GUIDE TO SRMBOK

PHYSICAL SECURITY SPECIFICATIONS AND POSTURES

The Security Risk Management Body of Knowledge (SRMBOK) was developed as an initiative of the Risk Management Institution of Australasia Limited (RMIA) in conjunction with Jakeman Business Solutions Pty Ltd (JBS), which provided the lead authors and financially underwrote its publication.

SRMBOK was written to contribute to the identification and documentation of agreed better practice in Security Risk Management. Copies of SRMBOK can be purchased from www.amazon.com

SRMBOK is also supported by many *Guides to SRMBOK* written by independent security professionals that provide more detailed guidance and examples of how the SRMBOK framework can be applied in practice. Whilst each of these Guides is peer reviewed prior to publication, any opinions and views expressed are those of the authors and do not necessarily reflect the opinion of RMIA or JBS.

Security Risk Management

Body of Knowledge

Abstract

*Establishing **security specifications** that deliver consistent and agreed levels of security protection based on the threat context is a challenge common to most organisations regardless of size or industry sector. This is particularly the case for organisations operating in different regions or countries, which face the added complexity of attempting to define specifications for security measures when terminology, materials and legislation are different.*

This section deals with the establishment of physical security specifications for organisations by providing detailed information on the various threat control measures that can be adopted, and which can be readily used as a basis for consideration/modification to suit your specific organisational situations.

*Most importantly, this section covers the concepts of **threat postures** and **security-in-depth**, whereby an organisation puts in place the basic 'buildings blocks' pertinent to their assessed threat context, which can then be built upon relatively quickly and efficiently as the threat context changes. It provides detailed information on:*

- *Physical Security Specifications*
  - *Access Control to Premises and Secure Areas*
  - *Physical Barriers and Hardenings*
  - *Locks and Keys*
  - *Alarms, Sensors and Monitoring Devices*
  - *Security Cabinets and Containers*

It has been written so that the guidelines for each of the above are separated from, and precede the suggested minimum recommended specifications for consideration in each component. In so doing, the guidelines can:

- *Be used to guide security treatments globally without fear of misunderstanding due to variations between country legislation or materials availability; and*
- *Be provided to contractors and other staff with a need-to-know, without disclosing how the organisation applies these specifications based on its own business context and enterprise security risk assessments.*

Dr Miles Jakeman
Citadel Group Limited

Miles is the Managing Director of the Citadel Group Limited. His key skills cover business strategy, program management and security risk management. Over a 20-year career, Miles has worked with the Australian Department of Defence, the Australian Security Intelligence Organisation (ASIO) and the Australian Federal Police, as well as with multinational companies. Sample assignments include:

- engaged to assist the Governments of Thailand and the Republic of the Philippines with assessing their national border management processes. This entailed examining all major elements of their border control systems and procedures, and recommending options to strengthen overall border security. Issues covered included people movement, human trafficking/smuggling, transnational crime and drug smuggling
- providing specialist security advice to Air New Zealand, the Commonwealth Government's Protective Security Coordination Centre, the Australasian Business Travellers' Association, and the Asian Development Bank amongst others
- preparing and delivering counter-terrorist command and control programs for the Indonesians, Chinese, Taiwanese and Thais - which were sponsored by law enforcement and intelligence agencies following the Bali nightclub bombing
- contracted within the Attorney-General's Department to implement a range of security-related projects post the 11 September 2001 terrorist attacks. These include implementing Australia's inaugural 'sky marshal' program on board Australian domestic and international airlines, and upgrading counter-terrorist response arrangements at all major Australian airports
- seconded from the Australian Army to a small team responsible for designing and implementing the Federal Olympic Security Intelligence Centre (FOSIC). The FOSIC was a Federal Government initiative that channelled security intelligence from various Australian departments and international security agencies into the New South Wales Police Force's operational-level security centre

Miles is a member of the Australian Institute of Company Directors (AICD) and the ACT Capital Angels, a preferred Risk Management Supplier to the Australasian Business Travellers' Association, an Associate of the Asia-Pacific Cabin Safety Working Group, and an Associate of RMIA. Miles has a PhD on the topic of Islamic intellectuals in Indonesia and their links to the country's political power centres and extremist religious groups. He also holds a Bachelor of Science (Honours) and a Graduate Diploma (Asian Studies). He speaks two foreign languages and received a University of New South Wales commendation in 1990 for academic excellence during his postgraduate studies.

Miles can be contacted at miles@jakeman.com.au or +61 (0)438 400 688

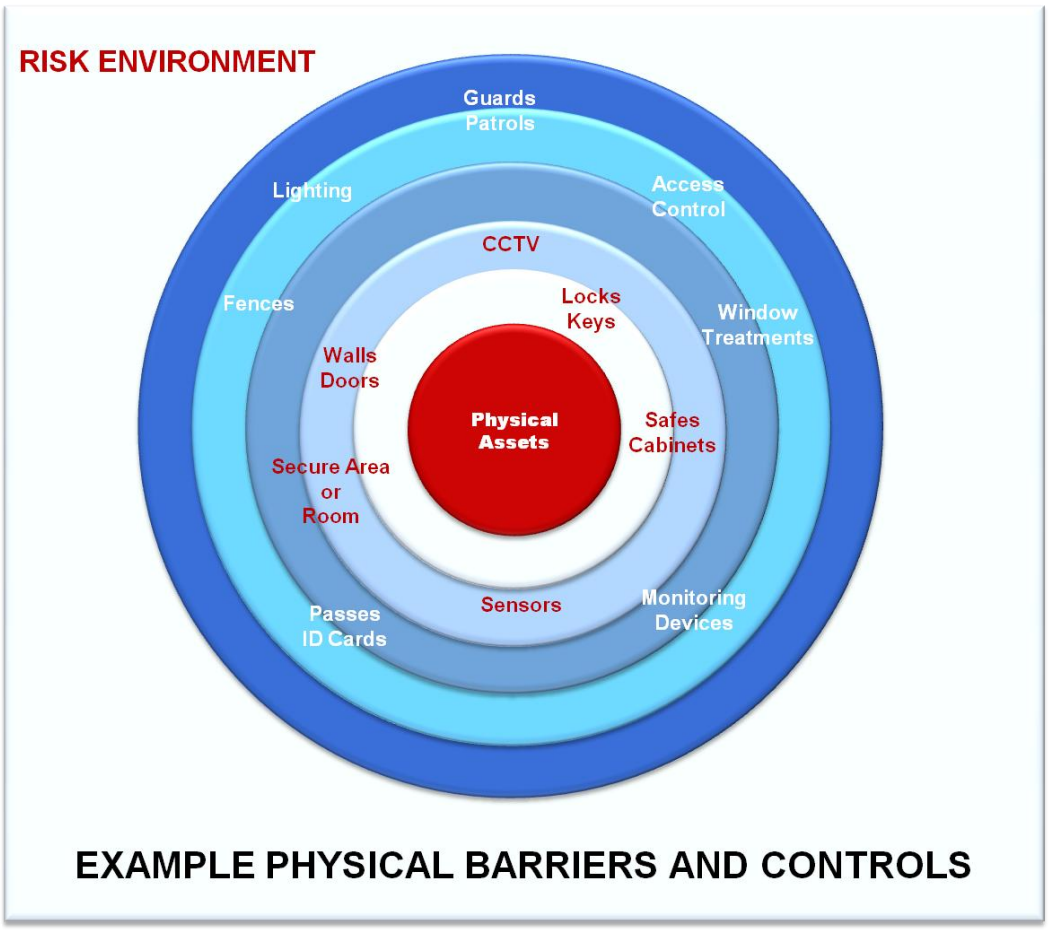
Contents

1. BACKGROUND TO PHYSICAL SECURITY

1.1. The Concept of Physical Security-in-Depth

Physical security measures are part of a comprehensive approach to the protection of organisational assets, such as sensitive information, resources and functions. This mix of protective security measures establishes a series of barriers, known as 'security-in-depth', that prevent or restrict unauthorised access or harm to organisational information and resources. It also puts in place mechanisms to detect and respond to security breaches within an acceptable timeframe.

The primary goal of a physical security program is to control access. The concept of barriers/measures has evolved to deal with this objective. These barriers/measures are typically arranged in concentric layers, with the level of security growing progressively higher as one approaches the centre:



Physical security controls include amongst others:

- barriers that deter, detect and delay unauthorised entry
- security alarm systems that detect attempted or unauthorised access and alert someone to the need to respond
- access controls that restrict access based on security clearance and a need to know
- security keys and containers that protect classified information

These are complemented by procedural and people security measures such as:

- implementing the 'need-to-know' principle that limits access to sensitive information to those people who need the information to carry out their duties
- a security classification system that identifies information needing special protection
- a personnel security system that ensures staff who need to access security classified information are considered suitable for access
- logical controls designed to minimise the security risks to organisational ICT systems

The advantage of adopting the security-in-depth principle is that security measures emanate from the function or resource requiring protection, thus providing a series of delays and deterrents to would-be intruders before they reach the function or resource. The intermeshing of appropriate physical and electronic barriers with procedural measures will usually prove more effective and less intrusive than reliance on one measure or one type of measure. It is unlikely that one measure alone can ever provide the necessary protection.

Security-in-depth only works effectively if everyone involved in handling security classified information or protecting official resources is aware of their responsibilities.

1.2. Principles of Effective Physical Security

Each business unit is responsible for providing an appropriate physical security environment to protect the organisation's staff, clients, and sensitive assets.

The appropriate physical security environment should minimise any adverse effect on the efficient and effective performance of organisational goals and objectives, without compromising the application of protective security measures.

An appropriate physical security environment is based on a thorough security risk review to identify, analyse and assess the specific risks faced by the organisation. This review will help management to develop a protective security plan appropriate to the organisation's functions and the security risks it faces.

Physical security measures should form part of a security awareness process, and employees, contractors and visitors should be briefed regularly on the physical security measures operating in the work environment, the functions and resources the procedures are designed to protect, and the security responsibilities of people working in that area.

If the business unit's function involves providing a service to members of the public on the organisation's premises, it is essential that they do so in a safe environment, as the organisation has a duty of care to members of the public interacting with the business unit.

2. PHYSICAL SECURITY SPECIFICATIONS

2.1. What is a Security Specification?

A security specification is a documented technical specification or other precise criteria used consistently as rules, guidelines or definitions of characteristics to ensure that materials, products, processes and services are fit for their purpose. Specifications should be determined and applied at the organisational level, implemented in a managed fashion (eg: through the development of policy and provision of concomitant funding), require a lead time to implement, and should form the basis of review/audit activities.

For example, an Australian organisation operating in a number of overseas locations may decide that, based on the varying threat level at its different locations, the following alarm systems are required as the minimum security 'specification' in all of its buildings:

Security Measure Area Type	Threat Level				
	Low	Moderate	Medium	High	Extreme
Building Protection *	Commercial Grade with back-to-base monitoring	Commercial Grade with back-to-base monitoring	Type 2	Type 2	Type 1**
Intruder Resistant Area	Type 2 Alarm system & peripherals				
Secure Room	Type 1 Alarm system & peripherals				

NOTES:

* Sensor-activated halogen flood lighting should be installed at both the front and rear of the office/residence to illuminate the immediate grounds area. A command switch for the lighting shall be installed within the house for manual override or for manual use of the lighting.

**** For all Type 1 security alarm systems (SAS):**

- Detectors should cover all entrance and exit points. All perimeter doors should be protected with balanced magnetic reed switches. All SAS hardware is to be located in the controlled perimeter.
- A Man-Machine Interface, (keypad), should be located within the residence in close proximity to the main entry door, and should provide for a 30-second delay on entry/exit. If power is lost to the residence, an uninterrupted power supply (UPS) or battery back up system should be used to provide power to the SAS for a minimum of four (4) hours.
- The SAS should be monitored by a host country accredited monitoring station, in accordance with Australian Standard (AS) 2201 or an equivalent specification.
- There should be written procedures in place in the event of an alarm. These may vary in accordance with operational requirements, but they must encompass instructions on contacting the staff and families, and a suitable response. Contingency plans should be put in place in the event of failure of the Type 1 SAS.

There are two principle challenges with the application of security specifications by threat level. The first relates to a situation whereby threat information is being received from different sources. For example, if the threat levels from the two information sources are different, it would be appropriate to assign a credibility and reliability rating (see table below) to these sources in order to determine the most likely threat level. If this approach fails to clearly determine the threat level, then prudence would suggest acting on the higher of the two levels.

A commonly used technique to overcome limitations associated with opinions or imprecise information is the Admiralty Scale. This scale provides a means of rating the reliability and accuracy (and hence usefulness) of information through a graduated alphanumeric scale. The *reliability of the information source* is assessed on criteria such as the previous quality of information supplied by the source, the situation, location, and likely access of the source at that time to the information collected. The *accuracy of the information* provided is assessed as an actual or perceived relative measurement in relation to each item of information received. For example, this can be based upon a comparison of the supplied information with other confirmed facts or other previously (but not necessarily confirmed) information, or with trends or patterns of other events or threats.

Reliability of Source		Accuracy of Information	
A	Completely reliable	1	Confirmed by other sources
B	Usually reliable	2	Probably true and accurate
C	Fairly reliable	3	Possible true and accurate
D	Not usually reliable	4	Doubtful
E	Unreliable	5	Improbable
F	Cannot be judged or assessed	6	Cannot be judged or assessed

Another approach is to adopt a green team and red team. Under this arrangement, the green team would develop the threat assessment and a second team (the red team) would then independently review the logic of the first group. In so doing, biases can be removed and the logic flow of deductions confirmed. Such an approach is also a useful tool in reviewing a range of documents, including procurement evaluations or risk treatment plans.

Table 1: Quantifying the Credibility and Reliability of Information

The second challenge involves a situation where an organisation is receiving threat information about multiple threat actors in the same location. For example, in the city of XYZ, the threat from Issue Motivated Groups (IMG) may be at a low level 1, whereas the threat from Violent Crime (VC) may be at level 3, Politically Motivated Violence (PMV) at level 2 and Espionage at level 3:

		THREAT LEVELS				
		1	2	3	4	5
INTRUDER ALARM SYSTEM	VC	S	M	M	M	M-Crypt
	IMB		S	M	M	M-Crypt
	PVM		S	M	M	M-Crypt
	ESP.	S	M	M-Crypt	M-Crypt	M-Crypt

Table 1: Example of Security Specifications for various Threat Actors

In this situation, and using the example specifications defined in Table 1 above, the appropriate specification would be to install an Encrypted (M-Crypt) alarm system as illustrated in Table 2 below:

		THREAT LEVELS				
		1	2	3	4	5
INTRUDER ALARM SYSTEM	VC	S	M	M	M	M-Crypt
	IMB		S	M	M	M-Crypt
	PVM		S	M	M	M-Crypt
	ESP.	S	M	M-Crypt	M-Crypt	M-Crypt

Table 2: Worked Example of Security Specifications for various Threat Actors

3. PHYSICAL SECURITY POSTURES

3.1. What is a Security Posture?

A security 'posture' is a practice or activity that can be implemented and/or modified at relatively short notice (eg: locking doors, putting on additional guards), and which can be undertaken against an agreed specification after changes to the threat level. A security posture at a higher threat level must build on the strengths of the posture implemented at the lower threat level.

Practices or activities that fall within an organisation's security posture are many and varied. Outlined below are some example practices that can be implemented or modified at short notice after changes to an organisation's threat level. Following this is a worked example of a security posture for an airline carrier flying into a number of overseas locations with varying threat levels at the different locations:

- Provision of threat-risk briefings
- Training (awareness, refresher, personal safety, group, emergency/evacuation, *et cetera*)
- Wearing/non-wearing of uniforms
- Wearing of passes and Sign-In books
- Individual and/or group travel arrangements
- Deployment and positioning of bollards at road or building entry points
- Deployment of static and mobile security guards (foot and/or vehicle mounted)
- Graduated carriage of weapons (none, batons/cuffs, then firearms)
- Rules of engagement/Orders for opening fire

SAFETY MEASURE	1	2	3	4	5
Briefings	Upon induction/ recruitment plus on an annual basis, all staff are to be briefed on local security plans and on protective security measures/ practices. Intelligence & Staff Safety summaries provided on each country as required, but no less than quarterly.	All staff to be briefed on change of Alert Level and threat where known. All staff to be reminded to be vigilant/inquisitive about strangers, to watch out for unidentified or unattended packages and vehicles. Monthly Intelligence & Staff Safety summaries provided on each country.	All staff to be briefed on change of Alert Level and threat where known. All staff to be advised of contingency and emergency response plans, and reminded to be particularly vigilant. Intelligence & Staff Safety summaries provided on each country as required but not less than weekly.	All staff to be briefed on change of Alert Level and specific threat. Intelligence & Staff Safety summaries provided on each country as required but not less than bi-weekly.	All staff to be briefed on change of Alert Level and specific threat. Intelligence & Staff Safety summaries provided on each country as required but not less than daily.
Uniform	No restrictions on the wearing of uniform except that security passes are not to be worn outside of airports.	No restrictions on the wearing of uniform except that security passes are not to be worn outside of airports.	No security restrictions on the wearing of uniform, unless the cabin crew manager imposes local restrictions.	No uniforms to be worn outside of airport precincts. Staff are to change within designated lounges.	Consider cancelling flights until Alert Level lowers. Otherwise as per Alert Level 4.
Gatherings	No restrictions.	As per Alert Level 1.	All travel to and from the airport to be undertaken as a group (in consultation with local police as necessary).	Upon disembarkation, all staff are to gather within the designated airport lounge until re-embarkation.	Consider cancelling flights until Alert Level lowers. Otherwise as per Alert Level 4.
Training	Basic aggression management training to be provided to all cabin crew upon induction.	As per Alert Level 1.	Staff receive refresher training or more specialist aggression management training being provided.	As per Alert Level 3.	As per Alert Level 3.
In-Flight	As per current company flight operations policy.	As per current company flight operations policy.	As per current company flight operations policy. Pre-boarding cabin security check undertaken by contractors or as per Alert Level 1.	Additional resources provided to allow alteration of precision timing schedule in order to facilitate Pre-boarding cabin security check to be undertaken by operating (outbound) cabin crew.	As per Alert Level 4.

SAFETY MEASURE	1	2	3	4	5
Other	Institutionalising a process to ensure all facilities and flight sectors are regularly assessed for weaknesses, and measures taken to mitigate these.	Communications checked with emergency response arrangements. Contracted hotel advised of heightened Alert and asked to review its security.	All local leave outside of the secure hotel area is cancelled. Contracted hotel asked to employ additional security staff in hotel precinct. Company Security to conduct on sight review. Consider arming flight crew.	Slipping is cancelled and crews move to transit patterns. Company aircraft to be guarded at all times whilst parked. Consider deploying a civilian security guard with cabin crew (or deploying with armed sky marshals). Local/airport security presence required.	Consider cancelling flights until Alert Level lowers. Consider only flying if supported by armed sky marshals. Company aircraft to be guarded at all times whilst parked. Local/airport and company security presence mandatory.

3.2. Advantages of Specifying Specifications and Postures

There are a large number of benefits associated with the establishment of security specifications and postures, including it:

- Helps the organisation's senior management make decisions about the level of risk the organisation is prepared to accept (that is, what is to be considered an acceptable or unacceptable risk)
- Ensures consistency in security arrangements
- Embeds a culture of risk management
- Assists with the development of business cases as it defines the resources required for treating risk
- Directly links security control with the threat, thus ensuring that which is of key value to the organisation has the most protection
- Allows for security reviews, audits and plans to be based on comprehensive and expected specifications

4. RECOMMENDED SPECIFICATIONS AND POSTURES

4.1. Access Control - Guidelines

4.1.1. Secure Areas, Rooms and Containers

Sensitive or classified information and equipment is usually used and stored in secure rooms or security containers inside secure areas to which access is closely controlled. This provides multiple layers of protection. There are three broad types of secure areas, classified by the degree of security protection they provide. A secure area can be a single room, a building or a complex consisting of a number of buildings. The areas are:

- Secure (S) - A Secure Area is one which is secured in a manner suitable for handling the most sensitive of an organisation's materials (up to and including TOP SECRET level in the national security context). The essential physical security features of a secure area include:
  - the area being safeguarded by a combination of Security Construction and Equipment Committee (SCEC) endorsed/ASIO approved physical barriers (such as tamper evident barriers highly resistant to covert entry with no unsecured openings)1
  - an approved means of limiting entry to authorised personnel only
  - a SCEC endorsed Type 1 security alarm system (SAS), which provides after hours coverage of all areas where classified material is handled and/or stored, and has a secure communications link to an effective response force2
  - guards patrolling internally after hours at irregular intervals not exceeding two hours, physically checking every security container to detect or restrict unauthorised access
  - the reaction to an alarm by a response force should be within five minutes, but not exceeding thirty minutes
- Partially Secure (PS) - A Partially Secure Area is one which is secured in a manner suitable for the handling of very sensitive materials (up to and including SECRET level in the national security context). The essential features of a partially secure area include:

[1] *Tamper evident barriers are barriers that provide three dimensional containment and have sufficient resistance to covert entry as to reasonably ensure that for a person to gain unauthorised entry and exit, without being apprehended, it would be necessary to damage or modify the barriers in such a manner that the breach would readily be evident.*

[2] *On site guards, conducting after hours internal patrols, physically checking every container at intervals not exceeding two hours, may be employed in lieu of a SAS, provided there are sufficient guards to respond effectively to incidents.*

  - the area being safeguarded by a combination of endorsed physical barriers (such as tamper evident barriers highly resistant to covert entry with no unsecured openings)
  - an approved means of limiting entry to authorised people only
  - guards patrolling internally after hours at irregular intervals not exceeding four hours, physically checking every security container
  - the reaction to an alarm/incident by a suitably-sized response force should be within five minutes but not exceeding thirty minutes
- Intruder Resistant (IR) - An Intruder Resistant Area is one which is secured in a manner suitable for the handling of sensitive or classified material up to SECRET level. The essential physical security requirements of an intruder resistant area include:
  - tamper evident barriers, resistant to covert entry, with no unsecured openings
  - an effective means of limiting entry to authorised people only

Areas that do not meet these requirements are known as unsecured areas and should not be used for the handling or storage of sensitive or classified materials.

Secure rooms, like security containers, can also be classified according to the level of protection they provide (Class A, B or C):

SECURE ROOM TYPE	COMMENTS
Class A Secure Rooms	• constructed of reinforced concrete, and • fitted with the following: – an A class door with two endorsed Manifoil combination locks, – approved volumetric intrusion detection devices, and – a micro switch fitted to the door to operate off the bolt of the lock.
Class B Secure Rooms	• constructed of masonry or concrete, and • fitted with the following: – a class B door with an endorsed Manifoil combination lock, – approved volumetric intrusion detection devices, and – a micro switch fitted to the door to operate off the bolt of the lock.

Class C Secure Rooms	• a solid core, steel-faced door, • SCEC endorsed locks, • approved volumetric intrusion detection devices, and • a micro switch fitted to the door to operate off the bolt of the lock.

Entry to Secure and Partially Secure Areas should be closely controlled. Factors that can impact on the access control needs of an area include the:

- Classification or value of the information
- Location, size and layout of the area
- Level of entry authorisation
- Number of entry points
- Nature of the business and operating hours
- number of employees and visitors
- need for an audit trail

The types of access control measures that could be applied, either in isolation or in concert depending on the nature of the threat, are:

- electronically controlled access system
- guards, attendants or receptionists
- passes and identity cards
- intruder awareness

4.1.2. Controlling Visitor Access

Within a secure or partially secure area, visitors (ie persons that do not possess an organisation-issued pass) should be escorted at all times. And all organisational staff should make it their responsibility to control their visitors' access.

Effective control of visitor access includes the use of a visitors' register. The register should generally include the:

- name of the visitor
- visitor's employer or private address
- name of the person being visited
- time of arrival and departure
- reason for the visit

A person who does not meet these criteria should be treated as a visitor.

A sample process for controlling visitor access is outlined below:

STEP	PERSON	COMMENTS
1	**Visitor**	• Advises the guard or receptionist of their arrival and purpose of their visit. • Completes and signs the visitor's register.
2	**Guard or receptionist**	• Telephones the person being visited and advises them of the visitor's arrival. • Issues the visitor with a visitor's pass.
3	**Visitor**	Displays their visitor's pass in a prominent position at all times during the visit.
4	**Organisation Representative**	• Authorises access for their visitor. • Escorts the visitor throughout the visit. • Ensures that the visitor does not gain unauthorised access to classified material. • Confirms that the visitor has left the establishment after the visit. • Returns the visitor's pass to the guard or receptionist at the end of the visit.
5	**Guard or receptionist**	At the end of the day: • Checks that all visitors' passes have been returned, and • Accounts for any visitors' passes that have not been returned.

The register should generally be covered to prevent visitors seeing the details of other visitors. It should also be held at a controlled point, such as by a guard, receptionist, or a designated person.

4.2. Access Control – Specifications

Minimum Recommended Organisational Specifications

The table below outlines recommended minimum security requirements that should be met for each of the three types of secure area. Additional security measures could be required as a result of your organisation's specific security risk review:

REQUIREMENT	TYPE S	TYPE PS	TYPE IR
Building Security			
Appropriately secured points of entry and other openings.	✓	✓	
Tamper-evident barriers resistant to covert entry.	✓	✓	✓
An approved means of limiting entry to authorised people only.	✓	✓	✓
Employee and visitor security			
All staff, contractors and visitors requiring frequent and on-going entry to the area, hold an appropriate security clearance.	✓	✓	
All must wear security passes in the area.	✓	✓	
All visitors are escorted at all times in the area.	✓	✓	
After hours Security			
After hours security involves either: • an approved Type 1 security alarm system with a secure communications link to an effective response force, providing coverage for all areas where classified information is stored; • an approved security alarm system designed for site-specific applications; or, • security guards conducting internal patrols and physically checking each security container at least every two hours.	✓		
After hours security involves either: • an endorsed security alarm system, installed to requisite specifications; or, • security guards conducting internal patrols and physically checking each security container at least every four hours.		✓	

Additional supporting policy requirements that should be considered include:

- Criteria for unescorted access
- Unescorted access should only be provided if a person has:
  - a suitable form of identification,
  - a legitimate need for access to the area, and
  - the appropriate security clearance.

Records

A record should be kept of everyone who enters and leaves a building or establishment outside of the normal working hours, showing their:

- name;
- organisation or company; and,
- time of entry and exit.

The record should be checked regularly by a designated staff member and any anomalies investigated.

Records should also be kept of all maintenance and repair work done in secure rooms or areas.

Records would generally not be required if an electronic controlled access system or security alarm system is installed.

Security Inspections

Before entering a secure area, all people should be asked to submit carried items and vehicles to a security inspection. The aim of these inspections is to prevent the unauthorised entry of dangerous items into the secure area.

4.3. Physical Barriers and Hardenings - Guidelines

This section deals with fences, vehicle barriers, security grilles and hardenings for walls, doors and windows. As with the previous section, it deals with *guidelines* for each component first and then provides recommended minimum *specifications* for consideration/modification to meet organisation-specific threat contexts. Following this, there is a detailed list of design considerations relating to the use of physical barriers and hardenings.

4.3.1. Fences - Guidelines

4.3.1.1. Introduction

A fence or wall can form a useful barrier and can identify the boundary of a protected or restricted area. The level of protection offered by a fence will depend on its height, construction, the material used to increase its performance or effectiveness such as topping, perimeter intrusion detection systems (PIDS), lighting or CCTV.

Fences provide only limited and temporary obstacles to unauthorised entry and should not be seen as standalone capabilities. Indeed they must be viewed as an integral part of wider security measures and infrastructure directed towards deterrence, prevention, detection and reaction to unauthorised entry or exit. The level of required security measures is based upon a risk assessment that addresses the likely enactment of such threats and the consequential effects, both in monetary and operational terms, of loss or damage to the asset.

In planning the siting and erection of security fences, the following factors are to be considered:

- Locating fences to provide sufficient stand-off distance from the protected asset to counter hand thrown devices (and their effects) from reaching the asset
- Minimising bends, corners and angles in the fence line and adding complementary security technology to provide additional surveillance where necessary
- Constructing the fence inside the limits of the organisation's property to permit organisational jurisdiction on both sides of the fence
- Siting the fences to be multifunctional to meet the requirements of 'normal' physical security, as well as during periods of increased tension through
- Timber should never be used as an alternate fence material because it usually requires high maintenance and it can be easily burnt
- Solid walls restrict visibility and require more surveillance. Caution should be exercised in selecting them as a preferred option because of the higher surveillance costs and potentially lower security effectiveness because of lack of sight lines
- A fence or wall can form a useful barrier and can identify the boundary of a protected or restricted area. The level of protection offered by a fence will depend

on its height, construction, the material used to increase its performance or effectiveness such as topping, PIDS, lighting or CCTV

4.3.1.2. Types of Fences

To meet the diverse requirements of organisations, SRMBOK divides fences into the classifications of *Property Delineation* and *Security Fences*. The type of fence to be used by an organisation should reflect the type of threat that needs to be countered; for example, terrorist, criminal, or vandals. Fences are graded according to the level of protection they offer, *Class 1* being the lowest security and *Class 4* the highest. Each of these is discussed in greater detail below.

Property Delineation Fences

Boundary Fences (Class 1)

A *Class 1* boundary fences is a fence designed with no particular security requirements and is any solid fence, wall or hedge at least 1.5m high. Such a fence is only intended to mark a boundary and to offer minimum of deterrence or resistance to anyone other than a determined intruder (Level D). They have very limited security applications.

Perimeter Fences (Class 2)

Perimeter fences delineate chancery/residency boundaries adjacent to public roads and public access areas. A *Class 2* perimeter fence is an anti-intruder fence that offers a degree of resistance to climbing and breaching by an opportunist intruder not having particular skills and using material and breaching items that are readily to hand (Level C). Types of Class 2 fences include:

- **Welded Mesh Anti Intruder Fence -** This is a specification BS 1722 (1990) Part 10 Anti-Intruder fence 2.9m high constructed with welded mesh fabric in accordance with SSG specifications and drawing 101-01
- **Palisade Anti Intruder Fence -** This is a specification BS 1722 (1990) Part 12 Steel Palisade fence security pattern 3m high type SP30
- **Expamet Fence -** A specification Expanded Metal (Expamet) fence security pattern with steel posts and Expamet 2089 at least 2.9m high
- **Steel Profile Sheet Fence (SPSF) -** A steel profile sheet fence 3m high constructed to an approved design using profile steel sheets at least 1.2mm thick
- **Brick/Block Wall -** A solid dense masonry wall at least 3m high and minimum thickness 100mm constructed of bricks or blocks having a minimum crushing strength of 7N/ sq mm. The resistance to climb over of the above Anti Intruder and Expamet fences can be improved by the addition of a topping of a 1m diameter barbed wire or barbed tape concertina coil. However, owing to the limited height and ease of climbing of the fences, barbed tape should not be used on perimeters where the general public has access to the fence

Other materials such as brick, iron, stone and concrete may be considered as alternate perimeter fences depending to some extent upon the material used in the construction of the facility being protected. If the facility is a showpiece, it may be appropriate to duplicate the material used, even though the cost of the perimeter fence may be higher as a result.

Security Fences

Standard Security Fences (Class 3)

Security fences delineate the boundaries of restricted areas. A *Class 3* security fence is an intermediate security barrier designed to deter and delay a resourceful attacker who has access to a limited range of hand tools (Level B). A Class 3 fence will normally be supported by other perimeter security systems. The design and construction will offer resistance to attempts at climbing and breaching. Types of Class 3 fences include:

- **Intermediate Security Welded Mesh Fence (ISWMF) -** The Intermediate Security Welded Mesh Fence is a 3.0m high fence constructed of narrow aperture heavy duty mesh with a barbed tape concertina topping giving an overall height of 3.9m built in accordance with SSG specification clauses and specification drawings PS/103, PS/103/01, PS/103/02, PS/103/03 and PS/103/04. This fence complies with BS 1722 Part 14: 1992 Category 4
- **Intermediate Security Palisade Fence (ISPF) -** This is an Improved Palisade fence 3.0m high based on BS 1722 Part 12 1990, Security pattern Type SP30 with barbed tape concertina topping giving an overall height of 3.85m constructed in accordance with SSG specification clauses and specification drawing SSG-106-02. Or, the Portcullis High Security Palisade Fence constructed in accordance with specification PSP6 1992. This fence has the same basic dimensions and construction materials as the SSG design
- **Intermediate Security Profile Sheet Fence (ISPSF) -** An Intermediate Security Profile Sheet fence is constructed to an approved design using 3m high profile steel sheets at least 1.2mm thick and a barbed tape concertina topping raising the overall height to 3.9m. This fence will need to be provided with a concrete kerb or sill unless the steel sheet is extended and buried into the ground by 300mm
- **Intermediate Security Wall (ISW) -** The Intermediate Security Wall is 3.0m high constructed of dense masonry of minimum thickness 190mm and having a minimum crushing strength of 7N/sq mm. A 150mm thick reinforced concrete wall with two layers of reinforcing mesh is also acceptable. The wall is topped with barbed tape concertina increasing the overall height to 3.9m. It may also be topped with revolving blades or spikes

High Security Fences (Class 4)

A *Class 4* high security barrier is designed to offer the maximum deterrence and delay to a skilled and determined intruder who is well equipped and resourced (Level A). It will be designed and constructed to offer a high degree of resistance to a climbing or breaching attack. The different types of Class 4 fences are as follows:

- **High Security Welded Mesh Fence (HSWMF) -** The High Security Welded Mesh Fence is a 3.6m high fence constructed of narrow aperture heavy duty mesh with a barbed tape concertina topping giving an overall height of 4.5m built in accordance with SSG specification clauses and specification drawings
- **High Security Palisade Fence (HSPF) -** The High Security Palisade Fence is a 3.6m high fence based on BS 1722 Part 12:1990 security pattern Type SP36 but with a layer of welded mesh or expanded metal mesh fixed between the pales and rails, and a barbed tape concertina topping giving an overall height of 4.5m constructed in accordance with SSG specification clauses and specification drawing SSG-106-03
- **High Security Wall (HSW) -** The High Security Wall is 3.6m high constructed of dense masonry of minimum thickness 190mm and having a minimum crushing strength of 7N/sq mm. A 150mm thick reinforced concrete wall with two layers of reinforcing mesh is also acceptable. The wall is topped with a 500mm diameter barbed tape concertina topping slightly increasing the overall height

Performance

The effectiveness of any security barrier will depend to a large extent on the level of security at the points of entry. Gates must be constructed to the same security specification as the fence; and control of entry must be maintained, otherwise the security of the fence will be negated.

Fences can be penetrated in one of three ways: over, under, or through. Methods of penetration include; catapulting over, jumping off a van, ramming flat by truck, burrowing under, cutting, throwing carpet over the top and scaling. Methods least likely to alert the attention of guards are popular as, depending on the back-up system, valuable penetration time may be gained. The time required to penetrate these fences is only a couple of seconds regardless of their complexity, as shown in the following tables:

CLASS 4 - HIGH SECURITY LEVELS

Attack Level	Minimum Delay in Minutes (Penetration / Climbing)		
	HSWMF	HSPF	HSW
A	3/2	3/2	5/2
B	6/4	7/4	8 /2
C	2	2	2
D	2	2	2

- Delay times for climbing attacks are given for unassisted attackers assuming only a stump of wood or equivalent is available for Class 4 barriers. Two attackers working together are likely to reduce the times given or even make those climbs deemed impossible, possible. The use of a ladder will have a similar effect. Attempts at surreptitious entry will increase delay times considerably.
- It is unlikely that any attack at this level will be successful and any that are will take an inordinate time to complete.

CLASS 3 - INTERMEDIATE SECURITY LEVELS

Attack Level	Minimum Delay in Minutes (Penetration / Climbing)			
	ISWMF	ISPF	ISW	ISPSF
A	1.5/2	0.5/2	5/0.5	4/2
B	3/3.5	3/3	8/1	7/4
C	2	2	2	2
D	2	2	2	2

- Delay times for climbing attacks are given for unassisted attackers assuming only a stump of wood or equivalent is available for Class 3 barriers. Two attackers working together are likely to reduce the times given or even make those climbs deemed impossible, possible. The use of a ladder will have a similar effect. Attempts at surreptitious entry will increase delay times considerably.
- It is assumed that a grapnel is available only for Level A attackers.

CLASS 2

Attack Level	Minimum Delay in Seconds (Penetration / Climbing)				
	Welded Mesh	Palisade	Expamet	SPSF	Wall
A	20/10	15/15	40/12	4/20	30/10
B	30/20	30/30	80/24	7/30	30/20
C	60/30	60/60	300/60	1/60	60/60
D	na/30	na/60	na/60	na/60	na/60

Service Life of Fences

The service life of fences varies considerably depending on the incidence of accidental damage and environmental factors. In normal circumstances:

- **High Security Palisade** fences should have a service life of at least 25 years and require little maintenance except for the repair of accidental or deliberate damage. High Security Welded Mesh fences should last 15-20 years and High Security Walls 50-100 years
- **Intermediate Security Palisade** fences should have a service life of at least 25 years and require little maintenance except for the repair of accidental or deliberate damage
- **Intermediate Security Welded Mesh** fences should last 15-20 years and Intermediate Security Walls at least 40 years
- **Standard Welded Mesh** and expanded metal fences should last at least 10 years as should profile steel sheet fences
- **Palisade fences** should have a service life of at least 20 years. A brick or block wall should remain serviceable for at least 30 years

- The service life of **galvanised barbed tape concertina** before it loses its efficiency is 7-10 years. However, in coastal environments and other situations where there is a corrosive atmosphere the service life is likely to be very much shorter and stainless steel barbed tape concertina should be used

4.3.2. Fences – Specifications

Minimum Recommended Organisational Specifications

Please refer to the following table and supporting explanatory 'Class' notes to determine the type of minimum fencing recommended based on the level of threat at the organisation's location:

Security Measure	Low	Moderate	Medium	High	Extreme
Perimeter fences		Class 1	Class 2	Class 3	Class 4

Class 1:

If a fence is required, the minimum specification to be provided should be a 1.5m multi-strand wire fence. A 25m corridor, free of undergrowth and boulders, should be provided on the inside of the boundary fence for vehicle access and to act as a firebreak. Chain wire fences should be installed to suit the particular site conditions, and in accordance with the appropriate specification. The bottom of the wire should be adequately anchored to prevent deliberate access by individuals or accidental damage by rubbish build-up. On a sloped site it may be necessary to provide a concrete kerb to prevent scouring of the soil creating openings under the fence. In addition the bottom of the fence may need a rail to anchor the wire and to maintain a small opening for the passage of surface water and debris that would otherwise build up against the fence causing corrosion or bellying of the wire and subsequent failure of the fence as a perimeter barrier.

In very sandy soils subject to wind erosion or where animals burrow, it may be necessary to provide additional mesh in the ground. A 600mm wide horizontal strip of mesh at ground level and a 150mm vertical strip below ground will prevent rabbits from burrowing. Other materials such as brick, iron, stone and concrete may be considered as alternate perimeter fences depending to some extent upon the material used in the construction of the facility being protected. If the facility is a showpiece, it may be appropriate to duplicate the material used, even though the cost of the perimeter fence may be higher as a result.

This type of fence is used to keep people and stock at a safe distance from the Perimeter Barrier of facilities and provides a basic security against missiles or bombs thrown from outside the cattle fence.

Class 2:

The minimum specification of security fencing to be provided for a threat requiring Class 2 fencing should be a galvanised, rail-less chain wire security fence and gates 2.44m high, topped with at least three strands of barbed (or similar) wire. Fences should be clear of obstructions such as trees, fixed equipment, or vehicle parking positions for a distance of 5m. Should a fence line cross ditches, drains or other obstacles, the opening produced by such obstacles must be secured against entry/exit by incorporating mesh bars or other appropriate means. A Class 2 fence may be supported by other perimeter security systems. Again, signs with wording "Trespassers Prohibited" provide a stronger, and legal, warning of the fact that the fence is a perimeter for a secured facility and should not be crossed. This can improve the surveillance of the Perimeter Barrier.

Class 3:

The minimum specification of security fencing to be provided for a threat requiring Class 3 fencing should be one of the above, with the addition of the following:

- The wire mesh is to be topped by razor tape
- A concrete base 250 x 250 mm should be constructed up to ground level throughout the length of the fence. The lower edge of the chain mesh should be within 50mm of the top of the concrete base
- One strand of tensioned barbed wire should be clipped to the lower limit of the chain mesh
- The security fences should be provided with outward focused lighting along their entire length
- A clearance of 25m should be maintained from either side of the security fence to all undergrowth, trees and structures

Class 4:

To meet this requirement, a double security fence should be constructed with the minimum width of the corridor between the inner and outer fences to be 5m. The outer fence should comply with the specifications of a perimeter fence. The inner fence should be constructed in accordance with the specifications for a specification security fence with the addition of intruder alarms and surveillance equipment, to which an identified, manned response capability is provided at all times. A Class 4 fence should also be supported by other perimeter security systems.

Signage:

Signs with wording “Trespassers Prohibited” provide a strong, and legal, warning of the fact that the fence is a perimeter for a secured facility and should not be crossed. Signs should be placed at distances to ensure that two signs are visible from any one position external to the fence.

The clear warnings and the fact that people trespassed through a fence are evidence that the organisation attempted to effectively protect the public from injury.

4.3.3. Vehicle Barrier - Guidelines

4.3.3.1. General

Vehicles loaded with explosives can inflict severe damage on buildings and critical facilities, potentially injuring large numbers of staff. Vehicles are effective because they are an expedient method for transporting large quantities of explosives to any convenient location.

The primary factor to consider when defending against this threat is the barrier penetration capabilities of the vehicle. Once the standoff distance for a structure has been established (based on the amount of explosives and acceptable damage and injury levels), a threat vehicle should not be allowed to get close to the structure where a greater level of damage could occur.

The gross weight of a vehicle (vehicle weight plus the weight of explosives or any other cargo) and its maximum attainable speed at the point of impact produces kinetic energy that must be absorbed by the perimeter barrier to effectively stop the vehicle from getting close to the intended target. Therefore, kinetic energy can be used as the primary basis for establishing performance requirements for vehicle barriers.

4.3.3.2. Site Surveys

The vehicle barrier selection and design process must always begin with a site survey. To accomplish this phase, a scaled map of the protected area must be prepared. The map should include the relative locations, major dimensions and descriptions of buildings and structures, roads, terrain and landscaping, existing security features, and property perimeter. It must also show features outside the perimeter that could be used to slow vehicle speed, prevent access to the perimeter barrier, or shield the structure from damage, if an explosion occurred. Based on this map distances and topographical features between the perimeter and the facility can be carefully analysed and the required levels of protection along the perimeter and security deficiencies if any, can be identified.

4.3.3.3. Integrated Systems

An integrated physical security protection system can be developed from the deficiencies identified in the site survey. Current security requirements and threats identified for the specific facility should be considered. Physical barriers, such as perimeter fences and active and passive barriers should be integrated with other security components and options to provide comprehensive protection. For example, vehicles attempting to penetrate the perimeter covertly can be detected, using perimeter sensors, lights, and closed circuit television (CCTV) and assessed. Sally ports can be used to detect bombs hidden in vehicles entering the facility. Bollards, ditches and planters can be strategically placed to improve performance and reduce the cost of the perimeter barrier. Clear zones can be used for early detection of a broad range of potential threats.

4.3.3.4. Vehicle Barrier Design and Installation

Vehicle Barrier Types

Vehicle barriers are categorised as either *active* or *passive*. Active and passive barriers can be fixed or movable, depending on how they are made, operated, or used. Some commercial barriers are dual classified, when they meet the requirements for both categories (for example, fixed-active, portable-passive etc). There is no industry-wide specification terminology for vehicle barriers. SRMBOK uses the following definitions:

- **Active Barrier Systems (ABS).** An active barrier requires some action, either by personnel, equipment or both, to permit entry of a vehicle. Active barrier systems include barricades; bollards, beams, gates and active tire shredders
- **Passive Barrier Systems (PBS).** A passive barrier has no moving parts. Passive barrier effectiveness relies on its ability to absorb energy and transmit the energy to its foundation. Highway medians (Jersey bounce) bollards or posts, tyres, guardrails, ditches and reinforced fences are examples of passive barriers
- **Fixed Barrier Systems (FBS).** A fixed barrier is permanently installed or requires heavy equipment to move or dismantle. Examples include hydraulically operated rotation or retracting systems, pits and concrete or steel barriers. Fixed barrier systems can be either active or passive
- **Portable/Movable Barrier Systems (PMBS).** A portable/movable barrier system can be relocated from place to place. It may require heavy equipment to assist in the transfer. Hydraulically operated, sled-type, barricade systems, highway medians, or filled 55-gallon drums that are not set in foundations are typical examples. Portable/movable barrier systems can be either active or passive

4.3.4. Vehicle Barriers - Specifications

Minimum Recommended Organisational Specifications

Please refer to the following table to determine the type of minimum vehicle barrier recommended based on the level of threat at the location:

Security Measure	Low	Moderate	Medium	High	Extreme
Building Protection			PBS	ABS	ABS

Vehicle Barrier Selection Checklist

The following checklist incorporates the selection process and the vehicle barrier design and installation requirements. Answers to the checklist questions should be used during the selection process for both active and passive barriers.

Design Factors

- What is the explosive threat?
- What is the weight of the threat vehicle?
- Is there sufficient standoff distance between the planned barrier and the protected structure?
- What is the expected speed of the vehicle?
- Can the speed of the vehicle be reduced?
- What is the calculated kinetic energy developed by the moving vehicle?
- Have all impact points along the perimeter been identified?
- Have the number of access points requiring vehicle barrier installation been minimised?
- What is the most cost-effective active barrier available that will absorb the kinetic energy developed by the threat vehicle?
- How many barriers are required at each entry point to meet throughput requirements?
- What is the most cost-effective passive barrier that will absorb the kinetic energy developed by the threat vehicle?
- Will the use of aesthetic barriers at some locations be necessary?
- Is penetration into the site a factor?
- If penetration into the site is a factor, is the standoff distance adequate after impact?
- Will traffic flow be affected by the barrier's normal cycle rate?
- Will the active barrier need to be activated at a rate higher than the normal rate?
- Will the barrier be required to be normally open (allow traffic to pass) or normally closed (stop traffic flow)?
- If normally open (allowing traffic flow), is adequate distance available between the guard post and the barrier to allow activation and operation of the barrier?
- Will the barrier be subject to severe environmental conditions?
- Do passive barriers installed along the perimeter provide equivalent protection to the active barriers?
- Do passive barriers interfere with established clear zone requirements?

- In case of power failure, will the barrier fail open or closed?
- Is this a temporary or permanent installation?

Selection Factors

- Will the selected barrier need to be aesthetically pleasing?
- Are appropriate safety features being considered?
- Will there be sufficient lighting at the active barrier location?
- Will electronic access control (card reader) be included?
- If so, are procedures in place to prevent tailgating?
- Will the active barrier require backup power?
- What is the available power source?
- Is training available from the manufacturer?
- Does the manufacturer have optional features available to meet operational, safety, security, and Repair and maintenance requirements?
- Has the selected barrier been crash-tested or are calculations/computer analysis available that will demonstrate performance capability?
- Will the active barrier be electrically or hydraulically powered?
- How will the barrier be controlled?
- Is the selected barrier designed to resist corrosion or other environmental effects?
- Will the active barrier function adequately within the temperature extremes present at the selected site?
- Are optional heaters and coolers available to compensate for temperature extremes?
- Is the active barrier capable of manual operation in case of power failure?
- Is the active or passive barrier the most cost-effective option available?

Installation Factors

- Is there a high water table?
- If so, can the excavation be adequately drained?
- Will active barriers be installed in areas that are under constant surveillance?
- Are barriers installed on both the entrance and exit sides of the access point?
- Are spare parts available for the active barrier?
- Will regularly scheduled maintenance be performed in-house or by contract?

4.3.5. Security Grille - Guidelines

4.3.5.1. General

Security grilles are used to cover openings in secure perimeters where a continuous barrier is required, but it is necessary to allow for the flow of air or the transmission of light. Grilles are also used to protect external building fixtures. Grilles will generally be designed to resist one or more forms of attack and can usually be categorized as follows:

- **Forcible attack resistant** (FAR) - Security grilles designed to resist forcible attack that are considerably robust and provide resistance to cutting, bending, and removal by both forcible and covert means. The frame, infill fabric, fixings and fasteners should be designed to resist the highest identified level of threat
- **Covert attack resistant** (CAR) - Security grilles designed to resist covert entry and to provide a delay after the first act of entering is made. This delay provides an opportunity for a response force to arrive and apprehend the intruder
- **Vandal attack resistant** (VAR) - designed to protect resources and assets against typical acts of vandalism, not to provide protection against forcible intrusion. They are generally of low to moderate strength to protect glass and external fittings against wanton damage. The infill fabric selected should provide small apertures to protect against thrown missiles, and mace like objects wielded by vandals. Vandal resistant grilles should provide moderate resistance to cutting, and removal by both forcible and covert means. Grilles designed to protect against vandal attacks should be fitted to the outside of windows or the externally exposed fixtures, which are to be protected

Each of these is covered in detail below.

4.3.5.2. Forcible Attack Resistant (FAR) Grilles

FAR Grilles for Windows

Security grilles fitted to windows to resist forcible entry are normally fitted to the outside of the window as this gives protection to the glazing and provides a clear deterrent. However, where an alarm system is installed the grille should be fitted inside of the glazing to provide a delay after the first act of entering is made, for example, the breaking of the glass. This delay provides an opportunity for a response force to arrive and apprehend the intruder.

FAR Grilles for Air Intakes

It is considered that ventilator and air conditioner intakes are unlikely to be exploited by intruders to gain entry to buildings as there is normally major plant installed immediately to the inside. However there may be some instances where protection of the plant is the main concern. Security grilles fitted to ventilator and air-conditioning intakes to resist forcible entry are normally fitted to the outside as this provides protection and a visible

deterrent. Security grilles fitted to such ventilator or air-conditioning intakes may be hung on hinges and secured using suitable door deadlocks and other hardware. Where an alarm system is installed, micro switches or balanced magnetic reed switches should be considered where the threat is significant.

Duct penetrations into Level 1 and Level 2 rooms may require installation of spigots, fire dampers and/or inspection plates. The duct penetrations may be either flanged or slip joints.

FAR Grilles for Air Ducting

It is considered that ventilator and air conditioner ducting is unlikely to be exploited by intruders to gain entry to buildings as there is normally insufficient space to do so as the ducts reduce in cross section near to the branches, outlets and registers. The possibility should not be dismissed lightly when the intruder might be highly motivated. Security grilles fitted to ventilator and air-conditioning ducting are normally fitted inside the ducting at the point where the ducting passes through a dividing wall between an area where little or no security is required and another where a higher level of security is required. These grilles should be fitted when the ducting is installed to avoid fitting difficulties. However, this working note includes a design for a security grille suitable for retrofitting to existing ducting. A clear viewing panel should be fitted on the secure side to allow the grille to be inspected on a regular basis.

FAR Grilles for Miscellaneous Openings

Any round opening that exceeds 200mm in diameter or rectangular opening that exceeds 150mm in more than one dimension should be treated as a possible point to be exploited by intruders. If the opening has no essential function it should be filled using materials of the same specification as the surrounding building fabric. It might be possible to fit a lockable cover or door, of equal or greater resistance to forcible attack, as the surrounding building fabric. If a grille is fitted it too should be at least as resistant to forcible attack or intrusion as the surrounding building.

4.3.5.3. Covert Attack Resistant (CAR) Grilles

CAR Grilles for Windows

Security grilles fitted to windows to resist covert entry are normally fitted to the inside of the window, particularly where a security alarm system is installed, to provide a delay after the first act of entering is made, for example, the breaking of the glass. This delay provides an opportunity for a response force to arrive and apprehend the intruder. The design emphasis must be to prevent entry by covert means.

CAR Grilles for Air Ducting

Ventilator and air-conditioning intakes are unlikely to be exploited by intruders to gain entry to buildings as there is normally major plant installed immediately to the inside. However, there may be some installations where this is not the case and other instances

where protection of the plant is of some concern. Security grilles fitted to ventilator and air-conditioning intakes to resist covert entry are normally fitted within the ducting at a point where the ducting passes through a perimeter wall or barrier.

CAR Grilles for Miscellaneous Openings

Any round opening that exceeds 200mm in diameter or rectangular that exceeds 150mm in more than one dimension should be treated as a possible point to be exploited by intruders. If the opening has no essential function it should be filled using material of the same specification as the surrounding building fabric. It might be possible to fit a lockable cover or door, of equal or greater resistance to covert intrusion, as the surrounding building fabric. If a grille is fitted it too should be at least as resistant to covert intrusion as the surrounding building fabric. Grilles described in this Annex are suitable for securing the voids which are normally found between the top of wall partitions and the underside of floor slabs or roofs where suspended ceilings are featured.

4.3.5.4. Vandal Attack Resistant (VAR) Grilles

VAR Grilles

VAR grilles are designed to protect resources and assets against typical acts of vandalism, not to provide protection against forcible intrusion. Grilles fitted to windows to resist vandalism are normally fitted to the outside of the window as this gives protection to the glazing and provides a clear deterrent.

4.3.5.5. Other Considerations with Security Grilles

Escape Mechanisms

In some instances, it will be necessary to fit security grilles to windows or doors which may need to be used as a means of emergency exit. In such cases both security and safety can be achieved by installing a hinged grille with a quick release mechanism which cannot be activated by manipulation using objects placed through the bars. The type of frame and fabric should be selected based on the perceived threat.

The frame should consist of two parts. One part, the outer frame, should be fixed and fastened to a permanent structural part of the building using tamper resistant fastener and intervals not exceeding 300mm on all sides. The other part, the inner frame, to which the grille fabric is welded, should be hinged to the outer frame using heavy duty hinges. If the inner frame is hung to open out, hinge bolts or similar devices, should be incorporated to resist removal of the grille at the hinged edge if the hinge pins are removed. The grille fabric should be welded into the frame.

The locking bolt should be fully enclosed by a steel case and operated by a remotely located release lever, knob etc. The linkage between the release lever and the locking bolt should be covered and protected. Alternatively the locking bolt can be connected to a remote release lever using an encased steel cable. The cable casing should be

supported to minimise the possibility of persons applying a force on the outer cable which could cause the locking bolt to release the grille. The release mechanism should be protected to prevent persons reaching through the grille or using some apparatus from outside the building to open the grille.

Aesthetic Considerations

The use of security grilles will be resisted in many installations because of their appearance and possible psychological effects on the occupants. Security grilles do tend to highlight the fact that the premises contain valuable resources or assets. Use of creative design and materials can usually reduce the visual effect of security grilles to an acceptable degree.

- **Materials.** Vertical, horizontal or slanted beams made from timber or rectangular hollow section steel can be used with good visual effect. Timber can then be stained or painted. Rectangular hollow section steel painted in modern colours can be just as effective. Ornamental ceramic, concrete or glass bricks can also be used with good effect in some applications
- **Placement.** It is often possible to slightly alter the actual location or route of a secure perimeter to improve the appearance of a secure grille or similar type barrier or to make it less conspicuous
- **Disguise.** It is often possible to disguise the security grille by the use of indoor pot plants or those of the climbing variety, which can be trained over the security grille itself. Artwork can also be used to lessen the visual effect of security grilles

Where an Alarm System is Fitted

Where a security alarm system is installed, security grilles fitted to protect a glazed aperture should be fitted to the inside of the glass. Grilles fitted in this manner, with appropriate security alarm detection devices, will then provide delay to intruders after an alarm is affected by the breaking of the glass. Grilles fitted to the inside also simplify cleaning and usually detract less from the appearance of the building. However, where protection against vandalism is required it is practical to place the security grilles to the outside of the glazed panel.

Inspections

Security grilles should be inspected regularly to ensure that they have not been tampered with or weakened by their environment.

4.3.6. Security Grille - Specifications

Minimum Recommended Security Grille Specifications

Please refer to the following table to determine the type of minimum security grille recommended based on the level of threat at the location:

Security Measure	Low	Moderate	Medium	High	Extreme
Building Protection	CAR*	VAR	VAR	FAR	FAR

* Or approved security glazing.

FAR Grilles for Windows

Strength - Security grilles for windows should be fabricated from metal, preferably steel, and are resistant to intrusion as the fabric of the building to which it is fitted. The grille should always be welded into a metal frame to provide a strong fixing. The fasteners must be equally strong and resistant to tamper or removal.

Specification - Specifications for a typical window security grille for protection against forcible attack are as follows:

- Frame: 50mm x 50mm x 6mm steel angle or equivalent RHS steel
- Infill Fabric: 12mm diameter vertical bars at 150mm centres, welded into the frame
- Spreaders: Spreaders to separate the bars should be placed at 500mm intervals
- Construction: All welded construction
- Fasteners: Grille should be fastened to a permanent structural part of the building using tamper resistant fasteners at intervals not exceeding 300mm on all sides

Variations - The above specification can be varied to suit the application. There would be few applications where it would be necessary to increase the bar diameter beyond 20mm. In some applications it will be acceptable to install a security grille of lesser strength. However, security grilles designed to protect against forcible intrusion should have a frame made from a minimum of 35mm x 35mm x 3mm angle steel and a mesh infill fabric not less than 8mm in diameter with multiple spreaders, such as F81 reinforcing mesh or equivalent grid type mesh.

FAR Grilles for Air Intakes

Strength - Security grilles for ventilator and air-conditioning intakes should be fabricated from metal, preferably steel, and equally as resistant to intrusion as the fabric of the building to which it is fitted. The grille should always be welded into a metal frame to provide a strong fixing. The fasteners must be equally strong and resistant to tamper or removal.

Specification - Specifications for a typical ventilator or air conditioner security grille for protection against forcible attack are as follows:

- Frame: 50mm x 50mm x 6mm steel angle or equivalent RHS steel
- Infill Fabric: 12mm diameter vertical bars at 150mm centres, welded into the frames
- Spreaders: Spreaders to separate the bars should be placed at 500mm intervals
- Construction: All welded construction

- Fasteners: The grille should be fastened to a permanent structural part of the building using tamper resistant fasteners at intervals not exceeding 300mm on all sides

FAR Grilles for Air Ducting

Strength - Security grilles for ventilator and air-conditioning ducting should be fabricated from metal, preferably steel, and be as resistant to intrusion as the fabric of the surrounding wall which the ducting passes through. The grille should always be welded into a metal frame to provide a strong fixing. The fasteners must be equally strong and resistant to tamper or removal.

Specification - Specifications for a typical ventilator or air conditioner security grille for protection against forcible attack are as follows:

- Frame: 50mm x 50mm x 6mm steel angle or equivalent RHS steel
- Fill Fabric: 12mm diameter vertical bars at 150mm centres, welded into the frame
- Spreaders: Where possible spreaders to separate the bars should be placed at 500mm intervals. Where spreaders cannot be fitted, the diameter of the bars should be increased to compensate
- Construction: All welded construction
- Fasteners: The grille should be fastened to a permanent structural part of the building using tamper resistant fasteners at intervals not exceeding 300mm on all sides

FAR Grilles for Miscellaneous Openings

Strength - Security grilles should be fabricated from metal, preferably steel, and equally as resistant to intrusion as the fabric of the building to which it is fitted. The grille should always be welded into a metal frame to provide a strong fixing. The fasteners must be equally strong and resistant to tamper or removal.

Specification - Specifications for a typical security grille for protection against forcible attack are as follows:

- Frame: 50mm x 50mm x 6mm steel angle or equivalent RHS steel
- Fill Fabric: 12mm diameter vertical bars at 150mm centres, welded into the frame
- Spreaders: Spreaders to separate the bars should be placed at 500mm intervals
- Construction: All welded construction
- Fasteners: The grille should be fastened to a permanent structural part of the building using tamper resistant fasteners at intervals not exceeding 300mm on all sides

CAR Grilles for Windows

Strength - Security grilles for windows should be fabricated from metal, preferably steel, and be as resistant to covert intrusion as the fabric of the building to which they are fitted. The grille should always be welded into a metal frame to provide a strong fixing. The fasteners must be equally strong and resistant to tamper or removal.

Specification - Specifications for a typical window security grille for protection against forcible attack are as follows:

- Frame: 35mm x 35mm x 3mm steel angle or equivalent RHS steel
- Infill Fabric: Steel mesh such as grid mesh, concrete reinforcing mesh or similar welded into the frame
- Construction: All welded construction
- Fasteners: The grille should be fastened to a permanent structural part of the building using tamper resistant fasteners at intervals not exceeding 300mm on all sides

CAR Grilles for Air Ducting

Strength - Security grilles for ventilator and air-conditioning intakes should be fabricated from metal, preferably steel, and equally as resistant to covert intrusion as the fabric of the barrier that the ducting is passing through. The grille should always be welded into a metal frame to provide a strong fixing. The fasteners must be equally strong and resistant to tamper or removal. Because such grilles are normally difficult to inspect for signs of tampering, the strength and resistance to forcible attack should be considered in some applications.

Specification - Specifications for a typical air ducting security grille for protection against forcible attack are as follows:

- Frame: 35mm x 35mm x 3mm steel angle or equivalent RHS steel
- Infill Fabric: 12mm diameter vertical bars at 150mm centres, welded into the frames
- Spreaders: Spreaders to separate the bars should be placed at 500mm intervals
- Construction: All welded construction
- Fasteners: The grille should be fastened to a permanent structural part of the building using tamper resistant fasteners at intervals not exceeding 300mm on all sides

Variations - The above specification can be varied to suit the application as applicable. Where the grille is fitted to ducting which passes into a strong room or vault, the grille should provide resistance to both covert and forced entry equal to that provided by the walls of the strong room or vault. Where an air duct passes through the wall of Secure Rooms, specifications for a suitable grille should be sought from a physical security professional. Rooms shall not be constructed with air or other ducting which exceeds that which is set out in the specifications for each level of room.

There will be occasions when it is necessary to retrofit grilles to existing air ducting. This can be achieved by fitting a 50mm x 6mm flat steel frame which is bolted together on the outside of the ducting. The bars which pass through the wall of the ducting and the frame are threaded both ends and when fitted into position are permanently fastened using nuts fitted to the threaded ends protruding from the frame. The grille is fitted on the secure side of the wall as close to the wall as possible. As it is not possible to fit spreaders to the bars, the diameter of the bars should be increased as the span increases to adequately resist spreading of the bars by an intruder. The nuts and other fasteners should be rendered tamper resistant by the use of superglue, tack welding or by the use of other tamper resistant measures.

It may be necessary in some installations to provide means to allow the grille to be inspected at regular intervals. This can be provided for by the fitting of an inspection window in a vertical wall of the ducting to the inside (secure side) of the grille close to the grille.

CAR Grilles for Miscellaneous Openings

Strength - Security grilles should be fabricated from metal, preferably steel, and equally as resistant to intrusion as the fabric of the building to which it is fitted. The fasteners must be equally strong and resistant to tamper or removal.

Specification - Specifications for a typical security grille for protection against covert attack are as follows:

- Frame: 35mm x 35mm x 3.5mm steel angle or equivalent RHS steel
- Infill Fabric: F81 reinforcing mesh, welded into the frames. Grid mesh or ornamental mesh of equivalent or greater strength may also be used
- Construction: All welded construction
- Fasteners: Grille should be fastened to a permanent structural part of the building using tamper resistant fasteners at intervals not exceeding 300mm on all sides

Variations - Where it is necessary to provide resistance to forcible attack, in addition to covert intrusion, the specification for forcible attack resistant grilles should be adopted.

VAR Grilles

Strength - Vandal resistant grilles should be fabricated from metal, preferably steel, and designed to resist hand thrown missiles. The grille should be welded into a mental frame to provide a strong fixing, however where the threat is low it may be satisfactory to wire the grille fabric to the frame. The fasteners must be resistant to tamper or removal.

Specifications - Specifications for a typical vandal resistant grille are as follows:

- Frame: 25mm diameter mild steel tube
- Fill Fabric: Chain wire mesh secured by 3mm diameter tie wire should be considered as the minimum fabric for vandal resistant grilles. Where vandalism is evident a heavier steel mesh should be specified. F81 reinforcing mesh would be considered the upper limit for vandal resistant grilles. If large aperture mesh is fitted it may be necessary to consider overlaying this with a small aperture wire mesh to resist small hand thrown objects
- Supports: Large grilles should be fitted with evenly spaced vertical support bars at intervals not exceeding 1200mm
- Construction: The frame should be of all welded construction. Wiring of the mesh fabric at intervals not exceeding 75mm is recommended
- Fasteners: Grille should be fitted with mounting brackets, welded to the frame at intervals not exceeding 200mm for fastening to a permanent structural part of the building using tamper resistant fasteners at intervals in keeping with the level of threat

4.3.7. Walls, Doors and Window Treatments - Guidelines

4.3.7.1. Overview

In determining the type of wall and window treatments required, it is important consider the different types of threat trying to be countered. These threats can include amongst others, espionage, bomb blasts, ballistic projectiles fired by criminals, and/or standoff weapons. Each of these is discussed below.

4.3.7.2. Espionage Threats

The level and type of espionage threat will be available from organisational threat assessments or, for government agencies, from DFAT and ASIO security risk assessments. Ostensibly though, the threat will be closely linked with the market sector and country in which the organisation is operating, the size of the commercial deal, and the relative importance or profile of the deal from a politico-economic perspective.

4.3.7.3. Blast Threats

A blast threat can be categorised as being either from a stationary or a moving bomb threat. Given the large variance in size of bombs possible a detailed discussion of each threat severity level has not been covered. The general principles are covered in the following sections. The damage caused to a structure is generally as a result of blast overpressure generated by the bomb blast and from debris moving at high speed as a direct consequence. In general, the pressure levels of a bomb blast decrease as the inverse square of the distance from the blast. Consequently, the further the distance from the blast the lower the pressure delivered to the structure.

Generally, when a blast wave strikes a building, the façade and windows will fail and, depending on the size of the blast, the walls and columns may suffer some deflection under the blast load. The blast wave will expand and diffract over the building and pressure will also be exerted on the roof and sides of the building. In order to harden a facility against blast and ballistic threats, the effectiveness of wall/window material thickness, weapon size, and standoff distance for the weapon must be considered. In order to minimise blast threats, it is preferable to locate car parks and access points for buildings away from critical functions. The routes of service vehicles or public roads should be separated from critical facilities by either distance or blast protection. Small vans should maintain a minimum separation from buildings of 50m and large vans should maintain a 100m separation. Car parking should be located no closer than 25m from any building where ever possible.

The use of glazed windows in facilities subject to a blast threat requires special consideration. The effect of the blast will cause significant personal injury to employees working in the facility and potentially to surrounding structures and personnel. Following the blast it is likely that the glass and material fragments remaining in the workspace may prevent the facility being reoccupied for quite sometime, even if the structure itself remains unaffected.

4.3.7.4. Ballistic Weapons Threats

In a ballistic attack, the aggressor fires various small arms weapons, including pistols, rifles, machine guns and other direct fire weapons from a distance determined by the range of the weapon and the accessibility of the target. A ballistic weapon attack requires line of sight access to the target being attacked. The ballistic threat posed by a bullet depends on its calibre, type, shape and weight, impact velocity, trajectory, energy and range. The design of facilities to counter ballistic weapons threats is not covered in this manual, but issues which require consideration are highlighted so that appropriate technical experts within industry can be consulted on their application.

4.3.7.5. Ballistic Protection Measures

Siting of the building and protection methods are used to limit or negate the effects of ballistic attack.

Siting Measures

As ballistic weapons require line of sight observation for use the simplest method of achieving ballistic protection is to limit sightlines or to extend the distances from a potential weapon position to the building.

- Facility Siting – The initial site selection should consider the ballistic attack. Facilities located on elevated ground would force a potential attacker to fire upwards. Under these conditions a person inside a building would be partially obscured and the projectiles would hit the building at an angle, thereby reducing their effectiveness. Facilities should also be located away from natural or man-made vantage points which could be utilised as firing points for ballistic weapons. The siting of facilities should also make due consideration for the location of roads and access ways as these may provide opportunities for ballistic weapons fired from moving or stationary vehicles
- Obscuration – The use of landscaping features, obscuration fences, walls and other non-essential structures may be used to block the sight lines to a facility. These measures must be considered in combination with other security measures on the site to prevent covert or forcible entry into the building

Building Measures

Enhancement of the building fabric can aid in the protection of a facility, its occupants and its business operations. In high threat environments, the key building components to be considered include:

- Layout – To limit the exposure of critical areas to bullets, preference is given to housing critical assets centrally within the facility. Entry ways and access ways should be located to prevent direct sight lines through doorways
- Walls – Wall construction depends on the threat severity and proximity to the blast, and will need to be designed with these issues in mind:

INTERNAL WALLS

Class	Bomb Threat [3]	Thickness	Comments
FEBR 1	Low	10-20mm	Standard gyprock sheeting or equivalent.
FEBR 2	Moderate	Intruder Resistant	Reinforced with 1mm mild steel.
FEBR 3	Medium	Intruder Resistant	Ballistic Steel - 3mm thick ballistic steel sheet or 6mm thick ballistic aluminium sheet or reinforced with Mild Steel Sheet - Stud walling sheeted with one layer of 6mm thick mild steel sheet or two layers of 3mm thick mild steel sheet. Or 75mm reinforced concrete.

EXTERNAL WALLS

Class	Distance from Bomb Threat [4]	Thickness	Comments
FEBR 4	> 50m from bomb threat	100mm masonry or 75mm reinforced concrete	Slab-to-slab construction. Reinforced with plywood and/or 1mm sheet steel mesh.
FEBR 5	30-50m from bomb threat	100mm concrete	Slab-to-slab construction. Reinforced with 3mm mild steel.
FEBR 6	< 30m	150mm concrete	Slab-to-slab construction. Reinforced with one layer of 6mm thick mild steel sheet or two layers of 3mm thick mild steel sheet. Concrete shall have ultimate compressive strength at 26 days of 30 MPa & be reinforced with 6mm diameter steel bars at 100mm centres each way. Must have an engineering study conducted.

- Doors – Because doors and openings are perceived by attackers to be more vulnerable than other components, the number of external doors should be minimised to reduce potential targets. A variety of door types can be used ranging from specification doors with steel plate, bullet proof panels or ballistic glass.
- Windows – The number, size and location of windows should be minimised to limit the number of potential targets available. Additionally, the nature of the window treatment should be based on whether there is a ballistic or blast threat. If the primary threat is from ballistic weapons (for example due to a high crime threat), the Australian Standard AS 2343 Parts 1 and 2 *Bullet Resistant Panels for Interior Use* should be used as the minimum specification. 5 This specification uses the following classifications:

[3] *Most likely source/size of an internal bomb threat is a backpack or 'suicide' belt (@<5kg).*

[4] *Most likely source/size of an external bomb threat is a car bomb or a standoff weapon, such as a rocket-propelled grenade.*

[5] Please note that the equivalent specifications to AS2343 Part 1 are:

- Class G0 - Resistant to attack by a 9mm military parabellum hand gun
- Class G1 - Resistant to attack by a 357 magnum hand gun
- Class G2 - Resistant to attack by a 44 magnum hand gun
- Class R1 - Resistant to attack by a 5.56mm rifle
- Class R2 - Resistant to attack by a 7.62mm rifle
- Class S0 - Resistant to attack by a 12 gauge shotgun (full choke) firing shot
- Class S1 - Resistant to attack by a 12 gauge shotgun (full choke) firing a single slug

Alternatively, if the primary threat is from blast weapons, the following guidelines should be considered:

EXTERNAL WINDOWS

Class	Distance from Bomb Threat [6]	Thickness	Comments
FEBR W1	> 50m from bomb threat	180micron film	
FEBR W2	30-50m from bomb threat	600micron film minimum	Consider using laminated glass or Polyvinyl Butyral (PVB).
FEBR W3	< 30m	750micron film	Use Laminated Glass of 33-35mm thickness or PVB. Noviflex resin should be used. The frame for glazing should also be to same rating as the glazing. Must have an engineering study conducted.

- Service Openings and Penetrations – Service openings and penetrations will only require protection when assets contained within the building can be directly targeted through them. Bullet-resistant louvres and dampers can be used to provide higher levels of protection.
- Roof Protection – Roof protection only needs to be provided when there are potential sightlines to the roof. Depending on the threat scenario a variety of measures may be used ranging from removal of skylights through to hardening of the roof structure. Alternatively a parapet may be provided on the roof to eliminate sightlines.

- British BS5051 Part 1 - Rating G1
- German DIN52290 Part 2 - Rating C2
- US Underwriters Lab US752 - Rating II

[6] *Most likely source/size of an external bomb threat is a car bomb or a standoff weapon, such as a rocket-propelled grenade.*

4.3.7.6. Standoff Weapons Threats

For the purposes of this manual the only standoff weapon threat considered is that of any rocket propelled grenade (RPG) variant. Other standoff weapons have not been considered, although the general principles contained in this section are applicable to the complete range of standoff weapons. A standoff weapon attack is usually directed towards killing or injuring personnel inside a building, with associate damage to critical equipment. Such weapons are not generally used to gain entry or cause significant damage to a building. Most of the damage caused is as a result of direct impact or spalling of the building fabric.

Defeat Mechanisms

The penetration of a rocket-propelled grenade (RPG) and the explosive effect it generates when hitting the structure, is limited primarily by material density, strength and the tendency of some materials to rebound onto the jet. Pre-detonation of the explosive warhead prior to impact with the building or limiting clear sightlines may also assist in defeating a standoff RPG attack:

- **Material Density -** The penetration achieved by the standoff weapon is approximately inversely proportional to the square root of the density of the material. Those materials which have a higher density are more effective at stopping a standoff weapon
- **Material Strength -** In general materials with a high brinell hardness number (BHN) have a better stopping ability
- **Rebound Defeat Mechanisms -** Rebound is a phenomena where target materials move back into the cavity caused by the jet from the standoff weapon and this mechanism then interferes with subsequent portions of the jet, reducing its penetrating capability. Only certain materials, such as steel, ceramics, aluminium and glass reinforced plastics exhibit rebound characteristics
- **Oblique Attack Effects -** Building surfaces which are at some angle to the potential line of attack create a thicker material cross section for the weapon to penetrate
- **Pre-detonation and Standoff -** Screens and barriers can be used to pre-detonate a standoff weapon away from the structure to be protected

4.3.7.7. Hardening Design Options

Site Layout

As standoff weapons still require line of sight in order to attack the facility, the facility should be sighted to limit or to block attack sightlines. Options for site layout include the use of man made and natural structures to obscure or block sightlines; siting the facility at a high point; or to cause the weapon to hit the facility at an angle, thereby reducing its effectiveness.

Sacrificial Areas

Sacrificial areas around the area to be protected will permit a degree of damage to the sacrificial area but reduce the effectiveness of the weapon against the protected area. Critical areas should be internal to the building and in the lower portions of its structure.

4.3.7.8. Barrier Construction and Pre-Detonation Screens

- **Wall Construction** – If a standoff weapon threat is likely to be a permanent threat against a facility the use of reinforced concrete walls, pre-detonation walls and screens is essential
- **Roofs and Floors** – Due to structural limitations it is likely that sacrificial areas are the only feasible methods of protecting roof and floor spaces from standoff weapons
- **Windows** – Areas to be protected from standoff weapons should be free from windows
- **Doors** – Foyer areas should be provided at entrances to protected areas or door openings, or door openings should be offset so that the doors are opposite a solid wall

4.3.8. Walls, Doors and Window Treatments - Specifications

Minimum Recommended Wall Treatment Specifications

Please refer to the following two tables and supporting explanatory notes to determine the type of recommended minimum *wall treatment* materials recommended based on the level of threat at a location:

INTERIOR WALLS:

Security Measure	Low	Moderate	Medium	High	Extreme
Building Protection	FEBR 1*	FEBR 2*	FEBR 3*		

EXTERIOR WALLS:

Security Measure	Low	Moderate	Medium	High	Extreme
Building Protection			FEBR 4	FEBR 5	FEBR 6

NOTES:

*** In customer/public areas**

Minimum Recommended Door and Window Treatment Specifications

Please refer to the following table and supporting explanatory notes to determine the type of minimum *door and window treatment* materials recommended based on the level and type of threat at the location:

BALLISTIC THREAT:

Security Measure	Low	Moderate	Medium	High	Extreme
Building Protection			Class G0	Class G1	Class G2

BLAST THREAT:

Security Measure	Low	Moderate	Medium	High	Extreme
Building Protection			FEBR W1	FEBR W2	FEBR W3

NOTES:

Parcel Tray / Voice Transfer:

- A parcel tray /voice transfer system should be incorporated in the counter top. The height of FEBR construction should not be less than 2.1 metres, with normal walling above this to the underside of the structural slab.

Mesh:

- Please refer to the specifications for security grilles previously within this Chapter for more detailed guidance.
- Gyprock panelling OR steel mesh should be fitted in ceiling cavities along the perimeter walls which adjoin publicly accessible areas and walls with adjacent tenants. If mesh is fitted, it should have a minimum of 8 mm rods on 100 mm centres. The mesh should be welded onto a 35 mm x 35 mm x 3 mm steel angle frame and secured in place by tamper resistant barriers. If Gyprock panelling is fitted, it should be secured to the ceiling and underside of the slab by tamper proof fasteners.

Doors:

- Should be sheeted with either 3mm thick ballistic steel, 6mm ballistic aluminium, 6mm thick mild steel, or two layers of 3mm thick mild steel sheet.
- All door hinges and locks should be to the same specification as walls, ie should be intruder resistant for at least five minutes.
- All doors should also be fitted with hinge bolts 300mm from the top and bottom of a door. The hinge bolt should consist of a metal section that extends from the hinge side of the door and engages with a metal receiving plate which is mounted into and fixed flush with the door hanging jamb.

4.3.8.1. Design Considerations

In addition to calculating the kinetic energy of a threat vehicle, there are other issues that must be considered before selecting an appropriate barrier system. These issues are discussed below.

Fencing

Fences should not be considered as protection against a moving vehicle attack. Most fences can be easily penetrated by a moving vehicle and will resist impact only if reinforcement is added. Fences are primarily used to:

- Provide a legal boundary defining the outermost limit of a facility
- Assist in controlling and screening authorised vehicle entries into a secured area by deterring overt entry elsewhere along the boundary
- Support detection, assessment, and other security functions by providing a "clear zone" for installing lighting, intrusion detection equipment and CCTV
- Deter "casual" intruders from penetrating into a secured area by presenting a barrier that requires an overt action to penetrate
- Cause an intruder to make an overt action that will demonstrate intent
- Briefly delay penetration into a secured area or facility thereby increasing the possibility of detection

In the field of security, perimeter barriers provide the first line of defence for a facility. The true value of a perimeter security fence comes in its association with other components of a security system. When perimeter security is required, the security fence forms the basic building block for the rest of the system.

Location

Active vehicle barriers can be located at facility entrances, enclave entry points (gates) or selected interior locations (for example, entrances to restricted areas). Exact locations may vary among installations; however, in each case, the barrier should be located as far from the critical structure as practical to minimise damage due to possible explosion. Also, locate support equipment (for example, hydraulic power, generator, batteries etc.) on the secure side and away from guard posts to lower the threat of sabotage and injury to security personnel. Passive barriers can be used at entry points, if traffic flow is restricted or sporadic (ie. gates that are rarely used). Passive barriers are normally used for perimeter protection.

Aesthetics

The overall appearance of a vehicle barrier plays an important role in its selection and acceptance. Many barriers are now made with aesthetics in mind that will blend in with the environment.

Safety

An active vehicle barrier system is capable of inflicting serious injury. Even when used for its intended purpose, it can kill or seriously injure individuals when activated inadvertently, either by operator error or equipment malfunction. Warning signs, lights, bells and bright colours should be used to mark the presence of a barrier and make it visible to oncoming traffic. These safety features should always be provided to ensure personnel safety. The following issues should be addressed to manufacturers and users to identify potential safety issues affecting the selection of an active barrier system:

- Backup power
- Emergency cut-off switch
- Adequate lighting
- Installation of safety options, such as alarms, strobes (or rotating beacons) and safety interlock detectors to prevent the barrier from being accidentally raised in front of or under an authorised vehicle

Once installed, vehicle barriers should be well-marked and pedestrian traffic channelled away from the barrier system. For high-flow conditions, vehicle barriers are normally open (allowing vehicles to pass) and used only when a threat has been detected. In this case, the barrier must be located far enough from the guard post to allow time to activate and close the barrier before the threat vehicle can reach it. For low-flow conditions, or where threat conditions are high, barriers are normally closed (stopping vehicle flow) and lowered only after authorisation has been approved.

Security

Vehicle barriers need to be ready to function when required. A potential for sabotage exists when barriers are left unattended or are located in remote or unsecured areas. For these installation conditions, tamper switches should be installed on all vehicle barrier access doors to controllers or hydraulic systems. Tamper switches should be connected directly to a central alarm station, so that security of the barrier system can be monitored on a continuous basis.

Reliability

Many barrier systems have been in production long enough to develop an operations history under a variety of installation conditions. Reliability data from manufacturers show less than a three-percent failure rate when these barriers are properly maintained. Some systems have been placed in environments not known to the manufacturer, while others have developed problems not anticipated by either the manufacturer or user.

Most manufacturers will help resolve problems that arise in their systems. Backup generators or manual override provisions are needed to ensure continued operation of active vehicle barriers during power failure or equipment malfunction. Spare parts and supplies should also be on hand to ensure that barriers are quickly returned to full operation. If a high cycle rate is anticipated, or the environmental impact from hydraulic fluid contamination is a concern the selection of a pneumatic operating system instead of hydraulic, is recommended.

Maintainability

Many manufacturers provide wiring and hydraulic diagrams, maintenance schedules and procedures for their systems. They should also have spare parts available to keep barriers in continuous operation. The manufacturer should provide barrier maintenance support in the form of training and operation and maintenance manuals. Maintenance contracts are available from most manufacturers and are recommended to ensure proper maintenance of the barrier and assurance that the barrier will function as intended. Reliability and maintainability data are available from most manufacturers. Yearly maintenance contracts are usually available from the manufacturer at about $300 to $500 per month. Maintenance contracts should include inspection, adjustment, cleaning, pressure checks on hydraulic systems and replacement of worn parts.

Cost

Traffic in restricted or sensitive areas should be minimised and the number of access control points limited. Reducing traffic flow and the number of control points will increase security and lower the overall cost of the system. Installation and operational costs are a significant part of the overall cost of a barrier system and must be addressed during the barrier selection process. Complexity and lack of specified components can result in high costs for maintenance and create long, costly downtime periods. Reliability, availability and maintainability requirements on the system also affect costs.

Barrier Operations

A barrier must be capable of operating continuously and with minimal maintenance and downtime to properly satisfy security requirements. System failure modes must be evaluated to ensure that the barrier will fail in the predetermined position (open or closed) based on security and operational considerations. Selecting a normally open (allowing access) or closed (preventing access) option should be evaluated based on traffic flow conditions at the site (either existing or expected) and the overall site security plan. Emergency operation systems (backup generators or manual override systems) should be in place to operate the barrier in case of breakdowns or power failure. If a normally open (allows traffic through) operation is selected, there must be sufficient distance between the guard and the vehicle barrier to allow activation and closing of the barrier.

Clear Zones

Barriers installed in clear zones should be designed so they will not provide a protective shield or hiding place. Tall, continuous barriers, such as planters, Jersey Barriers,

guardrails and other similar passive vehicle barriers can be a violation of mandated requirements if installed in a designated clear zone.

Environment

The environment needs to be considered during the selection process. Hinges, hydraulics or surfaces with critical tolerances may require heaters to resist freezing temperatures and ice build up. They may also require protection from excessive heat, dirt, humidity, salt water, sand, high water table and debris. If options for protection against environmental conditions are not available, the system may be unsuitable for a specific location. Maintenance should be increased and/or compensating options (ie. sump pumps, heaters, hydraulic fluid coolers etc.) selected for vehicle barriers subject to severe environmental conditions to ensure acceptable operation.

Installation Requirements

The vehicle barrier selected needs to be compatible with the available power source and with other security equipment installed at the selected site, such as perimeter intrusion detection and CCTVs designed to detect and assess covert penetration of the perimeter. Power requirements can vary depending upon the manufacturer and location of the installation.

Operator Training

Most manufacturers recommend operator training for active barrier systems. Operator training prevents serious injury and legal liability, as well as equipment damage caused by improper operations. If a manufacturer does not provide a thorough program for operator training, the user should develop a checklist for normal and emergency operating procedures.

Options

Manufacturers offer a number of optional features that can be added to the baseline systems. Some options enhance system performance, while others improve maintainability or safety. Options increase system cost and may also increase maintenance requirements. Selection of options depends on operational, safety, security, site and environmental conditions. Manufacturers can provide guidance on available options and will make recommendations that will enhance barrier operations.

Operational Cycle

The frequency of operation needs to be considered in the selection process. Where traffic flow is light, a manually operated or removable passive system may work well at considerable savings. However, for high traffic flow conditions (especially during peak hours), an automatically controlled system designed for repeated and fast open and close operation (pneumatic or hydraulic) would be more desirable. The use of one or more barriers at an entry point can also improve throughput.

Methods of Access Control

When selecting an active barrier, consider how vehicles will be allowed access. If a vehicle must be searched for explosives, a sally port design should be used, which will trap the vehicle between two active barriers while it is being searched. This will prevent the vehicle from proceeding into the secured area before it has been searched, and prevent escape. Access control can be accomplished with a staffed guard station or remotely using card or biometric access control devices that automatically activate the barrier (subject to random searches).

The barrier can also be operated from a protected location other than the entry control point, using CCTV and remote controls. Access control systems are available as options from vehicle barrier manufacturers. Vehicle sensing loops on the secure side of the vehicle barrier should always be included to prevent activation of the barrier until the vehicle has completely cleared the system. If card access control systems are used, procedures must be included to prevent tailgating (authorised vehicle must wait until the barrier has closed completely before proceeding).

Cost Effectiveness

Tradeoffs on protective measures may include:

- Locating the vehicle barrier to provide optimum separation distance
- Slowing down vehicles approaching the barrier, using obstructions or redesign of the access route
- Barrier open to permit access versus Closed to prevent access
- Active versus Passive barriers
- System-activating options; manual versus automatic, local versus remote, electric versus hydraulic
- Liabilities - Possible legal issues resulting from accidents, deaths, injuries and legal jurisdiction (i.e. state, local and federal) should be considered when deciding to install an active vehicle barrier system

Actions to Avoid

Do not install barriers that need to be installed below ground level in locations where there is a high water table. Unless the excavation can be drained, water collection will cause corrosion and freezing weather may incapacitate the system.

- Do not install barriers at entrance exit gates without also installing passive barrier systems along the remaining accessible perimeter of the protected area
- Avoid extensive protection of a large facility perimeter. Protection of individual buildings or zones within the perimeter is generally more cost-effective
- Avoid installing barriers where they are not under continuous observation. Most types of barriers can be easily sabotaged

- Avoid locating barriers immediately adjacent to guard posts to minimise possibility of injury
- Do not neglect to install barriers on the exit side, as well as the entrance
- Avoid long, straight paths to a crash-resistant barrier. Where this cannot be avoided, provide a passive-type barrier maze to slow the vehicle

4.4. Locks and Keys - Guidelines

4.4.1. Locks Overview

The lock is the most widely used method of controlling physical access. Locks are used for homes, vehicles, offices, safes, cabinets and briefcases amongst others. Locks are among the oldest of security devices and have amassed a slew of technical jargon to define the locksmith's craft.

Locks can be divided into three very general classes: 1) those that operate on purely *mechanical* principles; and 2) those that are *electrical* and 3) those that *combine* electrical energy with mechanical operations and are commonly associated with automated access control systems. Due to the wide range of systems available, Electronic Access Control Systems (EACS) are not SCEC endorsed. However, some individual components, such as electric locking, are endorsed as is biometric access control (retinal scan).

Most systems now available provide satisfactory performance but, as cost can vary significantly depending on the user's requirements, such as the level of security and complexity of reporting, EACS are best evaluated against a user's particular needs, rather than one system against another. There are a number of generic types of systems, some of which are outlined below.

There are several specifications that apply to lock designs and quality, including amongst others:

- European Standard EN 12209
- British Standard BS 3621 Locking Devices - Lock Cases
- British Standard BS EN 1303 Locking Devices - Cylinders
- American National Standard for Interconnected Locks and Latches ANSI/BHMA A156.12
- American National Standard for Mortise Locks and Latches ANSI/BHMA A156.13

For the purposes of this guideline and specification, the security and performance ratings in EN 12209 and BS EN 1303 have been used.

4.4.2. Mechanical Locks

A mechanical lock utilises some barrier arrangement of physical parts to prevent the opening of the bolt or latch. In such a lock, the functional assembly of components is:

- The bolt or latch that actually holds the movable part (door, window, etc.) to the immovable part (jamb, frame, etc.)
- The keeper or strike into which the bolt or latch fits. The keeper is not an integral part of the lock mechanism but provides a secure housing for the bolt when in a locked position
- The tumbler array that constitutes the barrier or labyrinth that must be passed to move the bolt
- The key or unlocking device, which is specifically designed to pass the barrier and operate the bolt

In most mechanical locks, the bolt and barrier are in the permanently installed hardware or lockset; the key or unlocking device is separate. However, in some mechanical locks that use physical logic devices, the entire lock is a single assembly. Examples of these include locks with integral digital keypads that mechanically release the bolt if the correct sequence is entered, and dial-type combination locks.

Lock systems used for high security applications are endorsed by the SCEC and details contained in the SEC. The application rating of a lock may be affected by the way it is installed or by the level of the security fit out of the area in which it is being used. For example, if a particular intruder resistant area lock were to be fitted to a perimeter fire door with no exterior keyway or door handle and the door suitably alarmed against intrusion, the lock could be considered as meeting a Secure Area application.

Commercial mortice locks do not provide the same level of resistance to forced attack as the endorsed level mortice locks, and are therefore only suitable for applications where these features are not required. Commercial mortice locks have the advantage of relatively quick cylinder replacement for key control purposes and protection of the lockset by being morticed into the door. Where the existing door thickness precludes the use of a mortice lock the use of a cylinder rim lock is recommended. Cylinder mortice and cylinder rim locks should be used with either a dead bolt or dead latching function.

4.4.3. Electrified Locking Mechanisms

Electrified locking mechanisms allow doors to be locked and unlocked by a remote device. The device may be a simple electric push button or a motion sensor, or may be a sophisticated automated access control device such as a card reader or digital keypad. In addition, many access control systems allow the use of Boolean logic to augment the control of electrified devices. Boolean logic lets you organise concepts together in sets; for example, ‘‘if door A is locked *and* door B is locked *then* door C can be unlocked.’’ This is useful in the design of mantraps and other high security operations. When considering failure and defeat mechanisms for locks, the addition of remote control devices requires that these other devices be included in the analysis.

Electrically controlled access locks are generally not suitable for stand-alone security because they cannot fulfil all the functions of a human sentry as they monitor only a limited portion of the observable range (visual, audible etc.) that can be observed by humans.

The degree of access control afforded by electronic locks should be varied to match the type of device used. Some electronic lock systems can identify only a code, which is either encoded on a card or a badge carried by the person or is memorised by the individual. The electronic lock system that relies on an encoded card or badge offers the least control because cards and badges can be lost, stolen or borrowed.

During periods outside working hours or when the area is otherwise unoccupied, the electrically controlled access locks should be supplemented by an appropriately endorsed keyed lock suitable for stand-alone security. In some cases this additional lock is, or can be, incorporated in the access control unit.

4.4.4. Combination Electrical-Mechanical Locks

Combination locks include a dial or dials onto which an access code is entered activating the lock to open the door. These are relatively inexpensive, in comparison to electronic access control systems and allow a high level of personnel throughput. One advantage of access codes is that they cannot be lost and subsequently found by unauthorised people unless written down. Their primary disadvantage is the ease with which the access code can be forgotten or passed to unauthorised people and their ability to be overseen by passers by.

Digital Cipher locks

These are similar to the combination locks above except that the access code is entered into a keyboard.

Card readers

Card readers are a means of electronic entry control, which read authorisation information that has been encoded onto a card. Card readers are highly effective access control devices. Most cards are difficult to counterfeit and the system has a high level of personnel throughput capability. Card reader technologies available are proximity, Wiegand, smart card, bar code, magnetic strip and magnetic bit technology.

Automatic combination locks

The more sophisticated types of combination lock systems actually identify the person seeking entry on the basis of some physical characteristic, such as fingerprints or dimensions of fingers. Some systems use a combination of code and identification of a personal characteristic, for example, a numeric code and fingerprint identification.

Some combination systems may perform additional functions, such as initiating an alarm or providing automatic personnel entry/exit inventory. The more common commercially available combination systems and their applications are digital cipher locks, card locks, hand geometry comparison locks, and fingerprint-comparative locks. Regardless of sophistication, electronic locking systems are convenience locks only and should only be used for personnel ingress and egress.

4.4.5. Biometrics

Biometric systems, even though they are more secure, are relatively slow in processing due to the amount of data stored for the biometric pattern. Listed below are a select range of technologies currently in use. A range of other technologies are available or in development.

Fingerprints

Fingerprints are considered one of the most reliable means of personnel identification. Automatic pattern recognition and computerised data processing facilitate fingerprint identification.

Handwriting

Automated handwriting verification systems are available that utilise handwriting dynamics such as velocity and acceleration. Statistical evaluation of these data indicates that an individual's signature is unique and provides a reliable method of verification of identity.

Hand geometry

These systems perform computerised statistical analysis of data used in identifying a hand. Hand geometry is a distinct measurable human characteristic, which is unique to individuals.

Speech

Speech is useful for identity verification and well suited to automated processing. Measurements include: waveform envelope, voice pitch period, relative amplitude spectrum, and vocal trait resonant frequencies.

Face Recognition

These systems perform computerised data capture of the infrared picture of the face. Face recognition using this technique is a distinct measurable human characteristic which is unique to individuals.

Iris Scanning

Iris scanning is a relatively new development that relies on the fact that the human iris is as unique as human fingerprints. The system is non-invasive and involves a photograph being taken of the iris, which is then mapped by a computer to produce a picture of all the unique elements of the particular iris. A small camera at an entry point captures the iris image of approaching persons and matches these with those stored in the system.

The system has not been fully tested and approved by T4 Protective Security, and care should be taken in using it until such tests have been completed.

Retinal Scanning

Retinal scanning involves a laser or infrared beam scanning the retina of the eye. It is not approved by ASIO's T4 Protective Security section, and is said to be less accurate than iris scanning. Because the system is invasive, in that a beam is shone into the eye, concerns have been raised over the use of lasers for this purpose.

Facial Thermography

A relatively new development is that of facial thermography, which involves temperature mapping of the entire face and the pattern of blood vessels. Little is known of the effectiveness of this technology currently, and it is not yet approved by ASIO's T4 Protective Security section.

4.4.6. Keys

Keys giving access to classified information/material and attractive assets are divided into two categories, these being *security keys* and *general administrative keys*.

Security Keys

The following keys are deemed to be security keys because give access to:

- security containers
- security briefcases
- a container protecting security keys
- major, important, sensitive and attractive assets

General Administrative Keys

General administrative keys are those that give access to support or domestic assets.

4.4.7. Key Storage

Keys not on issue are to be stored in a container that affords at least the equivalent protection of the area, or container, to which they provide access.

Outside of normal working hours, security keys should be locked away in a secure container. General administrative keys should be stored in a key cabinet. The cabinet should be secured to an internal wall.

4.4.8. Key Custody

People issued with keys should be made fully responsible for the secure custody of those keys until such time as they are returned to the custodian.

4.4.9. Key Registers

The receipt and issue of all keys is to be controlled through the use of key registers. Separate key registers are to be maintained for security and general administrative keys.

4.4.10. European Standard 12209 for Locking Devices

EN 12209 grades the security and performance of *locking devices* against 10 criteria, these being:

- Categories of Use
- Durability
- Door Mass
- Fire Resistance
- Safety
- Corrosive Resistance
- Security
- Latch Action Durability
- Operations at Extreme Temperatures
- Resistance to Side Load on Lock case

Each of these is outlined below.

Categories of Use -

- Grade 1 - Light Use
- Grade 2 - Normal Use
- Grade 3 - Extreme Use

Durability - Lock case mechanisms must complete the following number of cycles in order to conform to the equivalent grade:

Grade	Deadbolt	Latchbolt	Snib Mechanism
Grade 1	10,000	50,000	10,000
Grade 2	25,000	100,000	25,000
Grade 3	50,000	200,000	25,000

Door Mass - Not applicable to locking devices.

Fire Resistance - Fire resistance classification is in two grades:

- Grade 0 - No safety requirement
- Grade 1 - Product must have been subjected to a successful fire test

Safety - Safety classification is in two grades:

- Grade 0 - No safety requirement
- Grade 1 - All bolts must be operable by hand from the inside and must withdraw simultaneously with pressure not exceeding 6Nm

Corrosive Resistance

Grade	Resistance
Grade 0	No corrosive resistance
Grade 1	Mild Resistance (indoor use)
Grade 2	Moderate Resistance
Grade 3	High Resistance (outdoor use)
Grade 4	Very High Resistance (maritime use)

Security

Grade	Resistance	Comments
Grade 1	Privacy locks for internal doors	
Grade 2	Low security	
Grade 3	Quite high security	Five levers. Fastenings not visible from either side. Drill resistance of exposed parts

Grade	Resistance	Comments
Grade 4	High security	Five levers or more. Fastenings not visible from either side. Drill resistance of exposed parts. Deadbolt projection of 20mm or more. 360 degree turn of key.
Grade 5	Extra high security	Five levers or more. Fastenings not visible from either side. Drill resistance of exposed parts. Deadbolt projection of 20mm or more. 360 degree turn of key.

Latch Action Durability

Grade	Resistance
Grade 1	50,000 cycles at 10Nm side load
Grade 2	100,000 cycles at 50Nm side load
Grade 3	200,000 cycles at 120Nm side load

Operations at Extreme Temperatures

Grade	Comments
Grade 0	No requirement
Grade 1	T Min: -20 degrees C. T Max: +80 degrees C.

Resistance to Side Load on Lock Case

Grade	Resistance
Grade 1	1kN
Grade 2	3kN
Grade 3	5kN
Grade 4	7kN
Grade 5	10kN

Using the European Standard then, a *locking device* would have a 10 digit code similar to the following: 2 2 - 0 1 3 3 1 1 3.

Cylinder Security

BS EN 1303 uses a similar system of six digits for grading *cylinders*. However, the key digit of relevance to staff is the seventh digit (Cylinder Security). A summary of cylinder security grades is shown in the table below.

TESTS	Grades				
	2	3	4	5	6
Min No. effective differs	100	300	15,000	30,000	100,000
Max No. movable parts	2	3	5	6	6
Direct Coding on Key	YES	YES	NO	NO	NO
Min drill time (mins)	-	-	-	5	10
Resistance to attack by chisel	-	-	-	15kN	15kN
Resistance to plug/cylinder extraction	2.5	5	15	20	20

4.4.11. Overarching Lock and Key Guidelines

Keys and combinations provide the simplest and most direct route to a target. Unless strict control is exercised over the issue of keys, the value of most other protective physical security measures is negated. Accordingly, regardless of the types of locks and keys used, the following basic guidelines are recommended for most premises:

- **Exterior Gate and Door Key System** - This system should control all exterior perimeter doors and gates and should be independent of any other organisational locking system. If the perimeter doors are fitted with deadlocks, internal snibs should be removed and replaced with key operated cylinders. The keys to the internal cylinder should not be left in the cylinders. However for safety reasons (such as outbreak of fire) keys to the inside cylinder should be hung in a convenient place near the door. The key should be within easy reach of all occupants, including younger children, but out of sight and reach of persons looking into the house through windows and glazed panels. Should a "visitor" remove a key which has been left near the door for emergency exit then that key will not operate the external cylinder, thus preventing outside entry at a later time
- **Interior Area Lock and Keyway System** - This system should control interior locks within individual physical areas or facilities. Separate locking systems should be used for Intruder Resistant, Partially Secure and Secure Areas
- **Key Management**:
  - keys should only be issued against a signature
  - do not encourage transfer of keys between persons
  - all entries in key registers should be in blue or black ink, except for withdrawals, which are to be entered in red ink
  - completed pages should be retained for a period of at least 12 months from the date of the last entry
  - keep the number of keys issued for any one lock to a minimum
  - regular spot checks should be conducted and the results entered in the key register

- **Overall Lock and Key Coordination** - A single person or section should be responsible for the issuance, installation, repair, combination control/master keys, musters, and recapture of all locking devices

4.5. Locks and Keys - Specifications

Minimum Recommended Lock and Key Specifications

Please refer to the following table and supporting explanatory notes to determine the type of recommended minimum key and locks recommended based on the type of area to be secured:

Security Measure	Low	Moderate	Medium	High	Extreme
Exterior Gate & Doors	22-1133213	22-1134214	SEC Endorsed	SEC Endorsed	SEC Endorsed
Interior Areas*	22-1113203	22-1114204	SEC Endorsed	SEC Endorsed	SEC Endorsed

NOTES:

- * Important office doors should use a minimum 6 pin restricted profile *lock cylinder* (ie Grade 5 or 6 security).

4.6. Alarms, Sensors and Monitoring Devices - Guidelines

4.6.1. Security Alarm Systems

4.6.1.1. General

The installation of a security alarm system (SAS) does not, by itself, constitute having secured an area. Specifications in design, installation, maintenance, and operation are essential if a high level of security and reliability is to be achieved in the alarm system. Regardless of the type of SAS deployed, it will consist of the following components:

- A Detector
- The Annunciator
- Signalling Technology
- A Control Unit

There are three broad types of SAS, these being Type 1, Type 2 and commercial-grade SAS. Each of these is covered in more detail below. Minimum guidelines for each of these components are specified following the discussion on different types of SAS.

4.6.1.2. Type 1 Alarm Systems

In Australia, a Type 1 Alarm is a SCEC-endorsed high security alarm system for the establishment of a *secure area* for the protection of the most sensitive or most highly classified matter. Key features of a Type 1 alarm individual or group auditing of the alarm panel and site access, high communication line security through end of line modules, history and audit trail, Dedicated Encryption System (DES) encryption and the ability to transfer all event details to the next level of monitoring. This ability to recognise which sector or sectors are in alarm allows the monitoring station to make a value decision on whether the event is genuine or false or to determine the extent and the direction of a genuine intrusion therefore ensuring the response provided is appropriate.

The new designs also allow panels to be networked, in either a star or loop configuration, thereby allowing transfer of event information and control from alternative monitoring sites. Monitoring and response resources can therefore be rationalised. Individual programming can facilitate after-hours access by staff while maintaining site security. The audit function, which records entry/exit activity data, can be used to determine the extent of unauthorised activity. The panels and the peripherals are tamper protected to deter internal threat.

There are three manufacturers of Type 1 SAS in Australia with a number of SCEC endorsed products:

- CARDAX – FT Ultrasec
- CHUBB – MPM3, MPM4, MPM5 and HSMP
- HONEYWELL – High Security Manager and Excel XSMP

Details of the specific panels, detectors, end-of-line devices and monitoring stations for use with Type 1 systems can be found in the ASIO Security Equipment Catalogue (SEC).

4.6.1.3. Type 2 Alarm Systems

Type 2 security alarm panels are designed and endorsed for the establishment of *intruder resistant areas* for the protection of assets. These panels are suitable where there is negligible likelihood of a competent technical attack, both internal and external on the system.

The Type 2, which essentially uses the infrastructure of the Type 1 panel, is recommended for those large installations where full event reporting and remote re-setting of sectors is desirable. This can assist the monitoring station, as detailed for Type 1, and rationalise response forces, particularly if the individual sectors are in diverse locations.

The Type 2 is essentially a Type 1 system without the DES encryption between panel and end of line modules (EOLM). The endorsed Type 2 panels also allow for integration with proprietary access control systems. Type 2 may be used for the protection of classified matter where approved by ASIO for site-specific applications.

The Type 1 and Type 2 alarm systems allow security and operational convenience to be integrated into the one panel, thereby providing cost effectiveness in the selection of types of sectors required, and maintenance.

Integration is not always the best solution, due to alarms and access systems being controlled by the same PC and operator. This provides a risk to operational integrity as this mode of operation does not provide a redundancy in the event of PC failure. A separated access control and alarm system also permits control from each system and provides an audit trail across both systems, whereas an integrated system only provides a single layer of audit and allows control of both layers of security (access and alarm) by a single user.

Again, details of the specific panels, detectors, end-of-line devices and monitoring stations for use with Type 2 systems can be found in the ASIO Security Equipment Catalogue (SEC).

4.6.1.4. Commercial Grade Systems

Commercial grade (CG) alarm systems are those that are commercially available. Ostensibly, they differ from Type 1 and 2 alarms in that they utilise end of line resistors instead of the end of line modules. These systems are more easily defeated by technical

personnel. Outlined below are the suggested minimum guidelines for commercial grade systems.

Detectors

Regardless of the detector chosen, it must be able to initiate an alarm signal under any of the following conditions when:

- sensing a stimulus or condition for which it was designed to react
- primary power fails and secondary power does not take over properly; or
- a tamper switch or triggering mechanism is activated

Terminals are to be located within the detector enclosure and shall be readily accessible to permit wiring connections to be made.

Annunciators

Annunciator units should be designed so that when connected with the ancillaries into a detection circuit they provide the means to remotely monitor the condition and control the operation of the detection circuit. If possible, a tamper alarm should be generated when the line between the annunciator and the detector is opened, shorted, or grounded. Annunciator units should be electrically compatible with the detector and circuit supervision equipment described herein and shall be of modular design capable of being installed with other annunciators in a rack, console, or cabinet. Where necessary, individual annunciator units should be able to be furnished in appropriate enclosures. To the extent practicable, equipment related to the annunciator (such as standby battery, power supply, battery charging equipment, audible alarm, and circuit supervisor functions) should also be contained in the same enclosure.

The annunciator panel may have an access/secure switch and shall have an alarm resets switch. An alarm should create a lock-on condition to be displayed by both audible and visual means, which should require a manual restoration and controls to be provided to reset the system. A received alarm should cause the visual device to operate in a pulsing or flashing mode, or other visual indication. The annunciator should have a means of silencing the audible signal from a particular zone during prolonged alarm conditions. However, the visible signal should remain illuminated on the annunciator panel or CRT display until the system is restored to normal operation, except that the visual signal should be changed from pulsing/flashing to a steady mode. CRT displays should continue to show an alarm until all areas are secured. The silencing control should be connected so that the audible alarm signal would be activated upon receipt of an alarm from another zone. When a detection circuit is conditioned for authorised entry into the protected area (Access Mode), annunciators should continue to indicate alarms if circuit supervision limits are exceeded or any tamper switches are disturbed.

Signalling Technology

The annunciator should be provided with terminals for all required external connections. Circuit supervision units should provide security to the communication link between the detector and the annunciator. The level of security provided to the data information on the communication lines between the protected areas and the monitor will be dependent on the type of area being monitored.

Access Control Units

The premises control unit should be designed so that when operated it permits access to a protected area without activating an alarm signal. The unit should consist of circuitry installed in a metal enclosure, the cover of which should contain a two or more position, key-operated switch. The positions should be labelled ACCESS and SECURE plus whatever other labels are required to denote the functions designed into the unit submitted for qualification. Turning the switch from SECURE to ACCESS should alter the signal(s) to the annunciator and should deactivate the detection device; however the tamper switches should continue to be monitored. Turning the switch from ACCESS to SECURE should alter the signal(s) to the annuncitor and should activate the detection device to enable monitoring of alarm and tamper signals.

A standby-battery source for use in the event the primary power source fails should be provided. When fully charged, the standby-battery power source should be capable of maintaining full operation of the alarm system for not less than four (4) continuous hours at temperatures from minus 30°C (minus 22°Fahrenheit) to plus 49°C (120°Fahrenheit). Switch-over to battery power should be instantaneous and automatic upon failure or restoration of the primary power source and should not create alarms on annunciator modules, although the loss of primary power should be noted by separate indication.

4.6.2. Security Alarm Systems – Specifications

Minimum Recommended SAS Specifications

Please refer to the following tables and supporting explanatory notes to determine the type of minimum materials recommended based on the type of area to be secured:

Area Type	Minimum Security Alarm System
Intruder Resistant Area	Type 2 Alarm system & peripherals
Secure Room	Type 1 Alarm system & peripherals

Security Measure	Low	Moderate	Medium	High	Extreme
Building Protection	CG*	CG	Type 2**	Type 2	Type 1***

NOTES:

* Commercial Grade monitored system.

** Except where the espionage threat is Medium or higher, in which case a Type 1 SAS should be used with best available commercial support. In lieu of dedicated polling line, this may require a redundant line.

*** For all Type 1 SAS:

- Detectors should cover all entrance and exit points. All perimeter doors should be protected with Balanced Magnetic Reed switches. All SAS hardware is to be located within the perimeter of the residence.
- A Man-Machine Interface, (keypad), should be located within the residence in close proximity to the main entry door, and should provide for a 30-second delay on entry/exit. If power is lost to the residence, an uninterrupted power supply (UPS) or battery back up system should be used to provide power to the SAS for a minimum of four (4) hours.
- All detectors and hardware should be SCEC-endorsed. These items should be selected from the SEC.
- The SAS should be monitored by a host country accredited monitoring station, in accordance with Australian Standard (AS) 2201 or an equivalent specification.
- There should be written procedures in place in the event of an alarm. These may vary in accordance with operational requirements, but they must encompass instructions on contacting the staff and families, and a suitable response. Contingency plans should be put in place in the event of failure of the Type 1 SAS.

Sensor-activated halogen flood lighting should be installed at both the front and rear of the office/residence to illuminate the immediate grounds area. A command switch for the lighting shall be installed within the house for manual override or for manual use of the lighting.

4.6.3. Closed Circuit Televisions - Guidelines

4.6.3.1. Introduction

The term *closed circuit* means that the camera image is displayed via a complete or closed path from the camera to a specific display and/or recording device. Closed circuit television systems (CCTV) provide additional and remote ‘‘eyes ’’that enable minimal security staff to observe multiple remote locations, either in real-time or recorded for future review.

A CCTV system may include a single camera or multiple cameras. Coverage can include public areas, entrance and exit doors, common areas, conference and interview rooms and office external areas such as corridors. Regardless of the type of system, CCTV surveillance should respect employee privacy and comply with local laws in relation to covert and overt surveillance.

4.6.3.2. Functional Requirements

CCTV systems must be designed to meet specific set criteria. The systems are typically designed for a specific task such as facial recognition and vehicle registration identification or for general area surveillance. Superimposed text information such as time, date and camera identification on the cameras image is useful and should be recorded at all times with the picture image. As a preference, all office locations should have two trained staff able to operate and interrogate the CCTV equipment and download images.

4.6.3.3. System Design

Systems will generally be designed around 24 hour recording or event activated recording with 30 day archiving of recorded images. CCTV systems record images that may be of use to law enforcement agencies at a later date, therefore recorders, storage space and compression schemes. Adding a camera or two to an existing system may require adjustments to the amount of storage space or the rate as which images from each camera are recorded.

Motion detection or door contact alarms can automatically initiate a camera preset providing a high-resolution view of the alarmed scene.

Adequate balanced lighting should be provided in all areas viewed by cameras.

Back up power sources should be provided to last for at least 30 minutes, until either the system power is restored or the system is shut down in a manner that preserves the recording.

A major problem with picture clarity is noise. Electronic noise is present in all video systems and manifests itself as snow or graininess over the whole picture on the monitor and recordings. There are several sources of noise such as poor circuitry and excessive

heat. To ensure acceptable image acquisition, video cameras should have a signal–to-noise ratio of at least 48db.

Recording devices and CCTV computer should be stored in a separate secured room to the main office area for additional security of the system.

Frames rates can vary from anywhere between 2-3fps to 120fps and can be adjusted for individual cameras depending on the requirement of that camera. 15fps is typical for general recording and small business applications, 120fps is ideal for high risk applications and 30fps for all other situations. Pending installer advice, 15fps is a recommended working specification for most offices. Dual mode (B/W and colour) cameras should also be selected where available.

4.6.3.4. Equipment considerations

Typically, office CCTV systems will be colour stand-alone systems with 24-hour digital recording. System computers and hard drives et cetera should be physically located in a restricted access area within the office where possible.

Cameras

Cameras should be installed to cover all public areas of the office as well as airlock areas and regularly used public interview rooms.

- Analog video cameras should have an output camera resolution of at least 400 horizontal lines. Digital video cameras should have an output resolution of at least 480 horizontal lines
- Cameras will generally not be pan/tilt/zoom type but rather fixed dome types 4-6” size
- CCTV recording and camera lenses should be designed for general area surveillance and not facial recognition
- Where possible cameras should be colour and have a low light capability preferably under an illumination level at 2 lux
- In some locations wide-angle lenses will be required to ensure full coverage of the identified area
- The number, placement, and type of cameras should be sufficient to provide adequate coverage and detail in the monitored area
- There should be adequate balanced lighting in the monitored area
- Organisations should have documented procedures to ensure that staff know what to do in the event of a criminal incident
- Should be located where they cannot be easily tampered with or “accidentally” adjusted
- Camera fields of view should not be obstructed nor should cameras be pointed directly at bright light sources

- At a minimum there must be at least one camera for every exit to obtain an unobstructed frontal view of the head and shoulders of everyone exiting the office
- Cameras should be placed where they can record images with unobstructed views at each point of customer transactions such as reception counters. Cameras should be adjusted to ensure that they are in focus at the location where a visitor can be expected to be located
- Black-and-white versus colour considerations - While B/W cameras may provide better image resolution than colour cameras, the information available in colour images can provide important investigative information
- Cameras placed to cover images at public transaction points such as reception counters should be placed to observe as much of the area of interest (face and hands) as possible
- Dual mode (B/W and colour) cameras should be selected where available

Display

- Typically a singular screen will be used as the main monitoring screen; to be no less than 41cm measured diagonally across the screen
- All required CCTV activity should be monitored on the main monitoring screen and be recorded in “real time” (Note; slow scan should not be used as the principal recording system)
- A secondary monitor may be required to be installed where there is a physical guarding presence at the post
- Monitors should be positioned so that they are easily viewed by staff
- Monitors should be capable of being linked to switchers or multiplexers so that multiple cameras can be viewed from the one monitor at any time either via a split screen or screen auto scroll set up
- Recording

Individual security advisers should assess the local site requirements for:

- Screen splitter
- Motion detection / sequencers
- Frame storage:
  - Analogue video cassette recorders should record each image at a minimum line resolution of 240 visible lines
  - A minimum digital resolution of 450 lines can be used for digital video recorders using a digital video tape digital recorders using a hard disk or optical disk for storage must record each from a minimum resolution of 640 pixels in the horizontal direction and 240 or 480 pixels in the vertical direction
  - Image recording should be kept for a minimum of one month before being stored. After 12 months the tapes or disks should be reused

SRMBOK recommends 24 hour or event digital recording onto disk on a stand-alone computer.

Remote site recording

As a general rule, CCTV remote site recording is not used within our facilities. Should this be considered necessary for local site arrangements you should consult with Canberra security in the first instance.

CCTV recorder output devices

Digital recording systems must be capable of exporting exact duplicates of the digital image files to removable media.

CCTV maintenance and documentation

System components, including switchers, individual cameras, software programs and versions should be recorded and stored.

Adequate information for repairs, upgrades and downloading should be kept at the individual sites, including point-of-contact information for installers and repairers of at least two contract personnel.

Site plans showing camera locations, maintenance logs, and documentation confirming certification of the system should be kept on the site in a secure location.

Relevant local legislation should be checked to determine if warning signs are required to advise people that they are under surveillance.

4.6.4. Closed Circuit Televisions - Specifications

Minimum Recommended Specifications

Please refer to the following table and supporting explanatory notes to determine the type of CCTV system recommended based on the level of threat at the location:

Security Measure	Low	Moderate	Medium	High	Extreme
Building Protection		Should*	Should	Must	Must

NOTES:

*** All CCTV systems should:**

- Have a play back function.
- Capture at least one complete field per camera per second.
- Where activated from a sensor or detector, the recorder shall have sufficient storage to be capable of recording in this mode for a minimum of 30 minutes.
- In the event of alarm trigger, be capable of pre-recording prior to the event of a minimum of 30 seconds.

4.7. Security Cabinets and Containers - Guidelines

4.7.1. Storage Overview

Security containers are graded according to the level of protection they provide. For example, one accepted grading system in use refers to Class A, B and C containers:

CONTAINER TYPE	DESCRIPTION/COMMENTS
A	Provided with extensive anti-drill and explosion protection and secured by a single door with an endorsed combination lock. A specification two or four drawer filing cabinet may be fitted inside.
B	Provided with a degree of anti-drill protection and secured by an endorsed combination lock. B class containers are available as: • two and four drawer containers, • compactus storage of varying sizes, • two door cabinets, • horizontal and vertical plans cabinets, and • key safes. They comprise class B and class B 'Plus' containers. B 'Plus' containers are of heavier construction than class B containers, the latter being slightly stronger than class C containers.
C	Constructed to ensure that evidence of tampering would be apparent and secured with an endorsed key-operated security lock. Class C containers are available in the same configurations as B containers.

The class of security container or secure room required to adequately protect sensitive or classified information should only be determined following a security risk review because factors that will affect the class of security container required include the:

- level of classification
- value and attractiveness of the information to be stored
- location of the information (for example, in Secure, Partially Secure, or Intruder Resistant Areas)
- structure and location of the building
- control systems
- other physical protection systems (for example, locks and alarms)

The combination of security measures used to protect security classified information should be capable of showing evidence of covert entry.

4.7.2. Combination Settings

Combination settings should be memorised. The only written record of each setting for use in an emergency should be held in a wafer-sealed envelope, classified with the highest security classification of the material held in the container, and stored appropriately in another container. The setting is to be changed:

- when a container is first received by the organisation
- after servicing the lock
- at any time subsequently when there has been a change of custodian or other person knowing the combination
- when there is reason to believe the setting has been compromised
- in any case, not less frequently than every six months

Any compromise or suspected compromise of a combination setting short be reported immediately to the appropriate authority/responsible person.

4.7.3. Using Security Containers

The following table provides general guidelines relating to the use of containers:

ASPECT	GUIDELINE
Unlocked containers	When unlocked, the: • door should be kept open, • bolt should be returned to the locked position, and • key should be removed, if applicable.
Closed doors or drawers	Containers should be locked when the doors or drawers are closed.
Access to locks	Locks should be sealed on installation and after repair, so that access to the back of the lock is not possible.
Combination locks	Combination locks should not be opened in view of people who are not authorised to know the combination.
Labels	Labels should not: • be placed near locks, bolts or hinges to ensure that signs of tampering or unauthorised entry are visible, or • give any indication of the contents of the container. Open/Closed labels should not be used.
Keys	The responsible person should: • hold all duplicate keys when the container or room is locked, and

	• maintain a key register.
Combination Locks and Numbers	A record of the Combination numbers and Locks should be held by the responsible person in a double sealed envelope (with wafer seals). The envelope is to be marked with the names of those authorised to access the combination.
Movement	Before a security container is moved for any reason: • it should be completely emptied of all documents, • labels attached to the inside should be removed, and • the locking pins should be reinserted, if it is a Class A container.
Return	Before a container is returned to the store, the custodian should attach a signed certificate to its body stating that it has been emptied and checked. If the security container has a keyed lock, keys should be removed and sent to the store separately with details of their container. If the security container has a combination lock, lock should be reset to the manufacturer's specification setting (usually 40-50-60), or as shown in the instruction book, and the combination should be marked on the outside of the container.

4.8. Security Cabinet/Container - Specifications

Minimum Recommended Specifications

Please refer to the following tables and supporting explanatory notes to determine the type of minimum security cabinets/containers recommended based on the type of information to be secured and the area it is in:

Classification	Secure Area	Partially Secure Area	Intruder Resistant Area
Most sensitive information Top Secret Crypto *	Class A container	Not Applicable: this type of information should only be kept in Secure Areas. In exceptional circumstances, prior approval from the security specialist could be sought to waive this requirement.	
Highly sensitive information Secret Highly Protected	Class B container	Class A container	Class A container
Sensitive information Confidential Protected	Class C container **	Class B container	Class B container
Restricted X-In-Confidence	Class C container	Class C container	Class C container

Please note that floor loadings should first be checked to confirm their capacity to take the containers.

Notes:

* For government readers, CRYPTO is to be stored in accordance with its security classification marking, with additional handling requirements in accord with those detailed in ACSI 53.

** Alternatively, a lockable cabinet with a SCEC-endorsed lock should be acceptable.

Government caveat material should be stored in accordance with its security classification. For example, CONFIDENTIAL Australian Eyes Only (AUSTEO) or CONFIDENTIAL Australian Government Access Only (AGAO) information should be stored as CONFIDENTIAL information in an appropriate container.