – scientists, senior managers • Tiger Kidnap	Preceded by surveillance, possibly on- and offsite May also be perpetrated as part of a wider terrorist attack
Violent Criminal	**Deranged individuals** • Moving shooter attack • Sniper attack • Violence against employees, visitors or contractors	Could be little warning and random targeting
	Employees/Contractors • Physical violence against other staff	Difficult to prevent – will require onsite security to interdict
Subversives	**Disgruntled Employee/Former Employee** • Physical sabotage of Asset processes and infrastructure • Theft • Release of sensitive information • Introduction of malware to IT systems • Can be planned well in advance or be opportunistic in nature	Usually designed to cause financial loss and damage to reputation rather than casualties Former employees may be manipulated by or provide their knowledge to third parties listed above
	Manipulation • Use of influencing techniques (such as bribery) on employees by third parties to achieve access to information and Assets	Often carried out over long periods with information/access accrued on a piecemeal basis Third parties may include competitors, Hostile Intelligence Services, pressure groups, domestic extremists, other employees, investigative journalists, criminals

Source: PRISM™

Table B2n: Examples of Common Scenarios (cont.)

Threat Source	Generic Scenarios	Considerations
	Hackers • Hacking of Process Control/SCADA systems • Hacking • Denial of Service (DoS) Attack • Distributed DoS Attack • Malicious Hardware	Previous cases of hackers gaining control of Process Control Systems, most notably the Hoover Dam in the USA Electronic attack can be carried out internally, either directly by employees or by contractors associated with the servicing or maintenance of IT systems
	Activist Groups • Unauthorised entry via overwhelming gatehouse or scaling/breaching perimeter fences • Unfurling of anti-Asset banners • Vandalism and destruction of site Assets • Verbal and physical assaults against staff • Antagonising security elements and police in order to provoke response • Individuals 'locking on' to gates, grilles, vehicles, fences and other site Assets • Rooftop and 'sit-in' protests	Action by protesters can often be protracted, causing long delays in site operations and interfering with access Can illicit widespread media coverage and impact on reputation/public relations Peaceful protest can eventually escalate to violence. Factors include length of protests, MO of protest groups and reaction by security personnel
Natural Hazards	• Depending on site location but includes **fire, flood, earthquake, tornado** • Intensity and duration can vary significantly • Could affect sites where building codes are not stringent enough	Ability and availability of outside agencies to assist
Accidental Hazards	**Catastrophic accident** • Major explosion • Containment failure	Details can be taken from Process Hazard Analysis and previous safety reports
Consequential Hazards	**Supply-Chain Failures** • Loss of essential services • Loss of export route which may stop supply • Loss of customers	May need to review external third-party Assets

Source: PRISM™

B2.4 Summary

This phase of the risk assessment process has characterised possible Threats facing the facility by considering both Threat Sources and Threat scenarios. A significant amount of research and analysis is required to compile this information, and the more accurate it can be made the more effective the overall risk management process will be. This is because the scenarios generated from this phase will be utilised as the basis for all subsequent risk analysis and mitigation, helping to focus on specific rather than generic risks and countermeasures. It is important that this information is kept up to date in line with the latest Threat information, and this should be done as part of a formal review process conducted at regular intervals and in response to any specific incidents of concern.

B3 Consequence Assessment

Purpose: To provide a framework for assessing the consequences of each Threat Scenario in relation to both the Asset as a whole and each individual Critical Point at Risk. This is done by identifying the primary consequences at both the owner/operator level and community level, and subsequently assigning scores based upon the anticipated severity.

B3.0 Introduction

Once a range of Threat Scenarios have been developed the next stage is to assess the possible consequences that may result from each scenario occurring. The Reference Security Management Plan is primarily intended for use by owner/operators of Critical Energy Infrastructure (CEI) Assets which are of fundamental importance to the wider community with consequences (and subsequently risks) that need to be assessed not only on the owner/operator, but also on the community.

Whilst the extent of the owner/operators' legal responsibility for external consequences will vary from country to country, at the very least they will have a Corporate Social Responsibility to minimise risks posed to the community, and in many cases they will suffer some form of direct or indirect financial loss in not doing so.

As such it is important that the risk assessment phase considers both levels of analysis and this is catered for within the PRISM™ approach on which this guidebook is based. However, the extent to which risk mitigation strategies are implemented, and at what level, is left to the discretion of the individual owner/operator and/or the regulatory framework within which the Asset sits.

The assessment process itself considers how each Threat Scenario may impact upon each of the Critical Points identified in Section B1, as well as the Asset as a whole, and subsequently the type and severity of consequences that will result from this. Scenario/Critical Point pairs with little or no associated consequence can then be filtered out thus allowing a more focused set to be taken forward to the next stage. This assessment process is detailed below.

> *"Corporate Social Responsibility (CSR) is a concept where companies integrate social and environmental concerns in their business operations and in their interaction with their Stakeholders on a voluntary basis. It is about enterprises deciding to go beyond minimum legal requirements… in order to address societal needs".*
>
> *European Commission*

B3.1 Critical Point – Scenario Pairs

Before conducting a detailed consequence assessment it is worthwhile to consider the relevance of each Threat Scenario to each Critical Point (CP) identified previously. In some cases Scenario/CP pairs can be immediately ruled out due to an absence of any tangible consequence or a lack of inherent vulnerability of the component to the Threat Scenario. Some examples are provided below:

Table B3a: Scenario-CP Matrix

Scenario	Critical Components	Relevance/Comments
Sabotage of a critical component by a former employee	SCADA System	Should be considered
	Switchgear	Should be considered
	Gas Valve	Should be considered
	Management Team	Not relevant to this scenario (separate scenario should be used If Threat source is considered violent)
Stand-off RPG attack against the facility	Chemical Tanks	Should be considered
	Sub-station	Should be considered
	Management Offices	Should be considered
	Underground Storage Tank	Not relevant since there is no visibility or inherent vulnerability
Theft of Proprietary Information	Paper Files	Should be considered
	Electronic Data	Should be considered
	Water Intake Valves	Not relevant
	Pumping Station	Not relevant
A major flood of the entire facility	Transformer Compound	Should be considered
	Paper Files	Should be considered
	SCADA System Servers	Should be considered
	Oil Storage Tank	Not relevant

Source: PRISM™

At this stage the aim is not to assess consequences or vulnerability in detail – where there is any uncertainty as to whether or not consequences would arise from the Threat Scenario or whether the CP would be vulnerable to the Threat Scenario, the Scenario/CP pair should be taken forward for further analysis. For example considering the above scenarios it may be that the chemical tanks have a degree of resistance to RPG attack and would not necessarily fracture as a result. However, this will be explored in the Vulnerability Assessment phase and if necessary can be ruled out following a detailed analysis.

This filtering process should therefore be fairly intuitive and quick to complete. It will result in a table of Scenario/CP pairs ready for further analysis of individual consequences. This is shown in the following table, which combines the example Threat Sources and Scenarios from Section B2 with relevant Critical Points from Section B1 – which together make up the ‘Risk Scenarios’ that will be used for all subsequent analysis.

Table B3b: Risk Scenarios

Risk Ref	Risk Scenario			
	Threat Source	**Scenario Description**	**Critical Points**	
			Ref	**Name**
A: CRIMINAL THREATS				
A1.1	Terrorist/Religious Extremist/Al-Qaeda	An IED is hand-placed inside the facility and subsequently detonated	**CP0**	**ASSET**
			CP1	Import Manifold
			CP2	Dehydration Tank
			CP3	Gas Station
			CP4	Sub-station
			CP5	Oil Storage Tanks
A1.2		A hazardous chemical storage tank is sabotaged	**CP0**	**ASSET**
			CP6	Chemical Storage Tank A
			CP7	Chemical Storage Tank B
A2.1	Economic Criminal/ Sophisticated Individual	An employee uses his access to management offices to steal sensitive research material	**CP0**	**ASSET**
			CP8	Paper Files
			CP9	Electronic Data
A3.1	Subversive/ Environmental Activist	An activist group gain entry to the site and attempt to halt production	**CP0**	**ASSET**
			CP10	Control Room
			CP11	Production Hall
			CP12	Employees
B: NON-CRIMINAL THREATS				
B1.1	Natural Hazard/Flooding	Heavy and prolonged rain causes flooding across the site	**CP0**	**ASSET**
			CP4	Sub-station
			CP13	IT Server Room
			CP8	Paper Files
B2.1	Accidental Hazard/Explosion	A spark from a vehicle ignites spilled fuel and subsequently causes an explosion	**CP0**	**ASSET**
			CP5	Oil Storage Tanks
			CP3	Gas Station
B3.1	Consequential Hazard/ Outage – Essential Services	The transmission system operator experiences a major sub-station failure resulting in a loss of electricity to the site.	**CP0**	**ASSET**
			CP4	Sub-station
			CP2	Dehydration Tank

Source: PRISM™

B3.2 Risk Scenario Consequences

The next stage is to assess the potential consequences of each Risk Scenario both at the Critical Point level and the Asset level, assuming that the scenario impacts upon multiple Critical Points simultaneously.

For each scenario the *reasonable worst-case consequences* should be considered. For example it would be reasonable to assume that a terrorist group with a history of extensive hostile reconnaissance and desire to inflict mass casualties would target the facility during peak occupancy. However, it would be unreasonable to assume that they would target the facility when a north-easterly wind will blow chemicals in the direction of the nearest town if the prevailing wind is south-westerly (i.e. it is beyond their control).

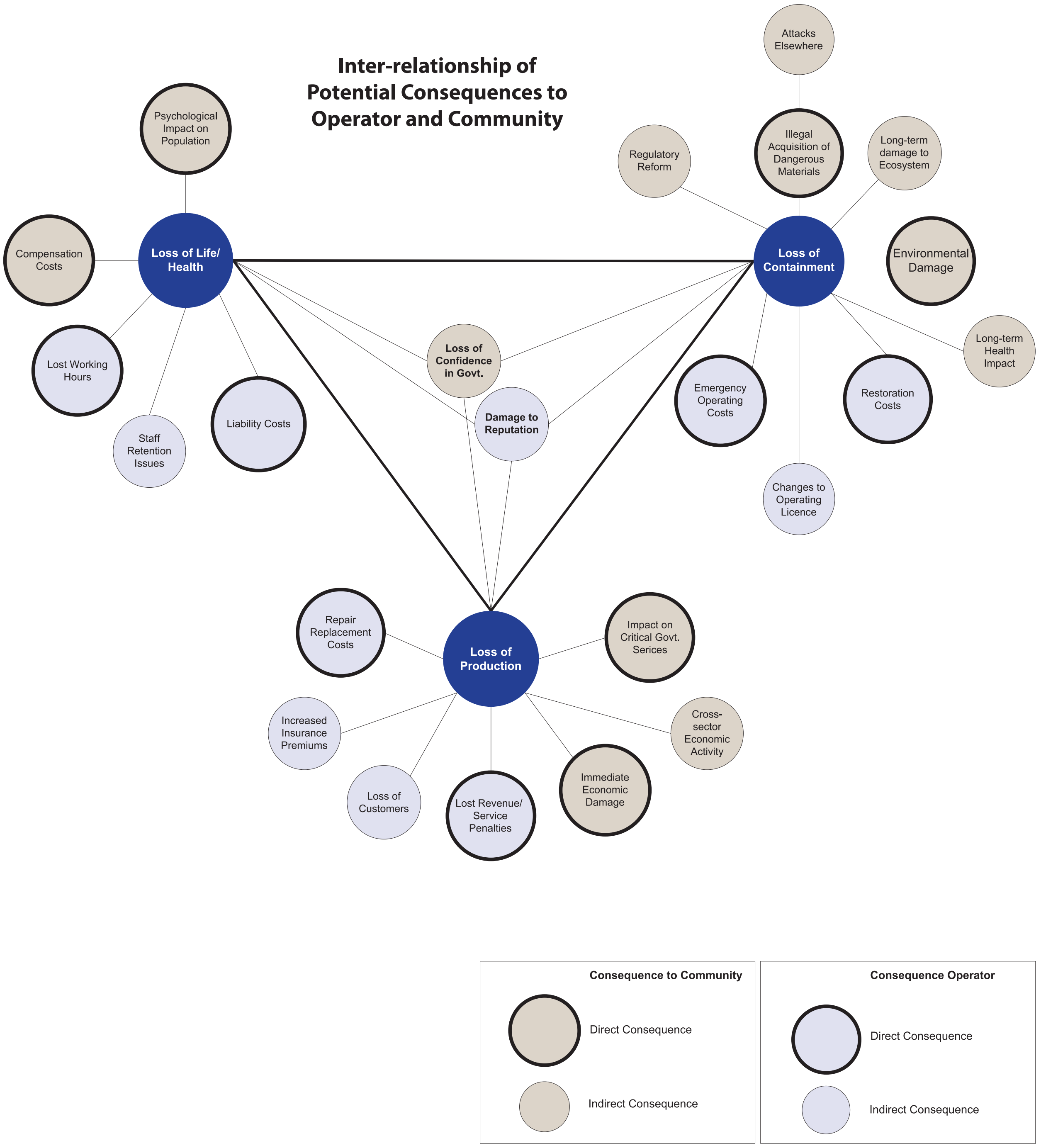
In the context of Critical Infrastructure facilities it is important for the Project Team to take into account not only those immediate consequences to the owner/operator, but also the wider offsite consequences to the socio-economic community that is dependent upon the supply from, and safe operation of, such facilities. In this respect even where the operator does not bear full legal responsibility for external consequences they have a Corporate Social Responsibility to minimise related risks and should therefore take ownership of such risks, albeit if in some cases external funding may be required to implement the full suite of necessary countermeasures.

In addition the owner/operator should also understand that the consequence chain is not linear in nature but tends to work in multiple directions, some of which can be unforeseen. For example the direct consequences of a major production outage may be much greater for the community than for the owner/operator (particularly as the operator will recoup most of their immediate losses through insurance). However, if this results in a fall in customer confidence or negative public perception, this could subsequently damage both corporate reputation and share price. Therefore, it is ultimately in the owner/operator's best interest to manage all risks relating to their infrastructure even where the direct consequences may fall elsewhere.

The interrelationship between various types of consequences is very complex, not least because of the potential 'ripple effect', and therefore difficult to assess accurately. However, in the context of critical energy infrastructure there are a number of primary consequences that are of greatest significance because they tend to create a web of interrelated secondary consequences for both the operator and the community. This is represented in Diagram B3a on the following page:

> *Therefore, it is ultimately in the owner/operator's best interest to manage all risks relating to their infrastructure even where the direct consequences may fall elsewhere.*

Diagram B3a


Inter-relationship of Potential Consequences to Operator and Community
Attacks Elsewhere
Psychological Impact on Population
Regulatory Reform
Illegal Acquisition of Dangerous Materials
Long-term damage to Ecosystem
Compensation Costs
Loss of Life/ Health
Loss of Containment
Environmental Damage
Lost Working Hours
Loss of Confidence in Govt.
Long-term Health Impact
Liability Costs
Emergency Operating Costs
Restoration Costs
Damage to Reputation
Staff Retention Issues
Changes to Operating Licence
Repair Replacement Costs
Loss of Production
Impact on Critical Govt. Serices
Increased Insurance Premiums
Cross-sector Economic Activity
Loss of Customers
Lost Revenue/ Service Penalties
Immediate Economic Damage
Consequence to Community
Direct Consequence
Indirect Consequence
Consequence Operator
Direct Consequence
Indirect Consequence

As illustrated in Diagram B3a all direct and indirect consequences of significance to both the operator and community can be related to three primary consequences of any given Threat Scenario: Loss of Health/Life; Loss of Production; and Loss of Containment. The definition of these three primary consequences in the current context is provided below:

1. Loss of Life/Health
This refers to the immediate loss of life or impact upon health as a consequence of the Threat Scenario materialising.

2. Loss of Production
This refers to the loss of production or other essential output as a consequence of the Threat Scenario materialising. This may be either a complete or partial loss for any given amount of time.

3. Loss of Containment
This refers to the loss of containment around critical Assets therefore allowing uncontrolled exposure or access as a consequence of the Threat Scenario materialising. This not only refers to dangerous chemical, biological, radiological or nuclear material, but also critical data (i.e. classified research, proprietary information) and anything else that could be used to significantly harm the business or the wider community.

Although other consequences exist – for example loss of non-critical Assets, vandalism, fraud etc – these three primary consequences are of greatest significance, particularly for CEI Assets, and can be used to reflect the potential severity of all related secondary consequences, which will be relative to that of the primary consequences.

In this way it is possible to represent the overall consequence of any given incident without the need to assess all possible downstream consequences to both the operator and the community, which requires complex and time-consuming research and statistical modelling techniques not easily accessible to most Project Teams. However, this type of advanced consequence analysis can be very beneficial at a government level and in future it may be that sufficient tools and support are made available to owner/operators to make this type of assessment more feasible. In the meantime, the Project Team should consider secondary consequences, recording those of particular significance to the resilience function (discussed in more detail at a later stage), but focus on the three primary consequences for scoring purposes.

When assessing these consequences the Project Team should consider both the extent of possible damage from each Threat Scenario as well as the criticality of the affected components and the potential downstream effects. It may also be necessary to conduct additional research regarding the severity of any given scenario and the environmental characteristics that may have an influence on consequences such as population density in nearby areas, adjacent hazards, wind directions etc.

The following scoring table B3c can be used to assign a consequence score to each Threat Scenario:

Table B3c: Threat Scenario Consequences

Score	Threat Scenario Consequences				
	Loss of Life/Health		Loss of Production		Loss of Containment
100	• Hundreds of thousands of fatalities, or • Millions of serious injuries	OR	• Complete loss of production for >12 months	OR	• Widespread release of CBRN material causing long-term human health impacts, or • Access to nuclear material by hostile groups
90	• Tens of thousands of fatalities, or • Hundreds of thousands of serious injuries	OR	• Complete loss of production for >6 months, or • >75% loss of production for >12 months	OR	• Widespread release of CBRN material causing short- to medium-term human health impacts, or • Access to very hazardous CBR material by hostile groups
80	• Thousands of fatalities, or • Tens of thousands of serious injuries	OR	• Complete loss of production for >1 month, or • >75% loss of production for >6 months, or • >50% loss of production for >12 months	OR	• Localised release of CBRN material causing long-term health impacts, or • Loss of hazardous material that could be used in a large-scale attack elsewhere, or • Loss of classified material that could undermine the government or be used to support nuclear weapons proliferation
70	• Hundreds of fatalities, or • Thousands of serious injuries	OR	• Complete loss of production for >1 week, or • >75% loss of production for >1 month, or • >50% loss of production for >6 months	OR	• Widespread release of toxic material causing long-term environmental damage, or • Loss of hazardous material that could be used in a small-scale attack elsewhere, or • Loss of classified material that could be used to support non-nuclear weapons proliferation
60	• Tens of fatalities, or • Hundreds of serious injuries	OR	• Complete loss of production for >1 day, or • >75% loss of production for >1 week, or • >50% loss of production for >1 month	OR	• Widespread release of hazardous material causing short- to medium-term environmental damage, or • Loss of data critical to the organisation, or • Loss of classified material that could be used to weaken the economy
50	• At least 1 fatality, or • Tens of serious injuries, or • Hundreds of moderate injuries	OR	• >75% loss of production for >1 day, or • >50% loss of production for >1 week, or • >25% loss of production for >1 month	OR	• Localised release of hazardous material causing long-term environmental damage, or • Loss of data critical to the organisation
40	• At least 1 serious injury, or • Tens of moderate injuries	OR	• >50% loss of production for >1 day, or • >25% loss of production for >1 week	OR	• Localised release of hazardous material causing short-term damage, or • Loss of sensitive commercial data
	Other Internal Consequences				
30	Moderate disruption to ancillary business processes, financial loss or reputational damage – recovery within weeks				
20	Minor disruption to ancillary business processes, financial loss or reputational damage – immediate recovery				
10	No significant consequence – nuisance factor only				

Source: PRISM™

B3.3 Consequence-based Prioritisation

The previous consequence assessment will result in a score being assigned to each Threat Scenario-CP pair as well as an overall score for the scenario as a whole. This is represented in the following table:

Table B3d: Risk Scenario Scoring

Risk Ref	Risk Scenario				Consequence Assessment	
	Threat Source	Scenario Description	Critical Points		Description	Score
			Ref	Name		
A: CRIMINAL THREATS						
A1.1	Terrorist/Religious Extremist/Al-Qaeda	An IED is hand-placed inside the facility and subsequently detonated	**CP0**	**ASSET**		**90**
			CP1	Import Manifold		70
			CP2	Dehydration Tank		40
			CP3	Gas Station		90
			CP4	Sub-station		70
			CP5	Oil Storage Tanks		60
A1.2		A hazardous chemical storage tank is sabotaged	**CP0**	**ASSET**		**80**
			CP6	Chemical Storage Tank A		80
			CP7	Chemical Storage Tank B		70
A2.1	Economic Criminal/ Sophisticated Individual	An employee uses his access to management offices to steal sensitive research material	**CP0**	**ASSET**		**60**
			CP8	Paper Files		50
			CP9	Electronic Data		60
A3.1	Subversive/ Environmental Activist	An activist group gain entry to the site and attempt to halt production	**CP0**	**ASSET**		**40**
			CP10	Control Room		40
			CP11	Production Hall		40
			CP12	Employees		30
B: NON-CRIMINAL THREATS						
B1.1	Natural Hazard/ Flooding	Heavy and prolonged rain causes flooding across the site	**CP0**	**ASSET**		**60**
			CP4	Sub-station		60
			CP13	IT Server Room		50
			CP8	Paper Files		30
B2.1	Accidental Hazard/ Explosion	A spark from a vehicle ignites spilled fuel and subsequently causes an explosion	**CP0**	**ASSET**		**80**
			CP5	Oil Storage Tanks		70
			CP3	Gas Station		80
B3.1	Consequential Hazard/Outage – Essential Services	The transmission system operator experiences a major sub-station failure resulting in a loss of electricity to the site.	**CP0**	**ASSET**		**80**
			CP4	Sub-station		80
			CP2	Dehydration Tank		30

Source: PRISM™

Before moving on to the next stage in the risk assessment process the Project Team may wish to consider prioritising scenario/component pairs based on consequence score and subsequently filtering out those that are of least relevance. This is particularly worthwhile for complex infrastructure whereby a large number of components may have been identified. However, it is also important to bear in mind that for some Threats such as theft the frequency of the event can result in a more significant consequence over time and is therefore worthy of assessment and inclusion in the risk register.

B3.4 Summary

This section of the risk assessment process has provided a framework for consideration of specific consequences in relation to the Threat Scenarios selected previously. The Project Team will have identified which CPs are relevant to each Threat Scenario and then considered the primary consequences likely to result if such incidents occurred. Following on from this, Threat Scenarios can be prioritised by consequence score, and where necessary those with the lowest scores removed from the assessment process.

The Project Team will have identified which CPs are relevant to each Threat Scenario and then considered the primary consequences likely to result if such incidents occurred.

B4 Vulnerability Assessment

Purpose: To provide a framework for assessing security system performance in the key functional areas of Detection, Delay, Response and Resilience. This is then used to determine firstly the extent to which each identified Critical Point is vulnerable to each Risk Scenario, and secondly the extent to which they are vulnerable to the potential worst-case consequences of each Scenario. As well as informing overall risk scores the analysis from this section will also form the basis for design of any necessary countermeasures under Phase C.

B4.0 Introduction

The next stage in the risk assessment process is to determine the Asset's existing level of vulnerability to each defined Risk Scenario and therefore the Likelihood that if these scenarios become a reality, they will result in the consequences previously identified.

The owner/operator may be familiar with a range of Vulnerability Assessment (VA) methods and survey forms that are in widespread use within the industry, many of which are also freely available on the internet. These typically fall into one of two groups – compliance-based assessments and performance-based assessments, the former being much more prevalent. Both types of VA are discussed below:

1. Compliance-based VA methods

These methods assess vulnerability against pre-defined policy, minimum standards or other criteria including individual perceptions as to what constitutes vulnerability. They typically take the form of a series of questions such as "Does the facility have a perimeter security fence?", "Is the fence well maintained?" etc. The advantage of this approach is that it is straightforward for the user to complete and requires limited knowledge or technical expertise. However, the significant disadvantage with compliance-based VAs is that they may not lead to an accurate appreciation of vulnerability to real-life Threats, so the countermeasures introduced as a result of this process do not always target the right areas or result in a reduction of actual risk relevant to specific scenarios.

For example, if a facility is facing determined intrusion attempts by sophisticated adversaries the existence of a perimeter security fence or the level to which that fence is maintained may not, in itself, have little bearing on the Asset's vulnerability to that form of attack. Instead it would be necessary to understand how that fence was likely to perform in the context of adversary capabilities, including the type of tools and climbing aids they are likely to use – even where it was a high security fence it may only delay the attackers by a few minutes at most. Similarly the existence of CCTV at the perimeter in itself does not mean that the adversary would be detected. In order to determine this with any degree of certainty it would be necessary to understand: how well the CCTV system performs under different type of conditions; whether the field of view, lighting and resolution are adequate to detect an intruder within the video scene; how efficient the remote monitoring function is; what the effect of shift changes between security personnel would be, etc.

Although generic vulnerability and resultant countermeasures may offer some degree of protection against low-level opportunistic Threats, they often do very little to mitigate more determined attacks. Even where security systems and technologies have the potential for high-end performance, if they are not designed to protect against specific Threats as part of an integrated security regime they are likely to be ineffective in a real-life scenario.

2 Performance-based VA methods

These methods are less commonplace in most sectors primarily because of a lack of awareness of their existence or method of use. However, they are increasingly used in the context of critical infrastructure protection, where the importance of accurately assessing vulnerability to defined Threats is greater. As the name implies, performance-based VA methods focus on assessing the actual performance of security systems, related procedures and infrastructure, usually in the context of specific Threat Scenarios or methods of attack. For example the fact that a facility had widespread CCTV coverage would have very little bearing on the assessed level of vulnerability to a sabotage attack, if there was no-one able to respond in time to prevent the attack from being successfully carried out.

As is evident from the above discussion the use of a performance-based VA approach has many advantages and is considered an essential tool in delivering protective security in one form or another across all types of energy infrastructure Assets. The potential disadvantage of this approach can be that it demands more effort and knowledge from the Project Team in order to complete. In its most advanced format the process typically takes a team of five or more Subject Matter Experts several weeks to complete. However, for the purpose of the Security Management Plan a simpler form of performance testing can be utilised and carried out by you independently if professional support is not available. The process for doing this is presented in the following sections, whilst further information and templates can be found in the relevant appendices.

B4.1 Key Aspects of Performance and Vulnerability

Before being able to conduct a performance-based VA it is necessary to understand the core aspects of performance in the context of security system effectiveness. In this respect a security regime has three core functions vital for success – Detection, Delay and Response (DDR).[1] For any given security incident it is essential to firstly **Detect** that the incident is occurring, secondly to **Delay** (or completely repel) the adversary long enough for an effective **Response** to intervene.

The Security Management Plan uses these three functions as the basis on which to assess security system performance and therefore determine vulnerability to each Threat Scenario. However, some forms of attack (particularly determined attacks by professional adversaries) can be extremely difficult to prevent and those responsible at a government level for Assets are becoming more and more aware of this. As such there is an increasing emphasis being placed on a fourth key function – that of Resilience. The definition and scope of Resilience is still evolving, but in simple terms it refers to the ability to mitigate the consequences of a hazardous event either by having the capability to resist damage caused by that event or recover quickly from that event. This is clearly a vital function for Assets and as such is included in the performance framework that runs throughout the Security Management Plan.

Although Resilience is sometimes taken to include incident Response capability, within the Security Management Plan it is considered to be a separate function, which starts after the event has occurred (and in respect of criminal Threats when the Detection, Delay and Response functions have failed to prevent the attack). It is used in conjunction with DDR functions to determine security system performance, albeit that DDR performance dictates the vulnerability to Threat actors or sources whereas performance in the area of Resilience dictates vulnerability to the potential worst-case consequences of the event that follows. The combined performance framework is summarised in the following diagram:

Diagram B4a: Detection, Delay, Response and Resilience

Detection

- The ability to detect that an incident is occurring, assess the type of incident and the necessary response.

Delay

- The ability to delay attackers or protect against the cause of the incident long enough for a successful response to be initiated.

Response

- The ability to respond effectively to the incident, preventing loss or damage of the Asset by successfully intervening before it is compromised.

Resilience

- The ability to mitigate the potential consequences of an incident either by resisting damage or quickly recovering from the consequences.

[1] Extensive research of the Detection, Delay and Response functions has been conducted by Garcia (2006, 2008) and is an excellent source of further guidance.

When conducting the performance-based VA as outlined in the steps to follow, the primary focus will be to assess performance in terms of the DDRR functions discussed above and their capability against each Threat Scenario.

This framework can also be used to assess vulnerability to non-criminal Threat Scenarios – early detection of the hazard is equally important as is the level of delay (or physical protection), the capability to respond and the resilience to resist damage or recover quickly. However, there is typically more emphasis on the Delay function and the extent to which the Asset has been designed to withstand the physical impact of the event in question (which for natural hazards can often be determined by identifying the building codes or engineering standards that the Asset was constructed to). Therefore, it is more appropriate at the scoring stage to assign an overall score for DDR performance rather than individual scores.

B4.2 Performance-based Vulnerability Assessment

The performance-based vulnerability assessment takes the form of a site survey and related testing, which will be used to gauge existing DDRR performance levels and identify factors which may affect the vulnerability of the Asset to each Threat Scenario. There are a number of successive and complementary methods for evaluating performance, each of which is explained below:

Observation

The information previously gathered during the Asset Characterisation process should be revisited by you at this stage and used to support the assessment process. The survey team should start by taking a tour of the facility and record the following information on a plot plan of the site:

- Location of Critical Points designated in B1
- Level of occupancy in each area or building
- Positioning of main security and safety systems
- Potential adversary access/egress routes
- Location and number of any security personnel with a response function
- Natural barriers or countermeasures
- Location of muster points, evacuation routes and emergency access/egress points

The next step will be to observe and evaluate each component of the existing security regime, including physical, electronic and procedural measures and related infrastructure. To do this it is recommended that your Project Team develops a list of all such measures and groups them by their performance function – either DDRR. An example of this is shown in the table below, whilst a full survey template is provided in the relevant appendices.

Table B4a: DDRR Sub-System Assessment

Function	Sub-system Assessments
Detection	Exterior Alarm Sensors/PIDS Interior Alarm Sensors/IDS CCTV/Alarm Assessment Alarm Communication and Display/SMS Access/Entry Control (detection elements – scanning, authorisation measures, door alarms etc) IT Security (network and information monitoring, electronic detection measures)
Delay	Perimeter Fencing and natural barriers Access/Entry Control (delay elements – gates, vehicle barriers, doors, locking devices etc) Structural measures (walls, windows, roofs etc) Safes Security hatches Blast measures SCADA and IT security (firewalls and other prevention measures)
Response	Security personnel Response procedures External Response Force (police, military)
Resilience	Crisis Management and Business Continuity measures Resilience/redundancy of infrastructure including process safety features Fail-over locations Supply-chain issues

Source: PRISM™

These items should then be evaluated in terms of the level of DDRR performance that they currently provide, completing the appropriate sections of the survey template. The survey team should spend as much time as possible observing the security systems and procedures in use, in order to identify both the level of capability as well as potential limitations. Interviews with security owner/operators and a review of incident logs will also assist in identifying performance issues.

Scenario-based Testing

In order to gain a greater appreciation of DDRR performance the Project Team should consider running a number of scenario tests and assessing the DDRR capability of the existing security regime. Example tests could include:

- Intrusion through the perimeter – single attacker/multiple attackers, different locations
- Intrusion into key areas or buildings
- Parking of suspicious vehicle adjacent to the site
- Use of false credentials or bluffing to gain pedestrian/vehicle access into the site
- Tailgating into restricted areas/Access to restricted areas by unauthorised employee
- Attempted removal of equipment or sensitive commercial information
- Evacuation – being sure to test alternative routes and secondary evacuation points rather than just routine drills

It is very important to inform security personnel and senior management that this testing is taking place, carrying out appropriate risk assessments beforehand. However, in order to ensure the response capability is accurately tested, specific timings of the test should not be given. In the event of any large-scale testing that may be noticeable from outside of the facility, the police and emergency services should also be informed.

System Performance Testing

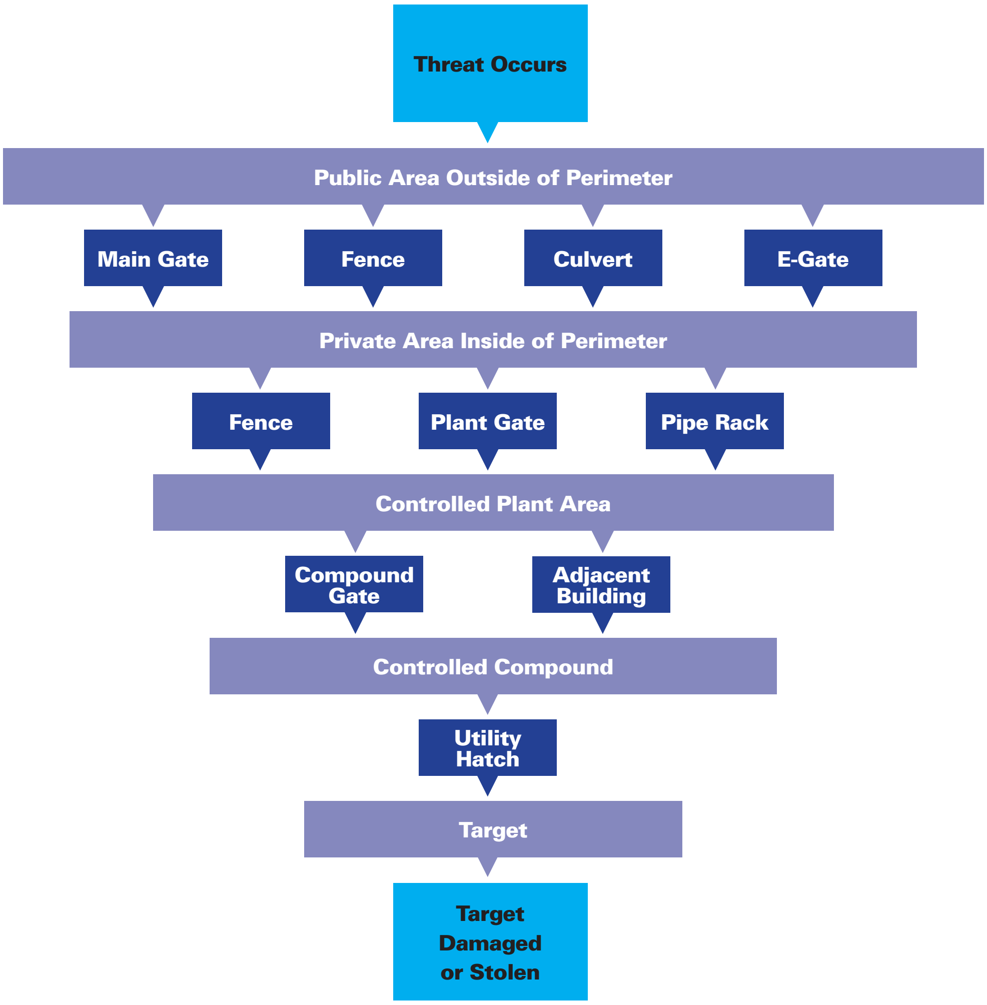
Technical system performance testing provides a quantifiable and objective method to establish DDRR performance. One recommended approach is the use of Rotakin™ testing to international standard BS EN 50132, Part 7 as this combines technical and scenario-based testing to provide a realistic assessment of CCTV performance and Probability of Detection. This type of testing will most likely require external support, however, can be very worthwhile for sites that have a range of electronic security systems already deployed and require independent verification of the level of performance that they provide.

B4.3 Vulnerability to Risk Scenarios

Once the general DDRR performance has been established through the survey and testing procedures the next stage is to assess the vulnerability to each Risk Scenario in terms of whether or not each associated Critical Point is likely to be compromised and if it were compromised the level of resilience to the potential consequences.

In order to do this a scenario analysis should be conducted to determine the different ways in which each Threat could occur and the specific level of DDRR performance that could be expected in relation to these events. The Threat Scenario can be 'played out' on paper by creating an Adversary Sequence Diagram (ASD), which shows each potential route that the adversary might take and helps to ensure that all potential vulnerabilities are considered. The ASD can either be drawn on top of the marked-up site plan that was created earlier or done separately as in the diagram on the following page.

Diagram B4b: Adversary Sequence Diagram



Source: PRISM™

When conducting this process you should review the information previously gathered in relation to the characteristics of the relevant Threat Source, and particularly their possible attack methods, access to tools/weapons and level of professionalism. It is also important to remember that Threats may emanate from within the organisation ('Insider Threats') and therefore access to Critical Points may be much easier for the adversary to achieve!

For each ASD completed the Project Team should consider the following performance and vulnerability issues, assigning scores to each of these:

Table B4b: Performance and Vulnerability Factors

Function	Vulnerability Factors	Vulnerability Score
Detection	At each point in the sequence what is the probability that the adversary will be detected?	
Delay	What delay will the adversary face at each point in the sequence? What is the total task completion time for the adversary, assuming that the easiest route is taken? What level of capability will be required to overcome the delay measures/can they protect the Asset indefinitely from this Threat?	
Response	If the Threat is detected does the facility have the capability to intervene or is an external police response required? How long will the response take? Will the response successfully intervene before the target is damaged or removed from site (taking into account adversary task time)?	
Resilience	In the event that the Threat Scenario was successful would the existing resilience measures have any affect in reducing the consequences identified previously?	

Source: PRISM™

The following criteria can be used for assigning vulnerability scores in relation to Detection, Delay and Response Criteria:

Table B4c: Vulnerability Criteria

VA Score	Vulnerability Criteria	Vulnerability Level
5	There is no capability to prevent this scenario from occurring and causing worst-case consequences	Very High
4	There is very limited capability to prevent this scenario from occurring and causing worst-case consequences	High
3	There is moderate capability to prevent this scenario from occurring and causing worst-case consequences	Moderate
2	There is significant capability to prevent this scenario from occurring and causing worst-case consequences	Low
1	There is a high degree of capability to prevent this scenario from occurring and causing worst-case consequences	Very Low

Source: PRISM™

Resilience scores are assigned using a different set of criteria as shown in table B4d below. **It is important when assigning Resilience scores to be realistic about the likely effect in reducing the overall consequences – just because a measure exists (for example secondary containment measures or business continuity procedures) it does not mean that it will mitigate every type of Risk Scenario.**

Table B4d: Resilience Criteria

VA Score	Vulnerability Criteria	Vulnerability Level
0.2	Existing resilience to this Threat Scenario is very high and expected to mitigate virtually all of the consequences previously identified	Very High
0.4	Existing resilience to this Threat Scenario is significant and expected to mitigate most of the consequences previously identified	High
0.6	There is a moderate amount of existing resilience to this Threat Scenario which will reduce some of the consequences previously identified	Moderate
0.8	Existing resilience to this Threat Scenario is limited and will only partially mitigate all of the consequences previously identified	Low
1	Existing resilience to this Threat Scenario is very limited or non-existent – it will not have any significant effect in mitigating the consequences previously identified	Very Low

Source: PRISM™

Once individual scores in the DDRR areas have been assigned for each Threat Scenario/component pair, this information can be entered into a scoring matrix and the overall Vulnerability assessed. This is shown in the following example – the full template is provided in the relevant appendices and can be used for this purpose (you will note that Resilience does not form part of the numerical VA score but is entered separately. This is because it will be used in the final risk assessment scoring as a consequence reduction factor).

Table B4e: Example Vulnerability Assessment Table

Risk Ref	Risk Scenario				Vulnerability to Threat/ Consequences				
	Threat Source	Scenario Description	Critical Points						
			Ref	Name	Detection Score	Delay Score	Response Score	VA Score	Resilience Score
CRIMINAL THREATS									
A1.1	Terrorist/Religious Extremist/Al-Qaeda	An IED is hand-placed inside the facility and subsequently detonated	**CP0**	**ASSET**	4	5	4	13	1
			CP1	Import Manifold	4	4	4	12	1
			CP2	Dehydration Tank	4	3	4	11	0.8
			CP3	Gas Station	3	5	4	12	1
			CP4	Sub-station	3	5	4	12	1
			CP5	Oil Storage Tanks	4	3	4	11	0.8
A1.2		A hazardous chemical storage tank is sabotaged	**CP0**	**ASSET**	5	4	4	13	0.8
			CP6	Chemical Storage Tank A	5	4	4	13	0.8
			CP7	Chemical Storage Tank B	5	4	4	13	0.8
A2.1	Economic Criminal/ Sophisticated Individual	An employee uses his access to management offices to steal sensitive research material	**CP0**	**ASSET**	5	5	4	14	1
			CP8	Paper Files	5	5	4	14	1
			CP9	Electronic Data	4	5	3	12	1
A3.1	Subversive/ Environmental Activist	An activist group gain entry to the site and attempt to halt production	**CP0**	**ASSET**	4	3	2	9	1
			CP10	Control Room	3	2	2	7	1
			CP11	Production Hall	4	2	2	8	1
			CP12	Employees	3	3	2	8	1
NON-CRIMINAL THREATS									
B1.1	Natural Hazard/ Flooding	Heavy and prolonged rain causes flooding across the site	**CP0**	**ASSET**				7	0.8
			CP4	Sub-station				7	0.8
			CP13	IT Server Room				7	0.8
			CP8	Paper Files				4	0.8
B2.1	Accidental Hazard/ Explosion	A spark from a vehicle ignites spilled fuel and subsequently causes an explosion	**CP0**	**ASSET**				12	1
			CP5	Oil Storage Tanks				10	1
			CP3	Gas Station				12	1
B3.1	Consequential Hazard/ Outage – Essential Services	The transmission system operator experiences a major sub-station failure resulting in a loss of electricity to the site	**CP0**	**ASSET**				14	0.6
			CP4	Sub-station				14	0.6
			CP2	Dehydration Tank				7	0.6

Source: PRISM™

B4.4 Summary

The recommended Vulnerability Assessment framework will allow the Project Team to identify performance in the key areas of Detection, Delay, Response and Resilience and subsequently gauge the level of Critical Point and Asset vulnerability to each Risk Scenario. The information compiled in this section will also be revisited during Phase C of the Security Management Plan when specific countermeasures aimed to reduce vulnerability or enhance Resilience are considered.

B5 Threat Likelihood Assessment

Purpose: To provide a framework for assessing the Likelihood that each criminal Risk Scenario will occur, taking into account Threat source capability to conduct each type of attack, as well as Target Attractiveness of both the Asset as a whole and individual Critical Points. It therefore mirrors the risk:reward decision-making process of the adversary in order to provide a more realistic and specific Threat Score.

B5.0 Introduction

Now that both Consequence and Vulnerability in relation to each Risk Scenario has been assessed, the next stage in the process is to consider the Likelihood that these Threats will materialise and affect the Asset or Critical Point in question. In this sense it is important to be mindful of the fact that the existence of a particular Threat does not mean that any given Asset or component will be targeted even if the level of Threat is very high. Threat actors usually have multiple targets to choose from and therefore only a small number may be affected.

The purpose of this Section is to assess how likely it is that the Asset and each critical component will be subject to attack. This is determined by combining the general Threat level established in Section B2 with an assessment of: first, whether each Threat source has the capability to conduct the specific attack in question; and second, how attractive each target is likely to be as a means of fulfilling their objectives. In this sense the assessment of 'Target Attractiveness' reflects the decision-making process that will precede all but the most opportunistic of attacks and is therefore a vital consideration when assessing the Likelihood of criminal Threats.

For non-criminal Threats where there is no deliberate intent this step is not necessary. Instead Likelihood is established by referring to Threat history as discussed previously. Threat scores can be taken directly from Section B2 and entered into the Likelihood Assessment table.

There are three parts to the Threat Likelihood Assessment process as explained in the sections that follow.

B5.1 Specific Threat Capability

Following completion of the Vulnerability Assessment it is now possible to more accurately assess the adversary's specific capability to carry out each Threat Scenario successfully. If the Threat Scenario is particularly difficult to carry out due to the required means, the Likelihood will decrease proportionately. For example many religious extremist groups, including Al-Qaeda, have demonstrated significant intent to conduct Chemical, Biological, Radiological and Nuclear [CBRN] attacks. However, this type of attack remains uncommon simply because of the difficulty in acquiring and weaponising the precursor materials. Similarly attacks on nuclear facilities would also be highly desirable and fit within the intent of such groups, however the actual Likelihood is significantly lower than, for example, a public transport system because of the level of capability required to defeat the sophisticated security measures surrounding such Assets.

This step therefore allows the Threat level score established in Section B2, which reflects the Threat source's general existence and intent to carry out attacks, to be further refined specifically in relation to each scenario and component pair by asking 'Are they actually capable of conducting this attack against this Asset or Critical Point?'

In order to correctly gauge the answer to this question it is necessary to review the Adversary Sequence Diagram (ASD) prepared for each Threat Scenario in the previous stage and consider what capability the adversary must have to conduct this attack successfully.

In this respect key considerations are:

1. How familiar do they need to be with the target in terms of its components, processes, and operations – can this be done through hostile reconnaissance or do they need support from an insider?
2. What skills and experience are required to conduct this type of attack – will they need to undergo specific training or recruit specialists?
3. What physical resources do they need – specialist tools, explosives, weapons, vehicles etc?
4. What level of determination will be required – will they need people willing to take their own lives or resist counter-attacks by police, military, trained guards or employees?

This information can then be cross-referenced with the known Threat history and characteristics of each Threat source in order to assess their level of capability in relation to each scenario and assign a capability rating using the following table:

Table B5a: Capability Rating for Threat Sources

Score	Criteria	Category
5	The Threat source is currently judged to have full capability to carry out this scenario.	Very High
4	The Threat source has capability in the majority of areas and could meet any additional requirements in the short term.	High
3	The Threat source has capability in some areas but will need to acquire significant additional capability which will take time to do.	Moderate
2	The Threat is not currently judged to have the necessary capability but might be able to acquire it in the medium-to-long term.	Low
1	The Threat is not currently judged to have the necessary capability or be able to acquire it in the foreseeable future.	Very Low

Source: PRISM™

As with other aspects of the Threat Assessment process it is important to update capability assessments on a regular basis.

B5.2 Target Attractiveness

When assessing Target Attractiveness it is necessary to consider all of the information previously gathered about the role, criticality, potential consequences and vulnerability of the Asset and its various Critical Points, and consider this from the perspective of each Threat source that may or may not choose to target the Asset.

Some of the questions you might ask about the Threat source are:

- Are they likely to recognise the potential value of the target?
- Do these characteristics offer the potential to fulfil the adversary's core objectives?
- Does the balance between risk and reward lie in their favour?
- Is this the best option for them or can their objectives be achieved more cost-effectively elsewhere?

Breaking these considerations down it is apparent that there are a number of key contributors to the attractiveness of any given target, which are:

1. Target Visibility
2. Risk of Failure
3. Level of Reward
4. Alternative Options

These factors are used in the guidebook to assess Target Attractiveness, which is a key consideration in relation to overall Likelihood. Given that the risk assessment process analyses risks at the component level as well as the Asset level each of these questions should be considered in both contexts.

> *If the Threat Scenario is particularly difficult to carry out due to the required means, the Likelihood will decrease proportionately.*

This is highlighted in the following table which presents key issues for you to consider in relation to each of the above Target Attractiveness factors:

Table B5b: Assessment of Target Attractiveness

Factor	Asset Level Considerations	Component Level Considerations
1. Target Visibility	• Is the facility as a whole an obvious target for this type of attack or is it relatively anonymous to outsiders? • Is the location widely known/highly frequented or is it in a private, well concealed area? • Does it stand out as a unique or critical Asset or does it look similar to other Assets within the sector? • Is it co-located with other infrastructures that may hide it or make the whole area seem of greater potential worth? • How much knowledge of the energy network would be needed to identify this as a critical Asset – is this knowledge publicly available?	• If a Threat source decided to attack this Asset how likely are they to target this component in particular? • Does the appearance of the component suggest that it is critical or is it hidden from view or anonymous? • Would it be identified as being critical through a cursory examination of the facility or would only technical employees recognise it as such? • Is it adjacent to other components that may increase or decrease the Likelihood of it being targeted?
2. Risk of Failure	• How difficult would it be to carry out this type of attack on the facility? • Does the facility as a whole appear to be a hard or soft target? • What visual deterrents exist around the Asset? • Is it surrounded by natural barriers, located in a high security area or adjacent to a police/military base? • Would the consequences of failure be of particular concern to the adversary?	• How difficult would it be to carry out this type of attack on the component? • Is the component highly vulnerable to this type of attack or are there weaknesses which can be easily exploited by this attack method? • What level of precision would be required to ensure success? • Is the component difficult to access, is it protected by armed guards? • Would there be adequate time available to destroy or remove the target?
3. Level of Reward	• Is the facility as a whole symbolic and would the attack be spectacular in nature? • Would targeting this facility as opposed to others offer additional benefits such as the potential for damage to adjacent facilities or symbolic sites, a high number of offsite casualties or damage to a specific type of environment? • Are there secondary targets within the facility such as VIPs or specialists that would increase the level of reward? • Does this type of facility fit with the core target profile of the Threat source or is it of secondary concern to them? • Is the level of reward offered by this facility proportionate to the risk of failure?	• What would the benefits of targeting this component over others be? • To what extent would an attack on this component fulfil the adversary's core objectives? • Does it have the potential to completely halt production, cause a specific hazard to human life or disproportionate consequences? • Is the component unique in any way, found in greater quantities at this facility or difficult to find elsewhere? • Is the level of reward offered by this component proportionate to the difficulty in targeting it and overall risk of failure?
4. Alternative Options	• What alternative facilities could the Threat source target to achieve their objectives? • Are they easier or more difficult to target? • Are they closer or further away from the adversary's support base or normal area of operations? • Overall do they offer a better or worse risk-reward ratio?	• What alternative components could the Threat source target to achieve their objectives? • Are they easier or more difficult to target? • How would the consequences and vulnerability differ? • Overall do they offer a better or worse risk:reward ratio?

Source: PRISM™

For each Threat Scenario and component pair the above target attractiveness factors can be scored using the following criteria.

Note that unlike other scoring in the guidebook, in this instance the Risk of Failure criteria is in the reverse order – a low score is given for a high risk of failure

Table B5c: Target Attractiveness Evaluation Criteria

Score	1. Target Visibility Criteria	Category
5	The Asset or component is both visible and symbolic or unique	Very High
4	The Asset or component is generally quite visible and identifiable	High
3	The Asset or component is visible to those who have a knowledge of the infrastructure or area	Moderate
2	The Asset or component is fairly anonymous and would be difficult to identify	Low
1	The Asset or component is completely anonymous	Very Low
Score	**2. Risk of Failure Criteria**	**Category**
5	There is virtually no risk of failure – the Asset/component is extremely vulnerable to this scenario	Very High
4	There is a low risk of failure with this scenario against this Asset/component	High
3	There is a moderate risk of failure with this scenario against this Asset/component	Moderate
2	There is a high risk of failure with this scenario against this Asset/component	Low
1	There is a very high risk of failure with this scenario against this Asset/component	Very Low
Score	**3. Level of Reward Criteria**	**Category**
5	The use of this scenario against the Asset/component provides an exceptional level of reward meeting all adversary objectives	Very High
4	The use of this scenario against the Asset/component provides a high level of reward and meets adversary objectives	High
3	The use of this scenario against the asset/component provides a reasonable level of reward meeting most but not all adversary objectives	Moderate
2	The use of this scenario against the Asset/component provides a low level of reward meeting few adversary objectives	Low
1	The use of this scenario against the Asset/component provides very little reward for the adversary and is unlikely to be considered worthwhile	Very Low
Score	**4. Alternative Options Criteria**	**Category**
5	The adversary does not have any other options to fulfil their objectives to the same extent – this provides a unique risk:reward ratio	Very High
4	The adversary has few alternative options to fulfil their objectives, but these would not provide as good risk:reward ratio	High
3	The adversary has some alternative options to fulfil their objectives but these would provide a similar risk:reward ratio	Moderate
2	The adversary has some alternative options to fulfil their objectives, a few of which provide a better risk:reward ratio	Low
1	The adversary has many alternative options to fulfil their objectives, some of which provide a much better risk:reward ratio	Very Low

Scores should be entered in the Target Attractiveness template provided in the relevant appendices to this report. The overall Target Attractiveness score will then be calculated as shown in the following example:

Table B5d: Target Attractiveness Example

Risk Ref	Risk Scenario				Target Attractiveness				
	Category & Name	Scenario Description	Critical Points		1. Viability	2. Risk of Failure	3. Level of Reward	4. Alternative Options	TA Score
			Ref	Name					
CRIMINAL THREATS									
A1.1	Terrorist/Religious Extremist/Al-Qaeda	An IED is hand-placed inside the facility and subsequently detonated	**CP0**	**ASSET**	2	3	4	3	3
			CP1	Import Manifold	2	3	4	3	3
			CP2	Dehydration Tank	2	2	2	2	2
			CP3	Gas Station	3	4	2	3	3
			CP4	Sub-station	2	4	3	3	3
			CP5	Oil Storage Tanks	1	1	3	3	2
A1.2		A hazardous chemical storage tank is sabotaged	**CP0**	**ASSET**	4	3	5	4	4
			CP6	Chemical Storage Tank A	4	4	3	5	4
			CP7	Chemical Storage Tank B	5	3	4	4	4
A2.1	Economic Criminal/ Sophisticated Individual	An employee uses his access to management offices to steal sensitive research material	**CP0**	**ASSET**	4	5	3	4	4
			CP8	Paper Files	5	4	3	4	4
			CP9	Electronic Data	2	5	2	3	3
A3.1	Subversive/ Environmental Activist	An activist group gain entry to the site and attempt to halt production	**CP0**	**ASSET**	5	5	5	5	5
			CP10	Control Room	5	5	5	5	5
			CP11	Production Hall	4	4	4	4	4
			CP12	Employees	2	4	3	3	3

Source: PRISM™

B5.3 Threat Likelihood Scoring and Prioritisation

Once assessments for each Threat Scenario have been made in the areas of Capability and Target Attractiveness this information can be entered into a scoring matrix and used in conjunction with the generic Threat scores from section B2 to calculate the overall Likelihood assessed. This is shown in the following example.

Table B5e: Threat Likelihood Scoring Example

Risk Ref	Risk Scenario				Threat Likelihood Assessment			
	Threat Source	Scenario Description	Critical Points		Intent (general Threat Score)	Capability	Target Attractive-ness	TLA Score
			Ref	Name				
CRIMINAL THREATS								
A1.1	Terrorist/Religious Extremist/Al-Qaeda	An IED is hand-placed inside the facility and subsequently detonated	**CP0**	**ASSET**	4	4	3	11
			CP1	Import Manifold	4	4	3	11
			CP2	Dehydration Tank	4	4	2	10
			CP3	Gas Station	4	4	3	11
			CP4	Sub-station	4	4	3	11
			CP5	Oil Storage Tanks	4	4	2	10
A1.2		A hazardous chemical storage tank is sabotaged	**CP0**	**ASSET**	4	3	4	11
			CP6	Chemical Storage Tank A	4	3	4	11
			CP7	Chemical Storage Tank B	4	3	4	11
A2.1	Economic Criminal/ Sophisticated Individual	An employee uses his access to management offices to steal sensitive research material	**CP0**	**ASSET**	5	5	4	14
			CP8	Paper Files	5	5	4	14
			CP9	Electronic Data	5	5	3	13
A3.1	Subversive/ Environmental Activist	An activist group gain entry to the site and attempt to halt production	**CP0**	**ASSET**	3	4	5	12
			CP10	Control Room	3	4	5	12
			CP11	Production Hall	3	4	4	11
			CP12	Employees	3	4	3	10

Source: PRISM™

As with previous assessment phases Risk Scenarios can now be prioritised on the basis of Likelihood score, and where a large number of variants still exist the Project Team may decide to filter out those that attract the lowest scores for example five or less. However, it is important to be sure that this does not completely remove certain types of Threat, but rather just specific Scenario/Critical Point pairs that are shown to be very unlikely in relation to others of a similar nature.

B5.4 Summary

The Threat Likelihood Assessment process is used to translate criminal Threat levels that are generic in nature into specific scores that relate to the Likelihood of each Risk Scenario materialising and impacting upon the Asset or Critical Point in question. This is done by assessing the Threat source's specific capability in relation to the Risk Scenario, along with the level of Target Attractiveness they are likely to perceive. On completion of this process the Project Team will have conducted all of the individual assessments necessary to calculate overall risk scores, which will be done in the following section.

B6 Risk Assessment

Purpose: To provide a method to calculate the overall level of risk in relation to each Risk Scenario, based upon the Threat, Vulnerability and Consequence Assessments conducted in previous sections. Subsequently to introduce the concept of a Risk Register, which will be used as a central repository for all Risk Assessment scores and metrics, and to provide guidance on how the results of the Risk Assessment phase can be analysed to inform subsequent reporting and Risk Mitigation activity.

B6.0 Introduction

The final step in the risk assessment process is to calculate the overall level of risk posed by each Threat Scenario and record them in a 'Risk Register'. The results can then be analysed and used by the organisation to determine whether or not specific mitigation measures are necessary to reduce risks to a level acceptable to the organisation, as well as to responsible government agencies.

There are three steps in this process as follows:

Step 1: Calculate Risks
Step 2: Create the Risk Register
Step 3: Analyse Risk Results

Each of these steps is detailed in the sections that follow.

B6.1 Risk Calculation

Risk consists of three components – Threat, Vulnerability and Consequence, a basic formula for calculating risk that is straightforward and well-established:

Threat x Vulnerability x Consequence = Risk

'Threat x Vulnerability' can also be expressed as 'Probability' or 'Likelihood' – in the current context the Probability/Likelihood of a successful attack (criminal risks) or the Probability/Likelihood of a 'Loss Event' (all risks).

The risk methodology used in the guidebook uses this formula as the basis for calculating risk scores for each Threat Scenario in order to provide a numerical basis for comparison of risks and consideration of countermeasures. However, it is done in a number of distinct steps using the scores calculated previously for each component of risk.

Step 1: Residual Consequence

First the Resilience score calculated during the Vulnerability Assessment ('Vulnerability to Consequences'), which ranges from 0-1, is applied to the 'potential worst-case consequences' score in order to determine a 'Residual Consequence' score, using the following formula:

Consequence x Resilience = Residual Consequence

In many cases the level of existing resilience may be inadequate to reduce consequences and therefore the resilience score will be 1 and the consequence score unchanged. However, where resilience measures are in place and would significantly mitigate potential worst-case consequences the resilience score will be between 0.2 and 0.8 and will reduce the consequence score accordingly, ensuring that the level of existing resilience is accounted for within the overall numerical risk score.

Step 2: Probability of Loss Event

The next step is to determine the probability of a Loss Event ranging from 0 (will not happen) to 1 (will happen). This is calculated using the scores from the Threat Likelihood Assessment and Vulnerability Assessment ('Vulnerability to Threat'), via the following representative formula:

Threat Likelihood x Vulnerability = Probability of Loss Event

(The actual formula used in the Risk Register for this purpose is '(Threat Likelihood + Vulnerability) / 30 = Probability of Loss Event' – 30 being the maximum combined score. This gives an overall probability value of between 0 and 1).

Step 3: Risk Score

The third and final step is to calculate the overall risk score. This is simply done using the following formula:

Probability of Loss Event x Residual Consequence = Risk

The risk score will be in the range of 0-100 with 0 indicating no risk and 100 indicating maximum risk. Further analysis of these scores will be discussed in Step 3.

B6.2 The Risk Register

The Risk Register is intended to be a ‘dynamic document’ that summarises all risk-related information and provides the organisation with a tool for ongoing risk management activity, monitoring and reporting. As such it should be updated on a regular basis in line with changes in the risk context. For example if a range of risk mitigation measures were introduced this should reduce the level of vulnerability and/or consequence and therefore the risk register should be updated to reflect this. Similarly if the Threat level associated with a particular scenario or group of scenarios were to change this should be accounted for in the Risk Register.

A Risk Register template has been developed for you to use for this purpose and is included in the Security Management Plan Template. Building on previous tables it summarises the outputs from steps B1-B5 and provides a means of calculating and recording risk scores for each scenario using the methodology outlined above.

An example of a completed Risk Register is shown in the diagram on the following page:

For example if a range of risk mitigation measures were introduced this should reduce the level of vulnerability and/or consequence and therefore the risk register should be updated to reflect this.

Table B6a: Risk Register Example

Risk Ref	Risk Scenario				Consequence Assessment		Vulnerability Assessment				Residual Consequence Score	Threat Likelihood Assessment		Probability of Loss Event	Risk Assessment	
	Threat Source	Scenario Description	Critical Points				Vulnerability to Threat		Vulnerability to Consequences							
			Ref	Name	Description	Conse-quence Score	Description	VA Score	Description	Resilience Score		Description	TLA Score		Description	Score
A: CRIMINAL THREATS																
A1.1	Terrorist/Religious Extremist/Al-Qaeda	An IED is hand-placed inside the facility and subsequently detonated	CP0	ASSET		90		13		1	90		11	0.8		72
			CP1	Import Manifold		70		12		0.8	56		11	0.77		43
			CP2	Dehydration Tank		40		11		1	40		10	0.70		28
			CP3	Gas Station		90		12		1	90		11	0.77		69
			CP4	Sub-station		70		12		0.8	56		11	0.77		43
			CP5	Oil Storage Tanks		60		11		0.8	48		10	0.70		34
A1.2		A hazardous chemical storage tank is sabotaged	CP0	ASSET		80		13		0.8	64		11	0.80		51
			CP6	Chemical Storage Tank A		80		13		0.8	64		11	0.80		51
			CP7	Chemical Storage Tank B		70		13		1	70		11	0.80		56
A2.1	Economic Criminal/ Sophisticated Individual	An employee uses his access to management offices to steal sensitive research material	CP0	ASSET		60		14		1	60		14	0.93		56
			CP8	Paper Files		50		14		1	50		14	0.93		47
			CP9	Electronic Data		60		12		1	60		13	0.83		50
A3.1	Subversive/ Environmental Activist	An activist group gain entry to the site and attempt to halt production	CP0	ASSET		40		9		1	40		12	0.70		28
			CP10	Control Room		40		7		1	40		12	0.63		25
			CP11	Production Hall		40		8		1	40		11	0.63		25
			CP12	Employees		30		8		1	30		10	0.60		18
B: NON-CRIMINAL THREATS																
B1.1	Natural Hazard/ Flooding	Heavy and prolonged rain causes flooding across the site	CP0	ASSET		60		7		0.8	48		6	0.43		21
			CP4	Sub-station		60		7		0.8	48		6	0.43		21
			CP13	IT Server Room		50		7		0.8	40		6	0.43		17
			CP8	Paper Files		30		4		0.8	24		6	0.33		8
B2.1	Accidental Hazard/ Explosion	A spark from a vehicle ignites spilled fuel and subsequently causes an explosion	CP0	ASSET		80		12		1	80		8	0.67		53
			CP5	Oil Storage Tanks		70		10		1	70		8	0.60		42
			CP3	Gas Station		80		12		1	80		8	0.67		53
B3.1	Consequential Hazard/Outage – Essential Services	The transmission system operator experiences a major sub-station failure resulting in a loss of electricity to the site.	CP0	ASSET		80		14		0.6	48		6	0.67		32
			CP4	Sub-station		80		14		0.6	48		6	0.67		32
			CP2	Dehydration Tank		30		7		0.6	18		6	0.43		8

*Source: PRISM*TM

As shown above the Risk Register records each Risk Scenario along with associated Consequence, Vulnerability and Threat Likelihood scores, subsequently calculating Residual Consequence, Probability of Loss Event and overall Risk scores. The Risk Scenarios form the basis for subsequent analysis and consist of the Threat source, Threat Scenario and critical component at risk. It is important that these Risk Scenarios are reviewed on a regular basis, particularly where new information on Threat source characteristics comes to light or where the physical infrastructure of the Asset undergoes significant modification or expansion.

The Risk Register template also includes space for a description of each risk factor and this should be completed to help those outside of the immediate Project Team understand each of the associated scores. Conditional formatting is utilised for the overall risk score, providing a visual indicator of risk category, which is applied using the following conversion table:

Risk Register Score	Description	Tier
>60	Very High	5
46-60	High	4
31-45	Moderate	3
16-30	Low	2
0-15	Very Low	1

The Risk Register is divided into two sections according to the type of risk – criminal or non-criminal. In some cases separate and perhaps more detailed analysis for certain non-criminal risks will have been completed (for example as part of a Process Hazard Analysis necessary for compliance with regulatory standards).

In this instance it is recommended that details of each identified hazard along with respective consequence and probability scores (with a suitable numerical conversion if in a different format) are copied across to the Security Management Plan Risk Register to provide a single ‘All Risks’ repository, subsequently allowing easy comparison, analysis and management reporting.

B6.3 Risk Analysis

Once the Risk Register has been compiled the next step is to analyse and interpret the results in order to provide the basis for reporting to risk owners (typically board-level management) and consideration of which risks fall outside of the organisation’s risk appetite and will therefore require specific risk mitigation actions. There are four elements that can be used to support this analysis – Risk Score, Consequence Score, Vulnerability Score and Threat Likelihood Score – each of which are discussed below in order of significance:

1. Analysis of Risk Scores

The overall risk score will provide the primary means of analysis given that it incorporates all individual components of risk. Risks can be ranked by overall risk score and prioritised on this basis. In addition operators should also compare each result to their risk appetite and strategic objectives as established in Phase A. Where this has been clearly defined a maximum tolerance level can be set above which specific countermeasures will be considered in order to reduce risks to an acceptable level. For the remainder of risks falling within the organisation’s risk appetite ongoing monitoring may be sufficient.

2. Analysis of Consequence Scores

For Critical European Infrastructure Assets in particular it is also worth ranking risks separately by consequence score. In certain cases the consequences of a particular risk may be of such severity that exceptional countermeasures could be justified even where the risk is relatively low. This is particularly so when the risk would have drastic consequences for the population, country or region, and not just the Asset or local area.

This type of consequence-driven risk management is a fairly common approach to Critical European Infrastructure protection at a government policy level, but can also be used as an additional analysis tool by owner/operators, with high consequence risks and possible countermeasures being considered on a case-by-case basis. Where countermeasures are relatively inexpensive in comparison to the consequence the owner/operator may decide that they are justifiable.

3. Analysis of Vulnerability Scores

Some owner/operators, typically those with lower risk appetites, may wish to implement measures that are designed to keep vulnerability at a certain level regardless of the external Threat environment or the potential consequences. In this case the results from the risk register can be ranked on the basis of vulnerability score and considered in relation to a maximum acceptable threshold. This can be particularly useful where there is significant uncertainty regarding the Threat environment or where it is desirable to have a common security standard across all Assets within a multinational company.

4. Analysis of Probability Scores

Finally, your Project Team can consider ranking risks by probability of a loss event. This can be useful to highlight risks that may in isolation have limited consequences but could pose a problem either as a result of the cumulative consequences of multiple losses over a period of time, or the cumulative impact on the perception of the facility – namely that it is insecure – which may lead to more serious forms of targeting.

Following on from the above analysis the Project Team will be in a position to present their findings to the Senior Management team and subsequently agree on a formal set of 'Protection Objectives' – the final step of Phase B discussed in the next section.

B6.4 Summary

The risk assessment process outlined above brings all of the individual components of risk together and calculates overall risk scores to represent the level of risk faced by the owner/operator in relation to each scenario. The Risk Register is a vital document within the overall risk management process and will facilitate activity in the areas of analysis, reporting, mitigation and ongoing monitoring.

The Risk Register is a vital document within the overall risk management process and will facilitate activity in the areas of analysis, reporting, mitigation and ongoing monitoring.

B7 Protection Objectives

Purpose: To provide a framework for the creation of ‘Protection Objectives’ as an output from the Risk Register, along with target risk reduction levels. These will be used as the basis for subsequent Risk Mitigation considerations as outlined in Phase C of the Security Management Plan.

B7.0 Introduction

Following on from the creation of the Risk Register and the analysis of risks facing the organisation, there are likely to be a number of risks that exceed the organisation's risk appetite and must therefore be reduced through various countermeasures. The purpose of this Section is to capture the strategic aims of the organisation in relation to risk mitigation through the creation of a series of specific 'Protection Objectives'.

B7.1 Creating Protection Objectives

Protection Objectives will be used as the basis for the design of risk mitigation measures as outlined in Phase C and as such are an important component of the risk management process. Although they are high-level objectives they also need to be specific to each risk in order to ensure that they lead to appropriate and focused countermeasures. Fortunately the scenario-based risk assessment process that has been undertaken in previous sections makes this very easy to achieve.

In order to create the Protection Objectives, you need to consider each of the Risk Scenarios that currently sit above the owner/operator's risk tolerance level, either due to overall risk score, consequence, vulnerability or probability score (as discussed in the previous section) and create a short statement outlining the objective of any risk mitigation measures as well as the level of risk reduction that is required, preferably in terms of an acceptable numerical risk score. At this stage it is not necessary for you to include specific countermeasures, just strategic objectives. For example a suitable Protection Objective may be 'Protect Chemical Tank A against sabotage attack' rather than 'Install Security Fencing around Chemical Tank A'.

In the majority of cases countermeasures will alter the vulnerability scores; however, occasionally they can also affect both Threat and consequence. For example, the Threat Likelihood could be reduced by making the Asset a less attractive target, whilst the consequences could be reduced through risk transfer measures such as insurance (although this is only likely to reduce the consequences to the owner/operator and not the wider community!).

In order to record this information a Protection Objectives section can be added to the Risk Register with three additional columns in it:

1. PO Reference
2. PO Description
3. Target Risk Level

This is included in the Security Management Plan Template, whilst an example of a completed set of Protection Objectives against each Risk Scenario is also shown in the following table.

Table B7a: Risk Register Protection Objectives

Risk ref	Risk Scenario				Risk Score	Protection Objectives		
	Threat Source	Scenario Description	Critical Points					
			Ref	Name		PO Ref	PO Description	Target Risk Level
A: CRIMINAL THREATS								
A1.1	Terrorist/Religious Extremist/Al-Qaeda	An IED is hand-placed inside the facility and subsequently detonated	**CP0**	**ASSET**	72	PO-A1.1-0	Provide comprehensive protection against an IED attack anywhere within the facility	<31 (low)
			CP1	Import Manifold	43	PO-A1.1-1	Protect the Import Manifold against IED attacks – moderate reduction in vulnerability required	<31 (low)
			CP2	Dehydration Tank	28	PO-A1.1-2	Existing protection is sufficient – consider general measures only	<31 (low) – achieved
			CP3	Gas Station	69	PO-A1.1-3	Protect the Gas Station against IED attacks – significant reduction in vulnerability required	<31 (low)
			CP4	Sub-station	43	PO-A1.1-4	Protect the Sub-station against IED attacks – moderate reduction in vulnerability required	<31 (low)
			CP5	Oil Storage Tanks	34	PO-A1.1-5	Protect the Oil Storage Tanks against IED attacks – moderate reduction in vulnerability required	<31 (low)
A1.2		A hazardous chemical storage tank is sabotaged	**CP0**	**ASSET**	51	PO-A1.2-0	Protect against sabotage of chemical storage facilities, which could cause off-site release and severe consequences	<16 (very low)
			CP6	Chemical Storage Tank A	51	PO-A1.2-1	Protect Chemical Storage Tank A from sabotage – significant reduction in vulnerability and increase in resilience required	<16 (very low)
			CP7	Chemical Storage Tank B	56	PO-A1.2-2	Protect Chemical Storage Tank B from sabotage – significant reduction in vulnerability and increase in resilience required	<16 (very low)
A2.1	Economic Criminal/ Sophisticated Individual	An employee uses his access to management offices to steal sensitive research material	**CP0**	**ASSET**	56	PO-A2.1-0	Protect all restricted and proprietary information from unauthorised access or removal	<31 (low
			CP8	Paper Files	47	PO-A2.1-1	Protect paper files from unauthorised access or removal – moderate reduction in vulnerability required	<31 (low)
			CP9	Electronic Data	50	PO-A2.1-2	Protect electronic data from unauthorised access or removal – moderate reduction in vulnerability required	<31 (low)
A3.1	Subversive/ Environmental Activist	An activist group gain entry to the site and attempt to halt production	**CP0**	**ASSET**	28	PO-A3.1-0	Existing risk level is deemed acceptable – general measures only	<31 (low) – achieved
			CP10	Control Room	25	PO-A3.1-1	Existing risk level is deemed acceptable – general measures only	<31 (low) – achieved
			CP11	Production Hall	25	PO-A3.1-2	Existing risk level is deemed acceptable – general measures only	<31 (low) – achieved
			CP12	Employees	18	PO-A3.1-3	Existing risk level is deemed acceptable – general measures only	<31 (low) – achieved
B: NON-CRIMINAL THREATS								
B1.1	Natural Hazard/ Flooding	Heavy and prolonged rain causes flooding across the site	**CP0**	**ASSET**	21	PO-B1.1-0	Existing risk level is deemed acceptable – general resilience measures only	<16 (low) – achieved
			CP4	Sub-station	21	PO-B1.1-1	Existing risk level is deemed acceptable – general resilience measures only	<16 (low) – achieved
			CP13	IT Server Room	17	PO-B1.1-2	Existing risk level is deemed acceptable – general resilience measures only	<16 (low) – achieved
			CP8	Paper Files	8	PO-B1.1-3	Existing risk level is deemed acceptable – general resilience measures only	<16 (low) – achieved
B2.1	Accidental Hazard/ Explosion	A spark from a vehicle ignites spilled fuel and subsequently causes an explosion	**CP0**	**ASSET**	53	PO-B2.1-0	Protect the Asset against ignition within hazardous areas and accidental explosion	<16 (very low)
			CP5	Oil Storage Tanks	42	PO-B2.1-1	Protect Oil Storage Tanks against ignition sources and accidental explosion – moderate reduction in vulnerability required	<16 (very low)
			CP3	Gas Station	53	PO-B2.1-2	Protect Gas Station against ignition sources and accidental explosion – moderate reduction in vulnerability required	<16 (very low)
B3.1	Consequential Hazard/ Outage – Essential Services	The transmission system operator experiences a major sub-station failure resulting in a loss of electricity to the site.	**CP0**	**ASSET**	32	PO-B3.1-0	Protect the Asset against loss of electricity supply	<16 (low)
			CP4	Sub-station	32	PO-B3.1-1	Protect Sub-station against loss of electricity supply	<16 (low)
			CP2	Dehydration Tank	8	PO-B3.1-2	Existing risk level is deemed acceptable – general resilience measures only	<16 (low) – achieved

Source: PRISM^{TM}

When the Protection Objectives have been completed they should be reviewed by the Project Team to ensure that they are all feasible and justifiable in light of associated risk levels, and that any other priorities have not been overlooked. Following on from this they should be formally agreed with the owners of each risk and signed off for actioning under the next Phase of the Security Management Plan.

B7.2 Summary

The Project Team will have now completed the Risk Assessment process in its entirety and will be ready to move on to Phase C of the Security Management Plan – Risk Mitigation. The above Protection Objectives, as well as the analysis conducted in the other areas of the Risk Assessment will provide the platform for the identification of Risk-based Performance Measures that will protect the facility from specific Risk Scenarios and ultimately prove to be the most cost-effective use of organisational resources.

B Annex 1: Additional Open-Source Information

The following list is not exhaustive and is provided as an example of the information available on the internet. It is important to remember that the information that can be derived from such sites provide the basis for independent evaluation before drawing Asset-specific conclusions. The quality of the analysis undertaken is critical to the quality of the recommendations that inform decisions later on in the risk assessment and design phases.

- UK Cabinet Office 'UK Resilience' – http://www.cabinetoffice.gov.uk/ukresilience.aspx
- UK Serious Organised Crime Agency – http://www.soca.gov.uk/threats
- Interpol – http://www.interpol.int/default.asp
- US Department for Homeland Security 'The Insider Threat To Critical Infrastructures' – http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf
- US Computer Emergency Readiness Team (part of US DHS) – Critical Infrastructure News http://www.us-cert.gov/control_systems/
- US DHS Homeland Infrastructure Threat and Risk Analysis Centre (HITRAC) – http://www.dhs.gov/xabout/structure/gc_1257526699957.shtm#1
- publicintelligence.net – US DHS Potential Terrorist Attack Methods – http://publicintelligence.net/dhsfbi-ufouo-potential-terrorist-attack-methods/
- Chapter 1 – FEMA 426 Reference Manual To Mitigate Potential Terrorist Attacks on Buildings – http://www.fema.gov/pdf/plan/prevent/rms/426/fema426.pdf
- Chapter 3 – The Design and Evaluation of Physical Protection Systems (second Edition), Mary Lynn Garcia.
- UK Govt – Centre for the Protection of National Infrastructure CPNI – http://www.cpni.gov.uk/theThreat.aspx
- German Ministry of Interior – Protecting Critical Infrastructure – http://www.bmi.bund.de/cln_183/SharedDocs/Downloads/DE/Broschueren/EN/Leitfaden_Schutz_kritischer_Infrastrukturen_en1.html?nn=441658
- Europol EU Terrorism Situation and Trend Report 2010 – http://www.consilium.europa.eu/uedocs/cmsUpload/TE-SAT%202010.pdf
- US Department of State – Country Reports on Terrorism – http://www.state.gov/s/ct/rls/crt/index.htm
- Chapters 1.4 and 3.3 US Department for Homeland Security – National Infrastructure Protection Plan – http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
- Guardian Newspaper Terrorism portal – http://www.guardian.co.uk/world/terrorism
- UK National Counter Terrorism Security Office – http://www.nactso.gov.uk/Threats.aspx
- US Interagency Threat Assessment and Co-ordination Group (ITACG) – http://www.nctc.gov/docs/itacg_guide_for_first_responders.pdf
- US National Counter Terrorism Centre (NCTC) – Worldwide Incidents Tracking System (WITS) – http://www.nctc.gov/wits/witsnextgen.html
- RAND Database of Worldwide Terrorism Incidents (RDWTI) – http://www.rand.org/nsrd/projects/terrorism-incidents/

Phase C

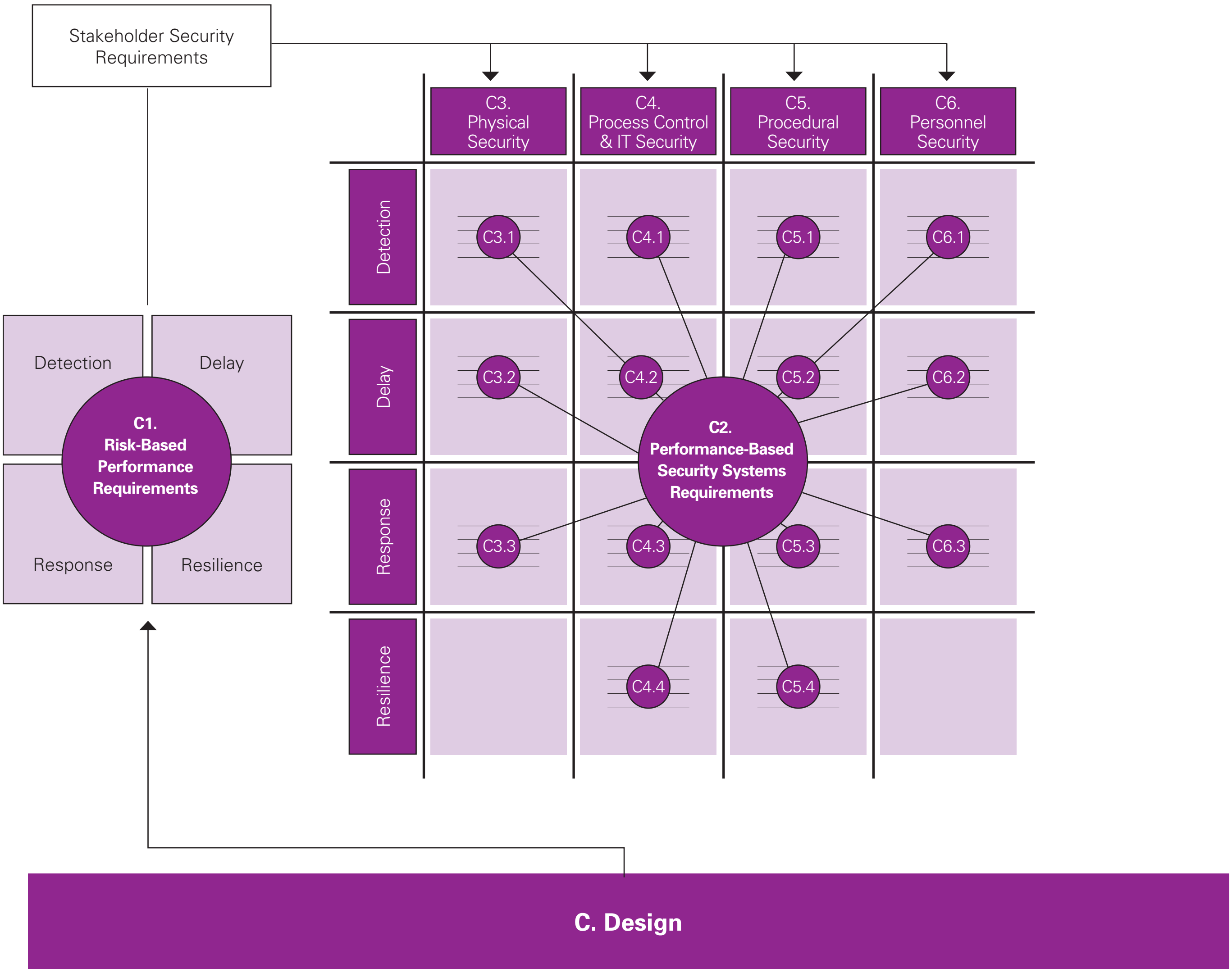
Design

Executive Summary – Design

The Design Phase will provide you with a structured methodology for designing and specifying the performance of an Integrated Security System (ISS) in line with the Protection Objectives established in Phase B and the specific risk profile of each energy facility.

There are a total of six complementary sections in Phase C, which when brought together provide the basis for the design of ISS performance and subsequently engagement with external specialists to translate this into a detailed engineering design (for the technological aspects at least). In this respect it is important to understand that infrastructure security design is a very complex area and despite the broad overview of the subject matter provided in the following sections, it is likely that the level of technical expertise necessary to design your ISS will only be available from external specialists in this field. It is important to ensure that where necessary external support is made available to the Project Team since the potential for cost overrun associated with a poorly designed project far outweigh the small initial cost of independent design consultancy.

The six sections in Phase C are shown in the following diagram and explained further on the next page.



1. Risk-based Performance Requirements
Ensures that the security systems are designed to mitigate risks and deliver an acceptable level of performance. The core functions of a security regime are Detection; Delay; Response and Resilience (DDRR) – these are used as the high-level design framework that links Risk to Performance.

2. Performance-based Security Systems Requirements
Introduces the Level 2 Design framework, which provides a method for identifying the sub-systems of the ISS and specifying the levels of performance from each component necessary to achieve the Risk-based Performance Requirements.

3. Physical Security
Details the range of Physical Security technologies that can provide capability in the areas of Detection, Delay and Response, along with Key Performance Criteria and example applications.

4. Process Control and IT Security
Provides guidance on applying the DDRR framework to the design of Process Control and IT Security measures, in particular those required to safeguard the critical Plant Process Systems from external interference. This section also includes suggestions for IT Disaster Resilience measures to add resilience to the facility and help to avoid a major service interruption.

5. Procedural Security
This section assists in the development of a mechanism to ensure that the owner/operator can effectively react to a security-related incident and recover back to a normal operating state as quickly as possible.

6. Personnel Security
Explains the requirements for personnel security management and outlines proposals for employee screening procedures. This mitigates the possibility of hiring personnel whose aims are to disrupt company operations.

By adopting the above methodology you will be able to follow a sequential process that allows you to design and specify the most important aspects of a robust risk mitigation solution – those that relate to its performance. Subsequently this will form the basis for engagement with external providers in a controlled manner, providing reassurance to Stakeholders that business risks will be mitigated in a cost-effective manner.

By adopting the above methodology you will be able to follow a sequential process that allows you to design and specify the most important aspects of a robust risk mitigation solution – those that relate to its performance.

C1 Risk-based Performance Requirements

Purpose: To introduce the concept of Risk-based Performance Requirements and provide a framework for you to identify the level of performance required in the areas of Detection, Delay, Response & Resilience, to meet all of the Protection Objectives established in Phase B.

C1.0 Introduction

The results of the Assessment Phase of the Security Management Plan will have been recorded in a Risk Register, along with an agreed set of Protection Objectives, which will have been signed off by the key Stakeholders. These Protection Objectives will now form the basis for the design of an Integrated Security System (ISS) that can mitigate associated risks to a level within the Risk Appetite of the Organisation. In order to ensure that these systems actually fulfil the protection objectives it will be necessary for you to ensure that a logical design process is followed.

This section will provide you with an introduction to the principles upon which the recommended design process is based and then to provide you further with an overview of that process, which will be split into the following two levels:

Level 1: Risk-based Performance Requirements

Level 2: Performance-based Security System Requirements

The remainder of this section will focus on the Level 1 design process, whilst the level 2 design process will be explored in the following section C2.

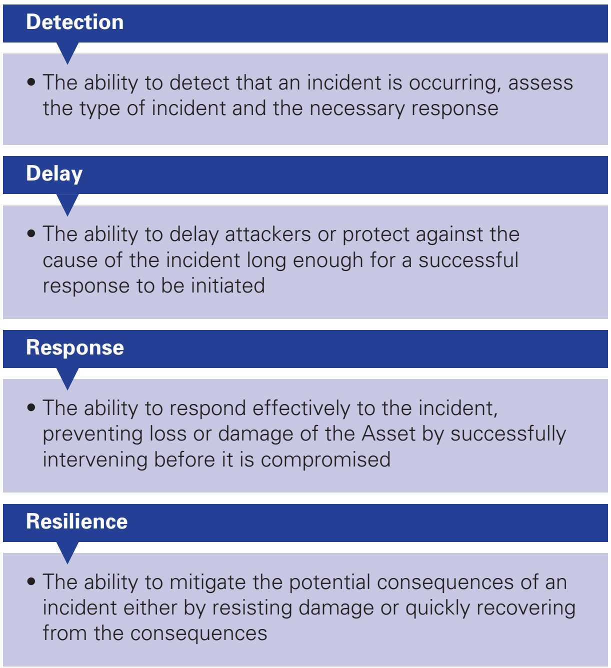
An Integrated Security System is formed by a combination of people, procedures and technology, successfully integrated within a single framework capable of providing the required level of protection against incidents that would otherwise cause damage to the facility and the Assets within it.

> “Contrary to common belief security is about much more than the latest CCTV cameras or IP technology. The key lies in a clear strategy which combines an appreciation of security risks allied with an understanding of how to mitigate those risks effectively through performance-based countermeasures that deliver quantifiable results. In the context of new-build infrastructure projects sustainable and cost-effective countermeasures can only be achieved by embedding security strategy and design principles within the project from concept stage onwards.”
>
> Extract from the Article ‘Body Armour Vs Band-aid: The Impact of Security Strategy on Infrastructure Investment’ by Ben Clay and Stephen Gregory published in Financier Worldwide in March 2010

C1.1 Principles of Risk-based Performance Requirements (Level 1 Design)

In order to be truly effective, Security Systems must be designed to provide the type of performance necessary to protect against the specific risks faced by the facility.
The idea of the Design process presented here is not for you to carry out the detailed engineering design of security systems, but rather to provide you with an understanding of how, in broad terms, you can accurately identify and specify the levels of security system performance necessary to mitigate the specific risks that you are facing and therefore fulfil your established Protection Objectives. This will allow you, without having the technical systems design capability, to specify performance criteria (rather than products) and subsequently engage effectively with external experts, whether design consultants or installers, to ensure that your requirements are met. Security providers can then, at a later date, be held accountable for achieving your requirements, providing that they are clearly articulated in the form of a 'Performance Specification' as discussed further in Phase D – Implementation & Review.

At this stage it is worth revisiting the core functions of any security regime, which were presented earlier in Phase B, since these will dictate the level of associated performance and can therefore be used as a framework for identifying your own Risk-based Performance Requirements. These are shown in the following diagram:



Detection

- The ability to detect that an incident is occurring, assess the type of incident and the necessary response

Delay

- The ability to delay attackers or protect against the cause of the incident long enough for a successful response to be initiated

Response

- The ability to respond effectively to the incident, preventing loss or damage of the Asset by successfully intervening before it is compromised

Resilience

- The ability to mitigate the potential consequences of an incident either by resisting damage or quickly recovering from the consequences

When considering the DDRR functions shown above, it is important to understand the following key points:

Key Points

1. Detection must precede Delay (otherwise intruders would have an indefinite period of time to overcome delay measures).
2. Detection should occur as early as possible in order to maximise available Delay time.
3. Assessment of the incident is required before a response force can intervene and therefore should occur as soon as possible after the time of initial Detection.
4. Balanced Detection and Delay measures are required – there should be no weak points.
5. Depending on the threat type 'protection in depth' may be required, such that security is not reliant upon a single system or component.

In order to be truly effective Security Systems must be designed to provide the type of performance necessary to protect against the specific risks faced by the facility.

The level of performance required within each of the DDRR functional areas will be dictated by the specific risks facing the facility and the required level of risk mitigation, which is expressed in terms of Protection Objectives. For example if a high-risk was posed by sabotage and the persons that posed the potential threat were skilled and determined it may be necessary to:

Detection

- Establish a high probability of detecting this type of attack (for example multiple layers of detection and access control)

Delay

- Create a robust physical delay for x minutes around critical Assets (for example windows, doors and hatches that could resist attack by a variety of manual and battery-operated tools)

Response

- Create an effective response, for example agreeement with local police to attend alarm activations within x minutes/provide an armed response etc

Resilience

- Ensure that the business held spares for all critical components in order to limit outage times if they were compromised and therefore aid resilience

The Level 1 Design Process that you should now conduct as part of your Security Management Plan will translate each of the established Risk Scenarios and associated Protection Objectives (for example ‘protect substation 1 from sabotage’) into Performance Requirements for each of the DDRR functions.

As demonstrated by the above example it will be necessary for you to know the likely capability of the threat source associated with each Risk Scenario so that you can identify the level of DDRR performance necessary to mitigate their actions. Therefore, you should refer back to the analysis of threat source characteristics and attack methods gathered previously, along with related Adversary Sequence Diagrams produced as part of the Vulnerability Assessment.

When identifying these ***Risk-based Performance Requirements*** keep in mind that at this stage the aim is not to select specific security systems or components (this will be addressed in subsequent stages), but instead to decide upon the overall level of performance required in each DDRR area in order to achieve each Protection Objective.

It is suggested that the ***Risk-based Performance Requirements*** are recorded along with the Protection Objectives in a table similar to that shown on the following page:

Table C1a: Risk-based Performance Requirement: Protection Objectives

Protection Objectives				Risk-based Performance Requirement			
PO Ref	PO Description	Existing Risk Score	Target Risk Level	Detection	Delay	Response	Resilience
PO-A1.1-0	**Provide comprehensive protection against an IED attack anywhere within the facility**	**72**	**<31 (low)**				
PO-A1.1-1	Protect the Import Manifold against IED attacks – moderate reduction in vulnerability required	**43**	<31 (low)				
PO-A1.1-2	Existing protection is sufficient – consider general measures only	**28**	<31 (low) – achieved				
PO-A1.1-3	Protect the Gas Station against IED attacks – significant reduction in vulnerability required	**69**	<31 (low)				
PO-A1.1-4	Protect the Sub-station against IED attacks – moderate reduction in vulnerability required	**43**	<31 (low)				
PO-A1.1-5	Protect the Oil Storage Tanks against IED attacks – moderate reduction in vulnerability required	**34**	<31 (low)				
PO-A1.2-0	**Protect against sabotage of chemical storage facilities, which could cause offsite release and severe consequences**	**51**	**<16 (very low)**				
PO-A1.2-1	Protect Chemical Storage Tank A from sabotage – significant reduction in vulnerability and increase in resilience required	**51**	<16 (very low)				
PO-A1.2-2	Protect Chemical Storage Tank B from sabotage – significant reduction in vulnerability and increase in resilience required	**56**	<16 (very low)				
PO-A2.1-0	**Protect all restricted and proprietary information from unauthorised access or removal**	**56**	<31 (low)				
PO-A2.1-1	Protect paper files from unauthorised access or removal – moderate reduction in vulnerability required	**47**	<31 (low)				
PO-A2.1-2	Protect electronic data from unauthorised access or removal – moderate reduction in vulnerability required	**50**	<31 (low)				
PO-A3.1-0	**Existing risk level is deemed acceptable – general measures only**	**28**	**<31 (low) – achieved**				
PO-A3.1-1	Existing risk level is deemed acceptable – general measures only	**25**	<31 (low) – achieved				
PO-A3.1-2	Existing risk level is deemed acceptable – general measures only	**25**	<31 (low) – achieved				
PO-A3.1-3	Existing risk level is deemed acceptable – general measures only	**18**	<31 (low) – achieved				

Source: PRISM™

OVERALL REQUIREMENTS				

When deciding upon your Risk-based Performance Requirements it is important to remember that the objective is to fulfil the agreed Protection Objectives and reduce associated risks to an acceptable level – it is not always possible or desirable to implement the highest level of possible protection, particularly where this is not justified by the level of risk, since this will result in unnecessary expenditure.

It is likely that various levels of performance will emerge under each function in accordance with the nature and severity of each risk. For example, one risk may require an Asset to benefit from a 5-minute delay, whilst another may require the same Asset to have a 10-minute delay. In this case the highest level requirement should be taken forward into the design process. However, it is also important to capture the different types of performance requirement that emerge from different risk scenarios. For example whilst two Protection Objectives may require the same Delay Time, this could be against very different attack methods (for example entry via manual attack versus entry by explosive charge).

C1.2 Summary

Once you have completed this section of the Security Management Plan you will have identified a range of Performance Requirements for the ISS based upon the specific risks to the facility and the agreed Protection Objectives. These Risk-based Performance Requirements will provide the foundation for all subsequent risk mitigation activity, helping to ensure that it is focused and cost-effective, thereby delivering the required level of protection to the facility and the Organisation. The next stage will be to identify the levels of performance necessary from individual Security System components to meet these requirements – this will be addressed in Sections C2-C6.

When deciding upon your Risk-based Performance Requirements it is important to remember that the objective is to fulfil the agreed Protection Objectives and reduce associated risks to an acceptable level

C2 Performance-based Security Systems Requirements

Purpose: To provide you with an overview of the second stage of the design process, which is to identify your requirements for security systems, components and associated performance criteria, based upon the required level of Performance established in the Level 1 Design process.

C2.0 Introduction

In the previous section an examination was made of the key security functions of Detection, Delay, Response and Resilience (DDRR), which were subsequently used as a framework to identify your Risk-based Performance Requirements in these areas. The Level 2 Design Process builds on this foundation by identifying your **Performance-based Security Systems Requirements** – i.e. the systems and sub-components that can be used to achieve the required level of Risk-based Performance established previously.

The following section will provide you with an overview of the Level 2 Design Process before individual components of an ISS are examined in Sections C3 to C6, providing important information on how these systems can be used to provide the required level of performance and risk mitigation.

C2.1 Principles of Performance-based Security Systems (Level 2 Design)

Function	Sub-system
Detection	Exterior Intruder Detection Systems Interior Intruder Detection Systems Access/Entry Control (detection elements – scanning, authorisation measures, door alarms) Video Surveillance Alarm Assessment Alarm Communication Alarm Control & Display Systems IT Network Monitoring Personnel Security – Recruitment & Vetting
Delay	Perimeter Security Fencing, Vehicle Barriers, Pedestrian Barriers Building structural delay measures Doors, windows and locking devices Safes Security Hatches Blast Barriers IT Security (firewalls and other prevention measures)
Response	Security Personnel External Response Force (police, military) Security Technology – Video Investigation & Evidence Incident Response Procedures
Resilience	Crisis Management & Business Continuity Procedures Resilience/Redundancy of Infrastructure Fail-over locations Supply-chain resilience

These sub-systems can be viewed as a menu of complementary options for creating the level of performance required in each of the DDRR functional areas. For example if a Level 1 Design Process identified a Risk-based Performance Requirement of a 10-minute Delay time around a particular Asset, this could be achieved as follows:

Delay Sub-system 1: Perimeter Fence	**= 1 minute**
Delay Sub-system 2: 200 metre stand-off	**= 1 minute**
Delay Sub-system 3: Security Door	**= 3 minutes**
Delay Sub-system 4: Safe	**= 5 minutes**
Total Delay	**= 10 minutes**

This example demonstrates that it is not only necessary to consider a variety of security measures but also to understand the level of performance that will be achieved by these measures. Many security systems fail to deliver because components only provide a general capability (to detect or to delay), and do not deliver the required level of performance to mitigate specific risks faced by the facility, including the attack methods that could be adopted by associated threat sources.

The Level 2 Design Process addresses this issue by providing a framework which you can use to identify the security systems, sub-components and associated performance levels which can be utilised to meet your specific Risk-based Performance Requirements in each of the DDRR areas. For each component of the ISS, a range of individual Performance Requirements and example applications are presented, along with a general discussion of related technologies, procedures or personnel. This will allow you to develop a clear understanding of your Security Systems requirements without any specialist design expertise. Subsequently, you will be able to use these requirements as the basis for effective engagement with external specialists, setting clear and focused performance criteria,which the detailed design and implementation of these systems must fulfil in order to be deemed successful.

C2.3 Relationship of Security Systems to DDRR Functions

As demonstrated in the table on the previous page the security components necessary to achieve the required level of performance across all of the DDRR functions are not limited simply to physical measures. Effective security requires an integrated approach which encompasses capability in the following main areas:

1. Physical Security
2. Process Control and IT Security
3. Procedural Security
4. Personnel Security

For example, whilst the Detection function relies heavily on Physical Security technology, it will not be effective without the correct Procedural Security capability, which will allow the appropriate Response to any given incident be initiated. These relationships are shown in the process diagram at the beginning of this section, in the form of a 'spider diagram', that matches the above components of an ISS to their various applications in delivering DDRR capability.

It is therefore important that you address your requirement for a holistic approach to 'security systems' design by implementing capability in all four system areas and ensuring that this capability matches the DDRR requirements established previously. This will provide a true 'Integrated Security' capability rather than a collection disparate technologies and components.

C2.4 Summary

Now that the principles of Performance-based Security Systems have been explained we can now move on to introduce you to different ISS components, and provide more detailed information that will assist you in specifying respective levels of performance that you require to fulfil your Protection Objectives.

However, it is important to realise that information provided in the following sections – C3 to C6 – is not exhaustive. It will provide an overview of the subject area and help guide you in the right direction, but given the complexity of Infrastructure Security Design it is likely that you will require further advice. For this reason it is important that in the early stages of your planning you seek independent expertise to support you in identifying the most cost-effective risk mitigation solutions.

C3 Physical Security

Purpose: To provide you with an overview of the main Physical Security systems and technologies that can be utilised to provide capability in the areas of Detection, Delay and Response, and thereby help fulfil your Protection Objective established in Phase B. This includes guidance on Key Performance Requirements for each Physical Security sub-system, which can later be used as the basis to formalise your requirements and engage effectively with external providers.

C3.0 Introduction

Physical Security will be the first area of the Integrated Security System (ISS) to be examined within the Security Management Plan, and can play a significant role in meeting your Protection Objectives established in Phase B. For the purpose of the Security Management Plan, Physical Security refers to 'the use of physical measures to protect Assets from damage, unauthorised access, removal or compromise'. This includes both physical barriers such as fences, doors and locking devices, as well as electronic security equipment such as CCTV, Intruder Detection Systems and Automatic Access Control Systems, and also Guard Force personnel in respect of their physical actions.

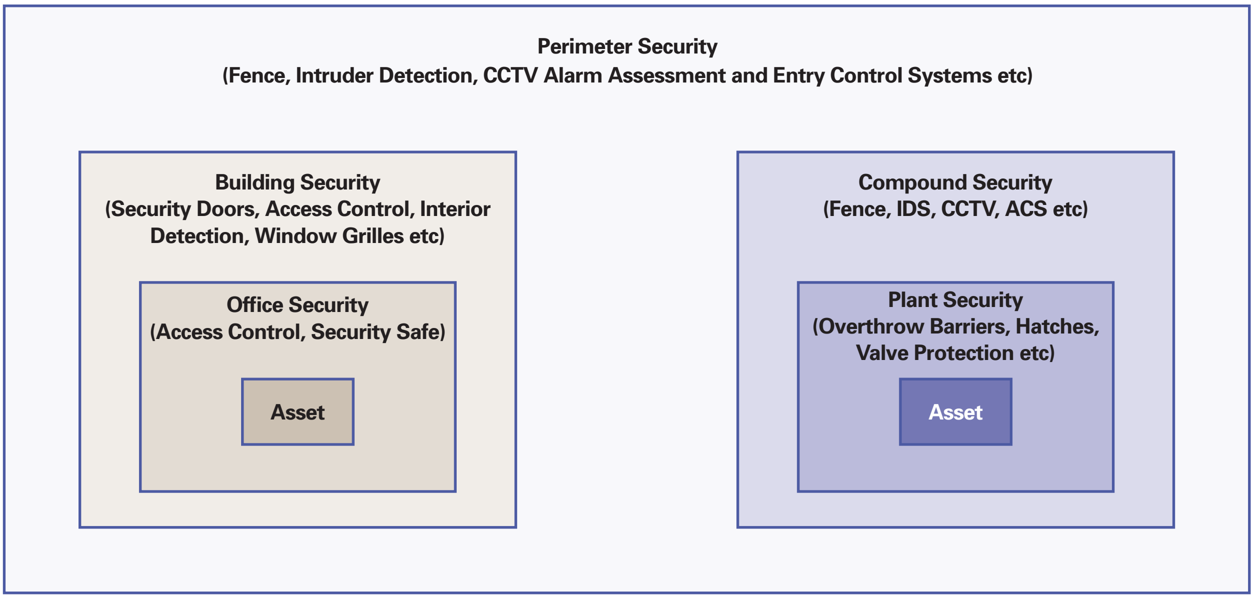
The following sections examine each of the main Physical Security sub-systems by functional DDRR area. They give an overview of related technologies and applications in order to provide you with an understanding of how you can utilise Physical Security measures to meet your specific ***Risk-based Performance Requirements*** as established in C1, and therefore your Protection Objectives as established in B7. Given the complexities of security technology you will not be expected to produce a detailed systems design from this information.

However, it will allow you to identify the level of security systems performance that may be necessary to protect your Assets against the risks identified previously, and to support you in the example Performance Requirements for each technology or sub-system provided. Later in the process you will be asked to draw up a list of ***Performance-based Security Systems Requirements*** prior to embarking on the implementation process outlined in Phase D of the Security Management Plan. This will allow you to engage effectively with external service providers, ensuring that they understand, and can be held accountable for, the required level of Security Systems performance.

It is important to emphasise that each Asset is unique and may require different physical security systems and technologies to achieve the required level of risk mitigation. For example some technologies are only suitable in specific environmental conditions, whilst others may only protect against certain types of attack methods. This is why the Security Management Plan framework focuses on Performance Requirements rather than specific products or technologies. Providing that you follow this process and consider the specific characteristics and requirements of each project or Asset you will avoid the 'one size fits all' approach, which is a common cause of poor Physical Security performance. In addition it is also worth considering the following overarching principles of a robust Physical Security regime:

1. Protection in Depth
This refers to the use of multiple layers of physical security to protect Assets, thereby increasing the likelihood that the adversary will fail to overcome one of these layers, each of which will require a distinct task to be completed – whether climbing a fence, bypassing an alarm system, or defeating a security door. As such it will demand more preparation and skill of the adversary than a single layer of Physical Security. An example of the Protection in Depth principle is shown in the following diagram:

Diagram C3a: Protection in Depth Principles


Perimeter Security
(Fence, Intruder Detection, CCTV Alarm Assessment and Entry Control Systems etc)
Building Security
(Security Doors, Access Control, Interior Detection, Window Grilles etc)
Office Security
(Access Control, Security Safe)
Asset
Compound Security
(Fence, IDS, CCTV, ACS etc)
Plant Security
(Overthrow Barriers, Hatches, Valve Protection etc)
Asset

2. Balanced Protection

Although the level of Protection offered by each layer of security outlined above may differ significantly, they should each provide a uniform level of protection around the Asset such that there are no significant weak points that can be exploited by the adversary. For example where a specialist security door protects entrance to a critical building, the same level of delay should be provided by the windows, walls and any other potential access points. This is referred to as Balanced Protection.

3. Redundancy

For high-risk Assets it is also important to consider the consequences of a component failure within any of the Physical Security sub-systems, and where necessary, build in redundancy to ensure that this would not lead to a compromise of the Assets. This redundancy could either be mechanical/electrical – for example a dual-redundant alarm communications network or a backup power supply to security equipment – or procedural – for example the deployment of a guard at an access point or an increase in patrolling of the perimeter until such a time as the system is repaired (in this respect maximum response time of external service providers should also be considered and built into maintenance contracts).

4. Adaptability

It is also important that the Physical Security System can be adapted to short-term changes in the threat environment in order to keep associated risks within acceptable levels during these periods. Although this is primarily achieved through Procedural Security and the application of 'Alert States and Response Levels' (as detailed in Section C5), Physical Security systems can also contribute to this, for example by use of rapid deployment intruder detection systems, temporary barriers, additional guarding, or changes in electronic configuration settings, in order to protect against heightened threat levels.

The principles of 'Protection in Depth', 'Balanced Protection', 'Redundancy' and 'Adaptability' should be kept in mind when reviewing the information in Section C3 and deciding upon the type of measures and related performance levels that will be required to meet the specific Protection Objectives for the Asset in question.

C3.1 Detection

Detection

- The ability to detect that an incident is occurring, assess the type of incident and identify the necessary response

The vast majority of energy infrastructure Assets will require a robust detection capability and in this respect there are three primary systems that will provide this, which are:

1. **Intruder Detection System**
2. **Access Control System**
3. **Alarm Assessment System**

The first two systems are used to generate alarms in response to potential threats, whilst the third system is used to assess the cause of alarms (a genuine threat or a nuisance alarm) so that the correct response can be initiated. The detection function is not complete until alarm assessment has taken place.

Each of the above systems consists of a number of components or sub-systems which contribute to the detection function. These are shown in the following diagram:

C3.1.1 Intruder Detection Systems (IDS)

- Exterior Intrusion Detection
- Interior Intruder Detection

C3.1.2 Access Control Systems (ACS)

- Unathorised Access Detection
- Unauthorised Materials Detection

C3.1.3 Alarm Assessment Systems (AAS)

- Video Assessment
- Alarm Communication
- Alarm Control & Display

In addition to the systems and sub-systems manual detection measures such as guard force observation and routine patrolling, general employee security awareness can also contribute to the detection function and these are discussed in further detail in Section C5 (Procedural Security). However, at this stage it is important to be aware that, in isolation, these latter measures do not typically provide an adequate Probability of Detection (PoD) to meet the Performance Requirements of most significant Assets – although very good at assessing alarm information, people are inherently limited in their ability to detect threats due to coverage (particularly for large facilities) and reliability.

Each of the Detection systems and sub-systems are examined in the following sections, where an overview of their function, types of technology, applications and Key Performance Requirements are presented, along with details of relevant standards and sources of further guidance.

C3.1.1 Intruder Detection Systems

A. General Characteristics

Intruder Detection Systems (IDS) offer the ability to detect unauthorised access in to a facility, building or secure area, with much greater reliability than that normally achievable through manual monitoring, and are therefore central to the Detection function. They can be deployed in a variety of applications both in outdoor and indoor environments depending upon the requirements of the facility or Asset in question. Whilst there are significant differences in exterior IDS (often referred to as Perimeter IDS or PIDS) and interior IDS, the performance of both types of system centres upon two factors – Probability of Detection (PoD) and Nuisance Alarm Rate (NAR). These are explored below:

1. Probability of Detection (PoD) – this refers to the probability that the IDS will detect an intrusion and is expressed as a percentage from 0-100% (although 100% is technically challenging to achieve, despite some manufacturer's claims). The PoD is not uniform for each type of technology since it depends not only upon hardware design but also on its suitability for the specific application in question. Key factors that must be considered include:

- Type of adversary (running, walking, crawling intruder etc)
- Adversary capability – can it defeat the IDS
- Environmental Conditions
- Installation and Sensitivity settings
- Acceptable Nuisance Alarm Rate (NAR)

As indicated by the last point there is often a direct relationship between PoD and NAR since the higher the sensitivity of the sensor the greater the number of nuisance alarms that will be generated.

2. Nuisance Alarm Rate (NAR) – this refers to the number of alarms not caused by genuine intrusions and is expressed as, for example, 1 per kilometre per day. This includes those alarms caused by environmental conditions such as wind, rain, animals, changes in temperature etc, as well as those caused by system faults (which are referred to as False Alarms). Since all detection systems will generate Nuisance Alarms it is necessary to have a means of alarm assessment to verify the cause of alarm as discussed in Section C3.1.4.

Each type of IDS will be based around a particular sensor technology with its own individual performance characteristics and strengths and weaknesses in certain areas. In particular each technology will have potential sources of Nuisance Alarm associated with its mechanical operation, as well as certain vulnerabilities that could allow an adversary to bypass the detection field or pass through it undetected. Therefore expertise is required in the design and specification of IDS if they are to deliver the required level of performance.

The following sections will provide you with an overview of different intrusion sensor technologies, along with their typical performance characteristics and applications, so that you can understand how they may be used to contribute to the Detection function and determine what the Key Performance Requirements are likely to be in relation to your particular Asset(s). Subsequently external support can be sought to design appropriate intrusion sensors and related detection systems that will meet these Performance Requirements in full.

.

> *Each of the Detection systems and sub-systems are examined in the following sections, where an overview of their function, types of technology, applications and Key Performance Requirements are presented*

B. Sub-Systems

B1. Exterior IDS

Exterior IDS can be used to provide detection around the perimeter of a facility, within a particular area of the site such as an outdoor compound, or even outside of the site to provide early detection of approaching threats.

As Exterior IDS are subjected to environmental conditions such as rain, wind, fog, vibration, humidity, animals and debris, there is the potential for a higher number of nuisance alarms when compared to indoor intrusion sensors. This makes efficient alarm assessment methods, such as integrated video surveillance, very important so that security personnel can quickly determine the cause of alarm (as discussed further in section C3.1.4). Even so it is still necessary to minimise these nuisance alarms in order to ensure that the operator retains confidence in the system and does not choose to ignore them. This requires a thorough understanding of both local environmental conditions specific to each facility and the performance characteristics of different sensor technologies.

There are four main types of Exterior Detection according to the type of sensor utilised – Fence-associated, Freestanding, Buried, and Video-based. Each of these is discussed below, whilst individual technologies and associated performance characteristics are summarised in the table that follows.

B1.1 Fence-Associated Sensors

Fence-associated sensors include fence-mounted cables and point detectors, Taut-wire Sensor Fences, Electric fences and Electric Field/Capacitance detectors. They all detect attempts to climb, cut or pass through the fabric of an existing security fence or a dedicated alarm sensor fence. Fence-associated sensors are terrain following and are therefore suitable for undulating ground conditions.

When considering the use of Fence-associated detection it is important to bear in mind that if the intruder manages to bypass the fence – for example by tunnelling underneath it, or bridging over it with a ladder, parked vehicle or existing structure – they will have also bypassed the detection system. Where capable and knowledgeable adversaries are anticipated, fence-associated sensors should only be used if fence construction provides significant protection against bridging and tunnelling attempts and therefore reduces this possibility, otherwise the PoD could be compromised. Where the highest PoD is required complementary sensors or layers of detection will be required.

B1.2 Freestanding Sensors

Freestanding detection systems include Microwave sensors, Active Infrared and Passive Infrared sensors, Dual-technology sensors (for example microwave and active infrared in a single housing), and Ground-based Radar. With the exception of active infrared beam alarms they provide volumetric detection meaning that the detection field covers a three-dimensional space. The detection field is generally invisible to the intruder therefore making it more difficult to bypass. As such they have the potential to offer a higher PoD than fence-associated sensors (dependent upon the specific application and environmental conditions) and are often deployed where adversary capability is likely to be high.

In most cases it is necessary to deploy freestanding sensors within an area where legitimate activity is not expected, for example in a 'sterile zone' between two fences or on the inside of a perimeter fence. This reduces nuisance alarms from both people and animals. However, where limited legitimate activity (from both people and animals) is anticipated outside of the perimeter they can be used to provide early detection of approaching threats. Ground-based radar is particularly suitable for covering large detection areas, which can also be limited by software configuration to avoid areas of legitimate activity.

Freestanding detection systems generally require line of sight between sensors and therefore are not suitable for undulating terrain or where obstacles are present within the detection field.

B1.3 Buried Sensors

Buried sensors include Ported Coaxial Cables, Fibre Optic Cables, Pressure sensors and Seismic sensors. As they are buried underneath the ground they are covert, terrain-following and difficult to bypass. Due to the ground works required for their installation buried sensors can be more expensive to install than freestanding sensors and fence-mounted sensors, however, they have the potential to provide a very high PoD.

As with freestanding sensors buried sensors are most effectively deployed within a sterile zone or area of limited activity to avoid nuisance alarms by people or large animals. Other potential sources of false alarm include standing water, vibration and metallic objects in or close to the detection field. If these can be avoided buried sensors can also provide a very low NAR.

B1.4 Video-Based Detection

Video-based detection, commonly referred to as 'Video Analytics' use software algorithms to detect changes in the video scene beyond pre-defined parameters. It can be used in a variety of roles including intruder detection, people counting, Asset tracking and left-object detection. It has the potential to offer a flexible and cost-effective detection system with the ability to utilise existing cameras and configure detection zones to rule out areas of legitimate activity.

Whilst significant technological progress has been made in this area, Video Analytics is still not considered a mature technology and therefore requires careful implementation, particularly for large deployments. In the past it has sometimes failed to live up to expectations, primarily due to unacceptably high NARs caused by environmental conditions as well as sub-optimal configuration, which with many systems can be a complex process.

However, there are an increasing number of successful deployments in the market and this is likely to increase as time goes on. If Video Analytics is being considered for higher security applications it is suggested that it is first trialled to see how it performs in the context of local environmental conditions, and preferably used to complement rather than replace other detection technologies.

B1.5 Sensor Performance Characteristics

The following table provides a summary of the main types of Exterior IDS technologies, along with their typical performance characteristics. However, it is important to be aware that performance can differ significantly between applications and with improvements in technology. In many cases it is possible to overcome certain limitations in performance, for example if freestanding and buried sensors are installed within a 'sterile zone' between two fences this will significantly reduce Nuisance Alarms from animals.

Whilst significant technological progress has been made in this area, Video Analytics is still not considered a mature technology and therefore requires careful implementation, particularly for large deployments.

Table C3a: Exterior IDS Performance Characteristics

Sensor Type	Probability of Detection											Potential for Nuisance Alarms									Costs		
	Slow Walk	Walking	Running	Crawling	Rolling	Jumping	Tunnelling	Bridging	Cutting	Climbing	Lifting	Wind/Vibration	Rain	Standing Water/Runoff	Snow	Fog/Sand	Large Animals	Lightning	Overhead power lines	Buried power lines	Equipment	Installed on	Maintenance
B1.1 Fence-Associated																							
Fence-Mounted	N/A	N/A	N/A	N/A	N/A	VH	VL	VL	H	H	H	H	M	L	L	VL	M	L	VL	VL	L	L	L
Taut Wire Fence	N/A	N/A	N/A	N/A	N/A	VH	VL	VL	H	H	H	VL	VL	VL	VL	VL	L	VL	VL	VL	H	H	M
Electric Fence	N/A	N/A	N/A	N/A	N/A	VH	VL	VL	H	H	H	L	L	VL	L	VL	M	L	L	L	H	H	M
Electric Field/Capacitance	VH	VH	VH	H	H	VH	VL	L	N/A	N/A	N/A	M	M	VL	M	VL	VH	M	L	VL	M	L	M
B1.2 Freestanding																							
Microwave	H	VH	H	M	M	M	VL	L	N/A	N/A	N/A	L	L	H	L	M	VH	L	L	VL	L	L	M
Active Infrared	VH	VH	VH	M	M	H	VL	L	N/A	N/A	N/A	L	L	L	M	M	VH	L	VL	VL	L	L	L
Ground-based Radar	H	VH	VH	H	VH	VH	H	H	N/A	N/A	N/A	VL	VL	VL	L	M	VH	L	VL	VL	H	M	H
B1.3 Buried																							
Ported Coaxial Cable	H	VH	VH	VH	VH	H	M	M	N/A	N/A	N/A	VL	M	VH	L	VL	M	M	VL	M	H	M	M
Seismic	H	VH	H	M	M	M	M	M	N/A	N/A	N/A	M	L	L	L	VL	VH	L	L	M	M	M	L
Fibre Optic Cable	H	VH	H	H	H	H	M	L	N/A	N/A	N/A	H	M	M	L	VL	H	L	VL	VL	M	M	M
B1.4 Video-Based																							
Video Analytics	H	VH	VH	H	H	H	VL	M	VH	VH	VH	M	M	L	L	H	VH	L	L	VL	L	M	H

Key: VL = Very Low   L = Low   M = Medium   H = High   VH = Very High

B2. Interior IDS

Interior IDS can be used to detect potential intrusions into buildings and similar sealed structures. As with Exterior IDS their performance is defined by PoD and NAR, however, they generally have a much lower NAR because they operate within a controlled internal environment not subjected to the same variety of nuisance alarm sources (the only exception to this being any sensors that are installed on the exterior of the building). In addition they are often confined to a smaller geographical area when compared with Exterior IDS, which are deployed around a large perimeter as would be found at most energy infrastructure facilities.

When specifying Interior IDS it is worth utilising European Norm (EN) 50131-1 ('Alarm systems. Intrusion and hold-up systems. System requirements'), since this sets out performance requirements for the system and each individual sub-component based upon four grades, as shown in the following table:

Grade/ Risk Level	Possible Intruder Capability	Suitable Applications
Grade 1: Low Risk	Opportunistic criminals with little knowledge of alarm systems and very basic hand tools	Domestic environment with audible-only alarm
Grade 2: Low-Medium Risk	Criminals with some knowledge of the building but limited knowledge of alarm systems and general tools	Large residential and small commercial systems such as Florists, Salons, Bakers etc
Grade 3: Medium-High Risk	Building contents perceived as high value, criminals likely to spend time planning their intrusion, be conversant with alarm systems and have a wide range of tools including portable electronic equipment	Most commercial facilities including bonded warehouses, computer shops, motor garages. **Medium Risk Energy Facilities**
Grade 4: High Risk	Security takes precedence over other factors – intruders will have the ability to plan and resource an intrusion in full and have access to sophisticated tools and the means to substitute vital alarm components	Military installations, critical infrastructure facilities, bullion and cash centres, government research facilities. **High-Risk Energy Facilities**

As such systems can be specified to meet one of the above risk grades, providing assurance that they will be suitable for the application in question. In this respect it is likely that most energy facilities will require Grade 3 or Grade 4 Interior IDS.

There are three main classifications of interior IDS – Boundary Penetration, Interior Motion and Proximity. These are discussed below whilst individual technologies and associated performance characteristics are summarised in the table that follows:

B2.1 Boundary Penetration Sensors

Boundary penetration sensors are used to detect attacks on or intrusion through the exterior of a building, whether a door, window, wall or ceiling. They provide linear or point detection and can either be covert or visible. The most common type of sensor is the Balanced Magnetic Switch installed on doors and windows. Other types of sensor include active infrared beam alarms, fibre optic detection cables, Break-Glass Sensors and other Vibration Sensors which can be mounted on the inside of walls and windows or even embedded within walls.

B2.2 Interior Motion Sensors

Interior Motion sensors detect intrusions into an internal space regardless of the point of entry and therefore provide volumetric detection capability. The most common type of sensor in use as the Passive Infrared (PIR) detector, which measures changes in background temperature associated with a person entering the detection field. Microwave detectors are also increasingly common as are dual-technology detectors which utilise both PIR and microwave sensors in order to overcome the potential limitations of each and therefore increase the PoD or reduce the NAR. Video Analytics can also be used as a very capable Interior Motion Sensor, being much less susceptible to Nuisance Alarms than when used in outdoor applications.

For many applications it is advisable to combine both Boundary penetration and Interior motion sensors to ensure full coverage and a high PoD. Given the modest costs of interior IDS when compared to many other security systems this is achievable within most budgets.

B2.3 Proximity Sensors

Proximity sensors are placed on or near an Asset in order to detect its continued presence and therefore generate an alarm if it is removed. They include capacitance sensors which detect people approaching the Asset and causing disturbances in the electrical field, and pressure sensors which are placed underneath or around an Asset, ideally concealed under a carpet so that they cannot be easily identified and bypassed. Proximity sensors are useful for specialist applications but should be combined with other types of sensor for high-security environments.

B2.4 Sensor Performance Characteristics

The following table provides a summary of the main types of Interior IDS technologies, along with their typical performance characteristics. However, as with Exterior IDS, it is important to be aware that performance can differ significantly between applications.

Table C3b: Interior IDS Performance Characteristics

	Slow Walk	Running	Crawling	Jumping	Bridging/Bypass	Tampering	Cutting/Climbing	Wind/Rain/Sand/Fog	Animals	Internal Heat Sources	Electrical Interference	Vibration	Equipment	Installed on	Maintenance
Sensor Type	**Probability of Detection**							**Potential for Nuisance Alarms**					**Costs**		
B2.1 Boundary Penetration															
Balanced Magnetic Switch	N/A	N/A	N/A	N/A	L	L	VL	VL	VL	VL	L	L	L	L	L
Active Infrared Beams	VH	VH	VH	H	L	M	H	M	M	VL	L	L	L	L	M
Break-Glass Sensors	N/A	N/A	N/A	N/A	L	M	H	L	VL	VL	L	L	L	L	L
Fibre Optic Cables	N/A	N/A	N/A	N/A	H	H	VH	L	L	L	VL	M	M	M	M
B2.2 Interior Motion															
PIR Detector	M	M	M	H	M	L	N/A	N/A	N/A	H	M	L	L	L	L
Microwave Detector	H	H	H	H	M	M	N/A	N/A	N/A	L	M	L	M	L	L
Dual-Technology Detector	H	VH	H	H	H	M	N/A	N/A	N/A	L	M	L	M	L	L
Video Analytics	VH	VH	H	VH	H	H	H	N/A	N/A	VL	L	VL	M	M	H
B2.3 Proximity															
Capacitance	H	H	H	H	M	M	N/A	N/A	N/A	L	M	M	M	M	M
Pressure	H	H	H	H	L	M	N/A	N/A	N/A	VL	L	L	M	L	L

Key: VL = Very Low L = Low M = Medium H = High VH = Very High

C. Applications

Exterior and Interior IDS are likely to form a central part of your requirements in the area of Detection and will require careful consideration if not already installed and delivering an appropriate level of performance. The starting point when deciding upon the type of systems and associated levels of performance necessary is to review your Risk-based Performance Requirements established in Section C1, along with the Adversary Sequence Diagrams that relate to the main Risk Scenarios and Protection Objectives of concern. This will help to determine at which points in the sequence IDS will be required, taking into account the location of identified Critical Points.

In line with the ‘Protection in Depth’ principle you should where possible implement multiple layers of detection around high-risk Assets in order to ensure that: detection occurs at the earliest opportunity therefore maximising available response time; detection still occurs even where an adversary manages to bypass one system; and detection capability is effective against the full range of Risk Scenarios. This can be achieved via the use of Exterior IDS deployed around the perimeter and critical compounds or areas, and Interior IDS installed in buildings containing Critical Assets. However, the majority of energy infrastructure will also have Critical items of outdoor plant where Interior IDS cannot be used to provide a secondary layer of protection. In this case it is advisable where feasible to create secondary compounds or security enclosures around these Critical Points (not least to provide additional and often essential delay) and apply detection accordingly. Even where this is not possible a virtual detection barrier can be formed with appropriate Exterior IDS technologies. This layered approach to detection will reduce the reliance upon expensive Perimeter IDS and in a few cases even negate it.

However where critical infrastructure is widespread throughout the plant, positioned close to the perimeter, or where a rapid response is required, it will become more important to maximise the PoD provided by Perimeter IDS. In this case complementary sensors integrated via an OR gate (i.e. only one sensor has to activate in order to generate an alarm) should be considered. They should be complementary in the sense that any inherent vulnerabilities in one sensor technology are overcome by another – for example the use of microwave sensors (vulnerable to bridging or tunnelling) with ground-based radar. However, because there will now be two sources of potential Nuisance Alarms it is also important to ensure that both sensor technologies offer the potential for a low NAR in the context of local environmental conditions. In addition it is vital to ensure that a continuous line of detection exists, where necessary using auxiliary sensors to cover potential access points through the perimeter.

For applications where the PoD is not quite as critical, and/or where it is necessary to reduce Nuisance Alarms, exterior IDS can be combined in an AND gate (i.e. where both sensors have to activate in order to generate an alarm). Consideration should be given to the use of sensors with different Nuisance Alarm sources in order to benefit from this, for example Video Analytics integrated with Ported Coaxial Cable Sensors or Fence-mounted sensors.

For building applications the lower investment typically required to implement IDS, along with a reduced potential for Nuisance Alarms when sensors are correctly specified, means that multiple sensor technologies should be used for the majority of facilities. In particular it is important to ensure that detection occurs regardless of the point of entry into the building, whilst further layers of detection provide coverage of individual rooms or areas at risk, taking into account potential ‘insiders’ who may have legitimate access to the building as a whole.

D. Performance Requirements

Although it is likely that you will need to engage external specialists to assist you with the design of any IDS it is important to first identify your Key Performance Requirements in this area, in order to provide the basis for design. The following table provides some examples of IDS Performance Requirements; however, they will need to be adapted to meet the demands of each specific Asset and associated risk profile.

Table C3c: **IDS Performance Requirements**

Area	Ref	Example Performance Requirements
Exterior IDS		
Probability of Detection (PoD)	PR1	The Exterior IDS will be capable of detecting all movements through a designated sterile zone, including walking, running, crawling and bridging attempts with a 95% PoD or higher.
	PR2	The Exterior IDS will be capable of detecting all attempts at cutting of the perimeter fence, climbing over the fence and burrowing underneath the fence, with a 90% PoD or higher.
	PR3	The PoD for all Exterior and Interior IDS will not be significantly compromised in the event that a single sensor technology is defeated or bypassed.
Nuisance Alarm Rate (NAR)	PR4	The NAR for the Exterior IDS as a whole will be no more than 5 per km of perimeter per day, measured as an average over any 1-month period at all times of year.
	PR5	The Exterior IDS will be suitable for use in the following environmental context without increasing the stated NAR; heavy wind; rain; fog; standing water; buried power lines; and large animals.
Coverage	PR6	The Exterior IDS will provide continuous coverage around the entire perimeter of the site including all potential access points, pipe racks and other structures crossing through the perimeter.
Accuracy	PR7	The Exterior IDS will identify the precise location of any intrusions through the perimeter to within 10m accuracy.
Operation	PR8	For the Exterior IDS it will be possible to independently disable all individual alarm reporting zones.
Integration	PR9	The Exterior IDS will support integration with the Access Control and Alarm Assessment Sub-systems, as well as existing Fire and Safety Systems.
Interior IDS		
Probability of Detection (PoD)	PR10	The Interior IDS for Building A will detect all attempts to penetrate the exterior shell of the building including windows, doors, walls and roofs, with a 90% PoD or higher.
	PR11	The Interior IDS for Building A will detect all persons entering into the building regardless of the point of entry and the speed and direction of travel, with a PoD of 98% or higher.
	PR12	The PoD for all Exterior and Interior IDS will not be significantly compromised in the event that a single sensor technology is defeated or bypassed.
Nuisance Alarm Rate (NAR)	PR13	The NAR for the Interior IDS will be no more than 4 per year for the building and all rooms to be covered as a whole.
	PR14	The Interior IDS will be suitable for use in the following environmental context without increasing the stated NAR; localised heat sources, electromagnetic interference and moderate vibration.
Coverage	PR15	The Interior IDS will provide full coverage of Rooms 1, 2 and 3 regardless of the point of entry into these rooms.
Accuracy	PR16	The Interior IDS will identify the individual room or specific areas within each room where the intrusion takes place
Operation	PR17	For the Exterior IDS it will be possible to independently disable all individual alarm reporting zones, either on an ad-hoc basis or during specific times of the day.
Integration	PR18	The Interior IDS will support integration with the Access Control and Alarm Assessment Sub-systems, as well as existing Fire and Safety Systems.
Standards	PR19	The Interior IDS including all sub-components will be designed, manufactured and installed to meet the requirements of EN 50131-1:2006, Grade 4.

C3.1.2 Access Control Systems

A. General Characteristics

The primary function of Access Control Systems (ACS) is to allow the authorised and legitimate movement of personnel, vehicles and materials into or out of a restricted facility, building or area, whilst detecting any unauthorised movements. They can also provide an element of delay; however, this depends upon the performance characteristics of the physical barriers and locking devices associated with the Access Control System, something which is explored in Section C3.2.

For the purpose of the Security Management Plan 'Access Control Systems' include the physical and electronic devices, supporting software, databases and procedures that facilitate the screening of people, vehicles and materials in accordance with facility or organisational policy, and therefore allow unauthorised movements to be detected. The following section provides an overview of the various sub-systems, technologies and practices that you can utilise to meet your Risk-based Performance Requirements in the area of Detection, and which, in conjunction with IDS discussed previously, can be used to detect a range of threats, including those from insiders. It focuses primarily on the deployment of various access control technologies, whilst further information on Procedural aspects can be found in Section C5.

B. Sub-Systems

B1. Unauthorised Access Detection

The majority of significant energy infrastructure Assets will require an electronic means of controlling access, whereby barriers and locking devices are controlled via an entry/exit reader operated via one of the following:

- Coded Token such as a Proximity Card, Key Fob or Vehicle Tag, which is issued to the user and must be presented to the Access Reader
- Personal Identification Number (PIN), which is known by the user and must be entered into the keypad to gain entry.
- A physical characteristic unique to the individual such as a fingerprint or hand shape, which is presented to a specialist biometric reader
- A combination of the above measures to ensure that their inherent vulnerabilities cannot be exploited – particularly important for high-security applications

The readers will be connected to either a local or central user database (the latter typically being a dedicated ACS Server) so that the information presented or input can be cross-referenced to the user's record and pre-assigned access rights allowing the system to determine whether or not access should be granted. Together these components form an Automatic Access Control System (AACS), which can provide the capability to efficiently and securely manage access to the facility by a large number of people, whether entering on foot or in a vehicle.

Although AACS is typically viewed purely as a physical means of preventing unauthorised access in to a facility, as with any delay measure success in this area is dependent upon adversary capability to defeat it. However, equally important and often overlooked is the ability of the AACS to detect unauthorised access attempts and subsequently alert security personnel to their occurrence so that a response may be mounted. Whilst this can be achieved in part by manual observation of access points by security personnel, for high-security environments this should be complemented with electronic detection as is done with Exterior and Interior IDS. To this extent the majority of AACS technologies can be configured to generate an alarm as a result of the following events:

- Access Attempt by Unauthorised Person
- Access Attempt by Pre-defined/Blacklisted Card Holders
- Door Forced Open (via monitored electronic locks or separate contact sensors)
- Door Held Open (for greater than x seconds – via monitored electronic locks/contact sensors)
- Door opened under Duress (via input of pre-defined Duress PIN code)
- Communications or Power Failure

These alarms will alert operators to potential activity of concern and as such an immediate response can be mounted to ensure that intervention takes place before the associated barriers and locks are defeated, or the adversary finds an alternative route of entry into the facility. For lower risk areas this form of ACS detection may be adequate without the need for a dedicated Interior IDS.

As indicated above it is also important to ensure that the integrity of the facility is not undermined by occupants leaving doors ajar/held open and this is best done by the use of monitored locks with alarm reporting capability. Fire exits are a common weakness in this respect, and it is recommended that the door hardware and ACS software are configured to ensure that an alarm is initiated whenever they are operated, which should only be in an emergency. This also applies to emergency exit gates through the perimeter of the site, which could provide an easy escape route for adversaries.

Another area that should be considered in any ACS deployment is the potential for 'tailgating' – i.e. following another person or vehicle through the barrier and therefore bypassing the ACS. Detection of tailgating can also be achieved electronically, either via dedicated proximity sensors or by use of Video Analytics applications. However, where it is also necessary for tailgating to be physical prevented – for example where the barrier or door provides access to a high-risk area, it is also important that the design of physical barriers supports. In the context of vehicle access control points this will typically require the use of two sets of barriers forming an airlock system in which only one barrier will open at a time. For personnel access points this can be achieved via the use of full-height revolving turnstiles. By implementing such measures less reliance is placed upon monitoring and response by security personnel, which is never foolproof, and therefore the opportunity for an adversary to gain access to the facility surreptitiously is reduced.

For very small facilities, individual buildings or rooms that have little throughput, the use of manual locks may be sufficient to control access. However, a strict and auditable key control regime will be necessary to minimise the risk of unauthorised access and the potential impact of lost or stolen keys. In addition it is important to realise that manual access control in itself will not offer any form of detection and therefore other measures such as robust IDS will be required to compensate for this.

B2. Unauthorised Materials Detection

A number of risk scenarios that you may be facing will involve the unauthorised movement of materials into or out of the facility, for example attempts to:

- Bring weapons or tools into the facility in order to attack people or Assets
- Bring Chemical, Biological, Radiological, Nuclear or Explosive (CBRNE) material into the facility with the intention of mounting an attack upon it
- Bring harmful material into the facility with the intention of contaminating or disrupting the production process
- Steal CBRNE material from the facility with the intention of using it in attack elsewhere, or selling it on to other parties to do the same
- Steal valuable components from the facility including items of plant, tools, IT hardware and sensitive information

In order to protect against the above risk scenarios where they are of concern, it will be necessary to have the capability to detect the movement of such materials into or out of the facility such that the appropriate response and prevention measures can be taken. This may require a range of methods that can efficiently detect covert and unauthorised movements, including screening and Asset tracking, as discussed below.

B2.1 Screening

Various screening methods can be implemented at key access points in order to detect the unauthorised movement of dangerous or illicit materials, the most common being the use of manual searching of people, baggage, vehicles or cargo by security personnel. This is usually carried out on a random basis, however, during heightened alert states or for high-risk facilities this may be conducted for all movements in and out of the facility. Further information on search procedures can be found in Section C5 – Procedural Security.

Where an Asset faces a high-level of risk from associated scenarios, or where the volume, size and type of movements preclude manual screening, it may be necessary to utilise various screening technologies such as X-ray and Explosive Detection Systems to ensure adequate Probability of Detection and throughput times. Before considering such technologies it is important to be aware that the majority do not provide fully automated detection – they require human operators to interpret the results and make rapid decisions regarding potential threats. In addition many technologies utilise some form of radioactive or chemical process and therefore it is vital that appropriate health and safety cautions are adhered to. For these reasons the use of technology-based screening requires well-trained operators both in terms of safe and effective system use as well as general threat awareness and incident response. It is also important that the systems are rigorously maintained by trained technicians, which can be considerably expensive.

The above factors should be taken into account when considering the deployment of screening technology, the main types of which are summarised in the following table. Specialist advice should also be sought to ensure that the selected technologies will deliver the required levels of performance in relation to anticipated threat profiles.

Table C3d: **Types of Screening Technology**

Screening Type	Technology	Uses	Strengths	Considerations/Limitations
Personnel	Personnel Handheld Metal Detector (HHMD)	Detection of metal during the searching of personnel at security checkpoints	• Relatively low cost • Can detect small objects • Can pinpoint the position of an object	• Effectiveness of search depends upon skill of operator • Searches take time to complete • Automatic sensitivity adjustment helps avoid improper use
	Walk-Through Metal Detector (WTMD)	Automated detection of metal during the screening of personnel at security checkpoints	• Higher throughput than HHMDs • Detection doesn't depend upon skill of operator and therefore is more consistent	• Detection performance and sensitivity must be matched to the threat – large or small handguns, knives etc. • Should be positioned away from large metallic objects such as moving doors • Performance should be tested on a regular basis with sample threat materials • Will not reliably detect single rounds of ammunition or detonators
	Body Imaging (X-ray Backscatter/ Full-body X-ray and Millimetre Wave)	To identify weapons and contraband items concealed on a person, or ingested by them	• Can identify non-metallic objects • Full-body X-ray can identify ingested contraband • Millimetre Wave can be used in a stand-off application	• For X-ray Backscatter and Full-body X-ray subject is being exposed to increased levels of ionising radiation – usually requires dispensation from relevant authorities • Can be controversial in some countries due to privacy concerns • Not always possible to tell whether an object is a threat – procedures for searching still required
Personnel/ Baggage	Explosive Vapour/Trace Detection	Detects vapour and/or particle traces of explosives from personnel or baggage	• Provides an additional form of explosives screening for high-risk sites • May detect adversaries in the pre-attack phase who have been handling explosives	• Can suffer from false alarms • Needs to be selected and configured to match operational environment and threat profile • Not effective against all types of explosives
Baggage	Baggage X-ray Systems	Provides screening of baggage for weapons and unauthorised materials	• Fast and efficient method of screening large volumes of baggage without the need to manually search them. • Many have image enhancement features to assist in identification of unauthorised materials. • Many have Threat Image Projection feature to test operator's effectiveness	• Heavily reliant upon skill of operators • Operators require extensive training and regular refresher training • Requires regular maintenance by external technicians

Source: PRISM™

Table C3e: Types of Screening Technology

Screening Type	Technology	Uses	Strengths	Considerations/Limitations
Vehicles and Cargo	Under Vehicle Screening	Aids visual inspection of underneath-side of vehicles before allowing them into a secure area	• Provides a more efficient alternative to the use of hand-held mirrors	• Does not provide automated detection – purely an image to aid searching • Does not provide any information about the contents of the vehicle • Does not provide good coverage of wheel arches – they should still be checked with a mirror
	Backscatter Detectors	Assists with the detection of explosives and drugs within vehicles	• Provides some assurance where it is not feasible to search all vehicles manually • Stand-off and mobile search capability	• Potential false alarm sources such as water and fuel – user needs to have an understanding of the structure being searched to know when a signal is received from an unexpected place
	Cargo Detection (X-ray and Millimetre Wave)	Screening Cargo and vehicles at port entry checkpoints or similar facilities	• Can detect weapons, explosives, drugs and stowaways • Mobile and static applications	• Millimetre Wave only suitable for soft-sided vehicles • X-ray requires cordoned-off area or appropriate shielding
Mail	X-ray Detection	Screening of mail to identify explosives and hazardous materials	• Provides an additional form of explosives screening for high-risk sites • May detect adversaries in the pre-attack phase who have been handling explosives	• Can suffer from false alarms • Needs to be selected and configured to match operational environment and threat profile • Not effective against all types of explosives
Environment	CBRN Detection	Monitor environment for release of CBRN materials	• Can provide early detection of CBRN release and therefore allow mitigating actions to be taken • Possible integration with building HVAC systems to limit spread of CBRN materials	• Not fully mature technology in a commercial environment • Possibility of false positive or false negative detection • Slow-time analysis may be required to confirm some activations

Source: PRISM™

B2.2 Asset Tracking

In addition to screening for weapons, hazardous and illicit materials, some facilities will also need to consider the use of further technologies to detect unauthorised movement of high-value Assets or provide reassurance that vehicle and container movements are legitimate and do not pose a threat. The primary technologies for this are Radio Frequency Identification (RFID) and Global Positioning System (GPS) tracking. Some examples of how these technologies can be deployed to protect Assets are provided below:

1. Valuable Equipment

RFID tags can be attached to valuable equipment such as critical spares, IT hardware and warehouse supplies, as part of an electronic inventory control system. Long-range RFID readers can be placed at warehouse and perimeter exit points and automatically generate an alarm if these items are taken from the site without correct authorisation.

2. Vehicles

Vehicle tracking via GPS can be used to ensure that company vehicles are following the correct course to their destination. Tracking systems offer a number of capabilities such as 'Geo-fencing' that alerts the operator to any divergence from pre-planned/authorised routes, which may indicate that the vehicle has been stolen, the driver requires emergency assistance (particularly important for remote or dangerous areas), or that the driver is involved in some form of unauthorised activity. Vehicle positions can be displayed on a Graphical User Interface (GUI) for monitoring purposes, and in some applications this can also be used to distinguish between those vehicles approaching the site that belong to the company, and those which do not and may pose a potential threat.

3. Freight Movements

High-Value or High-Risk freight movements can also benefit from GPS tracking to ensure that they remain on course or to provide assurance that containers entering a facility are legitimate and do not pose a threat. This usually requires co-operation and uniform technologies across several parts of the supply chain but can be important for some high-risk locations.

C. Applications

A robust, multi-layered Access Control System will be an important aspect of your security provision, providing the capability to detect unauthorised movement of people, vehicles or materials into and from the site. You should therefore review the information and analysis from the assessment phase to identify the type of activity of greatest concern and those parts of the facility that will require some form of access control including all potential routes to the Assets of concern as identified in the relevant Adversary Sequence Diagrams.

For many facilities some form of access control will already be in place, however it is important that adequate secondary controls are utilised to provide detection around identified Critical Points. This will also allow you to restrict access to essential personnel only, thereby reducing vulnerability to the threat from insiders, including both employees and contractors. For some facilities it may be appropriate to implement a number of separate zones each with independent physical and electronic access controls – for example an Administration Zone, Plant Zone, and Maintenance/Storage Zone. These access restrictions are best implemented by assigning user privileges within the ACS database according to the requirements of their role (and not solely on the basis of their seniority). Consideration can also be given to the use of an electronic 'Permit to Work' system linked to the ACS and the issuing of access tokens. Effective vehicle access control will also be vital, and for high-risk facilities access should be denied to all but essential vehicles, particularly in the plant area or in close proximity to any Critical Points. This will require the provision of external parking with pedestrian access routes into the facility.

Where an AACS is utilised you should consider the requirement for integration with any fire and safety alarm systems, such that some or all doors fail-open in the event of an emergency. In some countries this will be a mandatory requirement imposed by local authorities. However, it is important that this cannot be used to defeat the system – for high-risk buildings it may be acceptable to operate locks in fail-secure mode, or alternatively use procedural controls and response force coverage to ensure Assets remain secure. Depending upon the configuration of physical barriers the AACS can also be used to create occupancy lists for use in evacuation, or registration of personnel at Muster Points via dedicated readers.

You should also consider the requirement for screening at all entry and exit points in regular use, as well as in mail rooms where there is a risk of mail-bombs or the receipt of hazardous material. Depending upon the throughput and level of associated risk this can either be achieved via manual searching or some form of technology-based screening as discussed previously. Where possible these screening points should be physically segregated from Critical Points and populated areas of the site given the possibility of a serious incident causing disruption/damage, or requiring evacuation. Secondary access points should be available both for response by emergency services and for use as a temporary alternative to main access points.

Given that many energy facilities will contain hazardous, critical, or otherwise valuable materials within the boundaries of the site further measures may be required to ensure that they cannot be removed. These materials will have been identified during the Assessment phase along with their respective locations and this will help you to determine whether additional detection measures such as RFID or GPS tracking will be necessary to protect them.

D. Performance Requirements

The following table provides some examples of Key Performance Requirements for the ACS, and can be used as a starting point for developing your own set of requirements based on the type and level of risks facing the Asset and the agreed Protection Objectives established previously.

You should also consider the requirement for screening at all entry and exit points in regular use, as well as in mail rooms where there is a risk of mail-bombs or the receipt of hazardous material.

Table C3f: Access Control System Performance Requirements

Area	Ref	Example Performance Requirements
Unauthorised Access Detection		
Alarm Reporting	PR1	The Access Control System (ACS) will provide alarm reporting for the following incidents: • Unauthorised access attempt • Access attempt by black-listed/pre-defined cardholder • Door forced open • Door held open • Door opened under duress (via duress PIN code) • Reader communications failure
	PR2	The Access Control System will provide 100% reporting accuracy of the above events during onsite testing.
	PR3	The ACS will detect all attempts at tailgating by vehicles through the perimeter vehicle entrance, and delay or prevent such actions via integration with barrier controls.
	PR4	The ACS will detect all attempts at tailgating by personnel through perimeter entrances and entrances into Buildings A, B and C.
Operation	PR5	The ACS will require at least two types of credential to gain access – one which the person has with them and one which the person knows.
	PR6	The ACS will allow access permissions for each individual controlled barrier to be assigned to individual users or groups of user based upon role.
	PR7	The ACS will support the following anticipated peak throughput levels: • Main Entrance – Pedestrian 50 p/hr/Vehicle 20 p/hr • Building A – Pedestrian 30 p/hr • Building B – Pedestrian 10 p/hr • Building C – Pedestrian 10 p/hr
Integration	PR8	The ACS will support integration with other electronic security systems including fire and safety systems, Video Surveillance Systems and Exterior and Interior IDS.
Unauthorised Materials Detection		
Screening	PR9	It will be possible to detect the following materials entering the site with a high degree of certainty: • Large Weapons – firearms, swords • Small Weapons – knives, handguns
	PR10	It will be possible to screen all incoming mail (up to 500 items a week) for detection of metallic objects and explosive or incendiary devices.
	PR11	All screening locations will be physically segregated from other services and located at least 100m away from all Critical Points and offices.
Asset Tracking	PR12	It will be possible to detect the following materials being taken from the site with a high degree of certainty: • Critical Spares • IT equipment
	PR13	It will be possible to monitor the location of all company vehicles. Alarms will be generated when these vehicles move outside pre-defined areas or routes.

Source: PRISM™

C3.1.3 Alarm Assessment Systems

A. General Characteristics

Alarm Assessment is the means of verifying the cause of an alarm (which may be genuine or false) and determining the most appropriate type of response to that alarm. The detection function is not complete until Alarm Assessment has taken place and therefore it is extremely important that this is done quickly and efficiently in order to maximise available response time prior to an Asset being compromised.

In its most basic form Alarm Assessment consists of visual verification by security personnel at the scene of the alarm. Whilst this can be appropriate for very small or low-risk applications it is generally ineffective for significant Assets since the personnel have to travel to the scene of the alarm and identify the location of the intrusion before being able to make an assessment, by which point there may be insufficient time available to successfully intervene. In addition the response force may be unprepared for the type of incident taking place and therefore put themselves, as well as the Assets, at unnecessary risk. For large perimeter security applications where nuisance alarms will occur on a regular basis manual alarm assessment also results in inefficient use of resources and higher personnel costs.

In order to overcome the limitations of manual alarm verification it is now common to use Video Surveillance Systems in an Alarm Assessment role, and this will be a requirement for most energy infrastructure applications. Not only does this dramatically increase the speed and efficiency of the assessment process, it also increases the likelihood that the correct response will be initiated and in doing so minimises risks to security personnel and other occupants. For example if video verification of an intruder alarm shows an armed attack in progress it may be necessary for onsite personnel to remain in protected areas until an armed police unit can respond.

In addition to Video Assessment the Alarm Assessment System consists of Alarm Communications and Alarm Control and Display sub-systems – each of these three areas is explored below.

B. Sub-systems

B1. Video Assessment

Video Surveillance Systems are still commonly referred to as Closed Circuit Television (CCTV) Systems, however with the advent of Internet Protocol (IP) technologies many systems are now technically Open Circuit Television (OCTV) Systems as they are part of an open network, hence the shift towards the term 'Video Surveillance' (although the term CCTV is still used interchangeably to refer to both analogue and IP systems). However, in the context of the Detection function it is also important to distinguish between 'surveillance' or 'monitoring' and 'assessment'. When used in a general surveillance role video systems have very limited detection capability since they rely upon constant monitoring by security personnel, as well as full coverage of the area of concern. For large sites this may require hundreds of video monitors and tens of operators. Even where this is available numerous studies have shown that human operators are only effective in a detection role for short periods of time – typically in the region of 20 minutes or so. Therefore, for most applications the primary function of the video system should be that of Assessment.

A system which provides Video Assessment capability is significantly different to one that provides general surveillance capability since it is 'event-driven'. This means that specific video images are viewed when an event such as an alarm activation takes place, rather than relying on constant monitoring of all camera feeds. Although the appropriate camera can be displayed on the monitor via manual selection, it is preferable to integrate the video assessment system with the alarm system (either IDS or ACS) to provide automatic image-switching and display since this will reduce the time required for Assessment to take place. In addition it is vital that the displayed image provides adequate coverage of the alarm event to allow correct assessment. In this respect there are a number of Key Performance Parameters that will determine effectiveness in this area, which are: Coverage; Target Image Height; Resolution; Visibility; and Environmental Suitability. Each of these is discussed below. It is also worth pointing out that the Rotakin™ target and associated testing procedure outlined in BS EN 50132, Part 7 can be a very useful tool for establishing performance in all of these key areas.

B1.1 Coverage

The first consideration in relation to the performance of the Video Assessment system is the **coverage** required to facilitate effective assessment of all intruder alarm sources. To achieve appropriate coverage video surveillance cameras must be positioned and configured to provide full and even coverage of the entire assessment area, be it a sterile zone, entrance point, room or compound. Without full coverage of the areas of interest it is possible that an intrusion alarm will be ignored because the intruder is not visible in the associated video scene. Alternatively it may take longer to identify the intruder's location, direction of travel or level of potential threat.

When assessing the type of coverage required for any given application it is useful to consider the following three points:

1. What – needs to be seen?
Is it intruders on foot, in a vehicle, camouflaged, crawling, running etc. Or is it a process that needs to be monitored for irregularities such as leaks, interference or sabotage.

2. Where – will the activity take place?
At the perimeter fence line, in a sterile zone, at an access control point or building entrance, in a room or within a secure compound?

3. When – must the activity be seen?
Following an alarm activation (for how many minutes?), at all times of day and operating states or only when the area is unoccupied?

The above information can be graphically represented on a site plan to show the specific areas and activities of interest. This will subsequently dictate the placement of surveillance cameras and can be used as the basis for discussions with external specialists if required.

In some large applications it may not be practical or cost-effective to provide full coverage of all alarm zones and areas of interest simultaneously as this may lead to a very high camera count and associated infrastructure costs. One alternative is to use Pan, Tilt and Zoom (PTZ) cameras with pre-set positions for each defined alarm zone, integrated with the IDS to provide automatic image switching to the point of alarm. In this manner a single camera can cover multiple alarm zones. However, in this type of application it is important to ensure that the Security Management System is configured to give priority to alarm video such that all other user activity is overridden when the PTZ camera is required to move to its alarm preset. As discussed further in section B4 below, System Response Time will also be slower than when using dedicated fixed cameras and this should be considered in the context of the activity of concern. In most PTZ Video Assessment applications it is advisable to provide redundant coverage of alarm activations via two separate cameras, particularly where potential blind spots such as pipe racks, towers or buildings exist, as this will increase the likelihood that adequate coverage will be provided under all circumstances.

Whether using fixed or PTZ cameras particular attention should be paid to the area between adjoining alarm zones, which by way of example could be every 100m around the perimeter of the site. Cameras should overlap both vertically and horizontally to ensure that an intruder cannot go undetected in these areas.

To achieve appropriate coverage video surveillance cameras must be positioned and configured to provide full and even coverage of the entire assessment area, be it a sterile zone, entrance point, room or compound.

B1.2 Target Image Height

Although the provision of video coverage of all alarm areas is the starting point for effective Video Assessment performance, the level of coverage achieved is also a vital factor. If the target does not occupy a large enough proportion of the video image it may not be possible to discern whether or not the activity is legitimate (i.e. an intruder or an employee or a member of the public) or the extent and nature of the threat posed. In order to overcome this, the 'Target Image Height' parameter can be specified in accordance with the level of required performance.

In this context the UK's Home Office Scientific Development Branch (HOSDB) has provided useful guidance on various Target Image Heights necessary to achieve certain levels of performance, as outlined in the following table (please see HOSDB's 'CCTV Operational Requirements Manual 2009' for further information):

Category	Target Image Height (% of Monitor Screen Height)	Vulnerability Score
Monitor and Control	**5%**	An observer should be able to monitor the number, direction and speed of movement of people across a wide area, providing their presence is known to him; i.e. they do not have to be searched for.
Detect	**10%**	After an alert an observer would be able to search the display screens and ascertain with a high degree of certainty whether or not a person is present.
Observe	**25%**	At this scale, some characteristic details of the individual, such as distinctive clothing, can be seen, whilst the view remains sufficiently wide to allow some activity surrounding an incident to be monitored.
Recognise	**50%**	Viewers can say with a high degree of certainty whether or not an individual shown is the same as someone they have seen before. Alternatively a vehicle number plate should be identifiable.
Identify	**100%**	Picture quality and detail should be sufficient to enable the identity of an individual to be established beyond reasonable doubt.

Source: HOSDB

So as an example an effective perimeter Video Assessment capability would not only require full coverage of the entire perimeter but also for a human-sized target to occupy 10% of monitor screen height at any point around the perimeter, therefore allowing an operator to quickly identify the presence of the intruder following an alarm activation. To achieve this it will often be necessary to limit the length of detection zones such that associated cameras can deliver images of the target at 10% monitor screen height (usually to a maximum of 100m but quite often down to 50m depending upon the camera and lens selection). However, some perimeter IDS technologies can provide accurate detection within each zone (typically via software-defined sub-zones), thereby allowing larger camera separation distances whilst still achieving the required Target Image Height.

A second example where Target Image Height could be specified is in the context of a door leading into a critical room. On receipt of an alarm from the ACS the camera could display an image of the person entering through the door with a Target Image Height of 100% thereby ensuring that the identity of any intruders can be established beyond reasonable doubt.

B1.3 Resolution

The next performance parameter to consider is that of video resolution, which can also have a significant effect on Video Assessment capability. This is particularly so with contemporary technologies – the original research done by HOSDB and others with regards to suitable Target Image Heights for varying applications was based upon the PAL analogue video standard with a common video resolution of 576 vertical lines. However, with the advent of digital imaging technologies, resolutions of 1080p (1,080,000 pixels) or greater are now common and have the potential to reduce the required Target Image Height. For example HOSDB estimate that a 1080p video resolution may only require a target to occupy 38% of the monitor rather than PAL's 100% in order to achieve the 'Identify' function (the HOSDB guidance document provides further information on this including a conversion table for common digital resolutions).

However, just as higher video resolutions have the potential to improve Video Assessment capability, lower resolutions can significantly degrade it. When considering the issue of resolution it is important to be aware that real-life performance will be determined by the weakest link in the chain – which consists of camera, compression algorithm (for digital IP cameras), transmission medium, video management system and video monitor. So just because a camera has the capability to transmit 1080p images does not mean that the operator will benefit from this resolution – for example bandwidth limitations may require the image to be heavily compressed for transmission over the network, or the monitor may only support SVGA resolution. In this respect it is important to assess resolution at the monitor rather than rely upon theoretical camera specifications or get caught up with manufacturer's jargon, particularly relating to their claims regarding the benefits of 'megapixel' cameras. Although they can bring benefits to certain applications there are many other performance issues to consider. For example many megapixel cameras perform poorly under uneven or challenging lighting conditions since the size of the pixels are typically much smaller than those in standard definition cameras (because they need to squeeze more of them onto the sensor) and therefore cannot collect as much light. So in this respect pixel size is equally if not more important than the number of pixels, and whilst megapixel cameras may offer advantages in well lit environments where extra detail is beneficial, a standard definition camera is likely to be much more suitable for a typical energy facility perimeter application where there is a requirement for 24-hour surveillance under varying lighting conditions.

B1.4 Visibility

The next and possibly most important parameter to consider in relation to Video Assessment is that of Visibility – if the target is not clearly visible in the video image the operator will not be able to accurately assess the cause of alarm regardless of Target Image Height or Resolution. In this regard effective lighting is the key to successful performance since all conventional video cameras depend upon light to produce an image of the scene. When considering the use of both existing lighting and dedicated security lighting the following factors will determine suitability to support the Video Assessment function.

1. Lighting Type

For accurate colour image reproduction white light is required and can be provided by a variety of lamp technologies such as LED, Halogen and Metal Halide. Some lamp technologies such as Low-Pressure Sodium or High-Pressure Sodium are much less suitable for video applications since they emit orange or yellow light which produces poor colour rendition. Unfortunately they are commonly used as general background lighting and in this case should be supplemented with dedicated security lighting. This security lighting can either be activated during hours of darkness or on alarm only, in which case the chosen technology should provide near-instantaneous re-strike/switch-on times.

For some applications infrared (IR) security lighting can also be considered, providing a covert or semi-covert form of lighting suitable for monochrome image reproduction. This can be particularly useful where it is necessary to minimise light pollution or maintain anonymity of the site. However, it is important that IR-compatible cameras and lenses are used in such applications in order to provide accurate image reproduction under IR lighting conditions.

Where PTZ cameras are used in the Video Assessment system consideration should be given to directional security lighting mounted either side of the camera unit, and with the capability to provide even coverage throughout the camera's anticipated field of view and distance range. This type of directional lighting often delivers greater performance than static lighting because it allows the camera to operate when looking beyond well-lit areas, particularly for example outside of the perimeter where background lighting levels will be beyond the control of the facility owner/operator.

2. Lighting Level

Lighting levels or 'luminance' can be measured in either Lux or Foot Candles (1 Ft-C = 10.764 Lux). A digital lightmeter can be used to establish Lux levels with readings taken 30cm above ground level at regular intervals. Depending upon the security application in question a differing Lux level may be required to support effective Video Assessment. However, as an approximate guide a minimum of 5 Lux is required for colour images and 1 Lux for monochrome images.

Where PTZ cameras are used in the Video Assessment system consideration should be given to directional security lighting mounted either side of the camera unit, and with the capability to provide even coverage throughout the camera's anticipated field of view and distance range

3. Surface Reflectance
Lighting levels also need to be considered in relation to Surface Reflectance – the amount of light that is reflected from a given surface within the assessment area and therefore back to the camera lens to allow an image to be reproduced. Some surfaces reflect significantly more light than others – for example: Snow = 90%; Grass = 40%; Brick 25%; Black Top 5%. As such the amount of light necessary to produce an image will vary dramatically and could be up to 15 times greater for black surfaces compared with white surfaces. Whilst manufacturers typically claim that cameras will work at levels as low as 0.1 Lux in colour mode this is usually based upon surface reflectance of between 75%-90% (a white surface), which is rarely the case in most environments (hence the earlier recommendation of at least 5 Lux for colour video imaging).

For the purposes of Video Assessment surface reflectance should ideally be 60% or greater. This could be achieved for example by the use of white/grey gravel throughout the assessment zone, which is common for high-security perimeter sterile zone applications. This also provides a clear and uncluttered assessment area in which the intruder is likely to stand out from the background even with smaller Target Image Heights. Where dark surfaces are unavoidable it may be necessary to compensate for this through the use of security lighting with higher Lux levels.

4. Lighting Distribution
The even distribution of light throughout the assessment area is also vital for clear video images to be achieved. Shadows, uneven lighting and areas of contrast will obscure details in the video image and effectively result in much lower perceived resolution. This may be caused by both inadequate security lighting as well as light pollution from other sources such as gas flares and plant process lighting. As highlighted earlier this is a particular issue for many megapixel cameras due to the smaller pixel size. Similarly cameras with smaller image sensors such as ¼" CCD sensors, which are found in most 'Dome' cameras, will struggle to provide clear and crisp imagery under such challenging lighting conditions as found at many energy facilities. Therefore, where these conditions are unavoidable it is preferable to use cameras with larger physical sensors such as ½" CCD sensors, and/or sensors with larger pixel sizes. However, if possible, even lighting should be implemented using supplementary security lighting as required. In this respect a useful performance measurement is the ratio between average light levels and the darkest light levels, which should be no more than 3:1 (an equivalent alternative is a light:dark ratio of 6:1). Again this can be established via a lighting audit and use of a Lux meter, setting up a grid of 1m squares throughout the assessment zone and taking a reading in each square.

Where visible or IR lighting cannot meet all of the above requirements it will be necessary to consider other types of camera technology such as the use of Thermal Imaging Cameras which do not require any background lighting. Thermal Imaging Cameras can be particularly useful where it is necessary to cover long distances, avoid light pollution or operate covertly. However, since they typically provide a lower resolution image than conventional cameras they are less suitable for applications which require the ability to recognise or identify intruders.

B1.5 Environmental Suitability
A Key Performance Consideration in the context of energy infrastructure security is the suitability of outdoor Video Assessment Systems for the environment in which they operate, which will generally be considerably harsher than a typical commercial security application. As such the design of cameras systems and related equipment needs to take account of local environmental factors. Some examples of this are provided below:

- Cameras may require a remote-activated wash-wipe system to remove water, salt and debris from the housing screen and thus maintain good visibility. This is particularly the case in environments with frequent heavy rainfall, high saline content (i.e. adjacent to the sea), or dusty environments. Manual cleaning of cameras is inefficient and time-consuming particularly where they are spread across a large facility
- In windy locations it will be necessary to mount cameras on stable tri-axial towers (rather than poles) to reduce camera shake. Similarly this will also be required for cameras with large zoom lenses since any movement at the camera will be magnified
- Where an explosive atmosphere exists at a facility, as is common with many gas processing sites, it will be necessary to install security systems that are intrinsically safe and cannot act as a source of ignition. In this case explosion-rated equipment manufactured and operated in accordance with ATEX standards (European Directives 94/9/EC (ATEX 95) and 99/92/EC (ATEX 137)) will be required
- All Video Assessment components, as well as other security systems components should also be physically protected in environmental housings against anticipated environmental conditions including rain and dust, to ensure continuous and reliable operation. To achieve this components can be specified to meet various Ingress Protection (IP) codes as set out in EN 60529:1992. For example a housing rated to IP67 would provide protection against dust, light, and temporary immersion in water
- Where lightning is a possibility (the majority of locations) camera towers should be earthed to a local common ground in order to avoid damage during lightning strikes

Hopefully it is evident from the above examples that site-specific environmental conditions can play an important role in determining the performance of the Video Assessment system as well as other security systems, and should therefore be accounted for in the design process. The following sections move on to discuss the remaining Alarm Assessment sub-systems – Alarm Communications and Alarm Control & Display.

B2. Alarm Communication

The second Alarm Assessment sub-system is that of Alarm Communication, which in this context refers to the transmission of data, video and sometime audio signals between field-based equipment and control room equipment, thereby allowing alarm signals to be processed, cameras and other devices to be remotely controlled and assessment information such as video images and alarms to be displayed to operators at central monitoring locations. Although quite a technical and complicated area it is important to be aware of some Key Performance Issues pertaining to the Alarm Communication Sub-systems, as discussed below.

B2.1 Physical Transmission Paths

Depending upon the application there are a variety of physical transmission mediums that can be used for Alarm Communications and whilst a detailed examination of each of these is beyond the current scope of the Security Management Plan, a brief summary of the main ones that you may come across is provided in table 7 below:

Depending upon the application it may be that several different transmission mediums are required – for example fibre optic communications from field-based devices to the control room, structured copper cabling within buildings and possibly wireless communications between two sites where it is not feasible or cost-effective to install physical cabling. It is likely that specialist advice will be required to establish your exact requirements in this area as there are many more considerations than can be listed here.

Table C3g: **Physical Transmission Paths**

Transmission Medium	Applications
Coaxial Cable	Commonly used for video transmission in analogue CCTV systems. Transmits an electrical signal from the camera to the monitor, however suffers electrical impedance over distance and therefore only effective for shorter distances preferably no more than 500m – for example over a distance of 1,000m a signal loss of >40% would be experienced. Electrical interference from external sources can have significant impact on picture quality.
Unshielded Twisted Pair	Similar to coaxial cable except it provides a balanced signal between two wires and therefore suffers from less electrical interference. Requires either passive or active transmitters and receivers, the latter allowing transmission over distances of up to 1,500m.
Network Cable	Used for IP-based transmission over Ethernet Networks, most commonly in the form of Cat5e cabling which supports up to Gigabit Ethernet or Cat6 cabling which can support 10 Gigabit Ethernet, in both cases certain distance limitations apply. Available bandwidth will depend upon specification of switches, routers and network architecture, as well as bandwidth consumption by other devices and software limitations to prevent network congestion.
Fibre Optic Cable	Video and data is converted from electrical to optical signals for transmission over fibre optic cable – can be used to transmit both uncompressed analogue signals and compressed IP signals. Offers the greatest available transmission distances and least signal loss of any transmission medium, whilst also being intrinsically safe for explosive environments and difficult to tap into the signal undetected. Whilst originally very expensive, costs of fibre optic transmission are now very reasonable and it should be the preferred option for all large-scale security applications.
Wireless Transmission	Where physical cabling is not practical or too expensive wireless transmission can be considered for both analogue and digital systems. Various technologies exist depending upon the application, the most common being point-to-point microwave transmission, although more recently wireless mesh networks and 3G cellular networks have been used for security applications. There will usually be significant bandwidth limitations as well as various environmental conditions that could impact upon performance and reliability.

Source: PRISM™

B2.2 Redundancy

Whichever physical transmission medium is used for Alarm Communication, consideration should be given to the need for Redundancy, particularly in a high-security context. This will ensure that if the transmission path is accidentally or maliciously damaged the security systems will continue to function and the Alarm Assessment capability will remain intact. Where this is deemed to be a requirement it is important that the design provides physical redundancy via diverse transmission paths – if for example redundancy relies upon two cores within the same fibre optic cable it will be of little benefit when the cable is cut in half!

B2.3 The 'Analogue vs IP' Debate

One of the most important considerations in the area of Alarm Communications is whether the transmission of video will be based upon uncompressed or compressed communications, often referred to as 'Analogue vs IP Systems'. This will have a dramatic impact upon all other areas of the Physical Security System, including equipment choice, video image quality, recording, integration between various sub-systems, cost, operations and maintenance.

You will most likely be aware of the very high-profile introduction of IP-based CCTV systems a number of years ago and their gradual increase in popularity over traditional analogue CCTV systems, to the point where the latter are often completely dismissed for many new projects. However, as with other areas of technology this is as much to do with marketing and the commercial interests of leading manufacturers than it is do with performance, therefore it is worth discussing this area briefly.

The original promise of IP security technology was to dramatically reduce costs associated with transmission by enabling video and data signals to be transmitted over existing corporate IT networks, thereby removing the need for, and expense of, dedicated security cabling. However, within a few years it became apparent that for all but the smallest of applications existing IT networks did not provide adequate bandwidth to support video transmission, which requires vast amounts of bandwidth when compared to other data. As such the focus subtly shifted towards the flexibility offered by IP-based systems, particularly in terms of the ability to view and control any camera from any point on the network (using it as a 'Virtual Matrix System'), and to easily integrate with a range of other electronic systems such as Building Automation. In this respect IP certainly has many advantages over analogue systems, particularly for multi-site corporate applications and has understandably become popular. However, analogue systems (which in fact should not really be labelled as such since they now consist of mainly digital components) also have some significant advantages, particularly for infrastructure security applications.

The challenge for IP systems remains the fact that associated networks have a limited bandwidth capacity that has to be shared amongst all cameras and whilst this is steadily increasing with improvements in technology it is still rapidly used up by large video systems with hundreds or even thousands of video cameras. In effect this means that it is necessary to heavily compress images in order to reduce their size and therefore the amount of bandwidth it takes to transmit them over the network. As an example an uncompressed video stream from a single camera would take up the equivalent of around 140Mbit/s whilst a typical compressed video stream would use around 1Mbit/s or less – a significant difference which results in both reduced image quality and transmission latency (i.e. delays). In addition it is often necessary to reduce camera frame rates and resolution to minimise bandwidth utilisation, and/or to transmit video only on demand, which (particularly in the case of the former) could risk compromising the Video Assessment function. In contrast the use of uncompressed transmission particularly over fibre optic cable ensures that the image produced at the video camera is re-produced on the monitor instantaneously, at full frame rate and with virtually no loss in quality. Whilst some reduction in image quality is acceptable for most commercial applications, it can be problematic for infrastructure applications where cameras have to cover large areas under challenging lighting conditions, and where system response time is a key factor in effective Alarm Assessment (as discussed further in section B4).

So regardless of the marketing hype that you will no doubt have been exposed to, IP is not necessarily the de facto choice for new security projects – uncompressed transmission should also be considered for challenging environments particularly where image quality is more of a priority than flexibility. In this respect it is telling that many specialists in Critical Infrastructure security, whether manufacturers or design consultants, frequently state that IP is yet to deliver anything close to the performance of analogue in this context (albeit that they are also subject to the same industry pressures to move towards IP and so don't always go about making a point of this!)

All of this is not to say that IP-based systems cannot deliver in this type of environment, just that it is important to be aware of the unique demands of large energy infrastructure projects, which are dramatically different to your average commercial office or retail store, at which much of the latest technology is aimed. Therefore, it is vital to ensure that IP-based systems as a whole are very carefully designed to overcome inherent limitations, for example through careful network planning, reduced camera separation distances, or strategies to minimise the volume of video data sent across the network.

In fact an increasingly successful approach in the context of infrastructure security projects is to implement a hybrid option which aims to take advantage of the benefits of both types of system, whilst minimising their potential shortfalls. This could be implemented via the use of uncompressed video transmission over fibre optic cable from field-based cameras back to the primary monitoring location, thereby ensuring that operators have live, high-quality images upon which to base their Alarm Assessment, and subsequently providing a separate video output onto the network for display at other locations and integration with other systems.

There are of course many other factors which may influence the decision over whether to use analogue or IP-based security systems (not least the IT Manager's opinion!) and you will undoubtedly require specialist advice in this area. However, hopefully this discussion has provided you with a more balanced view of the subject than you will get from the media and many manufacturers and installers.

B2.4 Alarm Communication Security

Another important consideration for many energy facilities, particularly the likes of nuclear power stations and other high-risk Assets, will be the security of the data sent across the Alarm Communication system. If an adversary has the capability to intercept or interfere with this data it could make the security system as a whole vulnerable to compromise. As highlighted in the transmission table, fibre optic cable is probably the most difficult to tap into undetected since any such attempt can be identified as a reduction in signal strength providing that the fibre optic network is monitored (this type of network monitoring can be implemented very cost-effectively). On the other hand wireless communications are inherently the most vulnerable to intercept.

In order to reduce this vulnerability there are various types of encryption that can be applied to the Alarm Communications data and this is usually a worthwhile measure to implement. However, for video data the level of encryption applied will have a direct impact on transmission speed and bandwidth since it requires additional processing of the video signal. Therefore, there is usually a compromise between the two and so it will be necessary to consider the capability of threat sources as identified in Phase B in order to decide upon the right balance.

With IP-based Video and Alarm Communications there is an even greater inherent vulnerability since they are effectively transmitted over an open network, usually with multiple connections to the public internet. A quick internet search will highlight many resources for hacking IP Video systems, including video demonstrations showing how it is possible to take control of cameras and effectively bypass security.

These vulnerabilities have largely been suppressed or overlooked within the mainstream security market, in part because they are less relevant to lower-risk commercial applications which make up the bulk of the market space.

Although the vulnerability of IP-based security systems can never be completely eliminated there are a number of countermeasures that should be implemented, including the following:

- Where possible it is preferable to have a separate physical network dedicated to Security Systems transmission (this will also ensure that bandwidth utilisation from security data does not compromise business data and vice versa)
- Security Transmission over a dedicated Local Area Network (LAN) with no external connections will be far more secure than transmission over a Wide Area Network (WAN) that uses public internet or telephone connections
- Where security data uses the same network as other corporate or public data it should be transmitted within a dedicated and encrypted segment of the network or 'tunnel', known as a Virtual LAN (VLAN)
- Connections between security LANs and other parts of the network should be firewall protected
- Browser access to video streams should be limited to essential personnel only and password protected

It will be necessary for you to take advice in this area from the IT department and perhaps also external specialists, in order to ensure that a level of communications security appropriate to the facility's risk profile is adopted.

> *Another important consideration for many energy facilities, particularly the likes of nuclear power stations and other high-risk Assets, will be the security of the data sent across the Alarm Communication system.*

B3. Alarm Control & Display

The final Alarm Assessment sub-system is that of Alarm Control & Display, which provides the integration platform for all individual detection components including Interior and Exterior Intrusion sensors, Access Control devices, video cameras and lighting, and communications networks. As such it allows alarm signals to be received and processed, associated cameras to be switched into position, and video alarm images to be displayed to an operator for assessment, thereby completing the detection function. Although with smaller systems some of the control and display functions will be carried out manually, for large applications autonomous and seamless operation will be essential for effective Alarm Assessment.

In the past it has been common to have separate management platforms for each main sub-system (Video, Access Control and IDS), however, more recently technology has moved on to allow these to be integrated together to create a single platform, providing greater speed, efficiency and ease of use, and thereby enhancing Alarm Assessment capability. There are various methods for achieving this, including the following:

- **Integration of Video and IDS into the Access Control System (ACS)** – Traditionally it has been common for the ACS to be used as the main integration platform with video and IDS alarms viewed from within this environment. Although this works well for typical commercial applications, the level of sophistication in respect of video and alarm functions is often limited and therefore where these are high priority (as is common in most large infrastructure security systems) it is often more effective to use the Video Management System as the primary platform
- **Integration of ACS and IDS into the Video Management System (VMS)** – More recently Video Management Systems are offering greater support for integration of ACS and Intruder Alarms, as well as supporting functions such as remote operation of system doors and updating key settings. Although much of the administration of IDS and ACS will still need to be done separately, it allows operators to carry out their Alarm Assessment duties from within a single system, whilst retaining more sophisticated video functions
- **Integration of Video, ACS and IDS under a dedicated Security Management System (SMS)** – There are now several technologies on the market that are designed specifically as a single management platform for Video, ACS and IDS (as well as other electronic security and building automation systems). These Security Management Systems (SMS), sometimes also referred to as 'Physical Security Information Management' (PSIM) Systems can offer a powerful alternative to systems designed primarily for a single function, whilst some of them also perform additional tasks to help increase operator efficiency and reduce response times, such as the provision of instructions and procedures for operators to follow in response to certain types of incident

For most energy facilities the use of either a VMS or SMS platform is likely to provide the greatest level of performance in the area of Alarm Assessment and in each case the system should provide a single Graphical User Interface (GUI) which displays alarms, alarm zones and camera locations on a map of the site to greatly assist the operator in his role. However, all systems currently have limitations in terms of support for third-party systems and components (including IP systems, which up until now remain largely proprietary and require Manufacturers to release Software Development Kits to allow third-party integration). Therefore, when considering these technologies it is important to understand your requirements for integration of both existing and future electronic security systems and components, and ensure that the chosen manufacturer or system offers the capability to provide this. There is nothing more frustrating than making a significant investment in security and realising a few years later that it is not flexible enough to support new technologies that you now wish to utilise.

There are also various strategies to be considered in terms of how alarm and video information is handled within the management system, depending upon the requirements of the facility, the number of cameras and alarm sources and the number of operators. However, it is usually advisable to have dedicated alarm monitors separate to those used for general monitoring, so that when an alarm occurs it is immediately obvious to the operator that they need to make an assessment of the video, and it is also clear which video image corresponds to the alarm. In some cases it may be that video is only sent to the control room on alarm in which case the alarm screen will usually appear as a blank monitor until such a time as an alarm is activated.

Similarly it is also important that alarms are given priority within the system over all other monitoring activity, so that in the event of an alarm activation any other use of cameras is overridden to allow the images to be displayed for assessment. For some energy facilities video cameras may have a dual purpose – Alarm Assessment and process monitoring. Where both roles are considered critical it is advisable to have separate cameras and supporting infrastructure; however, where process monitoring is a secondary function it can be separated logically by the system, also by setting priority levels for different actions, operators or workstations.

With large systems the design and layout of the Control Room environment becomes increasingly important and will play a significant role in the extent to which Alarm Assessment can be carried out efficiently and with minimum delay. A significant amount of research has been conducted in this area and much of this is captured in the international standard BS EN ISO 11064 'Ergonomic Design of Control Centres'. It is therefore suggested that the control room design is compliant with this standard, including furniture and ancillary equipment. However, it also important that this is placed within the context of local operating requirements and to this extent it is necessary to map out all of the tasks that will take place in the control room and ensure that it is designed to optimise workflow efficiency.

Taking account of the above considerations will ensure that the Alarm Control & Display sub-system successfully integrates the other sub-systems into an efficient and seamless Alarm Assessment platform, and as such will be of central importance to the overall Detection function.

B4. System and Operator Response Time

Before moving on to consider Alarm Assessment System applications and example Performance Requirements, it is worth introducing two final performance parameters – System Response Time and Operator Response Time. System Response Time refers to the amount of time between an intruder activating an alarm and a video image of the event being displayed on the operator's monitor, whereas Operator Response Time refers to the length of time between the alarm image being displayed on their monitor and them identifying the cause of alarm/location of intruder.

For many detection applications there will only be a finite period of time after an alarm activation in which the intruder is visible within the detection zone and therefore it is essential that this activity is identified, which will only occur if both System and Operator Response Time are adequate. As such they are vital to the overall effectiveness of the Alarm Assessment function and a key indicator of how all three sub-systems (Video Assessment, Alarm Communications, Alarm Control & Display) are performing as an integrated system. Each of these parameters are now explored:

B4.1 System Response Time

The importance of the System Response Time parameter can be highlighted via a typical perimeter intrusion scenario. An intruder climbs over the perimeter security fence, in doing so activating a fence alarm, and once over the fence runs into the site passing through the video assessment zone in a matter of seconds. Presuming that the fence-mounted IDS is integrated with the Video Assessment system the video matrix switch will receive the alarm signal and either display the video image from the associated fixed camera(s) on the operator's alarm screen, or move the associated PTZ camera(s) into its pre-set position for the alarm reporting zone and then display the images on the operator's alarm screen. Subsequently the operator must identify the intruder within the video image, verify that it is a genuine threat and identify the direction of travel of the intruder so that a response can be sent to the right area or they can be tracked manually with adjacent cameras.

From this scenario it is clear that if the System Response Time is too long in duration the intruder will have already passed through the detection zone and as such the operator will be staring at an empty video image when it is displayed for assessment. In a worst-case scenario this will lead to a false alarm being declared when in actual fact an intruder is now inside your facility! It may also be apparent that System Response Time differs significantly according to whether or not fixed or PTZ cameras are used since the latter has to be moved into its alarm reset position before the image can be assessed by the operator. For this reason fixed cameras have traditionally been used in high-security applications in order to reduce System Response Time (and ensure that coverage is dedicated to Alarm Assessment). However, this requires shorter separation distances between cameras (typically 50-100m) resulting in increased costs of supporting infrastructure including power, communications, switching and recording systems. In addition because they have a narrow fixed field of view it is usually advisable to install PTZ cameras in a supporting role to allow intruders to be tracked.

In order to improve cost efficiency, particularly for large-perimeter applications, PTZ cameras can be considered as an alternative and providing the correct camera and lens specification is utilised, will usually allow separation distances of 200m or more, whilst still achieving a minimum 10% Target Image Height for Detection level performance (particularly where the IDS provides accurate point detection). However, if considering the use of PTZ cameras in this manner it is important to identify the available speed of the Pan and Tilt head and whether this is likely to be effective against anticipated threats. For example a common maximum pan speed is 40° per second and this would take almost 5 seconds to move the camera 180° as may be required in some circumstances. If this is not acceptable a more specialist (and expensive) Pan Tilt unit with faster speeds of up to 360° per second will be required.

Overall it is recommended for most applications that System Response Time should be between 1-5 seconds depending upon whether fixed or PTZ cameras are utilised, the former being preferable where speed is of the highest priority. Of this the electronic signalling and image display should take less than 800 milliseconds (however be warned – much greater delays can be experienced as a result of latency on poorly designed IP-based systems, due to bandwidth limitations/network congestion and/or heavy compression!). If System Response Time exceeds 5 seconds it is possible that the intruder will have already passed through the detection zone.

B4.2 Operator Response Time

Operator Response Time is also important, particularly for capable adversaries who may bypass individual security measures with significant speed. It is determined primarily by the success of the Video Assessment function – particularly Target Image Height, Resolution and Visibility of the intruder as explored previously, but also by the Alarm Control & Display functions including the extent to which effective system integration and control room design have been addressed. Although Operator Response Time may vary from anything between 1 and 15 seconds, if it is frequently taking longer than 3-5 seconds for operators to correctly assess alarm events this will indicate a significant weakness in one of the related areas, which should be rectified accordingly.

> *If System Response Time exceeds 5 seconds it is possible that the intruder will have already passed through the detection zone.*

C. Applications

In order to complete the Detection function it will be necessary for you to ensure that the facility of concern has a robust Alarm Assessment capability in place, in line with its Risk-based Performance Requirements established previously. In this respect it is important that you differentiate between general video surveillance/monitoring systems, which most facilities will already have in place, and systems which are event-driven and can provide true Video Assessment of all alarm sources, whether from Exterior and Interior IDS or the Access Control System.

It is also important that the Video Assessment sub-system offers adequate performance in terms of Coverage, Target Image Height, Resolution, Visibility and Environmental Suitability to facilitate effective assessment of alarm incidents. For smaller facilities this may be limited to key buildings or entrance points; however, for larger facilities this could include full Video Assessment capability around the entire perimeter of the site, and within specific high-risk areas such as Transformer Bays, Gas Stations and around Chemical Storage Tanks.

All of the data from alarm and video devices will need to be transmitted over a communications network for subsequent Control & Display, which may take the form of a dedicated fibre optic transmission network, structured copper cable network or even via wireless transmission in some cases. A key decision will be whether to use compressed or uncompressed transmission, both of which may be suitable depending upon the specific requirements and context. It will therefore be important to gain input from key Stakeholders and perhaps external specialists when making this decision, rather than simply relying upon advice from manufacturers and installers who, despite sometimes being a useful point of information, will also have their own commercial biases.

For most large systems it will be necessary to implement a sophisticated Security Management System to provide Alarm Control & Display functions, often within a dedicated Security Control Room, or an existing Operations Control Room where this is practical. When deciding upon the location for the Control Room it is important to ensure that it will not be compromised in the event of a major incident, either directly by damage being sustained to the building, or indirectly by having to evacuate the building. Therefore it should be located away from vulnerable areas such as the main entrance, and preferably in an inherently secure area such as the centre of the site. Where this is not possible the supporting Alarm Control & Display server racks should at least be installed in a protected space, whilst it would also be advisable to have a fail-over location for monitoring in the event that the primary location is lost.

D. Performance Requirements

The following table provides some examples of Key Performance Requirements for the Alarm Assessment System, and can be used as a starting point for developing your own set of requirements based on the type and level of risks facing the Asset and the agreed Protection Objectives established previously.

Table C3h: Alarm Assessment System Performance Requirements

Area	Ref	Example Performance Requirements
Video Assessment Sub-system		
Coverage	PR1	The Video Assessment system will provide full coverage of the entire perimeter of the site. All potential blind spots will be addressed with additional cameras where required.
	PR2	The Video Assessment system will provide full coverage of all vehicle and pedestrian entrances into the site and designated buildings within the site.
Target Image Height	PR3	An intruder of average height at any point around the perimeter will occupy a minimum of 10% Monitor Screen Height.
	PR4	Persons entering and exiting through all perimeter and building entrances will occupy a minimum of 100% Monitor Screen Height.
	PR5	Vehicles entering and exiting through all perimeter and building entrances will occupy a minimum of 50% Monitor Screen Height.
Resolution	PR6	The resolution of all perimeter cameras will be a minimum of 300 TVL, measured on the display monitor.
	PR7	The resolution for all cameras covering entry and exit points will be 400 TVL, measured on the display monitor.
Visibility	PR8	Dedicated LED Security lighting will be installed around the perimeter of the site, providing a minimum of 5 Lux illumination for 5m either side of the fence line.
	PR9	There will be a maximum average to dark:light ratio of 3:1 throughout the perimeter Video Assessment zone.
Environmental Suitability	PR10	All external video cameras will be fitted with a remote-activated wash-wipe system and will be enclosed in environmentally sealed housings rated to IP66 standards.
	PR11	Cameras will be mounted on demountable tri-axial towers, which will be provided with a local earth spike to protect against lightning damage.
Alarm Communication Sub-system		
Physical Transmission	PR12	A fibre optic transmission network will be installed around the site to provide live transmission of all video and alarm data back to the Control Room.
Redundancy	PR13	The fibre optic transmission network will provide physical redundancy in the event of damage to the cable or transmission units at any point in the network.
Compression	PR14	Video from all external cameras will be transmitted in live uncompressed format back to the primary monitoring location.
Security	PR15	All alarm communications will be encrypted to industry standards to prevent external interference.
	PR16	A dedicated security LAN will be used for alarm communications within the operations building, and any connections with other networks will be firewall protected.
Alarm Control & Display Sub-system		
Operation/ Integration	PR17	An IDS alarm at any point around the perimeter of the site will automatically switch a minimum of two CCTV cameras to their pre-set positions for the alarmed zone or sub-segment. All other system use will be overridden to allow this.
	PR18	The SMS will provide full integration with the IDS such that all alarms are displayed on a common GUI and can be processed within the SMS environment.
	PR19	The SMS will provide full integration with the AACS such that access events automatically trigger switching of adjacent cameras and that all main AACS functions (process alarms, activate and disable doors etc) are available from within the SMS environment.
	PR20	The SMS will provide integration options with a wide range of third-party technologies, and the manufacturer will make SDK codes available for any bespoke integration required in future.
Control Room Design	PR21	The Control Room layout will be designed in accordance with BS EN ISO 11064 standards and will provide dedicated workstations for each main type of operator role, such as IDS Assessment, Access Control, Supervision.
	PR22	The Security Control Room will be located in the Operations building in the centre of the site, with separate access controls. All server racks will be contained within a dedicated and physically protected communications room.
System Response Time	PR23	The System Response Time, measured from the time an alarm is triggered to the time that an alarm image is displayed on the video monitor, will be no more than 5 seconds.
Operator Response Time	PR24	The Operator Response Time, measured from the time the alarm images are displayed on the video monitor until the time the operator has correctly classified the cause of alarm will be no more than five seconds.

Source: PRISM^{TM}

C3.2 Delay

Delay

- The ability to delay attackers or protect against the cause of the incident long enough for a successful response to be initiated.

The delay capability is divided into three layers to provide the protection in depth principle outlined earlier in this section; these are:

1. **Perimeter Delay**
2. **Building Delay**
3. **Component Delay**

These three layers are made up of actual physical obstacles that an attacker must overcome to reach a point or area of specific security interest. The primary components that can be used to create the required level of delay in each area are shown in the following diagram:

C3.2.1 Perimeter Delay

- Topography
- Security Fencing
- Vehicle Barriers
- Pedestrian Barriers

C3.2.2 Building Delay

- Exterior Building Structure
- Building Access Points
- Strongrooms and Security Enclosures
- Protected Spaces

C3.2.3 Plant Delay

- Compounds
- Hatches and Enclosures
- Specialist Barriers

Measures should be selected with known delay performance characteristics to meet the requirements identified in Section C1, where necessary referring back to Adversary Sequence Diagrams, i.e. if a successful response will take 10 minutes to mount then it will be necessary to implement physical measures that will collectively provide at least 10 minutes of delay against anticipated threat sources and attack methods.

The delay function comprising elements of the above layers and sub-layers must be integrated with the detection function described in the previous section and the response function described later to form part of the integrated approach to Physical Security in the Security Management Plan. A determined attacker will eventually defeat an isolated physical barrier but the barrier combined with the detection function and appropriate response should achieve the Protection Objectives identified earlier in the process.

C3.2.1 Perimeter Delay

A. General Characteristics

A perimeter offers a clearly defined demarcation of an external area around a site and of the site itself. The perimeter also acts as a channel for vehicles and pedestrians to site entry/exit points where there are access control measures in place. A larger site may have several smaller perimeters or compounds internally around Critical Assets. A perimeter can be formed by a natural boundary, a purposely constructed fence or wall, or the exterior walls of a building. Each access point within a perimeter is a weak point and as such they should be kept to a minimum.

B. Sub-systems

B1. Topography

The topography of the area within which a site is located, in terms of the physical features of the land, can be effectively utilised to contribute to the delay function by providing barriers which make it difficult for adversaries to access the facility and therefore offer inherent security. Equally topography can also create specific vulnerabilities that need to be addressed through separate measures – for example a vulnerability to waterborne attack if the facility is located next to major rivers or the sea, or a vulnerability to vehicle attack if favourable gradients or traversable surfaces surround the Asset.

Some topographical features that can enhance the delay function include:

- Small rivers, moats or lakes (but preferably with no access from public waterways or the sea) can limit the opportunity for vehicle attack and make intrusion more difficult
- Hills and significant gradients which can protect against vehicle attack, provide natural blast resistance or enhance the anonymity of the site
- Ditches, small canyons or large rocks that help to slow movement of both people and vehicles towards the facility

Topography can be best utilised as part of the security function on new-build projects where there is an opportunity to influence site location, layout and civil design. In this respect the security department should be a Stakeholder in any new infrastructure projects, with involvement from concept stage onwards and representation on the project team. For large projects it is also worthwhile creating a Security Master Plan which clearly defines your security requirements in this and other areas and provides a framework within which the design engineers can operate.

For existing sites it is sometimes worthwhile to alter the existing topography of the land to establish an alternative perimeter or protect vulnerable areas of the site. For example a v-shaped ditch could be dug to protect areas against vehicle attack, landscaping could be used to create a natural blast berm, a watercourse could be extended or diverted to block access, or hedgerows and thorn bushes could be planted to provide privacy and delay against opportunistic intrusion. These types of measures can be further enhanced or reinforced by other components of the Physical Security System.

B2. Security Fencing

Security fencing can be used to demarcate a perimeter or restricted area, channel people to the appropriate access point, separate hazardous and non-hazardous or public areas, deter casual intrusion or rule-breaking, and provide some initial delay to more determined intruders. It is a common measure at most infrastructure facilities and will most likely form part of your Physical Security System in one form or another. However, it is also important to understand that most types of security fencing can be overcome by capable adversaries in a short period of time, either by tunnelling, bridging or cutting attacks. So whilst it may offer reasonable assurance against opportunistic attacks, secondary delay measures, as well as appropriate detection systems, will be essential to protect against certain threat scenarios.

There are a variety of different types of security fencing available, generally falling into one of the following categories:

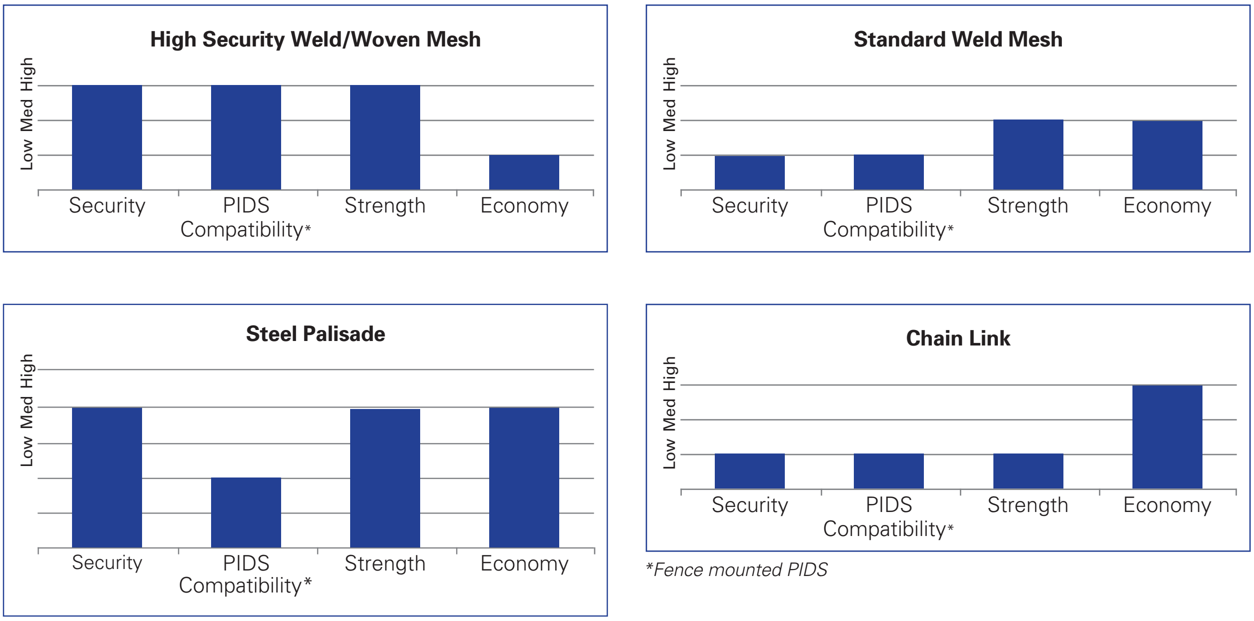
- High security weld/woven mesh
- Steel Palisade
- Standard weld mesh
- Chain link

The level of delay provided by each of these fencing types against climbing, cutting or bridging attacks can vary from around 10 seconds for basic chain-link fencing up to around 3 minutes for well-designed High-Security weld mesh fencing, which will typically use two layers of heavy duty weld mesh back to back, with a fence height greater than 4m, anti-climb topping, and concrete sill. As you would expect costs also vary accordingly.

Security fencing can be used to demarcate a perimeter or restricted area, channel people to the appropriate access point, separate hazardous and non-hazardous or public areas, deter casual intrusion or rule-breaking, and provide some initial delay to more determined intruders.

A general comparison of typical performance between the different types of security fencing is presented in the following graphs:

Diagram C3b: Security Fencing Performance



**Fence mounted PIDS*

**Fence mounted PIDS*

There are also various design and construction considerations which will determine the performance of security fencing, as summarised in the following table:

Table C3i: Security Fencing Design Considerations

Design Aspect	Considerations
Construction	The height above ground and any portion of the fence buried below ground, barbed wire, concertina barb tape or any other anti-climb topping. Possible construction of a concrete sill with integrated cable containment.
Access under the fence	Any drains, service tunnels or culverts that could provide access under the fence should be avoided or protected accordingly.
Alignment	The fence line should be installed in straight lines where possible with changes in direction kept to a minimum.
Positioning	The effectiveness of the fence should not be compromised by adjacent buildings, trees or other climbing aids, foliage and other areas of cover should be avoided with the introduction of a minimum 5m sterile area on either side of the fence to enable effective surveillance and alarm assessment.
Access Points	These should be kept to a minimum and constructed to the same standard providing the same delay as the adjacent fence line.

Source: PRISM^{TM}

When specifying fencing a useful standard that can be referred to is British Standard 17222, Part 10 (Specification for Anti-intruder Fences) and Part 12 (Specification for Steel Palisade Fences). These standards provide four performance levels from 1 (Low Security) to 4 (High Security), and therefore allow products certified to these standards to be specified.

Whilst for smaller facilities it may be appropriate to install a high-security fence around the entire perimeter, larger facilities may require a layered approach to fencing with a more cost-effective fence at the outer perimeter and higher-security fencing system forming a number of smaller compounds around specific Critical Assets. For high-risk applications consideration should also be given to the installation of a double-layer fence line around the entire perimeter, creating a sterile zone in which the intrusion detection system can be placed. In this context the inner fence should also offer the highest performance since it will be used to provide post-detection delay, whilst the outer fence can where necessary be of lesser strength as its main role is to demarcate the restricted area.

B3. Vehicle Barriers

Vehicle barriers are used at access points and other vulnerable areas around a perimeter in order to protect against unauthorised vehicular access (ideally only essential vehicle access should be permitted) by providing a physical barrier which prevents or delays incursion through the perimeter. As such they reinforce access restrictions and can be used to enforce stand-off distance around Critical Assets, as well as to ensure that speed and traffic management policies are adhered to.

In line with previous risk assessments and established Protection Objectives it is important to consider the types of vehicle-related attack that could be mounted on your facility (which could include explosive attack as well as theft attempts), and the related methods that adversaries may use to try to overcome any vehicle barriers that aim to protect against these attacks. In this respect there are six main strategies that they could adopt, as outlined below:

- Parked – placing a Vehicle Bomb adjacent to the perimeter where there is inadequate stand-off to protect Assets from an explosion
- Encroachment – manoeuvring through gaps in existing barriers to bring a vehicle closer to the Asset, or tailgating through access barriers
- Penetrative – ramming through a barrier
- Deception – use of a false identification to gain access
- Duress – a vehicle driver may have been targeted to act as a mule for an attack
- Tampering – covert tampering of a security barrier to render it ineffective

The design of vehicle barriers therefore needs to account for and protect against some or all of the above attack methods, which could be used individually or in conjunction with each other, as part of a layered approach designed to accomplish the adversary's objectives. It is also important to remember that with the exception of the Deception method, all of the above methods could be used at any point around the perimeter and not just at formal vehicle entrances.

One of the most important factors to be addressed in the context of vehicle barrier design is whether barriers must be able to resist Penetrative attack (which is not just used by terrorists, but also by determined thieves attempting to gain access to locations containing high-value goods) and this should be clear from your Protection Objectives established in Phase B. Where this is not considered a significant risk, standard vehicle barriers can be selected in accordance with functional requirements (dimensions, operating speed, durability etc). However, where it is necessary to protect against penetrative attack it is important that barriers are certified to provide the required level of impact resistance. In this respect it is recommended that products certified to PAS 68 – 2010: 'Impact Test Specifications for Vehicle Security Barriers' are chosen, and that the design and installation of barrier systems also conforms to PAS 69 – 2010: 'Guidelines for the Specification and Installation of Vehicle Security Barriers'. These two standards have been developed by the UK Government's Centre for Protection of National Infrastructure (CPNI), in conjunction with Transport Research Laboratories (TRL) and the British Standards Institute (BSI). Whilst other classification systems exist internationally, the product requirements set out in PAS 68 are currently the most rigorous available. They classify performance on the basis of vehicle mass, vehicle speed, impact angle, penetration distance and dispersion of major debris (which could result in secondary damage to the Asset).

> *One of the most important factors to be addressed in the context of vehicle barrier design is whether barriers must be able to resist Penetrative attack*

It is also important that vehicle barriers, particularly those designed to prevent penetrative attacks, are designed correctly and in this respect assistance from external specialists is likely to be required. For high-risk facilities it may be necessary to carry out a vehicle dynamics assessment to identify possible attack routes, vehicle speeds and angles of attack, as well as blast assessments to determine the required amount of stand-off distance to protect Assets and therefore the location of vehicle barriers used to enforce this. However, many facilities will require both impact-rated and non impact-rated barriers as part of an integrated solution, and therefore some general considerations are presented in the following table:

There are also a variety of different types of barrier that may be required to protect any given Asset – ranging from entry gates through to specialist continuous barriers that can protect an entire perimeter. A selection of these barriers are presented in the following table, along with information on their typical usage.

Table C3j: Vehicle Barrier Design Considerations

Design Aspect	Considerations
Throughput	How many vehicles will be entering and exiting the site per hour or day and as such how many mechanical operations per day will be required of the barrier.
Configuration	How will barriers be configured to support the access control function, whilst preventing tailgating and encroachment. A double barrier airlock system may be required at main entrance points, or minimum separation distances between barriers may be required.
Operation	How will the barrier be controlled – what type of integration with the ACS will be used, what safety features such as warning lights and sensors will be required. Will mechanical operation be possible in the event of a power failure.
Alternative routes	A survey of the site to identify any routes including angles of attack other than those leading to access points that could be used by a threat vehicle to penetrate the perimeter, specialist advice or Vehicle Dynamic Assessment may be required.
Foundations	Whether the space is available to accommodate the foundations for a vehicle barrier as essential services or tunnels running below ground may inhibit the installation of the barrier, specialist advice may need to be sought to clarify this issue.
Actual space	Whether the intended area of installation is adequate to accommodate the barrier.
Traffic calming measures	Could traffic calming measures be introduced to assist in mitigating the threat; Traffic management – how is the introduction of the barrier going to affect the normal flow of traffic if at all.
Environmental conditions	Such as flooding, snow and ice that may affect the barrier's operation or the traffic management.
Road conditions	The camber, surface, kerbs or other factors could affect any barrier installation.

Source: PRISM™

For high-risk facilities it may be necessary to carry out a vehicle dynamics assessment to identify possible attack routes, vehicle speeds and angles of attack, as well as blast assessments to determine the required amount of stand-off distance to protect Assets and therefore the location of vehicle barriers used to enforce this.

Table C3k: Alternate Barrier Types

	Impact-Tested Product (to PAS 68:2010)		Foundations		Installation		
	Yes	No	>.5m	<.5m	Permanent	Semi-Permanent	Semi-Permanent
Gates							
• Sliding	✓	✓	✓	✓	✓		
• Bi-folding	✓	✓	✓				
• Telescopic		✓					
• Swing	✓	✓	✓	✓	✓		
Bollards							
• Fixed	✓	✓	✓	✓	✓	✓	
• Rising	✓	✓		✓	✓		
Road Blocker	✓	✓	✓	✓	✓		✓
Drop-Arm Barrier	✓	✓	✓	✓	✓		
Planters	✓	✓	✓		✓		
Continuous Barrier							
• Concrete	✓	✓	✓		✓	✓	✓
• Steel	✓	✓	✓		✓	✓	✓
Steel Wire Rope Fence	✓	✓		✓	✓		

Source: PRISM™

B4. Pedestrian Barriers

Pedestrian barriers are used to provide authorised access through a designated entry point in the perimeter, and also to allow emergency egress if required. As with vehicle barriers they should be of a comparable standard to the adjacent security fence in order to provide adequate intrusion resistance. Pedestrian barriers within the perimeter should also be kept to a minimum and, as with the other perimeter delay measures, linked to the detection systems. There are two main types of pedestrian barrier used at the perimeter – swing gates and full-height revolving turnstiles – each of which is considered below:

Swing Gates – these are appropriate for low-risk access points or those that are used infrequently or constantly supervised. They can also be used as monitored emergency exit gates with a secure crash-pad operating mechanism. However, they are vulnerable to tailgating and therefore are less suitable for high-risk applications and those with significant throughput via electronic access control.

Turnstiles – these can be used for higher-risk applications or those with significant throughput, and are typically operated via electronic readers as part of the ACS. Full-height turnstile should be used to prevent casual bypass, whilst their design and position within the fence line is important to ensure that they do not become a climbing aid for intruders. In this respect some form of climb-over protection, such as the use of barbed tape on the roof of the turnstile, will usually be necessary.

When considering the installation of pedestrian barriers within a perimeter a number of design aspects should be addressed, including the following:

- The level of delay and attack resistance to be provided by the barriers should be identified
- It will be important to assess the likely throughput of pedestrians and ensure that barriers are specified and configured accordingly. For example a main entrance may require multiple turnstiles to provide adequate throughput
- If staff parking is offsite, the pedestrian barriers must ensure quick and efficient access for authorised personnel
- It will be necessary to monitor pedestrian barriers via the IDS and ACS to ensure that intrusions through the barriers are detected
- Pedestrian barriers may need to fail safe (i.e. open) at some facilities in order to meet local regulatory requirements.
- It should be possible to operated electronic barriers manually in the event of a power failure, for example via a key override system
- The physical locking mechanisms should not be vulnerable to defeat, or in respect of emergency exit gates should not be operable from outside of the facility
- Additional pass gates may be required to provide disabled access

As with other delay components pedestrian barriers will need to integrated with other Physical Security Systems and components in order to be effective and provide the required level of capability.

C. Applications

The layered approach to defending a Critical Asset is vital in ensuring you achieve the required delay to protect that Asset as identified earlier in the process. Consideration should be given to which perimeter delay measures can be implemented to protect the identified Critical Points, especially when located outdoors with no building delay available. Existing perimeter barriers on a larger site may be in place that may only require upgraded measures installed rather than the removal and replacement of the barrier with a high security perimeter. The creation of a sterile zone in this instance with effective detection should be considered if the area allows, this will potentially save time and resources and allow smaller, and more secure secondary layers around compounds to be constructed affording an increased delay capability to individual Assets.

Vehicle and pedestrian barriers should be kept to a minimum and if possible located within proximity to a security gatehouse to make control of access for authorised staff and visitors more manageable. The introduction of an "air lock" consisting of two forms of vehicle access barrier and space to reject access to unauthorised vehicles will enhance the controllability of vehicular access onto site, and reduce disruption to vehicles with authorised access during busy periods.

The layered approach to defending a Critical Asset is vital in ensuring you achieve the required delay to protect that Asset as identified earlier in the process.

D. Performance Requirements

Table C3I: Fencing and Barrier Performance Requirements

Area	Ref	Example Performance Requirements
Security Fencing		
Level of Delay	PR1	The perimeter fence must offer a resistance to cut-through attacks by all anticipated adversaries of at least 2 minutes.
	PR2	The perimeter fence must offer a delay to climb-over and burrow-under attacks from all anticipated adversaries of at least 1 minute.
Compatibility	PR3	The perimeter fence must support fence-mounted PIDS technologies so as to facilitate an adequate PoD and minimise the potential NAR.
Earthing	PR4	The perimeter fence must be earthed every 75m to provide protection against lightning and electrical events.
Configuration	PR5	A double layer of fencing will be installed around the entire perimeter, with a minimum 7m gap between the fences and 5m clear zone outside of both fences.
Minimum lifespan	PR6	The minimum lifespan of the perimeter fence must be 10 years backed by a manufacturer's warranty.
Standards	PR7	The perimeter fencing system must be designed, supplied and installed to meet the requirements of BS 1722-10:2006.
Vehicle Barriers – Impact Performance		
Performance Levels	PR8	The barrier should be able to withstand a 90 degree impact from a 7,500kg vehicle moving at a speed of 80km/h with zero penetration beyond the barrier.
	PR9	In the event of an explosion at the barrier location the construction of the barrier will be such that it does not fragment and cause additional damage to adjacent Assets.
Configuration	PR10	The integrated vehicle barrier systems will provide enforced stand-off around identified Critical Assets of at least 50m.
	PR11	The barriers will provide a continuous line of protection with a maximum permissible gap of 1.2m between any crash-rated measures.
Vehicle Barriers – Operational Performance		
Operation	PR12	The barrier will be operable via the AACS or remotely from the gatehouse building.
	PR13	The barrier will have an opening/closing speed of not greater than 6 seconds and will be certified for continuous operation.
Configuration	PR14	The barrier will allow a 5m-wide vehicle to pass through when in the fully open position.
	PR15	The barrier system will be design to prevent tailgating through the vehicle entrance, via the use of multiple barriers to create an airlock. A rejection lane will be incorporated into the design to allow unauthorised vehicles to be securely diverted away from the site.
Safety	PR16	The barrier will have a manual override to allow operation in the event of loss of power supply.
	PR17	The barrier will fail safe on the activation of site evacuation alarms to allow free exit from the site.
Pedestrian Barriers		
Delay	PR18	The pedestrian barriers will provide the equivalent level of cut-through and climb-over delay as the perimeter fence line.
Operation	PR19	The turnstile will be proximity card-controlled in both directions.
	PR20	The turnstile will have a continuous operating cycle and be suitable for throughput of 120 people per hour.
Safety	PR21	The turnstile will have a key switch override.
	PR22	The turnstile will allow free exit only on power failure.

Source: PRISM™

C3.2.2 Building Delay

A. General Characteristics

Building delay is the second layer in the protection in depth principle, or indeed on a site with no perimeter the building will become the first layer. With a building any of the main component parts can be compromised and allow unauthorised access to the Assets inside that building. Any building that houses a Critical Asset should be surveyed and adequate physical delay measures should be installed to meet the established Protection Objectives.

A key standard that can be referenced when specifying various components of the building delay sub-system is 'Loss Prevention Standard (LPS) 1175: Intruder Resistant Building Components, Strongpoints, Security Enclosures and Free standing Barriers', available from the Loss Prevention Certification Board. Related products are certified on the basis of the duration of physical delay provided and their resistance to different categories of attack tools. Therefore, it is possible to use this standard to specify products that will meet your specific risk-based performance requirements and provide a known level of physical delay.

B. Sub-systems

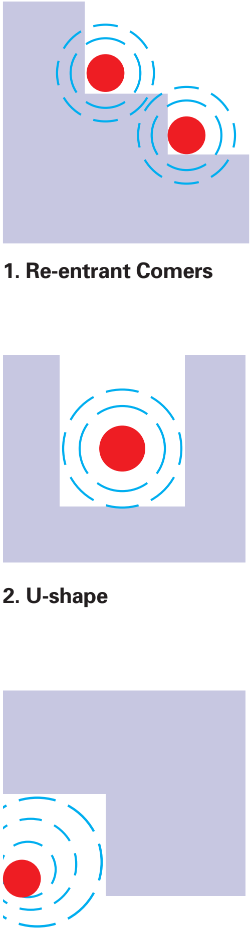
B1. Exterior Building Structure

Where a building contains significant Assets the structural exterior will need to be considered to ensure that it provides adequate delay against anticipated risk scenarios. This will include the fabric and construction of walls, floors, and roofs, and their respective resistance to physical attack and in some cases explosive blast. However, since retrofit structural measures are considerably expensive, where possible the requirements for structural security measures should be identified at the planning stage and incorporated into the building design. Where this is not possible it may be that secondary internal measures, such as the creation of security enclosures, can provide the required level of delay.

Although a building's exterior structure will provide adequate resistance to lower level threats, a determined attacker with the appropriate tools (angle grinder, small explosive charges etc) could break through an external wall in a reasonable amount of time, which could allow Assets to be compromised if supporting detection or response measures are also insufficient. Therefore, it is necessary to estimate the level of delay currently provided and whether or not this will be adequate in light of anticipated adversary capability. In some cases it may be necessary to consider specific construction or retrofit measures to increase penetration resistance, such as the use of double-skinned brickwork or steel reinforcements.

Where there is a requirement to protect buildings and occupants against explosion, it will be necessary to have a blast analysis conducted by an external specialist to identify the precise level of existing vulnerability (which will be dictated by a number of factors including building construction, available stand-off distance and type of explosive threat) and subsequently the countermeasures necessary to prevent structural collapse and minimise injuries caused by primary and secondary blast fragmentation. However, where adequate stand-off distance can be implemented structural measures may not be required. In the context of blast resistance it is worth being aware of the fact that certain building shapes can either accentuate or dissipate explosive blast, as shown in the following examples:

Diagram C3c: Shapes That Accentuate Blast

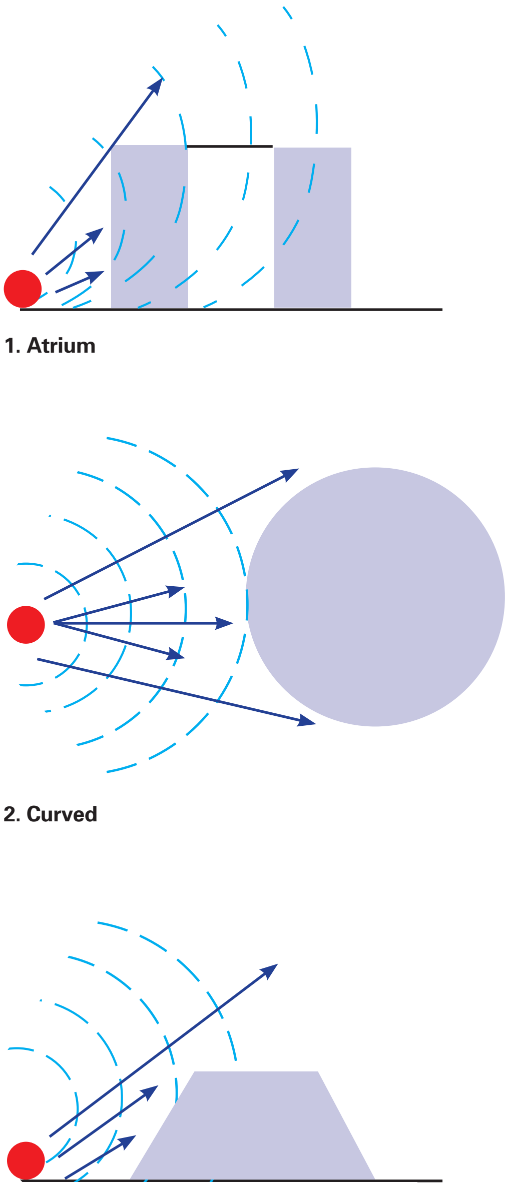


1. Re-entrant Comers

2. U-shape

3. Overhangs/Eaves

Diagram C3d: Shapes That Dissipate Blast



1. Atrium

2. Curved

3. Angled

Source?
For new-build projects there may be an opportunity to embed similar principles into the architectural design, thereby providing greater performance in this area in a cost-effective manner.

B2. Building Access Points

In the context of building delay it is important to consider all potential access points into the building in question and not just formal entrances. This will include all doors, windows, hatches vents, grates and louvres, all of which are offer intruders a potential route of entry into a building. Although access points at ground level may pose the greatest risk, other access points including those at basement, upper floor and roof level, could be accessible via external fire escapes, trees, drainpipes and other climbing aids, as well as tunnels, adjoining buildings and those within close proximity. The following delay measures will therefore need to be applied to provide Balanced Protection for the building as a whole, thereby ensuring that capable adversaries cannot take advantage of any weak points.

B2.1 Doors and Locks

The number of access doors into a building should be kept to a minimum with all other external doors for emergency egress only. Depending upon delay requirements a range of specialist security doors can be used to protect both external and internal openings from intrusion, and where required also provide fire or blast resistance. For intrusion resistance, products certified to LPS 1175 or an equivalent standard can be used to provide known delay performance. In this context It is important that any security-rated door that is installed should be fitted with the same frame, hinges, bolts and locking system (including emergency exit device) with which it achieved its security-rating since each of these components will have an impact on performance.

A lock must offer the same level of resistance to attack as the door into which it is installed, both against physical force and surreptitious attacks such as ‘picking’ of the lock or interference with associated electronic devices. The type of lock used around site will vary dependent on the application and the level of protection required, either operating mechanically or electronically. Examples of traditional mechanical locking devices include standard door locks, padlocks, handles and exit devices. Electronic locking devices include magnetic locks, electric strikes and solenoid-activated locking devices, the latter usually being less vulnerable to defeat by physical force.

Locking devices can be designed and specified in accordance with a number of European Standards as summarised in the following table:

Table C3m: Lock Type Device European Standards

Lock Type	Standard	Title
Padlocks	BS EN 12320:2001	Building Hardware – Padlocks and padlock fittings – Requirements and test methods
Cylinders	BS EN 1303	Building Hardware – Cylinders for locks. Requirements and test methods
Electromechanical	BS EN 14846:2008	Building Hardware – Electromechanically operated locks and striking plates. Requirements and test methods.
Emergency Exit	BS EN 179:2008	Building Hardware – Emergency exit devices operated by a lever handle or push pad, for use on escape routes. Requirements and test methods.
Panic Devices	BS EN 1125:2008	Building Hardware – Panic exit devices operated by a horizontal bar, for use on escape routes. Requirements and test methods.

Source: PRISM™

B2.2 Windows

All windows in the exterior of the building, or within vulnerable rooms inside the building, should provide an equivalent level of delay as doors and other measures. In this respect a useful standard to be aware of is 'EN 356: 2000 – Security Glazing Resistant to Manual Attack'. However, there are a number of other considerations as outlined below:

- Any windows in a building that are accessible but identified as non-essential should have glazing removed and be bricked up
- Alternatively suitable security-rated window bars or blinds can be installed on the inside of the window where this is more aesthetically desirable. This can also be used effectively to provide additional protection to existing windows
- Any opening windows in a building should be fitted with locks and opening restrictors
- For some applications bullet-resistant glazing may be required. 'EN 1063: 2000 – Security Glazing Resistant Against Bullet Attack' provides guidance and standards in this area

Where there is a risk of explosive threats special consideration needs to be given to glazing protection since flying glass fragments are typically responsible for around 60%-80% of all injuries in a blast event. There are three main types of countermeasure available in this respect:

- Anti-shatter film can be applied to existing glazing to prevent it from fragmenting into shards in the event of a blast. However, those in direct proximity to the window could still be injured by the imploding pane of glass and therefore bomb blast net curtains should also be considered to prevent this
- A more recent technology that can be used for existing glazing is security blinds that are certified to provide blast resistance
- For all new or upgrade applications specialist blast-resistant glazing and window frames should be used since this provides the most effective form of protection

As with structural blast resistance it is important to seek specialist advice when considering glazing blast resistance, since it is important that measures are designed to meet the specific requirements of each application.

B2.3 Hatches, Vents, Grates and Louvres

Hatches, vents, grates and louvres are all potential risks for physical intrusion, whilst they may also provide an opportunity to introduce contaminants into the building or set it on fire. There are a variety of specialist protection measures that can be installed to counter either or both forms of attack, such as security hatches, grilles and covers, many of which are certified to LPS 1175 or similar standards to provide known levels of resistance. Therefore, these access points should be afforded the same level of delay protection as any external doors or windows.

B3. Strongrooms and Security Enclosures

For many Critical Assets located within a building it will be necessary to install additional measures around the Asset itself, either to complement exterior measures and provide further delay, or to protect against attacks by insiders with legitimate access to the area. In some contexts this may require an individual secure area or zone to be created within a building with separate physical and electronic controls including use of appropriate security-rated products to protect access points similar to those outlined above. This can also provide a more cost-effective alternative to exterior building protection for very large facilities.

Where a large number of Critical Assets need to be protected consideration can also be given to the creation of a reinforced room within a building, often referred to as a 'strongroom', through structural reinforcement of walls, floors and ceilings, and appropriate physical and electronic access controls. When considering the requirement to install a strongroom there are a number of design aspects to consider. These include but are not limited to: the amount and type of equipment to be stored; the threat and risk scenarios identified in Section B and the accessibility of areas adjacent to, above and below the proposed strong room.

For individual Assets it may be more cost-effective to achieve your delay requirements via the use of a variety of Security Enclosures around the Asset itself, including cages, safes and secure containers such as filing cabinets, IT racks and storage boxes all with appropriate physical delay characteristics and locking mechanisms.

In addition to LPS 1175, the following standards provide guidance and product certification in this area and can be used to assist you in identifying your performance requirements and specifying technology (the LPS standards are freely available, whilst the European Standards usually have to be purchased – both are very similar, however, you may find more products available that are certified to EN standards):

Enclosure Type	Standard	Title
Safes and Strongrooms	EN 1143-1	Safes and Strongrooms
Safes and Strongrooms	LPS 1183	Safes and Strongrooms
Security Containers	EN 14450	Secure Storage Cabinets
Security Containers	LPS 1228	Burglary Resistance of Office Furniture and Lightweight Containers

B4. Protected Spaces

In order to protect personnel from CBRN attacks it may be necessary to create an area within a building which protects them against the effects of explosive blast and/or contamination, depending upon anticipated risk scenarios. These 'Protected Spaces' sometimes also referred to as Safehavens' or 'Bomb Shelter Areas' allow personnel to safely remain in the building when it is not safe to evacuate to external areas. This 'invacuation' option is increasingly important in light of recent terrorist attack methods, some of which have attempted to deliberately target people evacuating from a location following an initial explosion, via use of secondary IEDs placed at main exit routes or obvious muster points such as car parks. It may also be appropriate where a bomb threat has been issued but the location of the device is unknown, or where outside areas have been contaminated by a CBRN release.

Protected Spaces can either be implemented in the form of a dedicated facility or a dual-use facility, which serves some other purpose on a day-to-day basis. The latter option is more cost-effective and easier to justify in terms of the required investment, particularly if it can be achieved as an upgrade to an existing building or area within a building, rather than a new-build project. However, for many energy facilities it may be possible to utilise existing plant buildings for this purpose, where they are already designed to protect personnel against accidental explosions or chemical leaks. In this case it is important that the level of protection offered by such buildings is also suitable for anticipated threat profiles, which in some cases could pose a higher level of risk. Therefore it may be necessary to seek advice from a structural engineer with blast experience, as well as a specialist in HVAC design if CBRN protection is also required.

Where Protected Spaces are utilised it is vital to have in place effective procedures which dictate how and when they will be used, along with appropriate training for all personnel. Some form of notification system such as PA or dedicated alarm tone will also be required to notify staff of the need for 'invacuation', as opposed to evacuation.

C. Applications

The analysis undertaken in Phase B will have identified the location of Critical Assets; the potential routes, capabilities and methods of attack by adversaries, as well as the amount of delay required to protect Assets long enough for a response force to intervene. Where Assets are located within buildings it will be necessary to implement a range of protection measures to complement perimeter delay measures to provide adequate capability in this area. Of particular importance in this respect is to identify all possible access routes into the building and ensure that they are adequately protected. However, further measures may be required to provide additional delay or protect against insider threats and therefore a variety of internal security enclosures around each Asset should be considered in your assessment.

D. Performance Requirements

The following table provides some example Performance Requirements in the area of Building Delay:

Table C3n: Physical Security Requirement Performance

Area	Ref	Example Performance Requirements
Building Exterior		
Delay	PR01	The building exterior including walls, roof and floors will provide a minimum of 10 minutes' delay against a determined attacker equipped with a wide range of tools including disc grinders and other powered tools.
Blast	PR02	The building will be constructed to provide inherent blast resistance and prevent structural collapse in the event of Vehicle Bombs with 1000kg TNT equivalent yield being detonated at any point greater than 30m away.
Building Access Points		
Delay	PR03	All potential exterior access points into the building will be physically protected with components that each provides a minimum of 5 minutes' delay against a determined attacker equipped with a wide range of manual and battery operated tools.
Doors	PR04	External Security doors including frames, hinges and locking mechanisms will be certified to LPS 1175, Security Rating 3.
Locks	PR05	All security doors will be operated via solenoid-activated deadlocks linked to the ACS. Locking devices will in themselves be certified to EN 14846: 2008.
Windows	PR06	Attack resistant glazing certified to EN 356: 2000 will be installed in all exterior windows.
	PR07	Security blinds with certified blast and intrusion resistance will be installed inside all exterior windows.
Hatches	PR08	Any opening vent, louvre or opening more than 600mm2 shall be protected with a specialist security hatch certified to LPS 1175 and providing protection against the attempted introduction of contaminants into the opening.
Strongrooms & Security Enclosures		
Strongroom	PR09	The structural exterior of Room A will be reinforced to create a Strongroom meeting the requirements of EN 1143 resistance Grade II.
Safe	PR10	A safe will be installed to protect Critical Assets and will be certified to EN 1143, resistance Grade II.
Security Cabinet	PR11	A security cabinet will be installed to protect sensitive commercial information and will be certified to LPS 1228, Resistance Grade C.
Protected Spaces		
Blast	PR12	The existing operations centre will be upgraded to provide protection to occupants against all anticipated explosive threats.
Contamination	PR13	The Protected Space will provide a minimum of 60 minutes' protection to occupants in the event of an external release of chemical, biological or radiological material. HVAC controls and environmental sealing of the building will be designed specifically to achieve this.

Source: PRISM™

C3.2.3 Plant Delay

A. General Characteristics

In the context of the Security Management Plan Plant Delay refers to the layer of protection around external plant infrastructure, particularly that which has been designated as being critical to the function of the facility. Since this type of plant is located in outdoor areas it is inherently vulnerable to attack and whilst perimeter delay measures will offer some protection this is usually limited to a few minutes at most, and therefore may be insufficient to protect Assets long enough for a successful response to be mounted.

In this context it is important to consider other components that can provide further delay and therefore reduce the likelihood of key areas of plant being successfully attacked. However, given the size and complexity of outdoor plant at many energy facilities this is quite challenging to achieve and requires careful prioritisation of areas and components to be protected. Fortunately the Process Analysis and Asset Criticality Assessment conducted in Phase B will have resulted in a list of prioritised Critical Points, which can now be used in conjunction with Adversary Sequence Diagrams and established Protection Objectives to inform the design of any required Plant Delay measures. The following sections provide guidance and examples of the type of measures that can be utilised, although many of these will require bespoke systems to be designed for each facility.

B. Sub-systems

B1. Compounds

As indicated in the perimeter delay section it is advisable at larger facilities to use individual compounds to protect Critical Points or key areas, both in order to prevent non-essential access and casual intrusion by employees, visitors and contractors, and to provide additional delay to more determined attackers. Compounds will also provide an opportunity for secondary detection and access control measures to be applied.

These compounds will be similar in constructed to the perimeter barriers, typically utilising security fencing to provide the delay. However, as they are often much shorter in length than the perimeter, a higher level of security fencing is usually achievable within acceptable budgets. For very small areas consideration can also be given to the use of alternative materials with increased attack resistance such as steel profile sheets, brick walls or reinforced concrete walls. However, materials such as brick and concrete should not be used where there is also a risk of explosion in the vicinity since they will result in secondary blast fragmentation and increased damage to plant.

B2. Hatches and Enclosures

Where small Critical Points such as valves require protection it is possible to construct a variety of specialist enclosures with suitable security hatches to prevent unauthorised access. In this instance hatches should preferably be certified to LPS 1175 or an equivalent standard to provide predictable delay performance, whilst some form of blast protection may also be required.

One example of how this has been implemented elsewhere is by constructing a concrete enclosure around a critical valve and filling this enclosure with a product called 'Lytag' – a building aggregate made from pulverised fuel ash (the by-product of coal-fired power stations), which has the ability to absorb blast and therefore also protect the valve in the event of an explosion. The enclosure is then sealed with a specialist security hatch. When it is necessary to access the valve for maintenance purposes an industrial vacuum is used to temporarily remove the Lytag.

B3. Overthrow Barriers

Some critical items of plant may be vulnerable to objects being thrown at them – either Improvised Explosive Devices (IEDs) and incendiary devices or, in the case of electrical switch racks found at substations, simple metal objects which can cause them to short-circuit. This is a particular problem where vulnerable plant is located adjacent to the perimeter or in urban areas with problems of vandalism. In these scenarios consideration should be given to the installation of an overthrow barrier to prevent objects being thrown at Critical Points, particularly from outside of the perimeter where there may be limited ability to detect the presence of perpetrators.

The design of the barrier will need to take into account the size and position of the Asset in relation to the perimeter and therefore the possible trajectory of thrown objects. As such it will then be possible to install weld mesh or expanded metal panels on a metal frame in the correct position to intercept any objects. In an urban environment the overthrow barrier may also be constructed in conjunction with any noise pollution prevention barrier that may be required by planning regulations.

B4. Blast Barriers

Where the risk assessment has identified IED attacks as a concern it may be necessary to consider the use of some form of localised blast barrier to reduce the impact of the blast wave and/or protect critical areas of the plant such as gas stations or export manifolds against blast fragmentation. Prior to the installation of any such measures a blast study may be required to establish the level of mitigation required to protect against the anticipated type attack. Guidance may also be sought from the qualified personnel within an organisation as to potential for damage to the surrounding area if an adjacent Asset was to explode.

Where possible the maximum stand-off distance from a potential blast source to a Critical Point should be enforced with physical barriers discussed in previous sections as this will have the greatest impact in terms of reducing the effects of blast. In conjunction with this, secondary blast barriers can then be considered and may be formed from the topography of the land or man-made structures. Earthen berms can be constructed around a Critical Point to deflect blast upwards and absorb blast fragmentation. This type of blast barrier does however require considerable amounts of soil and space for installation. Similarly textile-lined mesh cages filled with earth can also be used to good effect. Alternatively specialist blast barriers can be installed and take the form of blast walls or complete structures preferably made of solid steel or concrete encased in steel.

Guidance may also be sought from the qualified personnel within an organisation as to potential for damage to the surrounding area if an adjacent Asset was to explode.

C. Applications

Where perimeter security measures are unable to provide adequate delay to critical outdoor plant, consideration should be given to the use of specialist Plant Delay measures to form a secondary layer of protection and provide the additional amount of delay necessary to allow a response force to intervene and/or protect against blast events. Each site will be unique in its requirements and therefore it will be important for you to identify what those are likely to be and where necessary seek support from internal or external specialists who can provide further advice and guidance and translate these requirements into a workable solution.

D. Performance Requirements

The following table provide some example performance requirements in the area of Plant Delay.

Table C3o: Plant Delay Performance Requirements

Area	Ref	Example Performance Requirements
Compounds	PR01	A compound will be installed around each of the identified critical areas of outdoor plant and will provide a minimum of 3 minutes' delay against cutting, climbing, bridging and tunnelling attacks by capable adversaries with a variety of tools and climbing aids.
Enclosures	PR02	A security enclosure will be designed and installed around identified critical points and will provide at least 5 minutes of attack resistance against capable adversaries with a variety of tools.
Overthrow Barriers	PR03	An 6m high overthrow barrier will be installed the length of the switch racks at sub-station 1 and will prevent objects being thrown onto the switch racks from outside of the adjacent perimeter.
Blast Barriers	PR04	A blast barrier will be constructed around the gas station from steel enclosed concrete to a height of 5m in order to prevent damage from blast fragmentation in the event of an explosion anywhere adjacent to the process area.

Source: PRISM™

C3.3 Response

Response

- The ability to respond effectively to the incident, preventing loss or damage of the Asset by successfully intervening before it is compromised or mitigating the potential consequences

Response components of Physical Security include the use of personnel and technology to intervene in a security incident whilst it is taking place and/or mitigate the impact of that incident after it has taken place. Where possible the former type of response is preferable to prevent Assets being compromised in the first place, however, in reality this is not always possible and therefore it is important to have some post-incident response capability as part of your ISS.

The Physical Security Response function can therefore be divided into the following components, all of which are necessary for a robust and well-developed capability in this area:

C3.3.1 Response Force

- Internal Response Force
- External Response Force
- Response Force Communications

C3.3.2 Response Technology

- Video Recording and Storage
- Video Analysis, Investigation and Evidence
- Access Control Logs

The following sections provide further information on how both personnel and technology can be utilised to achieve your needs for an effective Response, along with Key Performance Requirements and applications.

C3.3.1 Response Force

A. General Characteristics

Security Personnel can be used as a physical means of intervening in a security incident and protecting Assets, and in this respect contribute to the Physical Security function. Within the Security Management Plan this section addresses the different type of Response Force and various strategies for their deployment, whilst Section C5 outlines the procedural measures that can be adopted by the response force and other personnel in relation to a variety of incidents.

There are two primary categories of Response Force that can be utilised in the event of an incident – an Internal Response using security personnel employed or contracted by the organisation, and an External Response, usually in the form of Police or Military personnel. Depending upon the type and severity of the incident, as well as the local regulatory context, either or both of these may be appropriate and are considered further below.

B. Sub-systems

B1. Internal Response Force

Some form of Internal Response Force will be required for the majority of energy facilities, whether this is in the form of a full-time onsite Guard Force, as is likely to be required at large sites or a remote Guard Force based at another nearby location but able to respond to incidents in the required amount of time and also conduct occasional proactive patrols, as may be the case with small/unmanned facilities. On-call technicians or other employees can also be used to conduct regular visits to remote sites, visually checking Assets and any physical security systems for signs of damage or outage, however, they should not be used to respond to live incidents since they will not have the capability to intervene effectively and could place themselves at unnecessary risk.

In most cases the Internal Response Force will consist of dedicated security personnel, either directly employed or contracted, all of whom have specific training in security operations. Their role will include acting as a response force to an incident, as well as other general security duties such as gatehouse manning and access control, patrolling and personnel or vehicle searching. These duties will be laid out in specific assignment instructions, as discussed further in Section C5. In some cases they may also be involved in the Alarm Assessment function, however, for larger facilities dedicated control room operators should be used for this in order to ensure that the Detection function is not compromised by the Response function or other general duties.

The key function of the Internal Response Force will be to prevent, where possible, any security incidents resulting in loss or damage to the facility, its components, processes or personnel. Alternatively where this is not possible their role may be to contain or mitigate the severity of the incident, thereby reducing the associated level of loss to the organisation. In these respects there are a number of Guard Force strategies that can be adopted in response to any given incident depending upon firstly the type and severity of the threat, and secondly the capability of the response force to deal with it. These strategies are summarised below:

1. Interruption – this refers to the deployment of response force personnel to disrupt an attack by making their presence known to the adversaries in an attempt to disrupt their attack and encourage them to give up on their objective and exit the site before they are detained. This could also include verbal commands or instructions, either in person or via a Personal Address (PA) system. Since the Disruption strategy does not require physical confrontation with adversaries it is appropriate where security personnel have limited capability or are constrained in their actions by regulatory issues. However, it is only likely to be effective against opportunistic attackers since those with any real determination can chose to ignore the presence of the response force or their verbal instructions

2. Counteraction – this refers to physical intervention by security personnel and actions to counter an attack by an adversary. Examples of Counteraction include physically blocking the adversary's path, the use of reasonable force to prevent them from executing their attack and/or detaining them for subsequent arrest by Police. As such Counteraction requires a greater level of Guard Force capability it places security personnel at higher risk. To be effective against some forms of threat it may also require the use of armed security personnel. There are obviously significant legal considerations when initiating this form of response and therefore it is vital that the type of actions permissible by security personnel is clearly defined within their assignment instructions and training, and does not contradict any laws or regulations of the locality.

3. Containment – the third main response strategy that can be adopted is that of Containment, which attempts to contain the incident, usually until such a time as an External Response Force can intervene. Actions could range from simply monitoring adversary actions to allow External Response Forces to be effectively briefed on arrival and recording these actions in support of post-incident investigation and evidential proceedings (which will require a range of technology-based measures as discussed in C3.3.2) through to shutdown of vulnerable processes and partial or full evacuation of the site to mitigate the potential consequences of the event that is about to occur.

B2. External Response Force

At many facilities, particularly where an Armed Response Force is not practical or achievable, there will be limitations on the level of capability that can be provided by Internal security personnel, particularly with respect to determined threat actors willing to use force to achieve their goals. Therefore, it will be necessary to supplement the capability and actions of the Guard Force with arrangements for an External Response to certain types of incident. This is usually in the form of an emergency call-out, which in most countries is available at any location where criminal activity may occur, and therefore can be requested as required. However, for significant Assets it is advisable that certain arrangements are made beforehand for several reasons, as discussed below:

Firstly in order to determine your requirements for the Physical Security Delay function for any given incident you will need to calculate the time necessary for an effective Response to be mounted and therefore the amount of Delay that must be provided by security measures. Where certain risk scenarios demand an external response it will be necessary to liaise with police or military response agencies to ascertain their likely Response Time, which can vary significantly depending upon the location of the Asset and their available resources.

Secondly it is advisable to ensure that the External Response Force are familiar with the facility and are adequately appraised of any specific issues that may determine the best response strategy. This is particularly important for the energy sector, whereby many facilities will have hazardous processes that the responding force needs to be aware of. For example a gas facility with an explosive environment may dictate that police radios are not used within the facility, or that weapons can only be fired in certain circumstances. Similarly some electricity infrastructure will pose significant hazards to responding personnel and it may be that they can only enter some facilities after an engineer has made them safe to enter. For these reasons it is recommended that you develop a relationship with responsible authorities prior to any major incidents occurring and ensure that they have the information and any specialist training required to carry out their duties safely and effectively.

Thirdly for Critical Assets it is important to make the authorities aware of the significance of the facility and the type of specific risk scenarios that it may face. This will ensure that the responding agency gives the correct level of priority to the facility in the event of an emergency call, which will usually be formalised by appending notes to this effect on their site database and/or issuing you with a specific hotline or reference number. Where possible a visit to the site should also be arranged for area commanders so that they are familiar with the infrastructure and surrounding environment, and if necessary can develop a formal response plan.

In addition to an emergency response function, in some cases there may be Government authority for armed police or military units to be deployed at a facility on a permanent basis due to the criticality of that Asset, on a temporary basis as a result of an increased threat to the Asset or sector, or in response to a planned protest or demonstration by activist groups where a police presence is required for crowd control and possible dispersion. In any of these scenarios it is important to have very clear lines of communication, command structures and points of contact, as well as specific rules of engagement relating to the use of firearms, access to hazardous or restricted areas and the respective responsibilities of Internal and External Response personnel.

B3. Response Force Communications

In support of Response Force activity it will be necessary to have effective and secure communications available to security personnel when dealing with any incidents. This area is sometimes overlooked resulting in unnecessary weaknesses in response capability or the failure to respond effectively to certain types of incident. The following points should therefore be addressed in your security planning:

- Response Forces should not rely upon corporate telephony networks or cellular networks for primary communications due to the potential for outages and the lack of confidentiality
- Dedicated radio communications should be provided to the Response Force, where possible using encrypted communications technology
- A backup means of communication using an alternative technology such as satellite phone should also be available.
- Consideration should be given to the use of Codewords for certain types of incident such as bomb threats given that radio usage may be overheard by staff and visitors, which could otherwise induce unnecessary panic or compromise response actions
- At energy facilities which contain explosive environments security personnel should be provided with intrinsically safe radios certified to ATEX standards to allow them to communicate at any point within the site

In addition to the above requirements it is also vital that clear communication protocols exist between the Response Force and key members of the organisation such as security managers and emergency response co-ordinators, so that the correct people are notified in the event of an incident thereby ensuring that there are no unnecessary delays in the decision-making process.

C. Applications

For most facilities some form of both Internal and External Response Force capability will be necessary as part of the Physical Security function and it is important that these resources are reflective of the range of risk scenarios facing the Asset, thereby providing the required level of capability to mount an effective response to anticipated adversary actions.

In order to achieve this you should start by considering the type of Internal Response Force that will be utilised in terms of the numbers of personnel, level of training and required capabilities appropriate for the specific context in question. This will in part depend upon the response strategy selected for each main type of incident – whether Interruption, Counteraction or Containment – and in this respect it is important that the optimum strategy is identified prior to the event, and that security personnel are trained specifically on how and when each strategy and its various sub-components should be implemented to respond effectively to any given scenario. Specific incident response procedures can then be implemented and rehearsed on a regular basis, as discussed in Section C5 – Procedural Security.

Following on from this an appraisal of Internal Response Force capability will allow you to identify specific threats and attack methods, against which it is likely to be unsuccessful in protecting Assets and therefore external assistance will be required. Support from External Response Forces can then be considered as a means of enhancing response capability and should be negotiated in advance with relevant agencies to ensure that they are aware of the relative importance of the facility, understand the type of response that may be required and can plan for this accordingly.

> *In order to achieve this you should start by considering the type of Internal Response Force that will be utilised in terms of the numbers of personnel, level of training and required capabilities appropriate for the specific context in question.*

D. Performance Requirements

The following table provide some example Performance Requirements in relation to the Response Force sub-system:

Table C3p: Reponse Force Performance Requirements

Area	Ref	Example Performance Requirements
Internal Response Force	PR01	The Internal Response Force will comprise of 6 security personnel per shift, all of whom will be able to respond effectively to all incidents unarmed adversaries and related incidents.
	PR02	The response force will be trained in effective use of Interruption, Counteraction and Containment strategies, including both the operational and legal aspects relating to their effective use.
	PR03	The Internal Response Force will be provided with encrypted radio communications and will also use code words for major incidents such as bomb threats.
External Response Force	PR04	Contact will be made with External Response agencies proactively in order to inform them of the criticality and characteristics of the site and the anticipated threat scenarios that may be faced.
	PR05	An estimated police response time will be ascertained and incorporated into the design of physical delay measures aimed at protecting against armed or violent risk scenarios, where the internal response force will be unable to intervene.
	PR06	A communications plan will be agreed with the External Response Force and they will be provided with any specific training needed to operate safely when attending the site.

Source: PRISM™

C3.3.2 Response Technology

A. General Characteristics

In addition to the immediate response function carried out by security personnel it is also necessary to have a post-incident response function capable of allowing the incident to be analysed and investigated, and in many cases for evidential material to be gathered. Where it has not been possible to prevent the incident this offers the potential to mitigate the impact, for example through the recovery of stolen Assets, and reduce the likelihood of reoccurrence, either by prosecution of those involved, by providing valuable intelligence in respect of repeat incidents, or simply by identifying the failures in the immediate response strategy, subsequently allowing future remedial training and future enhancements. In certain circumstances evidential material may also help limit owner/ operator liability by demonstrating that they were not negligent in the course of events.

This type of post-incident response function is therefore a key component of an integrated Physical Security System. For facilities where there is no immediate response it may also provide the only means of mitigating the consequence of security breaches, although in this case it is important that the loss of the Asset is judged to be an acceptable risk to the organisation given that the effectiveness of this strategy can vary significantly depending upon a variety of factors.

The following sections examine the key response technologies that can provide you with capability in this area and should be considered in the context of your security provision.

In certain circumstances evidential material may also help limit owner/ operator liability by demonstrating that they were not negligent in the course of events.

B. Sub-systems

B1. Video Recording & Storage

The primary sub-system providing the post-incident response capability is that of Video Recording & Storage, which allows video surveillance images to be captured for later analysis and investigation. Although this may at first appear to be a straightforward area of provision given the range of sophisticated solutions on the market, it requires careful consideration for two reasons: firstly many systems actually provide far from adequate performance to meet investigative and evidential requirements; and secondly the recording architecture that is implemented can have a dramatic impact on other areas of the Video Assessment system (particularly with IP-based systems), sometimes to the extent that the detection function can also be compromised by poorly designed recording infrastructure. The key considerations are therefore highlighted below:

B1.1 Recording System Architecture

With small, single-site video systems the recording architecture will usually be straightforward and is likely to consist of a central Digital Video Recorder (DVR) with direct inputs from video cameras, or alternatively a single Network Video Recorder (NVR) connected to the security LAN. However, with larger, multi-site systems things can become significantly more complex, particularly where they are based on IP communications due to the limited bandwidth available, which often makes it infeasible to stream video from all cameras simultaneously over the entire network. This is important to be aware of – if the bandwidth requirements associated with centralised recording are not properly accounted for when planning system and network architecture you could later be faced with a system that can only record low-quality video and/or one which provides very poor or unreliable Alarm Assessment capability. This has unfortunately been a far too common occurrence in the security market over recent years.

In order to overcome the limitations of centralised recording in certain applications two main alternatives have emerged in recent years. Firstly and most recently manufacturers have introduced products that provide 'Edge-based' recording, i.e. recording at the camera location. This is usually implemented in the form of an SD memory card within the camera or encoder, although in a few cases solid-state memory is used (but is currently significantly more expensive). Edge-based recording limits bandwidth utilisation by storing video locally and only transmitting it over the network for review and retrieval when it is requested by the operator.

Although a logical approach, and perhaps suitable for small, low-risk applications there are significant concerns with edge-based recording, which has been described by some commentators as 'another example of manufacturers seeing the world as they want it to be and not as it is.' In this respect there are two main concerns – firstly Edge-based recording is inherently insecure given the possibility of unauthorised access, tampering or damage to the device (in some countries there are even debates around whether video evidence from these devices should still be admissible in court). Secondly their level of reliability is not yet clear, but in any case will be significantly less than typical RAID (Redundant Array of Independent Disks) storage devices common in most large applications. Harsh outdoor environments common in the energy sector may pose significant challenges in terms of reliability and any failures could result in the loss of critical evidence.

A similar but more robust alternative to Edge-based recording is that of Distributed Recording. This is appropriate for multi-site applications or very large single sites and works in a similar manner to Edge-based recording, in that video is only transmitted to the central control room on demand. However, in this case dedicated recording devices (preferably RAID compliant) are used and installed at each site or multiple locations within a site, typically within a communications room or similar secure area, each on a separate security LAN to allow video from nearby cameras to be streamed to the device for recording. They are then connected via a switch/router to a central storage server which allows video to be download on request for operator review. Where centralised storage is not practical a Distributed Recording architecture is therefore usually the best alternative and provides inherent redundancy, however, redundant recording devices and/or servers should still be used to minimise the possibility of data loss.

B1.2 Recording Parameters

The next important consideration in relation to the Video Recording sub-system is the level of recording quality necessary to provide usable investigative and evidential material. In this respect there are three main parameters that need to be selected – Frame Rate, Resolution and Data Compression (for digital systems these parameters are also relevant for live viewing as well as recording and similar considerations apply). Given that different cameras may have different operational functions it is important that these parameters can be set independently for each video stream. They are each discussed on the next page:

Frame Rate – this refers to the number of frames (or images in a digital system) that are recorded per second, defined as Frames Per Second (fps). It therefore determines how moving objects appear within the video stream, with 25fps (PAL standard) equating to real-time video, and anything less than 15fps resulting in a visible delay. As a general approximation each frame of data will amount to around 15-20Kb of data and therefore higher frame rates will require greater storage capacity (and transmission bandwidth for IP systems). As such it is not always practical to record at 25fps and in many cases this is unnecessary. For example if the objective is to record an evidential image of a person walking through an entrance there is little advantage of recording at 25fps, when only one or two frames are required to achieve this – a setting of 3-5fps would be perfectly adequate and significantly reduce the required bandwidth and storage capacity. In contrast if the objective is to capture a fast moving target, such as a running intruder or moving vehicle, a higher frame rate such as 12-15fps will be required. Therefore, it is important to identify the specific role of each camera and set the frame rate accordingly.

Resolution – the next key parameter is that of recorded video resolution, which will have a significant impact upon how usable video is in a variety of post-incident response functions. For example if video will be used to provide a general record of activity that has taken place – such as an intruder's time of entry, attack method or direction of travel – lower resolutions may be acceptable. However, if it will be used in an evidential capacity, for example to identify the intruder in a court of law, a much higher resolution will be required. Previously the majority of resolution settings were based upon the CIF standard (Common Intermediate Format), although with IP systems there are a variety of different resolutions now available to choose from. The main ones that you will encounter are shown in the following table, along with an indication as to whether they are likely to be suitable for general investigation only or for evidential material (although this obviously depends upon other factors such as camera placement, Target Image Height, Lighting etc):

Description	Resolution – pixels (h x v)	Likely Suitability
QCIF	174 x 144	General Post-incident Investigation only
CIF	352 x 288	
2CIF	704 x 288	
4CIF	704 x 576	Evidential Material
D1	720 x 480	
720p HDTV	1280 x 720	
1.3 Mega Pixel	1280 x 1024	
2 Mega Pixel	1600 x 1200	
1080p HDTV	1920 x 1080	
5 Mega Pixel	2592 x 1944	

Source: PRISM™

Resolution will also have a significant impact upon required storage capacity and bandwidth consumption, and therefore it is important to ensure that there is adequate capacity in both areas to achieve your requirements and match the capabilities of the camera – there is little point in investing in Mega Pixel cameras if the transmission and recording infrastructure will only allow them to be used at 4CIF level.

Data Compression – the third main consideration in recorded image quality is the level of compression that is applied to the data in order to reduce file sizes. Whilst 'lossless' compression, which does not impact upon image quality, is sometimes used there is a limit to the amount of reduction in data that can be achieved, and therefore 'lossy' compression is widely used and can deliver much smaller file sizes. However, since some of the image data is discarded it results in some level of reduced image quality in terms of loss of clarity, detail or colour, and the production of unwanted artefacts in the scene, referred to as 'noise'. Data compression is the biggest cause of image quality loss, particularly when bandwidth or storage limitations dictate that heavy compression must be used. Therefore it is important to ensure that this is not the case and also that the video recording system has the ability to adjust data compression levels as required.

Retention Period – the final recording parameter to be considered is the length of time that it will be necessary to retain video for until it is overwritten. In this context it is important to consider both the requirements of the organisation and also any local guidance or regulations from the police or other government bodies. In addition the number of video cameras in operation may also impose practical limits on the retention period, although the cost of storage has reduced significantly in recent years making longer retention periods more feasible.

Most organisations will retain images for a minimum of 7 days for internal purposes, however 14 or even 30 days is often recommended by police agencies in order to ensure that potential evidential material is available to them. Some organisations may also wish to store video for longer periods of time in case of any future internal investigation, and if this is the case it will most likely be necessary to export video to external disks for archiving.

B1.3 Storage Capacity

When the above recording parameters have been set it will then be necessary to consider the required storage capacity to meet these requirements. In this respect it is important that these requirements dictate the amount of storage capacity and not the other way around, which is a common occurrence and results in poor performance in this area.

The amount of storage required for any given application will depend not only upon the number of cameras in the system and the required frame rate, resolution and compression level for each one, but also on the complexity of each video scene. A manufacturer, consultant or installer should be able to help you calculate your requirements in advance, and subsequently identify suitable solutions to meet these in full.

B2. Video Analysis, Investigation and Evidence

In addition to the performance parameters outlined above effective post-incident response will require the ability to analyse recorded video in support of the investigative function, which may be conducted internally or by an external police force. In the latter case it is also important that video is handled and exported in such a way as to facilitate evidential and legal requirements, thereby ensuring that if necessary it can be used in any subsequent court proceedings. The following sections discuss these issues in more detail.

B2.1 Video Analysis Tools

Whilst nearly all video recording systems will have the some form of analysis capability this can vary dramatically from basic time and date searching, through to intelligent scene analysis using specialist software. In this respect it is important to consider how the security function is likely to utilise recorded video and the type of investigative activity that may be required at your facility. In many cases, particularly where there is extensive video footage from a large number of cameras, specialist analysis tools will be beneficial and this may be one criterion for systems selection. The main capabilities in this area are detailed below:

- Basic Search Functions – nearly all recording systems and management software will allow you to search recorded video on the basis of time and date, and retrieve segments of interest. This is suitable for situations where you already know approximately when an incident occurred. However, if this is not the case it may be necessary to review hours, days, or even weeks of video footage – a frustrating and time consuming process!
- Intelligent Search Functions – many higher-end products will also provide the capability for intelligent search of recorded video, by allowing various filters to be applied – for example movement within a particular area, new objects in the scene, direction of travel, number of people etc. Providing that the type of activity of interest is known this can effectively reduce the amount of time necessary to analyse video
- Automated Visual Catalogue – more recently some specialist add-on systems use Video Analytics algorithms to automatically catalogue details from the scene in a comprehensive database, which can subsequently be searched using specific parameters. For example a red car at entrance A during a specific time period could be searched for. At present this type of capability is primarily used by government agencies; however, it is likely to become more commercially widespread in the near future, along with supporting technologies such as facial recognition

B2.3 Investigative and Evidential Requirements

In order to support the investigative function it will be necessary to have some form of export capability so that a permanent record can be created and video is not overwritten. Most systems will provide a number of export options including CD, DVD, USB or removable hard drive. Where the exported video is in a proprietary format appropriate playback software should also be exported to the same disk, otherwise third parties will not be able to view the footage.

Where there is a possibility of video being used as evidence in court it is essential that correct procedures are followed to ensure the integrity and validity of the video recording or image, otherwise it may be inadmissible in any court proceedings. Since the legal requirements for evidential video vary from country to country you should seek advice of the local police department to find out the exact procedures that should be followed. However, this will usually include the creation of an audit record detailing all of the actions undertaken by operators when retrieving and exporting video, which should usually be to a non re-writable disk such as a CD-R. There may also be requirements for some form of encryption or watermark, which is commonly available as part of the system software. In addition authorities will most likely want to be reassured that the storage servers are housed in a secure location and cannot be tampered with, and that access to the workstation providing video retrieval and export functions is password protected.

> *Since the legal requirements for evidential video vary from country to country you should seek advice of the local police department to find out the exact procedures that should be followed.*

B3. Access Control Logs

Another important resource in security investigations is the Access Control System database, which will contain activity logs that can be searched by user, door, building and time/date. Where an incident such as a theft takes place, particularly where there is no sign of forced entry, these logs can be interrogated to see who entered the building or door at that time, be it a visitor, contractor or employee, and whether this activity fits with their normal routine or was unusual in any way. This information can be very useful in the investigation process, particularly where attacks have been carried out by insiders with legitimate access to the facility. The information can also be used proactively prior to any incidents, to identify suspicious activity such as unauthorised access attempts and access by personnel with no need to be in a particular area.

C. Applications

In support of the Response function you should consider how technology can be utilised for post-incident investigation, and therefore provide an opportunity to mitigate the consequences of an incident where it was not possible to prevent it in the first place. In this respect it is important to clearly identify your performance requirements at the outset and ensure that the systems that are implemented deliver against these requirements. In too many cases performance requirements are only realised after the systems are operational, when the limitations imposed by inappropriate or ill-designed technology become apparent. For example many smaller or less sophisticated systems will impose maximum frame rate and resolution settings for the system as a whole and whilst they may support recording from x number of cameras, this will not be at the levels required to facilitate effective post-incident response capability.

D. Performance Requirements

Some example performance requirements for the Response Technology sub-system are provided in the following table:

Table C3q: Response Force Performance Requirements

Area	Ref	Example Performance Requirements
Video Recording and Storage		
Recording System Architecture	PR01	Distributed recording within each local control room will be utilised to reduce bandwidth consumption (rather than edge-based recording at the camera).
	PR02	Redundant storage will be provided both in terms of individual disk failure within a storage array, as well as complete failure of any single storage device or location.
	PR03	Immediate access to alarm video will be possible without impacting upon the quality or availability of live video streams.
Recording Parameters	PR04	Video from all Perimeter cameras will be routinely recorded at 5fps and CIF resolution, however during an alarm event they will be recorded at 25fps/4CIF for 2 minutes pre-alarm and 15 minutes post-alarm
	PR05	Video from all entrance point cameras will be routinely recorded at 5fps and 4CIF resolution, however during an alarm event they will be recorded at 25fps/4CIF for 2 minutes pre-alarm and 15 minutes post-alarm.
	PR06	Recorded video will be stored for a minimum of 30 days before being overwritten. It will be possible to set the recording parameters in terms of images per second and resolution individually for all cameras.
Video Analysis, Investigation and Evidence		
Analysis Tools	PR07	The Video Management System will have in-built analysis tools allowing video to be retrieved by time/date/movement/objects/direction of travel.
Video Export	PR08	The Video Management System will allow video export to CD/DVD/USB/Removable Hard Drive, and will provide watermarks and other evidential features.
Video Evidence	PR09	Audit logs and procedures for the evidential handling of recorded video will be implemented in accordance with local regulatory requirements or best-practice guidelines.
Access Control Logs		
ACS Investigation	PR10	The AACS database will contain activity logs which can be searched on the basis of user/door/building/date/time and thereby provide a list of users who accessed or attempted to access a particular building or door around the time of a security breach.

Source: PRISM™

C3.4 Summary

Physical Security design is a very specialist and complex area, particularly in the context of the energy sector where unique demands are placed upon the related sub-systems and technologies, and where very specific system performance requirements exist. As such considerable space has been devoted to the discussion of Physical Security in the Security Management Plan, and whilst it will not allow you to produce detailed security systems designs it is hoped that this will have demonstrated the importance of performance over product and helped you to identify and interpret your own individual Physical Security System requirements in the areas of Detection Delay and Response.

You can now move on to consider the other areas of security provision which together will provide an Integrated Security System capable of achieving your protection objectives – namely Process Control and IT Security (Section C4), Procedural Security (Section C5) and Personnel Security (Section C6). Following on from this you will be asked to summarise all of your Security System Performance Requirements before moving onto the Implementation Phase, where they will be used as the basis to engage effectively with external providers and ensure that cost-effective risk mitigation can be achieved.

Physical Security design is a very specialist and complex area, particularly in the context of the energy sector where unique demands are placed upon the related sub-systems and technologies, and where very specific system performance requirements exist.

C4 Process Control and IT Security

Purpose: In this section we will discuss the functions and some of the definitions associated with Information Security, and how PRISM™ links Physical Security to Information Security.

By working through this Section you will be able to ensure that information captured within the process analysis is shared with the relevant Stakeholder group ensuring the Security Management Plan reflects information security issues.

The information will provide you with an understanding of where relevant National Guidelines should be followed in line with International best-practice.

C4.0 Introduction

A key stage in the design process is to understand the importance placed on Information Systems Security both in the context of a Business Service function and most importantly SCADA systems that control the operations.

Part of your Stakeholder analysis in Phase A will have identified who within the business has an interest in and therefore requires input on this subject. The vulnerability assessment will have given you an idea of where Information System risks lie and the importance of capturing these within your Security Design.

Remember this is not all about firewalls; it is also about prevention of access to the systems themselves. Traditionally these systems have been closed and so difficult to penetrate; more recently with the integration of business operation platforms, vulnerabilities have been exposed that require more detailed management.

The subject matter around Information Systems security is extensive and this section is written to ensure you are in possession of the right level of information to ask the questions you need to consider. Your Stakeholders have an interest so engage them and work with them – they will have specific reference material should you need to identify in more detail further aspects of this subject.

C4.1 Definition

Supervisory Control and Data Acquisition {SCADA} refers to a computer system monitoring and controlling a process, for example:

- Infrastructure Process
- Industrial Process
- Facility Process

So when viewing Information security in the context of physical security all the elements set out in the DDRR strategy are applicable and must be deployed in line with the Information Security Risk owner within the business.

There has been a substantial amount of information produced on the subject of information security and it will be important to distinguish between Business Management systems and SCADA systems in their vulnerability to disrupt critical operations. Remember that if there is an electronic link between both systems then vulnerabilities can be exploited across the network.

C4.2 Detection

Within Phase C3.1 decisions will have been made regarding the levels of physical security appropriate to the protection criteria agreed upon. The detection principles will be applied to the environment where Information Security vulnerabilities have been identified, and this can be described as a 'Boundary' between the physical, buildings, rooms and Computer Hardware; with the non physical electronic environment, where data is transmitted around a network.

The ability to detect unauthorised entry into an area identified as Information System critical will most likely come from the Perimeter Intrusion Detection systems or the Internal Detection System. In this context the layers will allow time to respond to an unauthorised entry into the 'Boundary Area'. It will be at this point that the electronic security environment may need to deliver a period of delay before the response element of your plan arrives.

In this context the following should be considered as part of this process and should be undertaken with the Risk Owner:

- Conduct an Audit to evaluate the Process Control System operation
- Agree the Threats faced by the Process Control System
- Evaluate and assess the impacts from disruption to the Process Control System

From a network detection perspective the ability to detect unauthorised activity is likely to be away from the source of the attack, so these can be considered as monitoring tools.

The ability to detect unauthorised entry into an area identified as Information System critical will most likely come from the Perimeter Intrusion Detection systems or the Internal Detection System.

C4.3 Delay

The design basis upon which the Risks have been evaluated will provide the opportunity to have built in sufficient delay in order to respond effectively to unauthorised access to the Information System. However it may be necessary to build in additional delay into the Information System through a variety of principles to achieve secure system architecture.

- Network Architecture
- Firewalls
- System Hardening
- Remote Access

It is important that this process is gone through with your IT department who may already have many of these issues addressed, but remember at this point it may not be someone coming in from the outside; the threat may be from someone already inside your business.

Delay activities are those that require authorisation to systems or data, these will typically be passwords, authorisation levels and encryption. Remember the purpose of delay is to elicit an effective response and in the electronic world delay can be a very short timeframe.

C4.4 Response

When reviewing the security environment around process control systems this must be looked at as part of an ongoing process. Process control systems require an evaluation process that provides immediate action should unauthorised access be identified on the system. The policies and procedures that will underpin your capability to respond correctly must be reviewed and evaluated. Ensure that the Risk Owner understands this and has in place the appropriate tools; does this link into your Security Management Plan?

Remember there are a variety of principles that can be followed and ensure that these are in place and if needed familiarise yourself with these.

Examples of what could occur may be disconnection from the network or alarms requiring intervention {Network Administrator).

C4.5 Resilience

The ability of an organisation to manage the resilience of a network requires continual monitoring to evaluate change and the impact that has on the security of the systems. It is important to remember that the denial of your systems may come from a variety of directions and so needs to link with Business Continuity or Disaster Recovery plans.

Recording events and how they were managed and resolved builds capability to face the same or similar challenges in the future. Initiating a swift response in line with your plan allows you to build resilience into the network and so provides you with a greater opportunity to provide assurance on the integrity of the systems.

C4.6 Summary

Process Control and IT Security link many critical components and place the management of Security Risk in two areas. First is with the Security Manager who needs to ensure that systems and procedures provide the correct levels of assurance that access to the Process Control Systems is sufficient. Second with the IT Security Risk Manager who understands the protection afforded to the system by the Security Manager and is able to implement appropriate layers within the IT system itself.

It is a partnership that will require an ongoing dialogue and exercising to ensure that the resilience required by the business to perform its operational function gives the required level of assurance.

C5 Procedural Security

Purpose: To explain the need for a security procedure and to clearly define how these link to the processes described within the PRISM™ Methodology.

It will allow you to consider the correct approach to ensure that your procedures meet all Stakeholder requirements and that any response will form a consistent and clearly defined process.

You will need to ensure that the procedures are discussed with the relevant Stakeholders to ensure all response plans link and underpin this procedure.

C5.0 Introduction

In order that a company can provide a framework for staff to effectively respond and manage security-related incidents there is a requirement for comprehensive and well structured site specific security procedures.

The basis of any security procedure requires that you have a broad understanding of the business reasons behind company decisions in order for you to formulate a response to specific security-related incidents.

Legal Obligations. Management have a duty of care to all persons, both staff and visitors, who are present within their facilities. Today, as a member of the European Union (EU), the focus is not just within your country's legal system but the broader EU legal implications that will require serious consideration and adoption.

Security Responsibility. As the person tasked with creating and implementing a Security Plan, you should have sufficient responsibility and be empowered with the appropriate authority to co-ordinate events, for without this responsibility any Security Plan will not be fully effective. This is discussed in more detail within Phase A of this document

Your core responsibilities should include, but not be restricted to the following:

- The production of the Security Plan
- Implementation of the Security Plan
- Ensure the Security Plan is regularly tested
- Point of contact for liaison with civil emergency services and local authorities
- Conducting regular reviews of security measures and procedures

Liaison with Local Emergency Services. The manner in which the local emergency services and other relevant, more specialist services (Anti-Terrorist Police Units, Bomb Disposal Team) respond to an incident within your facility will have an impact on how any Security Plan functions and all requests made by them must be incorporated within the plan. You should have close consultation with these services during the planning and writing stages of the plan. This interaction will ensure that you can get a good grasp on their response procedures. Any specific requests by these services for particular additions to the plan will require attention. For example:

- Specific 'stand-off' rendezvous (RV) points
- Specific entry point to facility
- May require specialist equipment to be stored within facility
- Detailed maps of facility as part of the plan
- Specific Point of Contact (POC) i.e Security Manager/ Facility Manager
- May require specialist communication equipment to be made available

During consultation with these services, it is envisaged that further 'bespoke' additions to the plan may be requested.

Protective Markings. It should be understood that any site Security Plan will incorporate very sensitive information and provide a detailed description regarding the manner in which a company and emergency services react to security-related incidents. As a consequence, the document should be strictly controlled and only those who clearly have a 'need to know' the contents should have access to it.

Need to Know

- Knowledge of PM material must be strictly limited to those security-cleared to the appropriate level and clearly have a need to know the information to complete their duties. No one by virtue of their standing within the company will automatically have access to such material

Furthermore, hard and electrical copies of the document should be strictly controlled and only those personnel or locations that clearly have a 'need to hold' the document should be in possession of such copies i.e. Main Guardroom, Control Room and Security Manager.

Need to Hold

- PM material must only be retained or held by staff that requires such material to conduct their duties efficiently

The site Security Plan should be annotated with a protective marking commensurate with the information contained within the document. The protective marking should be at a minimum:

'Confidential – Commercial'

C5.1 Detection

Detection

- In this section we examine how security procedural elements can contribute to the overall detection function

C5.1.1 Identifying Hostile Reconnaissance

> 'Identifying Hostile Reconnaissance is a means to predict and categorise the potential for inappropriate, harmful, criminal or terrorist behaviour'

Post-attack investigation has shown that there is a distinct pattern to the planning of a terrorist attack; it is also when the potential terrorist or criminal is at his/her most vulnerable. Having knowledge of what may occur, or the things to look for may give you an advantage when planning the security for your site.

Target Identification. Persons who plan a terrorist attack, in most cases want to achieve a media spectacular and cause disruption to the company or country's infrastructure; they also wish to escape from the area post-attack (except a suicide attack).

They are aware that sites will have different levels of security to protect it; as a consequence, one of the first things they have to achieve is the identification of a suitable target. Given what is said above, a terrorist or criminal will always try to identify a 'soft' target. A site with robust security procedures and strong physical protection will attract less interest and may force a terrorist to look elsewhere for a suitable target. (The term 'deter' is used to describe these elements throughout this document).

Surveillance/Intelligence Gathering. Once a target has been identified, a potential attacker will try to gain as much intelligence on the site as possible; they will be trying to identify weak points in the current security procedures or physical protection for them to exploit. This will include:

- Conducting surveillance to gain intelligence on security procedures
- Attempt to make contact with staff and befriend them in order to gain intelligence on the site
- Attempt to take photographs or video of security procedures or physical protection
- Conduct surveillance on the guards to try to identify patterns in their procedures i.e patrol times or routes

As stated earlier, this is a vulnerable phase for the attacker as there will be a requirement for them to get close to the site on numerous occasions and if site personnel are vigilant, the attacker may get spotted. Spotting the same vehicle watching the site at times when the site is most active, for example, shift changeover, seeing the same person walking past the site a number of times, seeing someone taking photographs or video, may all be indicators that the site is under surveillance. In all these cases, personnel should be instructed not approach these persons, but to report to security control for onward report to the Security Manager/Police.

Planning. Once an attacker has identified a target and found a vulnerable area within site security, the attacker will then begin the planning phase of their attack; they will decide what type of attack to conduct. Detailed explanations regarding methods of attack are covered within Phase B.

Rehearsal. Once the planning phase is complete and the potential attack method has been decided, there will be a requirement to rehearse the attack and to go through with the majority of the plan without actually executing the final phase, the attack. In order to ensure or give themselves a level of assurance that the plan will work, there may be a number of rehearsals, therefore the attacker may be seen a number of times, and may get spotted.

A site with robust security procedures and strong physical protection will attract less interest and may force a terrorist to look elsewhere for a suitable target.

Arming. There is an arming phase to the pattern where the bomb maker/explosive courier will make contact with the attacker. However, any chance of the attacker being exposed during this phase will be intelligence-led by the local security services and anti-terrorist Police.

Attack. Should the attacker get to this phase without being spotted, then there is a chance that he/she would be successful. However, using the same vigilant regime as stated earlier could help you spot a potential attack before it occurs. Once an attack is in progress and the site personnel are aware, the site emergency procedures should be invoked and managed by the senior member of staff and the Police must be alerted at the earliest opportunity.

C5.1.2 Entry Procedures

The manner in which staff and visitors are processed into the site is one of the focal points with regard to security. This should ensure that only authorised persons should be allowed access to the site.

Entry should be split into separate categories, for ease of reference these are detailed below:

Operational Staff. All staff should be in possession of a site or organisation specific photo pass and prior to entry into the site, all staff are to present this pass for inspection by a guard. Where no guard is present and a swipe/proximity card and Personal Identification Number (PIN) system is used staff are to be instructed not to divulge the PIN to anyone. It would also be good security practice not to print the name of the site on the card; this will mitigate the risk of anyone finding the pass knowing where it may give you access to.

Visitors. The manner in which you plan visitor access to the site depends on a number of things:

- The level of security at the site; this may be dictated by company or government policy
- What dangers visitors will be exposed to onsite?
- Is there an escort of visitors regime enforced?
- Any prohibited items?
- Age concerns i.e. minimum age for entering site?

There are a number of procedures you can put into place when planning for visitor access to the site, but again, dependent on the criticality of the site, this may well be enforced by company or government regulation:

- A sponsor must inform the gatehouse of any visitors a minimum of 24 hours prior to their visit
- Where this is not possible, for operational reasons permission should be sought from the Security Manager prior to the visitor being granted access
- All visitors must bring photo ID i.e passport or driving licence
- All visitors are to be escorted at all times
- All visitors must receive a safety brief prior to entry informing them of alarms or evacuation procedures
- All visitors must be requested to hand over any company specific prohibited items
- All visitors must be informed they may be subject to a bag search (please refer to Phase C5.)
- All visitors must be logged into and out of the site

Local procedures may dictate that all persons, including visitors, will be placed onto an electronic list which details who is onsite at any given time. This will be used by emergency services should there be an incident onsite and persons are reported missing.

Local procedures may dictate that all persons, including visitors, will be placed onto an electronic list which details who is onsite at any given time.

Vehicles. Organisation regulations and the current threat/response level should dictate the search procedures enforced within the site; as a rule of thumb the following is good security practice:

- 100% of vehicles are to be physically searched prior to entry into site. This should be conducted by suitably trained and competent personnel (Guards)
- Sponsor must give a minimum of 24 hrs' notice of any delivery that requires vehicle access
- The driver must be identified prior to any vehicle gates being opened
- If the vehicle has any passengers, only those required for operational reasons should be permitted access into the site
- A specification of contents must be produced to the guards to identify the load; this must agree with the details provided by the sponsor
- The vehicle must be escorted by an authorised person
- When allowing entry and where a vehicle 'airlock' is in operation, only one gate is to be opened at a time to prevent access and tailgating
- Should a vehicle require entry which is longer than the 'airlock' the vehicle should be searched outside the outer gate prior to being allowed entry. The guard should remain with the vehicle when both gates are open

It must be remembered that when searching both vehicles and persons' belongings, you are not necessarily looking to detect explosives or bomb components, however this is of primary concern you are also looking to detect prohibited items being taken into the site.

Prohibited Items. Where local procedures dictate, all persons entering the site must be asked to relinquish any item that the company has decided are not to be allowed onto site. A list of prohibited items should be clearly on view at the main entrance. Furthermore, all persons entering the site should be reminded to relinquish such items. Examples of items include:

- Ignition device – matches/lighters
- Electronic items – mobile telephones/car alarm remote control
- Firearms/knives or offensive weapons (Separate regulations should be enforced for Armed Police)
- Alcohol and non-prescription drugs. Prescription drugs may be taken onsite under authority of the Security Manager

Any retained item should be placed in a sealed bag and secured within the guardroom. The owner should be issued with a receipt for their items.

Restricted items. There may be items that either the company or Security Manager believes should have restrictions placed upon them regarding entry onto site. There are a number of reasons behind restricting certain items. For example, laptop computers are an electronic item and therefore a potential ignition source. Digital cameras, as well as being a potential ignition source could be used by visitors for industrial espionage activities. Approval to take an item classified as 'Restricted' should be under the written authority of the Security Manager or appointed deputy. Examples of such items are:

- Laptop or palm top computers
- PDAs
- Cameras

Searches of the Person or Belongings. The searching of a person can lead the company into a legal minefield. Prior to the instigation of this type of policy it is suggested that the Security Manager contacts the company legal department and receives written advice on how to proceed. It is suggested that the legal department is consulted regarding searching of bags, but this should not be an inhibitor to the instigation to this policy.

With regard to searching the person, the following should be observed:

- Unless local laws allow, a cursory body search (Airport style pat-down) should only be conducted by authorised persons such as Civilian/Federal Police
- All searches if authorised are to be conducted by same sex persons
- All searches are to be logged

With regard to searches of person's belongings, the following should be observed:

- You must receive the persons consent prior to conducting any search. If the person refuses, they should be informed that it is a condition of entry into the site that they agree to their belongings being searched. If the person still refuses, then they are not to be granted access and the Security Manager and their sponsor should be made aware
- Prior to conducting the search, it is wise to ask the person if they have anything within their coat pocket or bag that may injure the person conducting the search
- Only outer clothing that is removable from the person such as coats/jackets and bags may be searched
- Always wear appropriate protection, for example gloves
- If suspect items such as bomb components or weapons are discovered then the Police are to be contacted and requested to attend
- Religious or ethnic codes of dress are to be dealt with in line with company policy; advice should be sought from the HR Dept

C5.1.3 Security Guarding and Operational Duties

An important facet of the overall security of the site is the manner in which the site is guarded. There is significant financial outlay to have a permanent guarding presence and there will always be conflicting opinions regarding the use of guards to provide security for the site. All companies must conduct a robust risk assessment as to whether the company will utilise this type of Asset. By detailing a set of parameters for the guards to operate within a Security Plan will ensure that the guards act and respond to security-related incidents in accordance with company policy.

When engaging or entering into a contract dialogue with a prospective security guarding company, there are a number of issues that will require addressing:

- Licensing. Most countries have a government approved licensing authority with regard to manned guarding companies. This type of licence is designed to give employers or contract holders a level of assurance that the guarding company has achieved a level of competencies in line with government regulations. You should ensure that prior to entering into any dialogue with a guarding company that they hold the correct and current licence to operate within the host country. Be aware that this may include individual personal licensing for each guard.

Duties. The duties which can be assigned to a guarding company should include:

- Monitoring of technical security equipment i.e CCTV and Perimeter Detection systems
- High-profile patrols of the facility
- Response to security-related incidents
- Control of Entry procedures in line with company regulations
- Dissemination of information and conducting emergency call-out procedures
- Search of bags and vehicles
- Point of Contact for all routine security-related incidents
- Initial security screening of all mail/parcels entering site

> *All companies must conduct a robust risk assessment as to whether the company will utilise this type of Asset.*

C5.2 Delay

Delay

- In this section we examine how security procedural elements can contribute to the overall Delay function

C5.2.1 Site Security Systems

This section of the Security Plan should be used to give a short synopsis regarding what physical security systems are in use at the site and who or which section of the site is responsible for monitoring the equipment. It should also detail any additional aspects regarding enhancing the security systems such as training and maintenance of the systems.

This section can also be used to maintain a list of the installer of security equipment and any relevant contact details regarding maintenance or emergency call-out should there be a failure in any facet of the security system.

You could add a comment in order to empower the contracted guards or control room staff to act on their own initiative regarding critical failures with the system, especially during silent hours/weekends and holidays. Failure to quickly react to security system failures will result in degradation of the system performance as a whole and leave the site vulnerable to possible attack.

C5.3 Response

Response

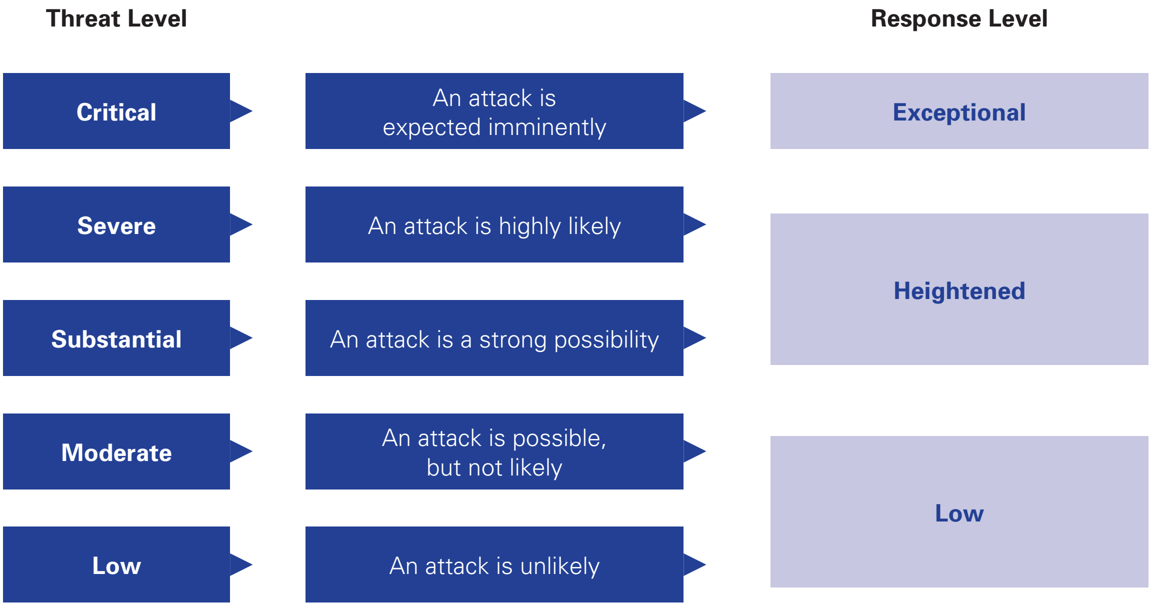
- In this section we examine how security procedural elements can contribute to the overall Response function

C5.3.1 Threat

Most countries operate a National Security Threat level system; you can access advice on the current threat through government open sources. Please remember that your organisation security response or posture will change in line with the current national threat level. However, this should not preclude an immediate/isolated escalation of the site's security posture should a direct threat be identified locally. Once you are aware of the current threat, it will then be possible for you to put into place a number of mitigation methodologies to counter the threat. These mitigation or 'Response' levels change and mirror the current threat against the site.

The **Threat** and subsequent **Response** levels should be based on a sliding scale as indicated below. However, it must be stressed that this scale is for illustration purposes only; country specific threat and response levels should be used:

Diagram C5a: Threat Level



Threat Level		Response Level
Critical	An attack is expected imminently	Exceptional
Severe	An attack is highly likely	Heightened
Substantial	An attack is a strong possibility	
Moderate	An attack is possible, but not likely	Low
Low	An attack is unlikely	

As the threat level increases, there are a number of 'Responses' to this threat that can be immediately put into place. This section deals with how you can put into place additional security measures that can be either enhanced or decreased in line with the threat.

Prior to starting this process, you should instigate baseline security measures or a 'Default Response Level'. These are measures that will permanently be in place irrespective of the current threat assessment. Such measure should include:

- Access to the facility must be strictly limited to authorised persons only
- When not in use, all gates and barriers must be in the closed/locked position
- Details of all visitors must be passed to the main entry point by the sponsor a minimum of 24hrs prior to arrival
- All vehicles using external site car parks to be monitored
- 100% searches of vehicles entering site
- All mail is screened by suitably trained staff; consider the use of a mail/parcel x-ray machine
- All unstaffed or rarely visited areas of the facility must be regularly patrolled by manned guard (if applicable)
- All staff should be aware of security procedures
- All staff should be security aware and report anything suspicious
- There should be an unknown/unescorted person challenge philosophy within the site

These baseline measures will form the foundation of any security enhancements in line with the current threat; the higher the threat/response level, the more robust and high profile the security procedures must be.

1 level up from the Default Response level: This should include 'additional' and sustainable protective security measures to be implemented, reflecting the broad nature of the threat, combined with specific business and geographical vulnerabilities:

- Patrolling by manned guards should increase
- A log of all vehicles using external car parks to be compiled
- Only essential visitors should be admitted – under guidance by the Security Manager
- Search of visitors' bags
- 10% searches of staff bags
- Robust checks of all incoming mail
- Cancel or delay any non-critical contractors' works Any critical works should be closely supervised
- Keep all staff informed of threat levels

2 levels up from Default Response level: This should reflect the 'maximum protective measures to meet specific threats and to minimise site vulnerability and risk'. These additional measures should include:

- Place all staff on full alert
- Maximise numbers of security guards
- Permanent high-profile patrols by security guards
- Additional checks of external car parks
- Close liaison with local Anti-Terrorist Police Unit
- Only visitors deemed essential by Security Manager should be allowed access to site
- 100% bag searches of all persons entering site
- Increase night-time patrols; consider the use of dog patrols
- Only essential vehicles, as specified by Security Manager, are to be allowed access to site

C5.3.2 Site Incident Response and Evacuation Plans

Purpose of Incident Response

In order that all personnel, including guards, have an understanding of the company's rationale behind the manner in which personnel employed within the site act and respond to a security-related incident, it would be prudent to include a brief explanation of the purpose of incident response. They may include, but not be restricted to:

- The protection of personnel, corporate image and infrastructure
- Assist emergency services during incident
- To comply with relevant laws and legislation
- To achieve a successful conclusion to a security-related incident

There are a number of incidents that will require a co-ordinated response from both the Security Manager and staff employed within the site. They may include, but not be restricted to:

- Unauthorised intrusion onto site
- Suspicious external activity
- Telephone Bomb Threat
- Suspicious Objects, including Improvised Explosive Device (IED)
- Postal Devices
- Chemical, Biological & Radiological (CBRN) Devices
- Protesters

In order that you fully understand what actions are suitable for nominated post holders during a security-related incident, it is suggested that he/she speaks to each person in order that their opinions are taken. The post holder will then become more receptive to the actions he/she will be expected to undertake. Furthermore, it is more logical for vital actions to be delegated to a post holder not an individual person. That person may, for various reasons, not be present during an incident and vital actions may not be done.

As an aid for those persons with nominated actions, it is suggested that a check sheet is placed within the Security Plan. This should allow the nominated person to methodically go through their actions and give a good level of assurance that all actions are completed. There should be specific sections within these check sheets for the person to complete by hand, for example the time each action was carried out. These check sheets will aid any post-incident investigation by either the Police or company security.

Each site and/or delegated person will require a bespoke checklist, but in order that you have an understanding regarding the actions to be taken and the layout of check sheets, a number of examples can be found at Annex 1 and 2.

C5.3.3 Chemical Biological Radioactive Nuclear (CBRN) Incident

Due to the particular complexities regarding a security-related incident involving a CBRN device, the following sections are designed to give you guidance to implement procedures to protect your staff from exposure.

The purpose of this framework is to assist you in the preparation of site-specific emergency procedures to respond to a CBRN incident. These are guidelines only and give generic advice on how to reduce the effects of a CBRN attack and how to deal with the incident should one occur. Local government or Police guidance should be sought prior to implementing any specific procedures regarding this type of incident.

Suspect devices come in many forms. They may arrive as mail or as larger packages, may be placed inside or outside buildings, and may contain explosives, CBRN materials, other poisons and hazardous materials. To an untrained eye, it is virtually impossible to determine whether a sealed box is an explosive device, or if it contains CBRN materials. Some devices may be a combination of the two. The principles for action on discovering a possible CBRN device are therefore largely the same as for any suspect item. But CBRN materials present other, often longer-lasting hazards than simple explosives. As a consequence, when compiling a security procedure document, a Security Manager needs to take into account additional considerations when handling an incident involving this type of devices.

CBRN devices could be used in many ways. The most likely are:

- Postal letters or packages
- Small amounts of agents released in enclosed spaces
- As a contact poison, smeared on regularly handled surfaces
- Insertion into an air conditioning system, air inlets, food or fresh water supplies
- A proxy device at an entry point or alongside a perimeter, such as an improvised blast or aerosol release (including hijacked toxic industrial chemical tankers or containers)
- Release from a covert or remote (timed) device, by spray or blast, from upwind of the intended target

Notwithstanding the above, consideration should also be given to a deliberate attack upon internal legitimately stored chemicals, which if released into the atmosphere or underground water supply could have a devastating effect offsite. Examples of such chemicals include, but are not restricted to, Condensate, Ammonia, Sulphur and Chlorine. Any stores, including amounts, exact location and protection measures regarding chemicals of this type should be recorded with the local Government environmental agency.

Any release of this type of chemical into the atmosphere or water supply should then invoke relevant legislation and procedures under either COMAH or SEVESO II.

C5.3.4 Procedural Security (Search)

The first level of any defence in protecting the site is through robust entry and search procedures, which should normally be conducted by the onsite guard force. As stated earlier, the manner and frequency of searches should be defined in line with the current threat and any response level.

C5.3.5 Procedural Security (Response)

With regard to an onsite incident which due to the involvement of legally held site chemicals, could have an impact to offsite infrastructure and persons, this will then invoke local COMAH and SEVESO II protocols.

With regard to site personnel, the following is a synopsis of the procedures that should be undertaken immediately upon receipt/report of a possible CBRN incident:

- It should be remembered that upon receipt of a threat or report of a suspected CBRN device, the emergency services are to be notified immediately
- Upon arrival, the senior Police or Government officer will take over primacy of all events and response to a CBRN incident
- If a suspected CBRN incident occurs in the open, occupants of surrounding buildings should immediately close all doors and windows and switch off both localised air conditioning and building forced-air circulation systems. Within your workspace all desk fans and PCs systems should be switched off
- Everyone should remain calm and stay within their buildings/ office until told to leave by emergency services
- Actions to be completed by the person finding a suspect device should be incorporated into your procedures

C5.3.6 Action to be taken on Detonation of a Suspected Device outside a Building

The following is advice that you should consider disseminating either through your security procedures or via a structured security education/briefing regime:

- If a warning is received, follow the instructions of the emergency services or Guards
- If no warning is received and a device detonates outside a building and any of the following occurs
- A strong smell of noxious fumes or unusual odours
- Unexplained or unexpected droplets or oily films or stains on surfaces and windows
- Unusual or unexplained liquid sprays, vapours or powders are seen
- Effects on living things, such as people or animals becoming nauseous, fainting, having difficulty breathing, having convulsions and becoming disorientated

The following actions should be taken:

- Immediately contact the Control Room and Guard House by landline and report the incident
- Shut off any office air circulation/conditioning systems, fans, photocopiers, printers, computers, heaters
- Close all windows and, on leaving a room, lock all doors, leaving the keys in the lock
- Go to a safe place within the building and await advice from the emergency services.
- DO NOT EVACUATE THE BUILDING until told to do so by the emergency services

C5.3.7 Post-CBRN Incident Recovery

The main focus of recovery is the protection of staff, corporate reputation and resumption of normal operating posture. With regard to staff, the full effects of a CBRN incident may not present themselves for some time after the incident. All staff suspected of being exposed to a CBRN incident will be extremely concerned regarding the short- and long-term effects on their health, the company should have access to crisis counsellors should staff require them. Furthermore, as much information as possible should be passed to staff regarding the possible after-effects of exposure.

C5.3.8 Telephone Bomb Threat Response

With regard to telephone bomb threats, it is good security practice to have a specific 'Bomb Threat Check List'. These should be easily accessible to all personnel who have an outside line. The check list should be completed as soon as possible after the event to ensure the integrity of the information. The check sheet should be easy to follow and offer a number of pre-formatted questions for the recipient of the threat to ask.

It must be remembered that the recipient of a telephone bomb threat will be extremely nervous and under a tremendous amount of stress. The use of these types of check sheets should ensure that some information will be collated and forwarded to the emergency services. An example of a check list can be found at Appendix 1.

C5.3.9 Search Plans

Prior to the planning of a search plan, there must be liaison between yourself and the emergency services, in particular the Anti-Terrorist Police and Bomb Disposal. They may wish for certain procedures to be undertaken during a search prior to their arrival. It is noteworthy that as soon as these services arrive, they will take full control of the incident and will require close liaison with both you and the person who either found the suspect device or took the threat phone call. The more information they have prior to entering the site regarding the location, description and any other relevant information, the higher the chance of disarming the device.

The search or Visual Check Plan should only be instigated by the Terminal Manager or Security Manager or their nominated deputies and will normally be in response to a bomb threat received in relation to the site. It must be understood that **all threats** against the site must be treated as real until such time they are either found to be false or the whole site is searched and nothing is found.

The emergency services will in most occurrences not wish to enter the site until such time the site personnel have conducted a visual search plan. This is due to them not having detailed knowledge of the layout of the site, including places where a device could be hidden. Site personnel who are knowledgeable about the layout of the site, especially their individual work area are better placed to complete the check quickly and more thoroughly, which of course is the object of the visual check plan.

When planning a visual check plan, you must take into account the critical infrastructure within the site and we suggest using the Red, Amber and Green methodology as detailed below:

Red Zones (Highest level). This would encompass areas where an attack could:

- Cause widespread death or injury inside or outside the site
- Cause very serious damage which leads to long-term closure of the site
- Cause maximum economic hardship to the company
- Cause irreparable damage to corporate reputation
- Give the attacker a media spectacular

Amber Zones (Middle Level). This would encompass areas where an attack could:

- Cause serious, but recoverable, damage to the site
- Cause injury to internal site personnel, but may affect personnel in close external proximity to the site
- Give the attacker media exposure but would not cause death inside or outside the site
- Cause grave embarrassment to the company and affect corporate reputation

Green Zones (Lower Level). The would encompass areas where an attack could:

- Cause some damage, but not to an extent which would affect the safe operation of the site
- Cause very minor injuries to only those directly affected by the attack, but not affect anyone external of the site
- Not give the attacker the media coverage intended
- Cause minor embarrassment to the company only

> *Should a suspect device be located, the decision must be made by yourself or nominated deputy whether there is a requirement to evacuate the site.*

C5.3.10 Evacuation

Should a suspect device be located, the decision must be made by yourself or nominated deputy whether there is a requirement to evacuate the site. The purpose of the evacuation is to move all personnel away from the area and into safe zones. All muster points and evacuation emergency gates are to be clearly marked and all visitors should be briefed as to the manner they make an emergency evacuation from the site.

C5.3.11 Media Response and Management

The primary aim behind this type of policy is to assist you in detailing the policies which should be put into place to protect the corporate reputation of the company should there be a security-related incident at the site.

Prior to putting into place any media response policy or internal training, it may be helpful to use a Media and Crisis Management company. Doing so should ensure that you have specially trained persons on hand to act on the company's behalf when dealing with the media. The media, especially if there was a major incident will be extremely interested in getting answers to both what occurred, why and how. One wrong answer or a comment made in jest could have major ramifications should it be taken out of context.

The importance of good media management during times of crisis was shown during 2010 with the Deepwater Horizon incident during which BP executives were criticized heavily for their handling of the press when under pressure in front of cameras and microphones.

Furthermore, the media will expect some form of regular updates or statements from the company – a contracted media company will be able to formulate documents such as ‘Holding Statements’ which will pass on relevant information to the media.

Any media company should be available to you 24 hours per day, 365 days per year and provide local response.

C5.4 Resilience

Resilience

- In this section we examine how security procedural elements can contribute to the overall Recovery function

C5.4.1 Post-Incident Recovery

As part of the company's quality assurance process, the Stakeholder analysis should have identified that 'recovery' from a security-related incident is a very important facet of the company's business methodology as a whole.

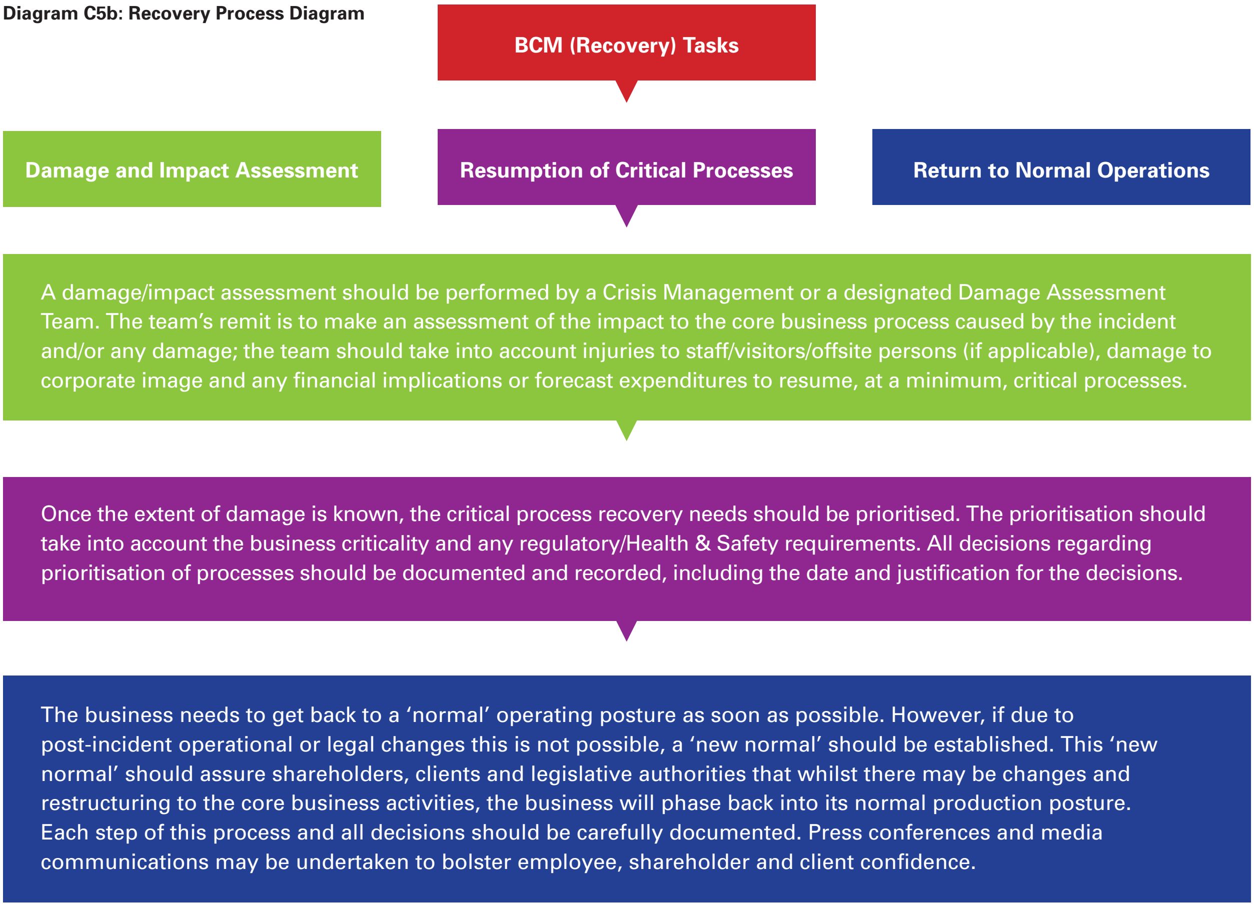
The aim of recovery is to aid the company in getting back to a normal operating posture and fulfil their contractual commitments, as soon as possible. The manner in which this is achieved should be set out within the company's Business Continuity Plan (BCP); however when putting together a policy for recovery within the security procedures, the company Crisis Management, Emergency Incident Response and BCP should be referenced.

C5.4.2 Business Continuity Considerations

In the event that a security-related incident results in a serious disruption to the operational effectiveness of the company, the BCP may be triggered and implemented. Should the plan be implemented, then it is recommended that you liaise closely with the company Business Continuity Advisor, regarding implementing security procedures that will complement, not hinder the plan.

The following is a short diagram indicating 'Recovery Process'.

Diagram C5b: Recovery Process Diagram



BCM (Recovery) Tasks

Damage and Impact Assessment

Resumption of Critical Processes

Return to Normal Operations

A damage/impact assessment should be performed by a Crisis Management or a designated Damage Assessment Team. The team's remit is to make an assessment of the impact to the core business process caused by the incident and/or any damage; the team should take into account injuries to staff/visitors/offsite persons (if applicable), damage to corporate image and any financial implications or forecast expenditures to resume, at a minimum, critical processes.

Once the extent of damage is known, the critical process recovery needs should be prioritised. The prioritisation should take into account the business criticality and any regulatory/Health & Safety requirements. All decisions regarding prioritisation of processes should be documented and recorded, including the date and justification for the decisions.

The business needs to get back to a 'normal' operating posture as soon as possible. However, if due to post-incident operational or legal changes this is not possible, a 'new normal' should be established. This 'new normal' should assure shareholders, clients and legislative authorities that whilst there may be changes and restructuring to the core business activities, the business will phase back into its normal production posture. Each step of this process and all decisions should be carefully documented. Press conferences and media communications may be undertaken to bolster employee, shareholder and client confidence.

C5.4.3 Post-Incident Investigation

A 'Security-Related Incident' can be defined as – any incident, physical or otherwise that compromises, or threatens to compromise, the security of the site.

Agencies such as the Police or Government Security Services will almost certainly take primacy regarding the actual criminal investigation following a security incident. You may well be looked to in order to supply senior management with answers regarding what occurred, how the incident occurred and what can be done to stop it occurring again and determining the lessons learned.

One tool that you may consider is the use of 'Post-Incident Debriefings'.

Purpose

- This will provide an opportunity for those involved, including outside agencies (Police) to put forward what went well, or indeed not so well during the incident. They will also have the opportunity to comment on possible improvements to the current security systems

Hot Debrief

- A Hot Debrief should be held immediately after the incident has occurred. It gives those involved a chance to share their views whilst the details are still fresh in their minds. It is important for you to record any views as 'bullet points' for future reference or to be used for future exercises

Structured Debrief

- This should be held days, even weeks after the incident. Participants will have had time to reflect upon the events and may be a little less emotional. It will allow a far more structured and formal approach and allow participants time to consider the effectiveness of the company's security procedures and operations

Agencies such as the Police or Government Security Services will almost certainly take primacy regarding the actual criminal investigation following a security incident.

C5

Annex 1: Guidelines for CBRN devices
Annex 2: Sample Checklists

Annex 1: Guidelines for CBRN devices

IF YOU FIND A SUSPECT CHEMICAL, BIOLOGICAL, OR RADIOLOGICAL DEVICE

If you discover a suspect item inside a building and you are concerned that it may contain CBRN material:

- If the item is still intact **DO NOT** shake, squeeze, or open it
- If it is an item of mail that you are already holding, place it in a transparent, sealable plastic bag or container. If you do not have a container cover it with anything to hand (e.g. clothing, paper, waste bin) and do not remove this cover
- Otherwise, do not touch or tamper with any suspect item or move it elsewhere
- Turn off all air conditioners, fans, photocopiers, printers, computers and heaters
- Close all windows and evacuate the room; lock all doors; leave the keys in the lock
- If practicable place a clearly visible warning on the door
- Go to an isolation room and avoid other people if you can. It is vitally important that you segregate yourself and others who may have come into contact with the suspicious package or substance to prevent further contamination
- Do not rub your eyes, touch your face or other people. Thoroughly wash your hands with soap and water as soon as possible
- Call Control Room and/or Guard House

IF A SUSPECT CHEMICAL, BIOLOGICAL OR RADIOLOGICAL DEVICE DETONATES OUTSIDE A BUILDING

If a warning is received:

Follow the instructions of the Emergency Services or the onsite Security Guards.

If no warning is received and a device detonates outside a building and any of the following happens:

- **Unexplained or unexpected droplets, or oily film, or stains appear on the surfaces or windows**
- **There are strong smells of noxious fumes or unusual odours**
- **Unusual and unexplained liquid sprays, vapours, or powders are seen**
- **There are unusual effects on living things, such as people or animals becoming nauseous, fainting, having difficulty breathing, having convulsions, becoming disorientated**

- Turn off all air conditioners, fans, photocopiers, printers, computers and heaters before leaving offices
- If time permitting and without endangering life secure all sensitive information within lockable drawers
- Close all windows and, on leaving a room, lock all doors, leaving the keys in the lock
- Go to a safe place (insert its location) and await instructions from security staff or the emergency services
- **DO NOT LEAVE** the building until told to do so by the emergency services

Annex 2: Sample Checklists

BOMB THREATS CHECK LIST

If you receive such a call it is vital that as much information as possible is obtained. As well as the obvious (accent, sex, age, etc.) careful listening may reveal other clues, e.g. background noise, presence of accomplices etc.

Once the call has ended DO NOT put down your receiver handset – the line may still be active and could provide valuable intelligence

Allow the caller to complete the message

1. DATE/TIME OF CALL________________________________HOURS

2. CALLER'S EXACT WORDS (KEEP PERSON TALKING – IT'S A BAD LINE; I CAN'T HEAR YOU; PLEASE SPEAK UP)

____

____

____

____

____

____

____

3. CALLER'S NUMBER IF SHOWN____

4. QUESTIONS TO ASK, IN THIS ORDER:

WHEN IS IT SET TO GO OFF?____

WHERE EXACTLY IS IT? ____

WHAT DOES IT LOOK LIKE? ____

WHAT KIND OF BOMB IS IT? ____

WHAT WILL CAUSE IT TO EXPLODE? ____

WHY ARE YOU DOING THIS?____

DID YOU PLACE THE BOMB?____

WHAT IS YOUR NAME? ____

WHERE ARE YOU? ____

5. IMMEDIATELY INFORM Security Manager (TIME) ___________________ (NAME)__________________________________

6. INFORM POLICE **(**TIME) ___________________ (NAME) __________________________________

7. COMPLETE THIS SECTION AS SOON AS POSSIBLE AFTER THE PHONECALL.

DESCRIPTION OF CALLER’S VOICE:

CHARACTERISTICS

- MALE □
- FEMALE □
- LOUD □
- SOFT □
- HARSH □
- HIGH-PITCHED □
- INTOXICATED □
- DEEP □

LANGUAGE

- EDUCATED □
- UNEDUCATED □
- REPETITIVE WORDS □
- MISPRONOUNCED □

ACCENT

- LOCAL □
- NON-LOCAL □
- ENGLISH □
- SCOTTISH □
- WELSH □
- IRISH □
- FOREIGN □

SPEECH

- FAST □
- SLOW □
- DISTINCT □
- DISTORTED □
- NASAL □
- DEFECTIVE □

MANNER

- CALM □
- DELIBERATE □
- ANGRY □
- RATIONAL □
- IRRATIONAL □
- INCOHERENT □

BACKGROUND NOISES

- ROADWORKS □
- RAILWAY □
- DOCKS □
- SCHOOL □
- PLAYGROUND □
- AIRCRAFT □
- TRAFFIC □
- PUBLIC CLOCKS □
- FACTORY □
- PUBLIC HOUSE □
- MUSIC □
- DISCOTHEQUE □
- ANIMALS □
- DOMESTIC □
- OFFICE □
- CHURCH BELLS □

OTHER: ____

ANY OTHER COMMENTS

____

____

7. TELEPHONE NUMBER CALL RECEIVED ON: ____

8. CALL MADE FROM: CALL BOX □ PRIVATE LINE □ MOBILE □

9. CHECK INFORMATION ON CALL LOGGER (IT STAFF)

SIGNATURE ____ **DATE** ______________________

SUSPECT EXPLOSIVE PACKAGES

Security Manager

Action	Time Completed
Commence own Log of Events	
Notify Terminal Manager/Deputy & Security Manager	
Contact Police (Emergency number ***). Inform them of the details of the incident. Advise on a safe rendezvous point	
Instruct all personnel **(via landline or word of mouth only)** to move to specified offices/safe area immediately. Instruct staff that they are **NOT** to use personal/vehicle radios or mobile 'phones until authorised by the Security Manager/Terminal Manager	
Consider the possibility of secondary devices, hazards and the potential injury from flying debris, when deciding upon any evacuation route. **Remember, whatever you decide, do not allow staff to pass through, or muster in, areas that have not been visually checked**	
Arrange to meet the recipient at the safe rendezvous point	
Contact Gatehouse Security Staff and advise them – i. The location of the suspect package ii. To prohibit access to the area around the package iii. To not admit persons or vehicles onsite without the express permission of the Security Liaison Manager/Terminal Manager iv. Not to use personal/vehicle radios or mobile 'phones until authorised by the Security Liaison Manager/ Terminal Manager	
Notify Site Control Room (Telephone –*************) of the incident	
Liaise with the Police Officers attending the Terminal	
Update the Site Control Room as to the progress/resolution of the incident	
Inform the Site Health & Safety Manager	
At the conclusion of the incident, ensure that: i. All personnel / relevant parties are advised that the incident has ended ii. A 'Security Incident Report' has been generated, in accordance with this Manual iii. Debriefing of the incident is arranged, in accordance with this Manual	

BOMB THREAT LETTER

PERSON RECEIVING THREAT LETTER

Action	Time Completed
Do not handle the letter unnecessarily, as this may damage potential forensic evidence. If you do have to handle the letter/envelope/contents, if possible use untreated disposable gloves	
Make a note of the contents of the letter, plus details of the envelope (postal address, postmark, etc.).	
If it is possible to photograph the letter without handling it excessively, this should be done – this will allow others to read the contents without handling the letter.	
If necessary, place in a clean, dry and secure place (for example, a locked desk drawer) where others will not touch it. A clean covering (such as an unused larger envelope or box file) is an alternative. Avoid the use of plastic document wallets, because some contain chemicals that may affect evidence preservation.	
Inform the Security Liaison Manager or Terminal Manager immediately, who should contact the police.	
Await further instructions from the Police/Security Liaison Manager.	

C6 Personnel Security

Purpose: To explain to the reader the requirement for robust personnel security management and to lay out how these link into the employee pre-screening process.

It allows you to mitigate the possibility of your organisation employing persons whose aims are to disrupt normal company operations.

Prior to implementation, you will need to discuss any employment pre-screening procedures with relevant Stakeholders to ensure compliance with any legislative requirements.

'Personnel Risk Management is a system of polices and procedures that manages the risk of staff and contractors exploiting legitimate access to an organisation's Assets or information for unauthorised purposes'. It is important to distinguish between Personnel Risk Management and Personal Security; the latter seeks to reduce the risks to the safety or well-being of employees – this is the realm of the HSE executive.

An effective personnel risk management regime seeks to:

Risk Reduction

- Reduce the Risk of employing personnel who are likely to present a security concern

Risk Likelihood

- Minimise the likelihood of employees becoming a security concern

Implementation

- Implement security measures in a manner that is proportionate to the risk

The use of these three steps should ensure an organisation can reduce the risk of insider activity, protect the organisation's Assets and information from theft, unauthorised disclosure or compromise and terrorist acts.

Why is a Personnel Risk Management Regime important?

There are elements within every society who seek to cause disruption or cause damage or embarrassment to an organisation's operational output; one way of achieving their goals is to exploit legitimate access to an organisation's Assets – the terms often used for these types of individuals is 'Insider, Mole or Sleeper'.

These people can take a variety of forms including disaffected staff, single-issue groups, investigative journalists, commercial competitors, terrorist groups or hostile intelligence services. Their motivations can be varied, political or religious ideologies, commercial intelligence gathering, terrorist targeting/intelligence gathering, financial gain, revenge or coercion.

As organisations implement increasingly sophisticated physical measures to protect their Assets such as CCTV, PIDS and Physical Barriers, the embedding of an insider into an organisation is becoming a more attractive attack method for those groups whose aims are to disrupt the organisation's operational output.

To combat this threat there are a number of defence methodologies that an organisation can implement to mitigate the risk of the wrong person being employed:

C6.0 Employment Pre-Screening (Vetting)

Effective pre-screening seeks to verify the credentials of employment applicants and to check that the applicants meet preconditions of employment such as whether the individual is legally permitted to take up any offer of employment. During the pre-screening process any attempts by the applicant to conceal important information or misrepresent themselves should come to light. To this extent, this type of pre-screening could be viewed as a test of character.

Moving on from this, where a role involves the individual holding a post which may give them access to more commercially sensitive material, or government information (Protectively Marked Material) a more robust pre-screening process becomes important. This screening then takes into account an applicant's integrity, reliability and possible previous criminal activities.

Identity

- Use of photographic ID (Passport or Driving Licence). The applicant must present an original only, not photocopies

Employment History

- Provide contact details of previous three years' employment history, including any references

Nationality and Immigration Status

- Use of original passport and any relevent and in-date UK Government issued immigration certification

Criminal Record

- Details of any previous criminal convictions. In line with any rehabilitation of offenders laws

In addition to this information, any prospective employee must give a reasonable account for any significant periods (6 months or more within the last 3 years) of any time unemployed or spent abroad. This should also include any periods whilst self-employed.

C6.1 Annual Security Appraisal Questionnaire

When conducting any personnel security checks on prospective staff, you must recognise that this is only a snap-shot of the subject at the time of checking. In the case of disaffected staff or those who may have, due to their position, been targeted/ recruited by an environmentalist group; this will almost definitely occur whilst that person is under employment.

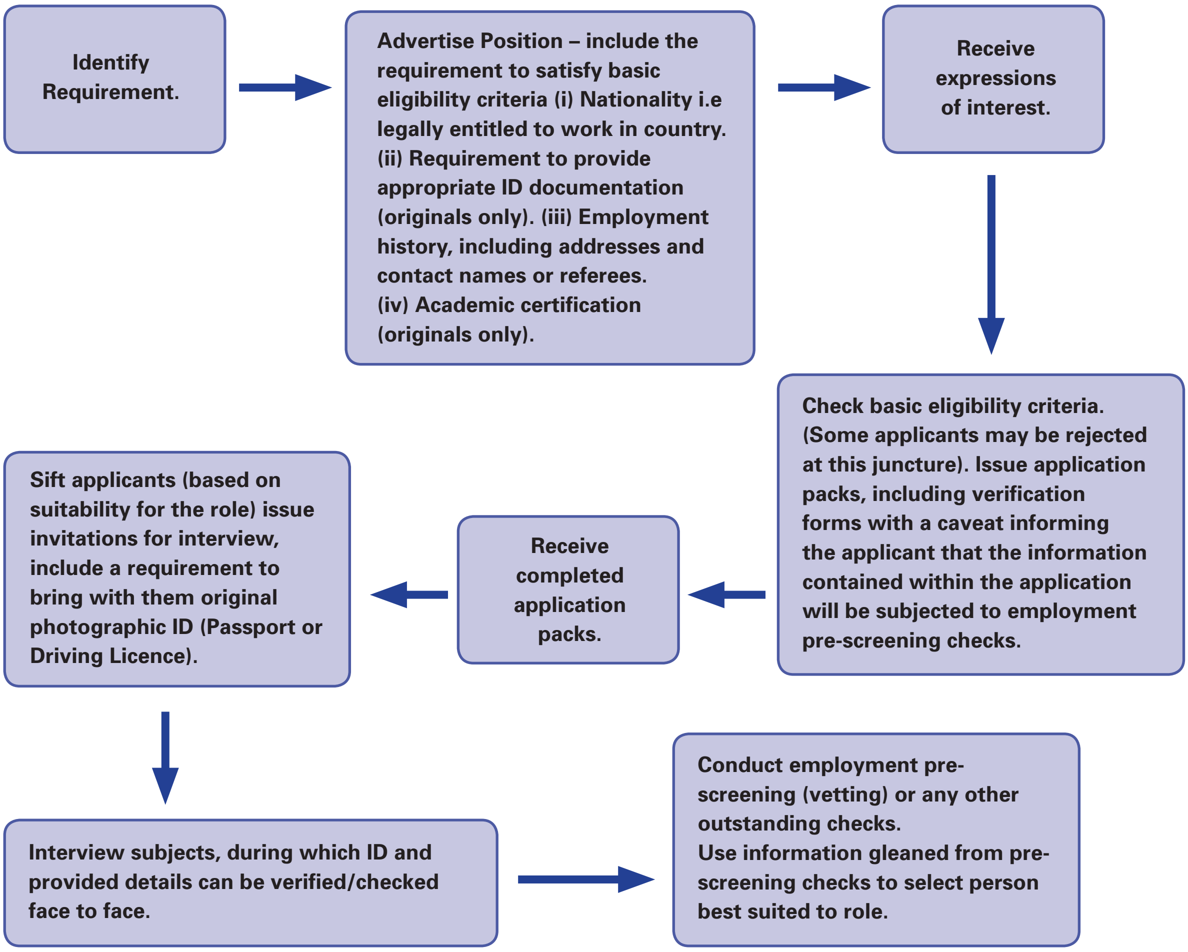
As a consequence any security check implemented prior to this event or occurrence will have no bearing on their current security threat to the company. One way of mitigating this risk is to conduct annual security appraisals using a very short standardised questionnaire which would be completed annually by the subject's direct supervisor.

The form requests a short synopsis of the performance of the subject over the previous years, including:

- Any significant security-related occurrences the supervisor deems relevant or may question the subject's integrity or reliability i.e. was the subject involved in any regular breaches to security protocols.
- Any significant lifestyle changes i.e sudden unexplained wealth or sudden lowering of personal standards.
- Significant changes in attitude against the company, good or bad.
- Has the subject declared any criminal convictions?
- Is there anything else about the subject that worries the supervisor, or that could indicate a matter of potential security concern?

Where it is found there is a possibility that the subject may have been involved in activities that could be detrimental to the company, a second employment screening check should be conducted. The results of which, if still found to be of concern, should be dealt with at senior management level in close consultation with the company legal representatives.

Diagram C6a: Pre-Employment Procedures



Identify Requirement.

Advertise Position – include the requirement to satisfy basic eligibility criteria (i) Nationality i.e legally entitled to work in country. (ii) Requirement to provide appropriate ID documentation (originals only). (iii) Employment history, including addresses and contact names or referees. (iv) Academic certification (originals only).

Receive expressions of interest.

Check basic eligibility criteria. (Some applicants may be rejected at this juncture). Issue application packs, including verification forms with a caveat informing the applicant that the information contained within the application will be subjected to employment pre-screening checks.

Receive completed application packs.

Sift applicants (based on suitability for the role) issue invitations for interview, include a requirement to bring with them original photographic ID (Passport or Driving Licence).

Interview subjects, during which ID and provided details can be verified/checked face to face.

Conduct employment pre-screening (vetting) or any other outstanding checks. Use information gleaned from pre-screening checks to select person best suited to role.

C6.2 On-Going Monitoring

As part of an organisations personnel security culture it is useful to conduct regular but infrequent audits of your security systems. This will allow management to ensure that personnel are adhering to the organisation security policies and procedures. A convenient offshoot of these checks and audits is the possible detection of unauthorised 'insider' activity.

If, whilst conducting such checks and audits, criminal violations are found, for example downloading images contrary to the national legislation or laws, then the appropriate authorities are to be contacted (Police). However, for infringements against company security policies, it is important to follow the appropriate disciplinary procedures; this will then send out a clear message that behaviour of this type will not be tolerated and in turn should encourage personnel to adhere to the organisations security policies and procedures.

There are a number of procedures that could be implemented to detect infringements against the organisations policies:

- Random checks of staff entering or leaving the premises for prohibited items, such as mobile telephones, personal digital assistants or sensitive documents
- Electronic detectors which are designed to alert a control room should a mobile telephone be used
- Random checks of websites visited
- Monitoring of electronic mail, including blocking mails over a set size

This is covered in more detail within Phase C4 of this document.

C6.3 Restricting Access To Sensitive Material

In order to put into place a delay strategy regarding access to sensitive or restricted material, principles such as the 'Need to Know' or 'Need to Hold' as discussed within Phase C5, you should enforce and ensure they are strictly adhered to.

The physical and electronic equivalent to these two principles is 'role based access'. This principle limits access to such material according to their role within the organisation. For example, access to financial restricted material would be restricted to only those who are employed within the finance department or access to personnel files would be restricted to HR staff only.

As with all things security-related, there is a requirement for regular reviews and audits; personnel may change positions or departments and could still have access to material now not within their scope.

Measures as described within Phases C3 & C4 should be referenced when planning or implementing procedures such as this.

As with all things security-related, there is a requirement for regular reviews and audits; personnel may change positions or departments and could still have access to material now not within their scope.

Phase D

Implementation & Review

PHASE D

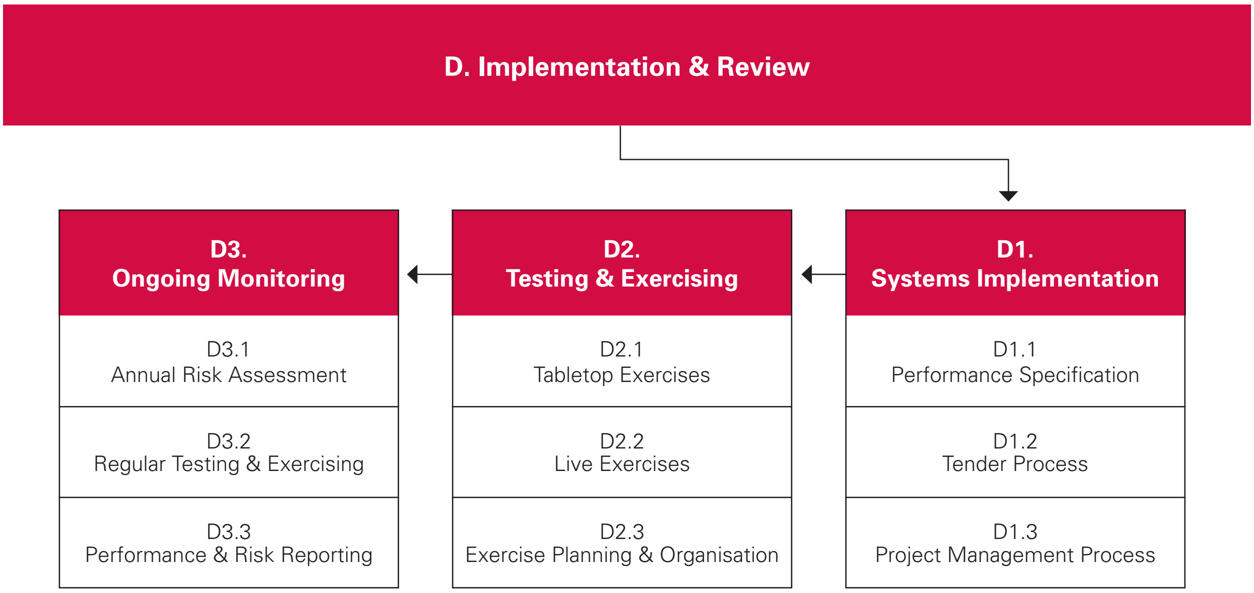
Executive Summary

Implementation & Review

Phase D details the procedures to be followed once the design stage has been completed and passed by the Stakeholders for implementation. It is broken down into three distinct sections which take the process from planning through construction and testing to monitoring performance against the risk indicators.

Although some areas of the separate sections may be governed by local laws and procedures, this Phase will give you a format with which you can foresee the method by which your project will move towards completion. Then, once completed, the ongoing training and monitoring that will need to be implemented to ensure that your site and employees remain focused to all Threats, current and perceived.

The three sections which make up this Phase are shown in the following diagram and outlined further below.



D. Implementation & Review

D3.
Ongoing Monitoring

D3.1
Annual Risk Assessment

D3.2
Regular Testing & Exercising

D3.3
Performance & Risk Reporting

D2.
Testing & Exercising

D2.1
Tabletop Exercises

D2.2
Live Exercises

D2.3
Exercise Planning & Organisation

D1.
Systems Implementation

D1.1
Performance Specification

D1.2
Tender Process

D1.3
Project Management Process

1. **Systems Implementation**
   a. **Performance Specification**
   This sub-section will provide you with guidance on the importance of a robust Performance Specification and incorporates performance criteria previously alluded to. It includes the production of a Performance Requirements identifying the security measures needed.

   b. **Tender Process**
   This sub-section will assist you to identify the procurement process most suitable for your project and provide information required to develop an evaluation process which will deliver value for money and remain transparent.

   c. **Project Management Process**
   This sub-section will provide you with an explanation of the project management process required to show that the security and resilience is delivered on time and in budget. It emphasises the need to appoint a Project Manager who is competent, capable and has the experience necessary to deliver your project to your Stakeholders' expectations.

2. **Testing and Exercising**
   This will define the process required to plan for an effective response to an emergency incident and further to plan, undertake and evaluate emergency exercises to ensure that response procedures are likely to be effective in mitigating real-life incidents and employees understand the actions required of them in an emergency to minimise associated hazards to both themselves and the facility at which they work.

3. **Risk Reporting**
   Following on from the risk indicators already agreed by the Stakeholders, this section will provide guidance on how you can put together a performance-based security risk report that will monitor performance against the risk indicators. The importance of this section is evident, because it will provide a critical analysis of how successful the Security Management Plan has been in delivering the objectives it sought to fulfil at the outset.

This final phase of the formation of a Security Management Plan completes the cycle towards the management of risk at your site in a cost-effective, quality-assured manner. All aspects of the security risk management process must henceforth be open to an audit process that ensures that a) the process has been implemented as well as it should be; and b) remains current and reflective of the dynamic environment it seeks to operate within.

D1 Systems Implementation

Purpose: The Systems Implementation section of Phase D is divided into three parts that form the initial processes to be considered as part of the post-Design phase. The three phases of D1 Systems Implementation (Performance Specification, Tender Process and Project Management process) are critical to moving any project forward to completion.

D1.1 Performance Specification To provide a template for the Security Manager which gives guidance on the importance of a robust performance specification and incorporates the Performance Requirements criteria agreed previously. This will support the discussion of the potential requirement for external support with detailed design and performance specification.

D1.2 The Tender Process To provide guidance for an owner/ operator in relation to the Tender Process and the provision of related technical and commercial evaluation templates.

D1.3 Project Management Process To provide an explanation of the Project Management Process required to ensure that the investment approved to enhance security and resilience around the Asset is delivered on time, on budget and represents value for money.

D1.1 Performance Specification

D1.1.1 Introduction

Having identified an Asset as being of critical importance and received the design advice as outlined in Phase C: Design; you will need to undertake a process to implement the required security enhancements in order to deliver an Integrated Security System (ISS) capable of meeting your Performance and Risk-based requirements, as identified in phases B and C of the process. This will not only have to provide a level of security commensurate with the assessed risks, but also deliver cost-effective results which demonstrate value for money to Stakeholders.

In order to ensure that the above requirements are met it is recommended that a Performance Specification be produced for all planned security enhancements. This key document is discussed in further detail in the following sections, along with key considerations for its creation.

D1.1.2 Planning

Before writing the Performance Specification for the required security enhancements it will be necessary to conduct some preparatory work which builds upon your formalised security system performance requirements as established in Phase C. This will include the following:

- Consultation with Stakeholders about what is needed and the budget that is available to fulfil the need
- Engagement with the market to understand the solutions that may be available and to get feedback on how the requirement may be best met
- Establishment of effective governance arrangements and resourcing plans
- If the owner/operator does not have the necessary expertise, the appointment of specialist security advisers to help ensure that the project is established on a sound footing

The above work will help ensure that you have the necessary resources and information available to produce an effective Performance Specification. In particular, consideration should be given to the use of an independent security design consultant to help translate your performance requirements into a detailed design, particularly for large or complex projects where most installation companies will lack adequate design expertise or may attempt to skew your requirements to meet their commercial interests.

D1.1.3 Creating the Performance Specification

The Performance Specification document will set out your performance requirements for each component of the ISS as well as the system as a whole in terms of what it must functionally achieve. It will subsequently become the basis upon which to Tender for the supply, installation and commissioning of the various security systems, whilst also providing objective performance criteria against which the standard of installation can be measured prior to project sign-off thereby ensuring that the contractor can be held accountable for the standard of installation and the successful implementation of your requirements. As such it is vital to the success of the Systems Implementation Phase and should be given significant time and attention.

As part of the Phase C design process, you will have identified Performance Requirements for each required security system, in line with your risk-based performance requirements in the areas of Detection, Delay, Response and Recovery (DDRR) as identified in C1. These will now be put to very good use since they will form the heart of your Performance Specification document. Providing that they are objective, clear and specific they will ensure that your requirements are understood by contractors and can be measured against to ensure that they are met.

Therefore, the starting point for the creation of the Performance Specification will be to set out all of your established performance requirements, grouped by individual sub-systems. You should then supplement this with the following information:

- Additional Performance Requirements for the ISS as a whole, where they have not already been covered. In particular you should ensure that the required level of integration between each sub-system is addressed
- Any specific functional requirements in terms of how the system will operate and the interfaces between technology and people
- Any specific Stakeholder requirements established in Phase A, such as how the system will integrate with existing technology, be managed by users and be maintained. This may also include any regulatory requirements that need to be met such as adherence to planning laws, building and fire codes or health and safety regulations
- Any international standards relating to security systems as discussed in various parts of Phases A, B and C of this document
- Any general environmental performance requirements in line with the context in which the systems will operate

Once all of the above information has been compiled it will then be necessary to decide upon the best method of producing a detailed systems design that meets all of these requirements. Unless there is specialist expertise available within the business this will usually require some form of engagement with external providers and the information already produced will provide an excellent basis for doing this. For smaller projects it may be appropriate to go directly to a number of technology providers or installation companies and ask them to draw up an appropriate design, which can then be used in addition to your own Performance Specification as the basis for the Tender documentation. However, as highlighted previously it is important to bear in mind that infrastructure security design is a very specialist area and the majority of such companies, whilst having specific knowledge in areas such as CCTV or Access Control, may not have the experience to translate your requirements into a design capable of delivering the most cost-effective solution in the context of a complex energy infrastructure environment. Furthermore nearly all such companies will have commercial bias towards certain products or maximising sales volumes.

For these reasons it is highly recommended, particularly for large projects, that you invest a small amount in independent design consultancy from a company with an established track record in the energy sector, since this is likely to result in long-term (and often short-term) cost savings. They will be able to provide an objective assessment of various technologies that can be used to meet your requirements and subsequently build upon your Performance Specification to include detailed designs, technical requirements and minimum standards for each component of the ISS, along with design drawings and suitable integration methods. This will complement the key performance requirements, ensuring that the design is cost-effective and the project scope unambiguous therefore leaving little room for variations or justifications for inadequate performance at a later date.

D1.1.4 Summary

At the end of this process you should have a comprehensive Performance Specification that defines the functional performance of the ISS. The Performance Specification must reflect and build upon the Security System Performance Requirements identified at Phase C, therefore ensuring that the risks identified in Phase B are adequately mitigated through the implementation of the eventual solution.

D1.2 The Tender Process

D1.2.1 Introduction

All Security Managers will be responsible in any project for achieving value for money, normally through fair and open competition. In addition they must comply with their legal obligations under Domestic Law and EU procurement rules, and adhere to the EU Treaty principles, the most important of these being:

- Equal Treatment
- Non-discrimination
- Mutual Recognition
- Proportionality
- Transparency

So this Section provides the relevant background information you will need in order to ensure that the procurement process you may undergo in order to deliver the ISS designed in Phase C is compliant and fair.

EU Procurement Directives provide for four main procurement procedures to be used by all persons. For straightforward procurements there is a choice between the open and restricted procedures. For more complex procurements contracting authorities are normally expected to use the ‘Competitive Dialogue’ procedure, which is where a contracting authority wishes to award a particularly complex contract and considers that the open or restricted procedure will not allow the award of that contract.

The EU Procurement Regulations define ‘particularly complex contract’ as a contract where a contracting authority is not objectively able to:

- Define the technical means capable of satisfying its needs or objectives, or
- Specify either the legal or financial make-up of a project

Step 1: Tender Procedure

There are four procedures available for choice.

I. The Open Procedure

Under the Open Procedure, all interested candidates who respond to an advertisement must be invited to tender. This procedure does not allow any form of pre-qualification or pre-selection.

II. The Restricted Procedure

Under the Restricted Procedure, interested candidates are invited to respond to an advertisement by submitting an expression of interest in which they reply against defined criteria relating to their organisation's technical capability and financial standing. A shortlist of candidates is then drawn up and invited to tender. There is no scope to negotiate with tenderers following receipt of bids.

Many Contracting Authorities prefer the Restricted Procedure. The separate selection and award stages allow them to restrict the number of candidates who will be invited to tender, which reduces cost and improves manageability.

III. The Competitive Dialogue Procedure

For complex procurements, the Restricted Procedure is usually too inflexible as it allows only limited discussion and dialogue with bidders. Contracting Authorities should therefore normally follow the Competitive Dialogue Procedure, unless there are exceptional circumstances that would justify the Negotiated Procedure.

The Competitive Dialogue Procedure is a flexible procedure, suitable where there is a need for contracting authorities to discuss aspects of the proposed contract with candidates. Under competitive dialogue, a similar pre-selection procedure is undertaken to that used for the Restricted Procedure. Shortlisted parties are then invited to participate in dialogue, which may have several stages. This helps to refine the requirement through supplier input and gives the opportunity for meaningful negotiations.

Once this stage is concluded, suppliers are invited to submit a final Tender. There is only one provision for the Contracting Authority to ask bidders to 'clarify, specify and fine tune' their final bids before a preferred bidder is chosen.

IV. Competitive Negotiated Procedure

This procedure is limited to very specific circumstances and should only be used where other procedures will not work. It may be valid when:

- Competition is not viable or appropriate
- Other procedures have not produced an acceptable Tender
- Work is needed for research and development purposes
- Where prior overall pricing is not possible

There are also circumstances where this procedure can be used without call for competition; however, the European Commission may look at the rationale for any negotiated contracting exercise.

Step 2: Evaluation of Tenders

Tenders are assessed against criteria set out in the Invitation to Tender advertisement or in the Tender Documentation. The assessment should follow the pre-defined evaluation strategy and be consistent with the ultimate objectives of the procurement/project. The financial and qualitative elements of Tenders are assessed separately.

Weightings may be applied to the criteria to allow price and non-price factors to be scored to reflect their importance to the project and to arrive at a final value for money judgment. For complex procurements, this process requires skilled and experienced staff, which may include external specialists who have knowledge of the main technologies that are likely to be proposed and can assess the technical merit of bids against the original Performance Specification and systems design. The final selection should be the Tender which offers best overall value for money.

Step 3: Evaluation Plan Templates

An essential component of evaluating Tenders of any sort is the preparation of a sound Evaluation Plan. An Evaluation Methodology document should provide assurance to the Contracting Authority, that the proposed approach is fair, transparent, consistent, EU-compliant and able to deliver the objectives of the project. Approval of the Evaluation Methodology must be obtained from the Contracting Authority prior to the issue of the Invitation to Tender.

There are a number of facets of the Evaluation Plan's construction and processes and brief analyses of these could be formulated along the following lines:

3.1 e-Evaluation

There are a number of e-Evaluation tools available. These tools assist the Tender Evaluation Team in working collaboratively, developing evaluation documents, structuring assessment criteria, evaluating Tender Responses in a secure, common working environment.

The benefits of using an e-Evaluation tool include:

- Improved efficiency through better co-ordination and visibility of the Evaluation Process
- Reduces risk by providing a robust and defensible audit trail of the evaluation and award decision, by providing visibility of the scores awarded by the Tender Evaluation Team
- Encourages the adoption of best practice by reusing previous evaluation models and processes
- Can be undertaken at the evaluator's desk creating flexibility
- Reduces the need for hard-copy documents

If it is the intention to use an eEvaluation tool, refer to the proprietary software to be used and ensure its application is reflected at the relevant stages in the Evaluation Methodology.

3.2 Compliance Checks

These checks will be undertaken in two stages:

- **Stage 1 – On receipt of Tenders**

  A cursory check to ensure all relevant documentation is included within the Bidder's Response, for example signed Form of Tender, Response to Specification.

- **Stage 2 – Pre-Qualitative Evaluation**

  A more in-depth check to ensure the level of detail required for example copies of supporting documentation (communication or marketing plan) and evidence (method statements, case studies, references) have been provided.

Any instances of non-compliance at either stage should be recorded and reported to the Evaluation Manager.

3.3 Qualitative Evaluation

The Qualitative Evaluation process will refer to those sections of the Tenderer's Response which relate to Specification, Technical Requirements, Mandatory Information Requirements, delivery and quality. This process will be undertaken independently and without sight of the Tenderer's price/cost submission.

These will be evaluated in accordance with the agreed evaluation criteria and weightings identified in the ITT. The table below gives an example of the criteria and application of weightings for a qualitative evaluation, weighting and criteria should be amended as required.

Table D1.2a: Qualitative Evaluation Assessment

High-Level Criteria	Low-Level Criteria	Low-Level Weighting	High-Level Weighting	ITT Reference
After-Sales Service	Availability	30%	**30%**	(Insert section, schedule, page number etc)
	Reliability	30%		
	Maintenance	25%		
	Staff	15%		
	Total	**100%**		
Technical Merit				
Delivery				
Quality				
Total			**100%**	

Source: PRISM™

A marking scheme with which to record the values of the Tenders submitted should be adopted and shown to be clearly outlined in the Evaluation Methodology. Responses to the above table will be scored using a pre-defined marking scheme and will be recorded along with the Evaluator's comments.

An example of the scoring definitions is provided in the table below, these are not comprehensive but can and should be adapted as each case dictates.

Table D1.2b: Qualitative Evaluation Scoring

Assessment	Score	Interpretation
Excellent	5	Exceeds the requirement
Good	4	Satisfies the requirement with minor additional benefits
Acceptable	3	Satisfies the requirement
Minor Reservations	2	Satisfies the requirement with minor reservations
Serious Reservations	1	Satisfies the requirement with major reservations
Unacceptable	0	Does not meet the requirement

Source: PRISM™

3.4 Commercial Evaluation

A detailed description as to the method which will be adopted to undertake a Commercial Evaluation will be included in the Evaluation Methodology which should consider:

- Price
- Cost
- Risk
- Legal Aspects

Details required of the scoring process will include:

I. Will the financials (price/cost) be evaluated independently of the rest of the Commercial Response?

II. How will the financials be evaluated and what will constitute a pass or fail?

III. Will the non-financial elements of the Commercial response (risk/legal) be formally scored?

3.5 Recommendations and Approval

An overview of the entire Evaluation Process will be undertaken to ensure that the Tender Responses have been evaluated in accordance with the approved Evaluation Methodology. Recommendations will be agreed upon and put to the appropriate authority for approval.

Step 4: Key Competition Factors to Consider

The following table sets out several points to consider on receipt of more than one competitive bid.

Table D1.2c: Evaluating Competitive Bids

Tender Process/ Contract Preparation	Ensure the same, relevant information is available to all bidders to demonstrate that the bid is winnable.
Duration of the tendering process	Consider optimal contract duration to achieve best competitive leverage.
Contract management	If competition is good, consider shorter contracts with break clauses to allow for regular competitions, thus realising the potential for optimal prices in a market that is dynamic and competitive.
Incentives	Include benchmarking provisions within the contract terms so that the contractor is incentivised to minimise costs, respond to market movements and maintain efficient performance levels.

Source: PRISM™

D1.2.2 Summary

As a result of using this Section, you should be able to identify which type of procurement process is suitable for your project; and develop a robust evaluation process to ensure that the process delivers the value-for-money solution you need to justify to the finance department who will approve the expenditure required to deliver the work.

D1.3 The Project Management Process

D1.3.1 Introduction

A project is a unique set of co-ordinated activities, with definite points at the start and finish, undertaken by an individual or a team to meet specific objectives within defined, cost and performance parameters as specified. It should have the following characteristics:

- A finite and defined lifespan
- Defined and measurable business products (deliverables and/or outcomes to meet specific business objectives)
- A corresponding set of activities to achieve the business products
- A defined amount of resource
- An organisation structure, with defined responsibilities, to manage the project

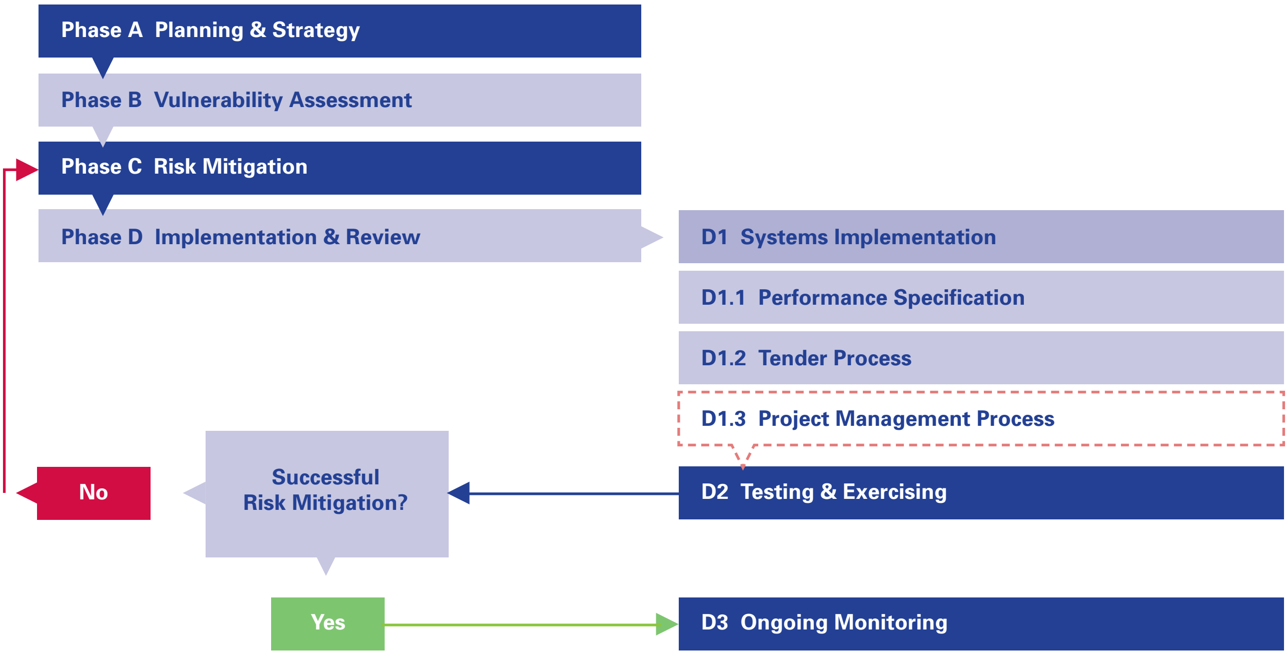
Project Management is a combination of the roles and responsibilities of individuals assigned to the project, the organisational structure that sets out clear reporting arrangements and the set of processes to deliver the required outcome. It ensures that everyone involved knows what is expected of them and helps to keep cost, time and risk under control.

Experience has shown that projects are inherently at risk – through overrunning on time and cost and/or failing to deliver a successful outcome. Such failures are almost invariably caused by:

- Poor project definition by the project's owners, perhaps because of insufficient consultation with Stakeholders or their failure to be specific about requirements and desired outcomes
- Lack of ownership and personal accountability by senior management
- Inadequately skilled and experienced project personnel
- Inadequate reporting arrangements and decision-making
- Inconsistent understanding of required project activities, roles and responsibilities

These points are as relevant for a project such as this and also for the project you have run to create the Security Management Plan in the first place, albeit involving less resources and investment – both require the same framework. It should be apparent early on in this section that project management is an integral part of the Security Management Plan. Diagram D1.3a alludes to the likelihood that poor project management will lead to failure at the Testing & Exercising stage of Phase D which in turn will require repetition, delay and expensive retrograde action.

D1.3a The Project Management Process as part of PRISM


Phase A Planning & Strategy
Phase B Vulnerability Assessment
Phase C Risk Mitigation
Phase D Implementation & Review
D1 Systems Implementation
D1.1 Performance Specification
D1.2 Tender Process
D1.3 Project Management Process
D2 Testing & Exercising
Successful Risk Mitigation?
No
Yes
D3 Ongoing Monitoring

Source: PRISM™

Project Management helps to reduce and manage risk. It puts in place an organisation where lines of accountability are short and the responsibilities of individuals are clearly defined. Its processes are clearly documented and repeatable, so that those involved in the project can learn from the experience of others. Key attributes of successful projects are:

1	A well-defined scope and agreed understanding of intended outcomes.
2	Active management of risks, issues and timely decision-making supported by clear and short lines of reporting.
3	Ongoing commitment and support from senior management.
4	A senior individual with personal accountability and overall responsibility for the successful outcome of the project.
5	An appropriately trained and experienced Project Team and in particular a project manager whose capabilities match the complexity of the project.
6	Defined and visibly managed processes that are appropriate for the scale and complexity of the project.

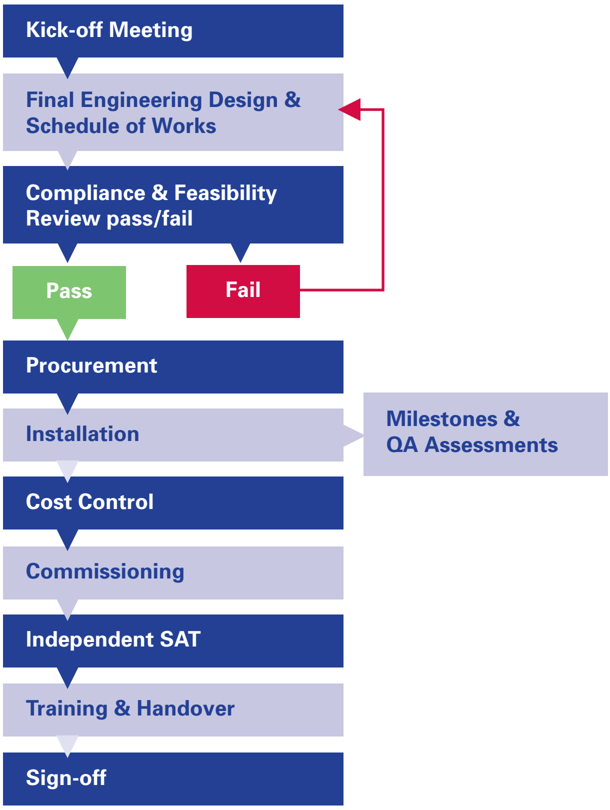
D1.3.2 Project Management Process

The Project Management Process (PMP) is an adaptable procedure that, due to the very nature of the task, has to be robust and transparent and yet at the same time, able to accommodate the changeable circumstances that exist. Any project will have four key elements around which the PMP will sit. These are:

- Resources – people, equipment, material
- Time – project duration, deadlines, delays
- Money – costs, contingencies, budgets, overspends
- Scope – project size, objectives

In addressing the challenges that face a Critical Infrastructure Security Enhancement Project the PMP has been divided into distinct parts, each part being represented in the process map illustrated in diagram D1.3b and explained in more detail later on in this section. Some of the constituent parts of the process map will be given more time and focus depending on the nature of the project in question, the composition of the Project Team, local conditions and methods adopted by the Project Manager; however, each part should be addressed at some time during the project.

D1.3b The Project Management Process



Source: PRISM™

Kick-off Meeting – The beginning of a project requires a meeting to introduce the key project members and Stakeholder representatives. There is no set template for conducting the kick-off meeting but the following points should be covered:

- Project framework to determine project objectives and criteria for successful completion
- Establish project governance – who does what, reporting procedures, responsibilities
- Establish sequence of events and determine timelines
- Establish key milestones
- Define the quality management plan and change control procedures

Final Engineering Design & Schedule of Works – Once appointed the Contractor will produce a Final Engineering Design which sets out exactly how the chosen systems will be installed, configured and integrated with existing systems. This will include detailed engineering drawings, wiring diagrams, topographical mapping with co-ordinates for outdoor equipment etc. The contractor should also produce a detailed Schedule of Works and project plan which establishes a timetable for the steps necessary to complete the project, including any requirements from the client such as permits and access. The Schedule of Works must take into account the following:

- Dependencies within the project
- Resource allocation
- Duration
- Deadlines
- Identifying deliverables and the activities needed to complete
- Linking activities in their logical sequence
- De-confliction between contractors
- Elements that may delay or add unavoidable additional time – weather, public holidays, local laws regarding working hours
- Constant review of the Works Schedule and weekly project meetings to discuss progress

Compliance & Feasibility Review – Before allowing the appointed contractor to commence with the procurement and installation phase, the Final Engineering Design should be reviewed to ensure feasibility and compliance with the performance specification, thereby ensuring that any errors or omissions are identified at the outset and can be corrected without additional costs or project overrun. The owner/operator's MEP, Civil and IT departments are likely to be best placed to assist with this review, although external support from independent security specialists may also be required. In addition the Schedule of Works should be carefully reviewed to ensure that it meets the overall project management plan and will not cause unnecessary operational disruption to the Asset.

Procurement – The Contractor will usually be responsible for procurement, however they should be asked to provide a detailed procurement plan in order to ensure that the ordering, receipt and acceptance of items required for the installation is managed correctly. Depending on the nature of the project, the procurement process may involve multiple suppliers and can also be used to specify how supplier relationships will be managed. Effective procurement management will also ensure that agreed service levels are maintained and budgets met. Whilst there are no universal methodologies for procurement management, the following elements should be addressed in the Contractor's procurement plan:

- Supplier/Client agreements established early on with service levels agreed as part of the contract – Define your requirements
- Selection criteria for choosing suppliers
- Establish controls to verify specifications and manage changes
- Budgetary limitations
- Review performance of suppliers in line with contracts
- Delivery issues
- Lead-in times for components
- Component dependencies
- Inclusion of procurement issues as part of project meetings
- Supplier capability to meet short-notice changes

Installation – Milestones & Quality Assurance Assessments – Once the Installation has begun, the project is overseen by the Project Manager and Project Management Team. On completion of each phase in the construction (Civil Works, Fencing Installation, First Fix, CCTV etc) consideration should be given to the use of independent Auditors to issue Quality Assurance certificates in relation to the standard of installation and compliance with the original design. Exceptions to this should be reported immediately to the Project Management Team for prompt action to be taken to solve the shortfall. Depending upon the quality of preparation for the design of the project, any oversights in the designs can be dealt with by way of Variation Orders which allow for an approved change to be made to a specification or to the project.

Cost Control – Cost Control is the application of processes in order to provide realistic analysis of the project's budgetary progress. Cost Control should:

- Be initiated early and included as an integral part of the regular project meetings
- Report budgetary anomalies to the Project Team as early as possible
- Document cost changes and fluctuations
- Identify causes of cost changes
- Investigate cost changes and recommend corrective measures to re-establish parity between actual and budgeted costs
- Establish that actual costs are in line with industry standards – 'Value-for-Money'

Commissioning – On completion of the installation phase the project enters Commissioning. This is defined as 'a quality oriented process for achieving, verifying and documenting that the performance of the systems meets defined objectives and criteria'. Commissioning ensures building quality using peer review and in-field or onsite verification. Further, the commissioning process formalises review and integration of all project expectations during planning, design, construction, and occupancy phases by inspection and functional performance testing and oversight of operator training and record documentation. As part of the commissioning process contractors should prepare a method statement outlining the sequence of examinations and tests that are to be carried out.

Independent Site Acceptance Testing (SAT) – In addition to commissioning procedures carried out by Contractors, it is important particularly for large high-value/risk projects to conduct independent Site Acceptance Testing, which objectively measures the level of systems performance against the original performance requirements in a quantifiable manner. For example in the context of the Video Assessment system Rotakin™ testing to international standard BS EN 50132, Pt7 can be conducted as a means of establishing performance in this manner. This type of testing will provide assurance that the ISS has been installed correctly and will provide the anticipated level of protection and risk mitigation. Results can also be used for lifecycle auditing to ensure that the system is being correctly maintained and continues to perform to required levels. Any failures or weaknesses identified during Site Acceptance Testing will require remedial action before the systems achieve the required standard and are passed for Project Sign-Off. Providing that the Tender documentation and installation contract have been correctly structured this will usually be at the expense of the contractor.

Training & Handover – Given the highly technical nature of many of the elements that go to make up an ISS, it is prudent to ensure that staff who will operate and manage such systems get appropriate training on the systems before they are operational. Neglecting appropriate training and handover is likely to lead to inappropriate use of the installed systems and therefore an increased likelihood of system failure to meet protection objectives. Furthermore, operating an ISS without the right training and handover may increase operational costs (such as maintenance call-outs) and degrade the lifespan of the systems.

The requirement for training and handover should form part of the Tender Process and subsequent contractual agreements. The level of training and handover will be dependent on factors such as what systems have been installed, the experience and technical proficiency of operator staff, time available and cost. Training should ideally include full explanations and demonstrations on all installed security systems. As part of the handover, contractors should supply the operator with hard and soft copies of as-built drawings and Operation and Maintenance (O&M) manuals. Until an agreed training and handover package has been conducted, the project should not be signed off.

Sign-off – Project Sign-off is the final milestone in the PMP. It is a formal agreement between the Project Manager, Contractors and Stakeholders stating that the project is complete, that it meets the client's requirements as defined in the design and Performance Specification and that all parties have met their contractual obligations. The sign-off confirms that there are no further issues to be addressed.

D1.3.3 PMP Problems

It is not uncommon for the PMP to encounter difficulties and although the list below is not exhaustive, there are a number of indicators that can warn the operator that the project may need reviewing:

- The works schedule is not met and/or there is budget overrun. These are especially problematic if they occur early in the project as small problems early on tend to get larger
- Underestimation of the extent of the project and lack of understanding of objectives
- Project Team members miss project meetings or maintain poor communications
- Deliverables are not completed or milestones are ignored
- Regular use of unscheduled overtime by contractors in order to meet deadlines
- Poor integration of contractors and Stakeholders in the PMP process
- Lack of understanding of responsibilities
- Poor definition of responsibilities within the Project Team

D1.3.4 Summary

The Project Management Process is not rigid and allows for a degree of flexibility necessary to ensure that a complex project reaches a satisfactory conclusion. There are a number of alternative models you can choose from depending on what kind of project you need to deliver. It is essential that you appoint a Project Manager who is appropriately qualified and has the experience necessary to lead a security enhancement project of the complexity required. Good Project Managers pay for themselves on critical projects because they bring specialist skills that can make the difference between a project being delivered on time and budget and in line with Stakeholder expectations, or not.

D2 Testing and Exercising

Purpose: To define the process required to plan for an effective response to an Emergency Incident and test capability in this area through a range of tabletop and live exercises. Subsequently to provide a framework for post-exercise evaluation to ensure that opportunities for improvement in emergency response capability are identified and embedded within future activity.

D2.0 Introduction

The need for responding to an Emergency Incident is driven from an event that is unexpected but has been planned for, and executes a number of well rehearsed processes. The purpose of this section is to take you through the theory and process for running Emergency Exercises and using these to develop and test Emergency Response capability. The process that will be described is adaptable for any scale of Emergency Exercise and goes through a step-by-step process to ensure your exercise is safe, effective and meets your objectives.

So what is an Emergency Exercise?

An Emergency Exercise is the term that you will use to describe the task of evaluating and reviewing emergency plans. This is done by way of simulating an emergency scenario and evaluating the responses and actions required as the scenario progresses.

Why run Emergency Exercises?

You will have spent time to ensure that key internal and external Stakeholders are kept informed of what is required to implement the Security Management Plan, but a critical part of communication takes place when dealing with a response to an Emergency Incident. It is imperative that staff are aware of the role they play and the actions required of them during the response phase so they are effective. Emergency Exercises are undertaken to give confidence in the accuracy, completeness and practicability of the plans. An exercise can give responders confidence to carry out their role, evaluate equipment and validate training.

Types of Emergency Exercise

Emergency Exercises are commonly split into two categories: Table Top Exercises and Live Exercises. Either of these types of exercise can involve just one organisation or multi-agency players and can be scaled to meet the needs, budgets or regulatory requirements of an organisation. Given the levels of complexity that exercises can be run at, it is worth running smaller-scale exercise testing specific areas in order to familiarise staff with the processes before moving up to large-scale entire Asset multi-agency exercises.

D2.1 Table Top Exercises

A useful definition for you to consider is:

> **“Table Top Exercises are usually based on simulation. They usually involve a realistic scenario and timeline. The player will normally be expected to know the plans and they are invited to test how the plan works as the scenario unfolds.”**

The basic format for a Table Top Exercise is to divide players into syndicate groups, usually with a mixture of agencies or departments in each syndicate. All the groups are presented with the scenario in stages, via written injects, and are asked to discuss the response issues. Questions or discussion topics can be presented to aid the discussions. The timings of these injects can be matched to a realistic timeline for the developing scenario, or can be spaced at set intervals that allow enough time for discussion.

Table D2.1a: Example injects into a basic Table Top Exercise

Inject 1	**Initial Notification**
Scenario	This will provide information background information such as the time, date, wind direction and number of people onsite. There may be reference to what alarms have been activated and how personnel are first aware that something may be wrong onsite.
Issues	What actions should be taken onsite? Who would you tell at this time? What should staff onsite do? What do the plans say should happen? What issues do you envisage?
Inject 2	**Initial Response**
Scenario	Update with information such as if personnel are all accounted for, what alarms are showing, what can be seen on CCTV and what are the initial consequences of the incident.
Issues	What is happening onsite? Who is in your response team? Where will you manage the response from? What is each person's role? What form/checklists are you using? What external responders do you require? What do the plans say should happen? What issues do you envisage?
Inject 3	**Communications**
Scenario	Update with information about the impact of the incident, for example what can be seen or heard, what reports have been received from personnel onsite. Information regarding which external emergency services are onsite and where site personnel are.
Issues	What information are you giving to personnel onsite? How? What information will the Emergency Services require as they arrive onsite and who will pass them this information? Who else needs to be informed about the incident? Who will talk to the media and what will your message be? What do the plans say should happen? What issues do you envisage?
Depending on the Objectives for the exercise you could include an inject on media, recovery, evacuation, Public Information, etc. and tailor the questions to ensure they are relevant to the experience of the players and to the agency that the players come from.	

Source: PRISM™

D2.2 Live Exercises

> **"Live Exercises are a live rehearsal for implementing the plan. They are useful for testing logistics, communications and physical capabilities. They are excellent for training through experimental learning, helping develop confidence in their skills and providing experience of what it would be like to use the plans or procedures in a real event."**

Like Table Top Exercises, Live Exercises can involve just internal players or include those from external agencies. They can be as simple or as detailed as required to meet your objectives. Examples of Live Exercises could include:

- Evacuation of personnel from site
- Activation of search teams
- Setting up a response team
- Co-ordination with external agencies

Live Exercises are normally a mixture of controlled play and free play. Controlled injects will be introduced to the exercise at set times, for example alarm notification, intruders entering site, Emergency Services arrival at site, journalists arriving, phone calls into the gate house and control room, notification of explosions, fires and casualties.

Free play is when the players are able to respond to the scenario as they would in reality. Combining controlled play and free play will enable testing of the degree of flexibility of the plan and the validating of any pre-identified aspects.

D2.2.1 Live Exercise Safety

The importance of the safety of personnel during an exercise is paramount for you. All those involved in the exercise; including players, observers, directing staff, role players, and so on, must be given a safety briefing prior to the exercise to ensure they are aware of any hazards onsite and advised of any safety issues including Personal Protective Equipment (PPE) requirements.

Live Exercises should have a dedicated Exercise Safety Officer to ensure that no actions are carried out that cause a danger to personnel on the site. A Risk Assessment should be carried out, and agreed and shared with all agencies involved.

Examples of safety considerations for a Live Exercise onsite include:

- External players are not familiar with the hazards onsite
- Responders bringing prohibited items onto site
- Availability of appropriate Personal Protective Equipment
- Emergency Services may not have Intrinsically Safe (IS) radios
- Concerns of neighbours if Emergency Services vehicles are seen attending the site
- The plant may still be running during the exercise
- Security of the site – do all those involved in the exercise need to be security cleared?
- Is there any confidential or sensitive information on the site?
- First Aiders needed in each area of Exercise Play. Consider using Ambulance personnel if they are participating in the exercise
- If there is going to be unprecedented activity onsite consider informing the Emergency Services control rooms so that they are aware that there is an exercise taking place

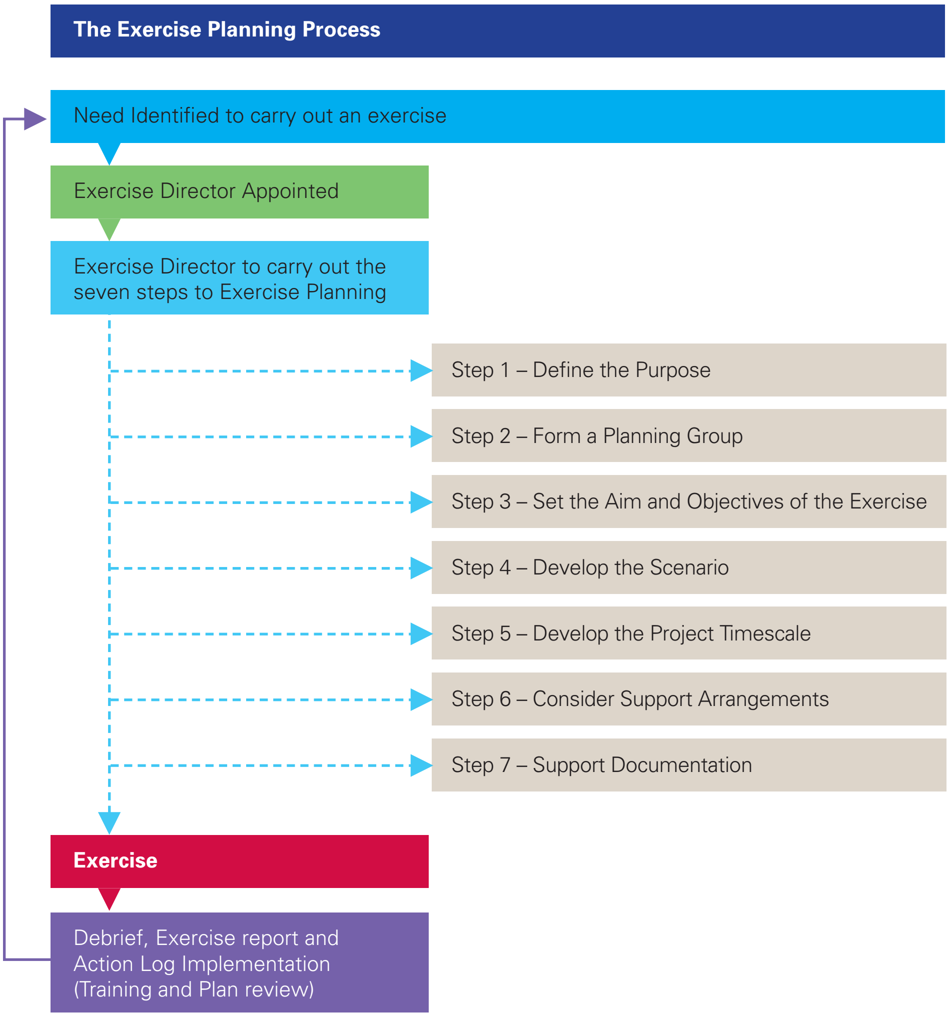
D2.2.2 Code Words

A code word should be identified prior to the exercise and published to all involved. This word could then be used to identify that a real incident has occurred that is not part of the exercise. This could be used as notification of a real emergency or message during the exercise or if there is a real casualty. Example of commonly used code words you may consider must be relevant to the local context.

D2.3 Exercise Planning & Organisation

When planning an exercise it is important that you remember to follow a structured process. The following process details a seven-step approach which you may like to consider when planning an exercise. Whatever the type or scale of the exercise you are planning; this process will help you ensure that your exercise is effective and efficiently managed. The information below gives you guidance on what should be considered during each step of the process.

Diagram D2.3a: Exercise Planning Process



The Exercise Planning Process

Need Identified to carry out an exercise

Exercise Director Appointed

Exercise Director to carry out the seven steps to Exercise Planning

Step 1 – Define the Purpose

Step 2 – Form a Planning Group

Step 3 – Set the Aim and Objectives of the Exercise

Step 4 – Develop the Scenario

Step 5 – Develop the Project Timescale

Step 6 – Consider Support Arrangements

Step 7 – Support Documentation

Exercise

Debrief, Exercise report and Action Log Implementation (Training and Plan review)

Source: PRISM^{TM}

So you can now see the importance of appointing the correct Exercise Director to ensure that the process is followed.

Step 1 – Define the Project

Ensure you agree and record which plans or procedures are to be exercised. Agree the scope of the exercise, for example are you exercising all or part of the plan, are you rehearsing personnel, do you want to test resource availability or compatibility and is the exercise validation of previous training?

Step 2 – Form a Planning Group

This will help you ensure the planning phase offers a valuable learning opportunity for those involved. To ensure you have the correct people on your planning group:

- Consider the experience and expertise needed and available
- Consider including external agencies/companies
- Do not include those who you want to be involved as a player during the exercise
- Include a Safety Officer

Consider using the Planning Group as the Exercise Directing Staff during the exercise as they will already be aware of the bigger picture and understand the thought process behind the objectives and scenario.

Step 3 – Set the Aim and Objective for the Exercise

It will be of value to you if the exercise has one Aim and up to eight Objectives.

There should only be one Aim and every aspect of the exercise must be justifiable to the Aim. The Aim should answer the question, "What are you hoping to achieve from the exercise as a whole?"

Examples of an Exercise Aim include:

- To evaluate the revised security plan
- To demonstrate the onsite resource capacity and compatibility with other responders' resources
- To practise working with the Emergency Services onsite

There should ideally be three to eight Objectives, all of which should serve the Aim. Each organisation or department participating in the Exercise may, in addition, have their own Objectives.

Examples of Exercise Objectives include:

- To ensure timely evacuation of site
- To practise personnel in using the Response Team check lists
- To evaluate how journalists would be treated and who would talk to them
- To evaluate the information management process between site personnel and the Emergency Services

Step 4 – Develop a Scenario

Ideally a Risk Register should be used to assist you in the decision-making process when developing a scenario. Higher risks to your site or process should be a priority for planning and exercising.

Your scenario should be realistic and within the scope of the plan being exercised. It needs to be able to create the activity needed to achieve the Aim and Objectives. When agreeing a scenario you should consider the need for it to be affordable and manageable.

Once you have outlined the scenario you can decide on the type of exercise, Table Top or Live, which is required to meet the Aim and Objectives. Legislation may dictate the type of exercise that is required.

You also need to consider what injects you will need to meet your Aim and Objectives.

Step 5 – Develop the Project Timescale

Prepare your plan with 'milestones' throughout the planning process. This will assist you to keep the planning process on time.

Consider including:

- Any pre-exercise training that is required
- Development of injects
- Procurement of resources/hire of venue
- Briefing for players, observers, role players and directing staff
- Debrief following the exercise
- Issue of the Exercise Report

Step 6 – Consider Support Arrangements

There are many added extras that may be required to run an exercise. When considering what you require you should be aware of any budget restrictions. Things that you may need to consider include:

- Appoint Directing Staff and Umpires
- Arrange for emergency cover during the exercise
- Preparation of the site/location
- Security issues – security clearance of players
- Use of code words
- Special effects/smoke machine hire
- Role Players
- Photographic Services
- Refreshments

Step 7 – Supporting Documentation

Your documentation from the planning stage, exercise play and the debrief sessions should be kept.

Documentation (depending on the scale of your exercise) could include:

- Exercise Instructions. Given to all involved in the exercise to ensure the right people arrive in the right place, with the right kit, at the right time and in the right frame of mind for the exercise. The Exercise Instructions will include details on the Aim and Objectives, exercise format, venue, briefing etc.
- Briefing for Players, Umpires, Observers, Directing Staff etc
- Schedule of Injects
- Risk Assessment
- Evaluation form

After following the Seven Steps you should be in a position to run an effective exercise. Following the exercise you will need to ensure that there is a debrief and that an Exercise Report is produced which will highlight any lessons identified during the exercise.

D2.3.1 Debriefing

Every exercise should be debriefed. This will ensure that the response to the scenario can be evaluated and lessons can be identified. Debriefing provides you with the opportunity to evaluate efficiency, to learn from experience gained and also offer a source of information to assist in future planning, training and exercising.

The debrief process should be non-blame and offer all involved the opportunity to have their say. There are several types of debrief. They can be conducted immediately after the end of the exercise or a few days later. They can involve personnel from a single organisation or can be multi-agency.

It is important that any lessons identified during the exercise and through the discussions in the debrief are added to an Action Log. The recommendations in the Action Log should be assigned an owner to take them forward for the organisation and given a priority or timescale for completion.

Consider sharing any recommendations with other sites/organisations so learning can be maximised.

D2.3.2 Exercise Report

For completion, it is important and useful for you to produce an Exercise Report. The report should highlight both the positive and negative observations from the exercise and should conclude with recommendations for the future.

The Exercise Report should ideally cover the following points:

- References (which Emergency Plans were within the scope of the exercise)
- Introduction and background to the site and exercise
- Aim and Objectives
- Format that the exercise took
- Participants – including Players, Observers, Directing Staff etc
- Scenario
- Details of the Debrief and Evaluation process
- Lessons that have been identified and any recommendations
- Conclusion

Who's Who – Key Roles during an Exercise

We have outlined some of the roles that are required during an exercise. The numbers required will vary depending on the scale of the exercise.

Exercise Director – This person has overall responsibility for the planning and for the exercise itself.

Exercise Directing Staff – They will manage the exercise injects, administration and logistics support. They consult with and report to the Exercise Director. There would normally be Exercise Directing Staff from each agency or department involved in the exercise. For a Live Exercise you would have Directing Staff in each location of exercise play and for a Table Top Exercise you would have Directing Staff facilitating each syndicate group.

Safety Officer – Will advise on all safety issues at all the locations to be used for the exercise. They will be responsible for compiling the Risk Assessment. The Safety Officer may stop any actions during the exercise if they are unsafe.

Liaison Officers – If you are organising large exercises you may need to appoint Liaison Officers to escort visitors. This may include media observers, VIPs or invited guests.

Umpires – You will appoint these, and are normally drawn from the agencies taking part in the exercise. Umpires access the performance of participants and evidences if the exercise objectives have been met.

Observers – Their role is to watch and listen but should have no input. Observers are there to learn from the exercise and use the experience to inform planning in their own environment. Specialist observers could include, Health & Safety Executive, Environment Agency etc.

Role Players – They have to act out the role given to them. Role Players could include casualties, journalists, intruders or other roles specific to the exercise.

Injectors – At an appropriate point will inject message inputs into exercise play. This could include making phone calls pretending to be from relatives, customers, other agencies or updating with new information. This could also be given as a paper inject with an update of the scenario.

Administrative Support – This ensures that all paperwork and records relating to the exercise are kept and auditable. This could include the updating of training records, registration of players, briefing sheets, evaluation forms or other documentary information required.

D2.4 Summary

It is hoped that this process sets out for you a clear framework for you to develop a progressive programme of table top and live emergency response exercises which will allow you to test capability in a variety of areas, including co-ordination with external emergency response authorities where appropriate. You will subsequently be able to evaluate the performance of the organisation in responding to an emergency incident and implement any improvements and additional staff training in areas where capability is shown to be limited. It will be for you with your management team to discuss what will be required from the exercise process and the key to success is to ensure you and your team benefit and gain from the experience.

D3 Ongoing Monitoring

Purpose: To provide guidance on ongoing monitoring activity including annual Risk Assessments, regular testing and exercising and Risk Reporting. In addition to demonstrate how to put together a security risk report that monitors performance against the risk indicators agreed by Stakeholders during the process. This report needs to look like and form part of the performance and risk-based reporting one would expect an owner/operator to have in place.

D3.0 Introduction

The Risk Register is the engine at the centre of PRISM™ as it reflects all the analysis derived from Phases A and B about security risk appetite and mitigation. It is a dynamic document that should be updated both as part of a formal review process on an annual basis, but also when anything changes in the internal or external environment that might require an adjustment or review of the analysis. This is as you would expect with any strategic and financial planning within the Organisation – things change! As such it is necessary to conduct regular Risk Assessments along with Emergency Response Testing and Exercising to identify these changes, and have an effective reporting framework in place to ensure all Stakeholders are aware of current Performance and Risk factors and can make informed decisions on future security risk management activity. These issues are discussed in the following sections.

D3.1 Annual Risk Assessment

In order to capture any changes in the risk context around each Asset it is necessary to re-evaluate risks on a regular basis. As such it is recommended that you implement a formal policy of conducting an annual Risk Assessment for all significant facilities. The Risk Assessment should follow the same process as outlined in Phase B of the Security Management Plan, although it will usually be less time-consuming than the original assessment since much of the existing analysis will remain relevant and can be re-validated and updated as required.

The Threat Assessment is a key area for consideration when conducting repeat Risk Assessments since Threat environments can change rapidly and dramatically in a short period of time (for this reason it should also be re-assessed throughout the year following any significant security-related incidents that take place at the facility, at similar facilities, or in the same geographical area). When reviewing and updating the Threat Assessment it is therefore important that you spend time reviewing the latest Threat information from your established sources, and considering how this will affect your previous assessments. As well as an increased or decreased level of Threat, developments could manifest themselves in terms of changes in likely methods of attack or capability of certain Threat sources, in which case it may be necessary to amend or add to the selected Threat scenarios which form the basis for subsequent risk analysis. Subsequently this will have a knock-on effect on both Consequence and Vulnerability Assessments.

The Vulnerability Assessment is also a key area for review since security systems performance can change over time as a result of either systems degradation or weaknesses in procedural measures, particularly by guard force personnel who are probably amongst the lowest-paid workers in the organisation and tend to develop ‘bad habits’ if not properly supervised. Vulnerability may also be affected by changes in the infrastructure – that new substation that operations forget to inform the security department about (hopefully not but a common problem!) or the new type of hazardous chemical that is now being used to enhance production, For these reasons it is recommended that the Vulnerability Assessment be repeated in full for all major security systems and processes. Where technical testing has previously been carried out and objective performance measurements taken this can also be repeated and the results compared against original measurements to highlight system degradation, which may indicate insufficient maintenance or lack of suitability for environmental conditions.

The Consequence Assessment should also be reviewed and although much of this will remain the same, it could be affected by either changes in: Threat Scenarios; facility processes and materials; number of workforce; or adjacent/co-located hazards.

Once all of the above assessments have been carried out respective scores can be updated accordingly and any significant changes in risk profile highlighted to the management team. Section D3.3 provides more information on Performance and Risk Reporting methods to help ensure that you have the necessary tools to communicate these changes effectively and support decision-making by risk owners.

D3.2 Regular Testing & Exercising

In conjunction with the Annual Risk Assessment it is also important to implement a programme of regular Emergency Response Exercising as a means of testing capability in this area and ensuring that the facility and its personnel maintain a high level of preparedness to deal with any major incidents and hopefully mitigate the consequences.

The guidance presented in section D2 will provide the framework for this testing and exercising, and it is worth reiterating that you should aim for continual development in this area, increasing the depth and breadth of capability amongst staff through successive exercises that have specific and targeted goals. For example a series of initial exercises might develop capability in the areas of communications, evacuation procedures, or search procedures, whilst later exercises may seek to test co-ordination with external response agencies. Whatever the purpose of each exercise it is important that performance is assessed objectively and that the key weaknesses and learning points are captured for subsequent exercises.

D3.3 Performance & Risk Reporting

One of the key messages of PRISM™ is that the security risk management framework needs to be embedded into other internal control mechanisms, in particular, risk management in general, strategic and financial planning and quality assurance. So it is important to ensure that the key indicators from the Risk Register are:

(i) Incorporated in the Organisation's central Risk Register AND/OR

(ii) Incorporated into a Risk-based Performance scorecard used by the Organisation to track how well it is delivering against its strategy.

What you need to do is to find out how risk and performance reporting works within your Organisation and assess how you can embed the key indicators from the Risk Register you have created, into that framework. Again remembering that the more you can align security risk alongside the processes that should be in place to cover other internal controls, the more likely you are to gain the acceptance and ownership of the Security Management Plan.

This is about linking together both ends of the process you have undertaken from Planning & Strategy to Implementation & Review and it is a key measure of the success with which you have been able to promote security risk awareness within your organisation by undertaking this process.

Remember – strategy and risk are two sides of the same coin:

Strategy is about how organisations create shareholder value and Risk is about how they protect that shareholder value.

Performance reporting is how organisations can tell whether they are actually delivering the performance expected by Stakeholders on both sides of the coin.

In our experience, there are many different reporting formats that organisations use to monitor risk and performance, no one format is better than any other. However, there are a number of key elements that you should expect to see and these are set out in the following table:

Table D3.3a

Issue	Comment
Key Indicators	These will be a combination of ratios and actual measures that are derived from the Risk Register for security risk, and others. Also from financial and operational key performance indicators that have a positive and negative impact on value creation.
Format	Similar to a scorecard with the indicators grouped under headings, with the target shown as traffic lights alongside the actual outcome.
Owner	The owner of the main Risk-based Performance report is likely to be the Finance Director or Managing Director of the organisation. The former because their team will collate the information required to compile the report and prepare any commentary on it for the Executive Management Team and external Stakeholders.
Targets	The report will have targets. The Risk Register will have these for security risk, but again these will be set for other risk and performance indicators. The owner will identify what the margin of reporting is around each target eg. green = above target; amber = within 5%; red = amber for two consecutive reporting periods or >5%.
Consequences	Actions to occur if amber or red need to be decided upon – an exceptional monitoring approach would be required.
Audience	Who receives the Risk-based Performance report will dictate its success. It should be part of the main Management Information pack prepared for the Board and Executive Management Team.
Frequency	This may differ from indicator to indicator.
Trends/ Analysis	There will be space on the report to show certain trends highlighting variances and this is important to do across all indicators, if only to verify the appropriateness of the targets that have been set for performance and risk appetite.
Review	The indicators on the Risk-based Performance report should be reviewed formally on an annual basis – this should focus on past trends, actions taken, looking ahead etc.
Communication	The Risk-based Performance report should be communicated across the organisation. It may be that some indicators are sensitive or only apply at corporate level, but given that good performance and risk management is driven from the actions and behaviours of individuals from the bottom up, it is important for each part of the owner/operator to understand how their area impacts further up the organisation and feeds into the corporate, consolidated report.
Data Accuracy	The credibility of any Risk-based Performance report resides on the confidence that users have in the veracity of the source data. It is imperative that this is compiled and reviewed so that a) it can be checked and b) there is full knowledge of what each indicator means. Most of this should be relatively easy to identify from the security Risk Register.
Guidance notes	These will need to be produced to support the communication process and must be updated after each annual review. You will need to ensure that any security risk indicators are properly reported upon, so providing an explanation to the finance department or head of risk, will help ensure the right messages are left with those who need to know.

Source: PRISM™

Of course, how the report is used will tell you whether it has any value in the organisation or is simply another tick-box exercise. Remember in Phase A we mentioned that it is one thing to have excellent processes in place, but if the environment around those processes stifles their application – they are worthless.

> **"Risk management is not a science – it's an art. Sophisticated risk models do not prevent accidents and mistakes and nor do detailed policies and procedures. If the prescriptive, compliance-led approach to banking regulation worked – and I use that example as shareholder value in both sectors depend upon risk being taken daily – why is the FSA (Financial Services Authority – the financial services regulator in the UK) being dismantled? The interplay reflects the environment the risk management 'toolkit' operates within. That environment stifles or stimulates the critical debate about risk appetite, discourages or promotes the right mindset, separates or aligns the tools that embed risk such as strategy, planning, budgeting, personnel management and performance – so there either is, or is not, evidence of a living consequence-led risk management environment – before the post-mortem".**
>
> Reprinted from 'Points of View' an article in Energy International magazine August 2010 written by Harnser Group

D3.4 Summary

Given how quickly the risk environment around a facility can change, Ongoing Monitoring is an essential component of the Security Management Plan. This will require Risk Assessments, Testing and Exercising to be conducted on a regular basis. Once the process of compiling the Security Management Plan has been completed, and following all subsequent assessments, evidence of its success lies solely with the effectiveness of the reporting that flows from the work done. The importance of this stage of the process cannot be underestimated. The best chance of success here is to find out what other risk- and performance-based management information is produced and then ensure the key risk indicators from the Risk Register form part of it. Ownership will then go further up the management chain ensuring that attention is being focused on security risk and not just financial and operational risk.

If you would like further advice about the format and content of alternative Risk-based Performance reports, please post your question either to **info@harnsergroup.com** or on the Security Managers Forum on **www.prismworld.org** and these can be provided to you.

Bibliography

Glossary and Acronyms

Bibliography

1 ASIS. (2005). Business Continuity Guideline. 1st document. ASIS: USA.

2 ASIS. (2008). CSO Organizational Standard. Vol.1. ANSI, Inc: USA.

3 ASIS. (2009). Organizational Resilience. Vol.1. ANSI, Inc: USA.

4 ASIS. (2007). Information Asset Protection Guideline. Vol.5. ANSI, Inc: USA.

5 ASIS. (2009). Physical Security Guideline.

6 ASIS. (2009). Pre-employment Screening Guideline.

7 ASIS. (2003). SRA Guideline. ASIS international: Alexandria, Virginia.

8 ASIS. (2008). Threat Advisory System. Vol.4. ASIS International: USA.

9 Home Office. (1994). Bombs Protecting People and Property. 4th ed. Home Office: Britain

10 Booz, Allen & Hamilton. (2005). Convergence of Enterprise Security Organization. The Alliance for Enterprise SRM:

11 CPNI. (2010). Guide to Producing Operational Requirements for Security Measures.

12 Bernard, Ray CS. (2003). Homeland Security and your Business. Security Technology & Design Magazine.

13 QSG. (n.d). Industry Report Economic Use of Security Infrastructure within the Oil and Gas Industry.

14 RIBA. (n.d). RIBA Guidance on Designing for Counter-Terrorism. TPS: London.

15 Department of Homeland Security. (2008). Risk-Based Performance Standards Guidance. V.2.4. Washington, DC.

16 NaCTSO. (2005). Secure in the Knowledge. London.

17 ODPM. (2004). Safer Places. Queen's Printer and Controller of Her Majesty's Stationery Office: London.

18 ODPM. (2009). Safer Places Counter-Terrorism Supplement. Queen's Printer and Controller of Her Majesty's Stationery Office: London.

19 API. (2005). Security Guidelines for Petroleum Industry. 3rd ed. API Publishing Services: Washington, DC.

20 US Govt. (2005). Energy Assurance. Energetic D Street Office: Washington, DC.

21 Home Office (2005). Your Business Keep Crime out of it. 1st ed. The Home Office Crime Reduction Centre: London.

22 Basel Committee on Banking Supervision. (2009). Range of Practice and Issues in Economic Capital Frameworks. Basel: Switzerland.

23 Basel. (2001). Consultative Document/ Operational Risk. Basel: Switzerland.

24 FSA. (2007). Operational Risk Management Practices. FSA: London.

25 HMCS. (n.d). Safe and Secure.

26 Sandia. (n.d). Security Risk Assessment Methodologies. Sandia Corporation: USA.

27 London Chamber of Commerce & Industry. (2005). The Economic Effects on Terrorism on London. Press & Public Affairs: London.

28 Abt. (2003). The Economic Impact of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability. Abt: Cambridge.

29 GAO. (2010). CI Protection. US Govt: Washington, DC

30 HM Treasury. (2006). Thinking about your Risk. HMSO: Norwich.

31 ISO. (2007). Committee Draft of ISO 31000 "Risk Management – Guidelines on Principles and Implementation of Risk Management". V.4. ISO Office: Geneva.

32 ISO. (2007). Committee Draft of ISO/ IEC Guide 73 "Risk Management- vocabulary". V.4. ISO Office: Geneva.

33 US Govt. (2009). National Infrastructure Protection Plan. Homeland Security: USA

34 Dr. Woo, Gordon. (2002). Natural Catastrophe Probable Maximum Loss. V.8, part 7. British Actuarial Journal: London.

35 Dr. Woo, Gordon. (2003). Quantifying Terrorism Risk for Insured Portfolios. AON conference.

36 RAND. (2005). Estimating Terrorism Risk. RAND corporation: US

37 RAMCAP. (2009). Reduce Risk, Increase Resilience. ASME:

38 IRM. (n.d). Risk Management Standard. London.

39 SANDIA. (n.d). Risk Assessment Methodology for Physical Security.

40 PWC. (2010). Convergence of Security Risks. PWC: UK.

41 Sandia. (2002). A Scalable Systems Approach for CI Security. Sandia: California.

42 Whitehouse. (2003). The National Strategy for the Physical Protection of CI and Key Assets. Whitehouse: Washington.

43 National Institute of Justice (NIJ). (2002). A method to Assess Vulnerability of U.S Chemical Facilities. Final version. U.S. Department of NIJ: Washington.

44 CPNI. (2006). Personnel Security Guide. NSAC: Norwich.

45 NISCC. (n.d). Scada Security Good Practice Guide. London.

46 CPNI. (n.d). Risk Assessment for Personnel Security.

47 Cohen, N., Galtuso, J., & Brown, K.M. (2009). CCTV Operational Requirement Manual 28/09.p.No. 28/09. HOSDB: UK.

48 Aldridge, J. (1994). CCTV Operational Requirement Manual. V.3. P. No. 17/94. HOSDB: Sandridge St Albans.

49 Home Office. (2009). Safer Place CT Supplement. HO: London.

50 Cabinet Office. (2004). Civil Contingencies Act 2004: A Short Guide. Cabinet Office: UK.

51 BCI. (2005). BCM Good Practice Guidelines. V. 2005. BCI: London.

52 AESRM. (2009). Alliance for ESRM-Convergence Articles. AESRM: UK.

53 Basso, G., Fricko, O. & Reuter, A. (2006). Estimated Recovery Times for Energy Infrastructure. Counteract.

54 Nieuwenhuijs, A. & Verstoep, R. (2007). Method for Interdependency Analysis. EURAM.

55 Cavenne, F., Ulisse, A., Nieuwenhuijs, A. & Luiijf, H.A.M. (2007). EU – Common Risk Assessment Methodology. EURAM.

56 EPCIP. (2010). Cross-Cutting Criteria for European Critical Infrastructure.

57 Toft, P., Bieliauskas, A., Lopes-Ferreira, H., Mengolini, A. & Faas, H. (2006). Terrorism & European Energy Security. Counteract.

58 EPCIP. (2008). Identification Guidelines.

59 London First. (2003). Expecting the Unexpected. London First: London.

60 FEMA. (2003). Mitigating Attacks on Buildings (FEMA426). FEMA: U.S.

61 FEMA. (2003). Insurance, Finance & Regulation Primer (FEMA427). EEMA: U.S.

62 FEMA. (2005). Mitigating Potential Terrorist Attacks (FEMA452). FEMA: U.S.

63 FEMA. (2006). Safe rooms & Shelters (FEMA453). FEMA: U.S.

64 Bernard, R. (2008). Convergence of Physical Security & IT. RBCS.

65 Booz, Allen & Hamilton. (2005). Convergence of Enterprise Security Organization. ASIS.

66 Engebretson, David. (n.d). Guide to Networking for Physical System.

67 Atlas, Randall. (n.d). 2ICN Security & CPTED: Design for CIP.

68 Federal Office for Civil Protection and Disaster Assistance, ed. (2008). Protecting CI – Risk & Crisis Management. German Ministry of Interior: Berlin.

69 Sandia. (n.d). Risk Assessment Methodology for Physical Security. Sandia: U.S.

70 Garcia, ML. (2008). Design & Evaluation of Physical Protection Systems. 2nd ed. BH: USA.

71 Garcia, ML. (2006). Vulnerability Assessment of Physical Protection Systems. Elsevier BH: USA.

72 Norman, L. Thomas. (2010). Risk Analysis and Security Countermeasure Selection. CRC Press: USA.

73 Business Continuity Institute. Good Practice Guidelines.

74 US Department of Justice. (2002). A Method to Assess the Vulnerability Assessment of US Chemical Facilities.

75 RAND. (2005) Estimating Terrorism Risk. RAND: USA.

76 Broder, James. (2006) Risk Analysis & the Security Survey. 3rd ed. BH: USA.

77 EU Risk Assessment Methodology (EURAM). (2007).

78 Centre for the Protection of National Infrastructure (CPNI). Process Control and SCADA security – General Guidance.

Glossary

Term	Definition
Access Control Systems	A system which enables an owner or authority to control access to areas or resources in either a physical facility or a computer based information system.
Algorithms	Complex mathematical formulae or rules used to solve complex problems. In CCTV they are used to achieve digital compression of a video picture.
Asset	A useful or valuable quality, person or thing, an advantage or resource.
Balanced Protection	Whichever way an adversary attempts to infiltrate or achieve any of the goals they will meet with an element of the protection surrounding the organisation.
Commissioning	A quality orientated process for achieving, verifying and documenting the performance to ensure a system meets defined objectives and criteria.
Cost Benefit Analysis	A technique designed to determine the feasibility of a project or plan by quantifying its costs and benefits.
Countermeasures	An action, process, device or system that can prevent or mitigate the effects of a threat.
Critical Points	Those parts or areas of a process that would cause maximum disruption to the process if they were critically damaged or destroyed.
Delay	The element of a physical protection system designed to delay/impede adversary access.
Dependencies	Articles that rely on or that are controlled by someone or something else.
Design Basis Threat	Fundamental principle of physical protection should be based upon the current government evaluation of the threat level. This evaluation is formalised through a threat assessment process. A Design Basis Threat is derived from this threat assessment.
Desktop Exercise	Allows participants to test, preview and explore plans, roles and responses in a low pressure environment.
Detection	The act of discovering or the fact of being discovered.
Disgruntled employee	An employee who has become discontented and angered with the actions or perceived actions of an employer and who may be willing to take some action that will harm that person or their business.
Entry Control	A means by which entry to an area is controlled and permitted only to those persons authorised access.
False Flag Vehicles	Vehicles designed or adapted to deceive in such a way that they appear to be something they are not.
Global Positioning System	A space based global satellite navigation system that provides reliable location and time information.
Guards	Onsite security facility.
Hoax	A false claim.
HVAC Systems	Heating, Ventilating and Air Conditioning. Computerised control system for climate control in buildings.
Indirect Fire	Aiming and firing a gun without relying on a direct line of sight between the gun and its target.
Infrared	Light or energy in that portion of the electromagnetic spectrum having a longer wavelength than visible light.
Injects	Hypothetical events to add into training scenarios as exercises proceed.
Insider	A person with official duties/employee who has access to confidential information about an organisation's activities and would be in a position to use that information to the detriment of the organisation.
Intellectual Property	Any intangible Asset that consists of human knowledge and ideas.
Intrinsically Safe	Protection technique for safe operation of electronic equipment in explosive atmospheres. Ensures that the available electrical and thermal energy in the system is always low enough that the ignition of the hazardous atmosphere can not occur.
Invitation to Tender	A call for bids or request for tenders is a procedure for generating competing offers from different bidders looking to obtain an award of business activity.
Key Performance Indictators	A quantifiable measurement of performance which are used by organisations to evaluate progress in achieving their goals and targets.
Logical Impact	The result of a course of action that can be foreseen by using commonly held principles.

Term	Definition
Loss Event	An occurrence or circumstance that produces a financial loss or negative impact on Assets.
Milestone	A significant scheduled event in a project, usually the completion of a major deliverable.
Modus Operandi	Methods of operating. Normal mode of operation.
Multi Agency	A group of agencies or organisations generally with a common aim.
Muster Point	A place where everyone in an area is ordered to go when there is an emergency.
Need to Hold	Protectively marked material must only be held by those staff who require such material to conduct their duties efficiently.
Need to Know	Knowledge of protectively marked material must be strictly limited to those security cleared to the appropriate level and clearly have a need to know the information to complete their duties.
Nuisance Alarm Rate	Rate of alarms that can be expected to be detected by an intrusion detection sensor that can be attributed to known causes. These causes are unrelated to intrusion attempts.
Operational Requirement	Qualitative and quantitive parameters that specify the desired operational capabilities of a system and serve as a basis for determining the operational effectiveness and suitability of a proposed concept/system.
Performance Specification	Written requirement that describes the functional performance criteria required for particular equipment, material or product.
Perimeter	The boundary line or the area immediately inside the boundary.
Personal Identification Number	A secret numeric password shared between a user and a system which can be used to access a system.
Physical Security	Describes the measures that prevent or deter attackers from accessing a facility, resource or information stored on physical media.
Predictive Profiling	Method of threat assessment designed to predict and categorise the potential for criminal and/or terrorist methods of operation based on an observed behaviour, information, a situation and/or objects.
Process Hazard Analysis	The foundation for process safety and risk management of highly hazardous process systems. They assist in identifying hazard scenarios that could adversely affect people, property or the environment.
Protection Indepth	A number of protective devices in seuqence.
Radio Frequency Identification	The use of an object or tag applied to or incorporated into a product, animal or person for the purpose of tracking using radio waves.
Real-time	The actual time during which a process or event takes place or describes the process by which the operation of a computer or data is processed within milliseconds.
Response	The element of a physical protection system designed to counteract activity and disrupt the threat.
Ripple Effect	Indirect effect that spreads out from the direct or main effect to reach areas or population far removed from its intended or original purpose or target.
Risk Appetite	The total risk that an organisation is willing to take to achieve its strategic goals and meet obligations to Stakeholders.
Risk Assessment	A component of the risk anaylsis process, involving the identification, evaluation and estimation of the levels of risk associated with a given situation, action or process and their comparison against agreed standards to allow a determination of an acceptable level of risk.
Risk Management	The process of analysing exposure to risk and determining how best to handle such exposure.
Risk Register	A risk is an undesirable future event. The register analyses risks and drives action to reduce the likelihood of the risk, increases visibility of the risk, ability to handle the risk and reduce the impact of the risk should it occur.
Rotakin	Performance test target for CCTV systems. Used to monitor and maximise camera performance in any CCTV system to ensure identification of intruders, vehicles etc is possible.
Soft Targets	A military term referring to unarmoured/undefended targets which need to be destroyed.
Stakeholder	Stakeholders are defined as those parties who have an interest in, and influence on an organisation and can affect or be affected by the organisation’s actions, objectives or policies.

Term	Definition
Sterile Zone	Area between the outer and inner perimeter fence where no activity occurs during normal operations.
Strategy	A plan of action or policy or the method by which the adversary plans to achieve their objectives.
Subcomponent	Individual parts of a component.
Subversives	Refers to an attempt to overthrow structures of authority. All wilful acts that are intended to be detrimental to the best interest of the government and do not fall into categories of treason, sedition, sabotage or espionage.
Supply Chain	Entire network of entities directly or indirectly interlinked and interdependent in serving the same consumer or customer. Consists of the movement of materials as they flow from their source to the end customer. It is made up of the people, activities, information and resources involved in moving a product from its supplier to customer/consumer.
Surveillance	Close observation of a person, group, places or things by visual, aural, electronic, photographic or other means.
Target Attractiveness	The appeal of an object of attack that may produce the result demanded.
Targets	An object of attack.
Tender	Sealed bid or offer document submitted in response to an invitation to tender containing detailed information on requirements and terms associated with a potential offer.
Thermal Imaging	The ability to see an environment with or without visible illumination using infrared radiation.
Threat	A potential or actual adverse event that may be malicious or incidental and can compromise the enterprise or integrity of an Asset.
Threat Actor	Who or what may violate the security requirements (confidential, integrity, availability) of an Asset. Actors can be from inside or outside the organisation.
Tiger Kidnaps	A crime in which an abduction forms part of a robbery. A person of importance to the victim is held hostage as collateral until the victim has met the criminal’s demands.
Topography	Detailed description or representation of the natural and artificial features of a landscape.
Variation Order	Client approved variation to a contract, requirement or similar. Technical term used for an approved technical change to a project.
Vetting	Process of examination and evaluation generally referring to performing a background check on someone prior to grant of approval or clearance.
Video Analytics	Practice of using computers to automatically identify things of interest without having an operator to view the video.
Vulnerability	An exploitable weakness and the degree to which people, property, resources, systems, economic or destruction being exposed to a hostile agent or factor.
Vulnerability Assessment	Process of identifying, quantifying and prioritising (or ranking) the vulnerabilities of a system.

Acronyms

Term	Definition
AACS	Automated Access Control System
ARC	Alarm Receiving Centre
BCM	Business Continuity Management
BLEVE	Boiling liquid expanding vapour explosion
BSA	Bomb Shelter Areas
CBRN	Chemical Biological Radiological Nuclear
CCTV	Closed Circuit Television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors.
CEI	Critical European Infrastructure
COMAH	Control of Major Accidents and Hazards
CQA	Close quarter attack
DBT	Design Basis Threat
DDRR	Detect Delay Response & Resilience
DID	Design Intent Document inclusive detailed description of the projects goals and requirements as defined by the Stakeholders and project team.
DOS	Denial of service
GIS	Gas Insulated Switchgear
GPS	Global Positioning System
GUI	Graphical User Interface
HQ	Headquarters
HSE	Health & Safety Executive
IDS	Intruder Detection System
IED	Improvised Explosive Device
IR	Infrared
ISS	Integrated Security System

Term	Definition
KPI	Key Performance Indicator
LED	Light Emitting Diode
MI	Management Information
NAR	Nuisance Alarm Rate
OCTV	Open Circuit Television
PDA	Personal Data Assistant
PFD	Process flow diagram
PIDS	Perimeter Intruder Detection System
PIN	Personal Idetification Number
POB	Persons on board
POC	Point of contact
POD	Probability of Detection
PPE	Personal Protective Equipment
PRISM	Performance & Risk-based Integrated Security Methodology
PTZ	Pan Tilt Zoom
RFID	Radio Frequency Identification
RPG	Rocket propelled grenade
RV	Rendezvous
SAA	Small arms attack
SAT	Site Acceptance Test
SCADA	Supervisory Control and Data Acquistion. A computer system for gathering and analysing real time data.
SMS	Small Messaging Service
VBIED	Vehicle Borne Improvised Explosive Device
VOIED	Victim Operated Improvised Explosive Device (booby trap)

harnser
group

Harnser (UK) Ltd
69-75 Thorpe Road
Norwich NR1 1UA
United Kingdom

Tel: +44 (0) 1603 230534
www.harnsergroup.com

Design: **www.fifthring.com**