Independent Schools Victoria

SECURITY RISK MANAGEMENT TOOLBOX

Revision 1.1

Revised Date 15 October 2014

How to Use the Tool Box and Guidance Material

The material should be used in conjunction with the relevant Australian Standards and Codes of Practices described within the work shop to develop a security risk management program as a component of the Independent Schools Victoria Compliance Framework.

By utilising the guidance material and complying with the relevant Standards, individual schools will be able to demonstrate that they have exceeded sound good practice in the discharge of their duty of care and diligence requirements under prevailing State Occupational Health and Safety Regulations.

The aim of the tool box is to supply simple but effective checklist or pre-formatted templates that assist directing and recording the iterative steps to develop a security risk management framework and supporting programs. The check lists are generic and should have additional elements added to suit individual requirements. It should also be noted that it is often better for this type of activity to view the check lists as an aide memoir to avoid the inexperienced practitioner becoming too focused on only the checklist content, thus missing other important aspects that need to be identified or further progressed.

This tool box workbook has been divided into two sections. The SRM section must be utilised in conjunction with the Independent Schools Victoria Compliance Framework as it deals solely with the additional functions required for SRM that need to be applied over and above the generic application of risk management.

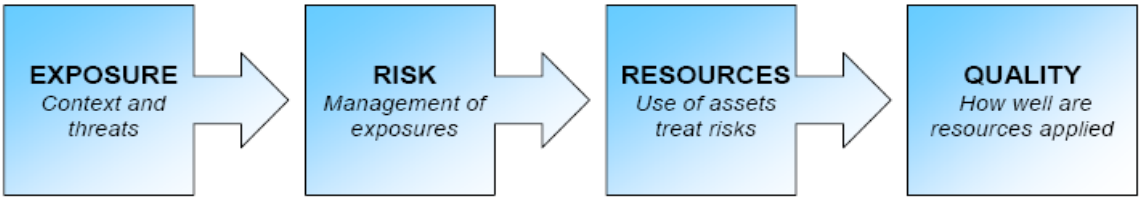
Section 1 SRM Process	**Section 2 Security Survey Process**
Step 1 Communication and Consultation	**Checklist:**
Step 2 Establish the Context	Preliminary
Step 3 Risk Identification	Crime Risk
Step 4 Threat Analysis	CPTED Space Assessment Questions
Step 5 Risk Evaluation	Writing the Report
Step 6 Security Risk Treatment	Security Marketing
Step 7 Monitor and Review	**Aide Memoir for Design of:**
	Intrusion Alarm, CCTV and Access Control
	Windows and Glass
	Exterior Lighting
	Buildings
	Construction Site Security

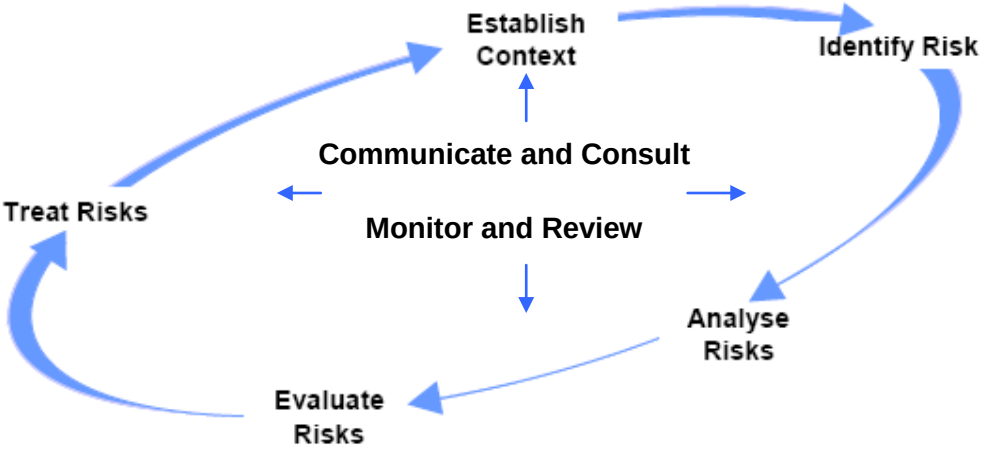
Section 1 – School Security Risk Management

People – not acts of god, mechanical failures or management systems – create security threats (Talbot and Jakeman, 2009).

Security Risk Management is the processes and culture that is implemented to maximise benefits and minimise adverse effects of security-related threats by supporting the preparedness, protection and preservation of people, property, information and your school's capability. Security risk management is an integral part of sound risk management practice and the fallout from unseen events can have wide ranging effects on your school and local community. The ability to understand and manage security risks as part of a holistic management system provides sound protective systems to prepare, protect and preserve staff, students, school property and its information.

Resource limitations, your school's culture, risk tolerance and changing threat environments mean that the balance between risk and reward is continually in flux and will often vary. In many respects, Security Risk Management involves the application judgment regarding understanding your school's exposures, the application of school resources and monitoring the quality of your school's protective systems to target a level of risk which is cost effective and 'as low as reasonably practicable'.



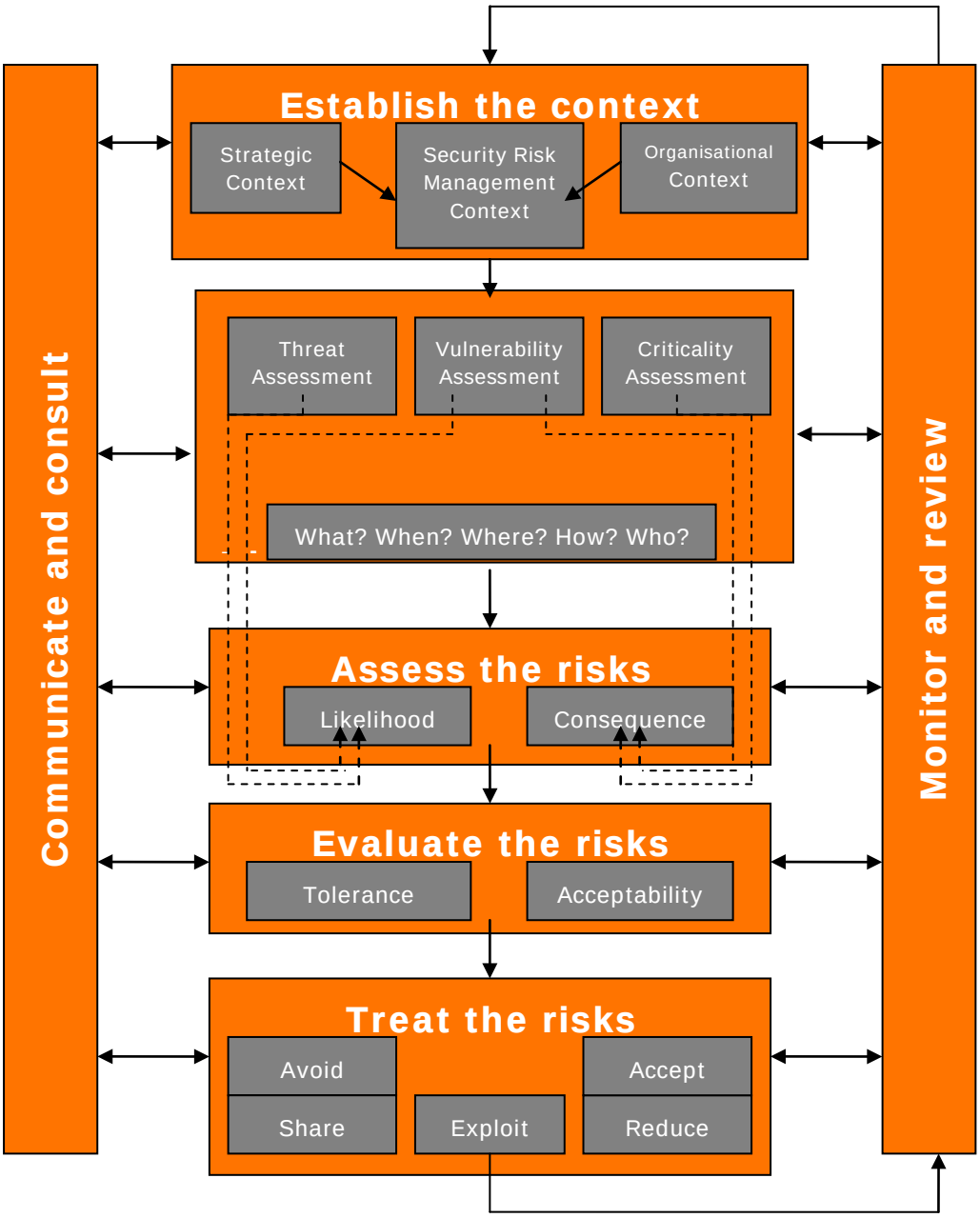


The security risk management process can be broken down into these seven basic steps[1].

[1] Standards Australia. (2009) AS/NZS ISO 31000: 2009 *Risk management*. Standards Australia International Ltd

- **Communicate and Consult.** This step is an on going process that occurs before, during and after the risk assessment to gather information, keep stakeholders informed and to disseminate the findings of the risk assessment to those who need to administer risk treatments. This will assist in the identification and proper analysis of risks and ensure that treatment priorities are consistent with management guidelines.
- **Establish the Context.** This step is to define the scope of the risk review by setting the context of the risk assessment in terms of the external security context, the internal security context, the risk management context and the context of existing risk controls. This step also includes developing the security risk criteria based on management's security objectives and priorities, and defining the parameters for the remainder of the process.
- **Identify the Risks.** This step is to determine who and what is at risk and the nature and sources of harm (threats) with the potential to harm people or assets, and the vulnerabilities taking into account existing security measures. The most effective way of documenting this step is to produce a Risk Register.
- **Analyse the Risks.** This step is to analyse the risks by estimating likelihood and consequences in the context of existing security control measures. Each security risk is analysed to determine how significant the potential risk is to the Department. Risks are given a rating to distinguish serious risks from minor ones. The purpose of the risk rating is to help distinguish minor risks that can be managed by normal procedures, from more serious risks that require direct management attention and input, new treatments and close monitoring.
- **Evaluate the Risks.** Once risks have been rated, management must decide which risks are unacceptable without new or additional treatments. This decision should be made by comparing the risks with the security risk criteria. Low-level risks will generally continue to be managed by routine procedures. Higher-level risks, however, will normally not be accepted without treatment. Unacceptable risks are assessed against the security risk criteria and prioritised for treatment action. A list of risks in order of treatment priority is compiled for management approval in the security risk register.
- **Treat the Risks.** This step is to identify the range of options for the treatment of risks assessed to be intolerable or unacceptable; to determine the cost effective risk control strategies available to reduce likelihood and/or consequences; and to develop treatment plans. The recommended treatments are detailed in the security risk treatment schedule. Once management have selected treatments and responsibilities for their implementation, they are then detailed in the general security plan which acknowledges the Australian Government's minimum mandatory security standards and the Department's security objectives.

- **Monitor and Review Risks.** Continuous monitoring ensures that changes in the risk environment are detected. Risks, and particularly the sources of risk, need to be monitored constantly to detect changes that may alter risk management priorities. Substantial changes require a partial or complete review to ensure the security plan is still relevant. Even if there has been no substantial change, the security plan is constantly reviewed to ensure the risk treatments and strategies remain effective, cost-efficient and relevant to the Department's circumstances and continue to address areas of need to achieve the security objective[2].



[2] Standards Australia. (2006). HB 167: 2006. *Security Risk Management.* Published by Standards Australia (Standards Association of Australia)

Step 1 – Communication and Consultation

A critical element of any risk management process is to develop and implement a communications strategy encompassing each of the security risk management process elements[3].

Communication Requirement	Considered Issues	Examples
Audience	▪ Primary ▪ Secondary ▪ Opportunistic	▪ To Staff ▪ To Students ▪ To local community
Content	▪ Simple ▪ Technical ▪ Unambiguous and clear	▪ Appropriate terminology
Assumptions	▪ Social ▪ Religious and cultural	▪ Understood by social groups
Expectations	▪ Recipient ▪ Stakeholder	▪ Management of the school ▪ Primary Secondary audience ▪ Board
Sensitivities	▪ Political correctness ▪ Empathy	▪ Potential offensiveness to minorities ▪ Awareness of local/personal contacts
Mode	▪ Language ▪ Readability ▪ Disability	▪ Person to person, meetings, mail ▪ TV, radio, print media ▪ Internet, journals, books, pamphlets
Accessibility	▪ Language ▪ Readability ▪ Disability	▪ Multilingual messaging ▪ Visually/hearing impaired, colour blindness
Boundaries, barriers and constraints	▪ Legal ▪ Governance ▪ Political ▪ Social ▪ Technical ▪ Business ▪ Reputation ▪ Obligations ▪ Cost	▪ Regulatory requirements ▪ Due diligence acceptability ▪ Local values, customs ▪ Capabilities, feasibilities ▪ Policies, confidentialities ▪ Public and stakeholder confidence ▪ Moral, ethical, contractual, regulatory obligations ▪ Cost benefit
Performance	▪ Measurement and monitoring	▪ Key performance indicators

[3] Standards Australia. (2013). SA/SNZ HB 436: 2013 *Risk management guidelines*: Companion to AS/NZS ISO 31000:2009. Published by Standards Australia (Standards Association of Australia)

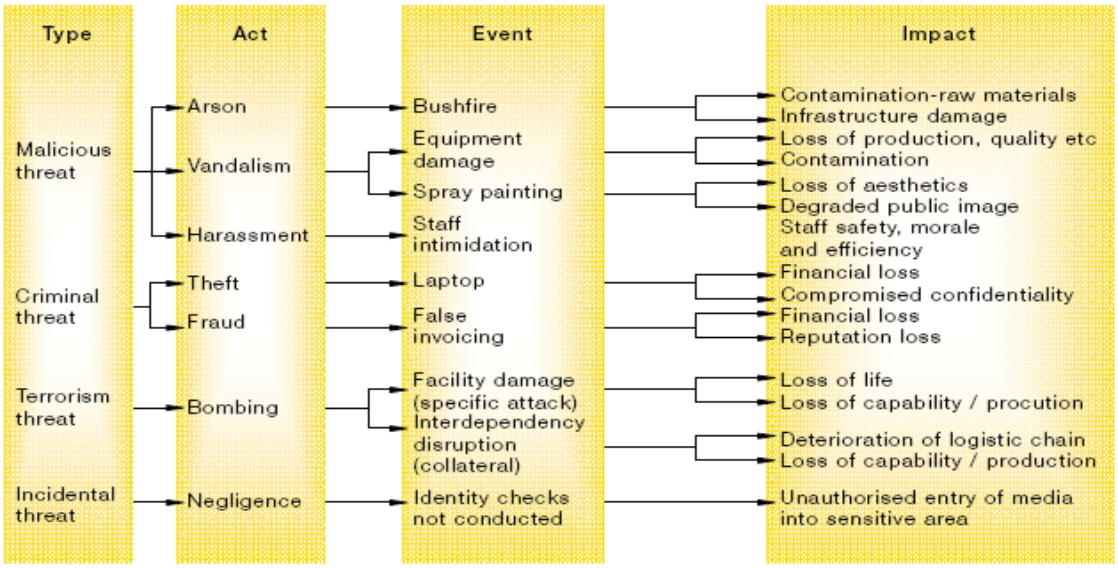
Step 2 – Establish the Security Context

Security Risk Management needs to be conducted in a manner that is appropriate to the organisation's type, culture, operational issues and the wider environment within which it operates. In particular, security risk management needs to be appropriate to the prevailing and emerging risk environment. Establishing the context is critical because it sets the basis on which all subsequent Security Risk Management activities are conducted. Establishing the context is the principal activity in developing the scope for Security Risk Management.

Context Elements	Typical Questions
Commitment	▪ What are the key success drivers of: - Senior management? - Middle management? - Staff? ▪ How can better understanding and management of Security Risk Management complement or enhance these drivers? ▪ How are security issues currently affecting management and staff performance
Goals and objectives	▪ What are the goals and objectives of: - The organisation? - Department? - Project? - Individual? - Community? - Society?
Process or program	▪ What constraints exist with adopting the chosen approach of Security Risk Management?
External context	▪ What is the relevance of changing economic conditions? ▪ What new legislation is on the books? ▪ What are the prevailing/changing social conditions? ▪ In what activities are key competitors engaged? ▪ What are the expectations of suppliers, customers, communities, shareholders and other stakeholders?
Internal context	▪ What are the key programs, projects, activities identified in this year's business plan? ▪ What resource limitations exist? ▪ What are the key findings from internal audit reports? ▪ What are recent trends in security and OHS near misses and incidents?
Security risk management context	▪ What security concerns/issues have been identified recently? ▪ What are the objectives of the proposed Security Risk Management activities? ▪ What decisions need to be made, and by whom? ▪ What is the scope of the proposed security risk management activities? ▪ What critical assets, people, information, process have been identified? ▪ What general or specific threats have been made? ▪ How are security issues currently affecting management and staff performance? ▪ What apparent vulnerabilities exist?

Step 3 – Security Risk Identification

Risk identification is concerned with creating a well thought out and comprehensive determination of the sources of risks and potential events that will have an impact upon the individual's, organisations, or community's objectives. The identification of risk can be assisted by considering the outputs of more traditional approaches such as threat, criticality and vulnerability assessment as useful inputs into the identification process[4].



Core Questions	Comments
Where can it happen?	
When or how frequently can it happen?	
Where can it happen?	
Who could be involved in creating the risk?	
Who could be impacted by the risk?	
How or why could the risk arise?	
What measures are in place to prevent or manage the risk?	
How reliable is the data/information?	

[4] Standards Australia. (2006). HB 167: 2006. *Security Risk Management.* Published by Standards Australia (Standards Association of Australia)

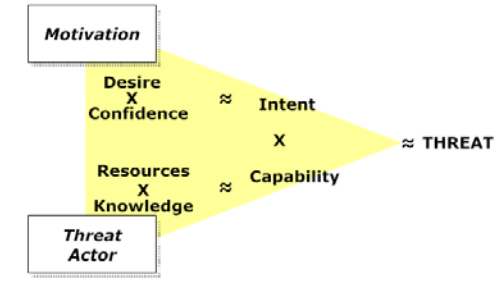
Step 4 – Threat Analysis

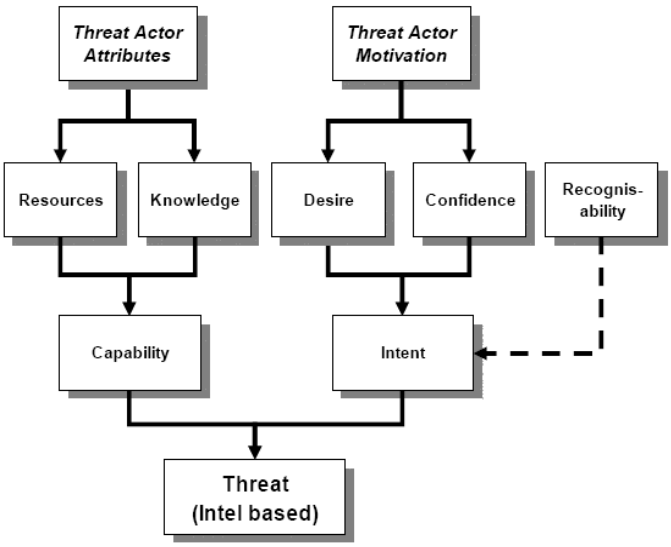
Threat sources identification and assessment worksheet

Consequently, the first necessary activity in any security process is to understand the threat. Does a threat exist? Do any criminally, politically or issue motivated threat actors pose a significant risk to the organisation and if so, what are the likely attack vectors?

Threat is usually assessed and described using a combination of INTENT and Capability of a Threat Actor (whether individual or organisation) to attack or adversely impact an item of value such an asset, function or capability[5].

The twin drivers of 'threat', intent and likelihood are themselves functions of the motivation and attributes of the Threat Actor.





Threat source	Act	Event	Impact
(e.g.) disaffected employee.	Malicious damage, sabotage, vandalism, arson.	School campus damage. Fires lit in gymnasium. Intellectual property stolen. Perimeter fences cut, access gained to exterior of main buildings. Slogan graffiti sprayed on walls of administration office.	Loss of use of gymnasium due to asset damage, increased media attention and some potential for moderate reputational harm, cost of refurbishment and replacement of assets.

[5] Standards Australia. (2006). HB 167: 2006. *Security Risk Management.* Published by Standards Australia (Standards Association of Australia)

Step 5 – Security Risk Evaluation

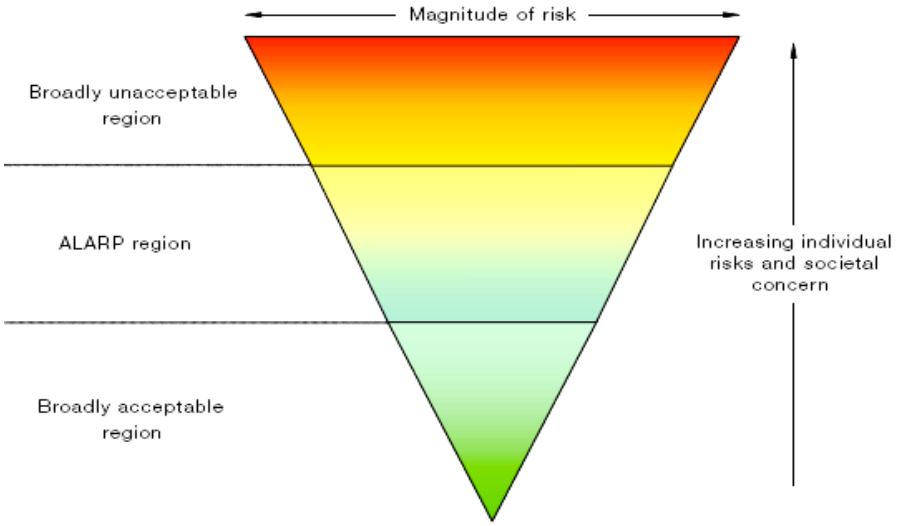
Evaluating security risk involves determining which risks are tolerable, and which risks require further attention (e.g. treatment). Criteria for determining tolerability should originally have been developed whilst establishing the 'context', and will usually include defining appropriate consequence and likelihood tables and establishing levels where different actions may be required.

Evaluation criteria could vary depending upon, for example:

- Prevailing political, stakeholder or community sensitivities and expectations;
- The nature or types of the security incident involved;
- Existing or emerging security incident trends;
- Strategic or business priorities;
- Resource availability for treatment; and
- The ability of the organisation, community or individual to absorb losses.

Decisions on the tolerability of risk could for example be based upon single level decision criteria that divide security risks that require treatment (intolerable) from those that do not (tolerable) for example:

- All security risks of 'High' or 'Extreme' ratings – must receive immediate attention, with reporting to the Chief Executive and/or the Board;
- All security risk of 'High' rating must receive attention within 24 hours;
- Security risk above 'Significant' where controls are less than 'Effective' – is intolerable; or
- Any security risk with potential safety or reputational consequences above 'Moderate' is intolerable, where controls are less than effective.



Step 6 – Security Risk Treatment

Security risk treatment plan example:

School		**Location**	
Date of risk review			
Treatment planning conducted by		**Date**	
Treatment planning approved by		**Date**	

Risk	Treatment objectives	Options	Cost Benefit Analysis	Treatment strategy	Completion date	Interdependencies with other risks	Implementation responsibility
Vandalism resulting from fence breach	Reduce likelihood of fence breach	Repair existing fencing	Accept	Engage contractors to repair fence	Within 4 weeks	Nil	Simon Head, Maintenance Manager
	Improve likelihood of detection of breach	Replace with heavy gauge fencing	Reject	Engage security consultants to identify CCTV technical requirements, siting solutions	Within 2 months	T server room introduction of CCTV monitoring	Will Young, ICT Manager
		Introduce motion detectors	Reject				
		Introduce CCTV on fence lines	Accept				
		Increase frequency of security patrols	Accept				

Step 7 – Monitor and Review

Monitoring of risk provides the capability to respond effectively to changing environments. The concepts of monitor and review therefore become of critical importance to the conduct of Security Risk Management. The concept of 'monitor and review' is based around the need to:

- Continuously examine the external and internal environments and reconsider the context and its effect on security risk management
- Redevelop the analytical outputs of the Security Risk Management process to reflect the changing context
- Assess the efficiency and effectiveness of treatment plans in mitigating the risks identified
- Re-evaluate the appropriateness of treatment activities to manage a dynamically changing risk environment
- Measure the effectiveness and success of communications and consultation activities undertaken
- Ensure that timely and adequate improvements are implemented
- Continuously examine the conduct of the security risk management process and to adjust it to meet changing organisational needs and capability
- Ensure appropriate governance through reporting to appropriate authorities, regulators, boards, stakeholders, management and staff as required
- Focus on both conformance and performance measurement.

Core Questions	Comments
Continuous monitoring:	Undertaken on a frequent or ongoing basis, this involves routine checking by the process operators of changes in risk level, control breakdowns, incident occurrence, or established indicators of these (e.g. alarm monitoring). The aim is to ensure that implemented treatments and controls remain effective and that new risks are not being created.
Line management reviews:	Periodic reviews of processes, policies, practices and systems, their risks and treatments. These reviews are often targeted at specific higher or changing risk issues (including assurance activities such as control self assessments, etc). The aim is to ensure that treatment and control strategies continue to be relevant, efficient and effective
Centralised reviews:	By internal or external audit capability (e.g. financial transaction audits). The aim is usually to ensure compliance with internal and externally mandated requirements so these reviews are highly selective in their focus. Reviews such as simulation exercises and penetration testing also provide awareness and training opportunities beyond the monitoring objectives
Scanning:	Reviewing the internal and external environments for changing or emerging risk. The aim is to provide an early appreciation of emerging issues to allow sufficient time to act upon them. Although virtually sine qua non at a strategic level, it should be Adopted as a monitoring practice at all levels of the organisation.

Section 2 – School Security Survey

Preliminary Checklist	
Survey conducted by:	**Date and time:**
School location/general description:	
Historical data reviewed/analysed:	
Local crime statistics:	
School records:	
Other trends analysis data:	
What are the key business processes, are there any critical nodes:	
What are there acceptable levels of business outage (refer business continuity planning process):	
Site documentation requirements:	
Operational constraints and authorisation:	
Preparation of checklist/aide memoirs:	
Necessary equipment:	
Protective security measures inc. policy and procedures:	
Insurance arrangements:	
Policy, plan, procedure and practice review procedures:	
Incident reporting procedures:	
Others (list):	
Asset/location areas that have been included:	
Building and perimeter security (includes vulnerability identification)	
Lighting (internal and external)	
Vehicle movements and accessibility	
Access control (staff, contractors, visitors)	
Access control (locking systems/key and electronic card issue and control)	
Personnel vetting procedures (staff and contractors)	
Alarms and alarm response arrangements	
Office security (inc. cash/valuables handling and inventory control	
Security guards and response arrangements	
Document security practices (inc. mail handling and general deliveries)	
Information technology and communication procedures (inc. disaster recovery)	
Emergency protection and response procedures (includes criminal, fire, suspicious parcel, bomb, chemical/biological etc, business continuity planning and relationships with emergency response agencies)	
Front office procedures, if applicable, (inc duress/response arrangements)	
Staff awareness procedures (inc personal safety/evacuation/general security)	
Others (list):	

Crime Risk Checklist	
Function	**Outcome**
Building/complex occupant consultation	
What areas contain items that are sensitive or of value i.e. safes, audiovisual equipment etc.	
What are the main crime spots in the building	
What level of protection is required	
Document and understand cash holding, handling and transit arrangements	
List valuables locations within the school, decide vulnerability to criminal attack, and recommend target hardening for those locations	
Review entrances in the building to reduce to a minimum	
Determine the general crime risk for the neighboring area	
Understand the level of police patrol and police activity in the area	
Determine the distances from the campus to the local police and fire stations	
Verify that the security related components / materials being used in the facility meet State, National standards of Codes of Practice	
Be aware of the cleaning and security contracts for the facility, and assess dependability, intelligence and reliability	
Other comments:	

Aide Memoir for Design of Intrusion Alarm Systems			
Alarm	**Comment**	**Yes**	**No**
Installed or proposed system satisfies: AS 2201.1 Intruder Alarm Systems, Systems Installed in Clients Premises AS 2201.2 Intruder Alarm Systems, Central Stations and Signalling Links AS 2201.3 Intruder Alarm Systems, Detection Devices for Internal Use AS 3000 SAA Wiring Rules Telstra Australia Specifications The Local Electricity Supply Authority Regulations. ISO 9000 QS for Design, Development, Production, Installation and Servicing of Electronic Systems.			
Ensure system coverage for vulnerable material in protected areas.			
Decide on instant, delayed audible warning or silent alarms.			
Decide on choice of detectors to meet operating environment: PIR (Dual Technology) / Glass break sensors Door reed switches / Duress buttons Roller shutter contacts / Kick bar switches Ultrasonic detectors / Audio sensors			
Match level of protection to building security risks for: Site perimeter / Target protection Internal traps / Overall construction			
Specify: Line supervision – DC/AC/Authenticity/Encryption End of line module type Panel type – Stand alone / Networked Sufficient zones (with allowance for growth) Line monitoring Control Centre Maintenance			
Review system for interference: Radio Frequency Interference (RFI) Electromagnetic Interference (EMI)			

Aide Memoir for Design of CCTV			
CCTV	**Comment**	**Yes**	**No**
Define a clear idea of what you want the system: To do How it should perform What you want to see and where			
QUALITY – are the pictures good enough? Appropriate resolution, level of compression and number of pictures per second Type and style of lens and monitors to be used As a minimum – subjectively test system for adequacy The quality of the recorded or printed pictures may differ from the live display Time and date information is often critical to an investigation The quality of the pictures should not be compromised to allow more to be squeezed onto the system Regular maintenance should be conducted on all aspects of the system			
STORAGE – what should I keep? How should I keep it? The system should be operated and recorded pictures retained in a secure environment Electronic access controls, such as passwords or encryption, should not prevent authorised access to the system or recordings The system should have sufficient storage capacity for 31 days good quality pictures The system should be capable of securing relevant pictures for review or export at a later date			
EXPORT – can the pictures be easily exported from the system? A simple system operator's manual should be available locally to assist with replay and export The operator should know the retention period of the system and export time for various amounts of data The system should be able to quickly export video and stills to a removable storage-medium, with time and date integral to the relevant picture Export should include any software needed to view or replay the pictures The system should have an export method proportionate to the storage capacity Pictures should be exported in the native file format at the same quality that they were stored on the system			

PLAYBACK – can the pictures be easily viewed by authorised third parties? The playback software should: ▪ have variable speed control including frame by frame, forward and reverse viewing ▪ display single and multiple cameras and maintain aspect ratio i.e. the same relative height and width ▪ display a single camera at full resolution ▪ permit the recording from each camera to be searched by time and date ▪ allow printing and/or saving (e.g. bitmap) of pictures with time and date The time and date associated with each picture should be legible Once exported to removable media it should be possible to replay the files immediately			
The purpose of the picture has to be clearly defined, cognizant of the system design and ultimate function of the system. Decide if individual cameras must: Detect: That there is a target within the FOV and the operator can locate that target i.e. the target appears to be our employee Recognise: That the operator with a high degree of certainty recognises the target i.e. the target is an employee or is not known by the operator Identify. The operator can clearly identify and describe the target i.e. it is Joe from stores			
FOV should be measured to assess the required distance, either horizontal or vertical			
Design or application of CCTV should be based on a sound risk management process: This should address the physical area to be monitored and/or proposed target. Site plans should be produced that show proposed camera coverage, targets, areas of interest and high value assets			
The problem must be identified within the operational requirement: What is the proposed target? What is the activity by the target that may require surveillance? Define the purpose of observation based on the DRI principle of detect, recognise or identify Consider what factors are required to achieve success in surveillance Who will respond to the detection of the target? What is the necessary response time to achieve success? Once a target is identified and response is activated, how long is observation required? For the system to be effective, what environmental conditions may it have to operate under? When the activity occurs what will the observer do?			

How will the observer know when and where to look? How quickly does the observer need to respond to the activity? Who will make the observation on which the response is based? What and where is the location of the observer?			
Other Design Considerations Mission Statement – A mission statement should be developed that presents the objectives and purpose of the CCTV system Automation – Wherever possible the CCTV system should be automated Overt or covert cameras CCTV Signage Power failure and redundancy Recorded Evidence Blind camera syndrome – defined as the public perception of safety, reinforced by the belief that there is a trained CCTV operator behind each camera ready to react to a situation they view Training – consideration given to level, type and quality of training for operators			
Control Room Poor design can greatly reduce the effectiveness of the CCTV system – consider: Architecture. May include the size, shape, location, service facilities and windows of the control room Environment. Includes the lighting, temperature and ventilation of the control room Workstation. The workstation design which should consider height, size, position of equipment, layout, work surface area and surface of the workstation Furniture. Includes the chair, bookshelfs and storage area Monitors. Size, position, tilt, type, mounting, system information and number of cameras per monitor Control Panel. Type, design, position of the control panel and associated control functions Management. Operators viewing time, standard operating procedures, multiple tasks, training, and what to watch, how, why and when			
System designed, operated and maintained to: AS 4806.1-2006 – Closed circuit television (CCTV) – Management and operation AS 4806.2-2006 – Closed circuit television (CCTV) – Application guidelines AS 4806.3-2006 – Closed circuit television (CCTV) – PAL signal timings and levels			

Aide Memoir for Design of Access Control System (ACS)			
Card access control	**Comment**	**Yes**	**No**
Tailored Approach to ACS – utilises: Thorough understanding of the facility and organisation, observing its security, operational user and any other requirements Designed according to best practice while addressing the organisation's needs Communication and consultation with the appropriate personnel regarding all matters associated with ACS Users interact with the System is practical and effective			
System designed/provides: Deters intrusion Detects intrusion Delays intruders Can respond to intruders			
System is effectively: Planned and designed Installed Integrated Programmed Commissioned and tested Credential issuing and database developed Policy, procedure and system work instructions developed System operators/users trained			
System components selected to match environment/end user requirements: Card type – Magnetic / Electric circuit continuity / Passive electronic / IR optical Tamper alarm Battery back-up Database/software/hardware management and maintenance Credential issuing and return Dynamic programming and system operation Policy and procedure enforcement System monitoring and review System troubleshooting and recovery Data gathering and investigations System upgrades and expansion:			
Site location defined: Number of entry control points and passes Rate of persons passing through control point Number of levels of access to be accommodated			

Aide Memoir for Design of Windows and Glass			
Frame and Glass:	**Comment**	**Yes**	**No**
Locks provided to defeat direct/covert attack			
Electromagnetic locks: Solenoid assembly to produce the magnetic field attached to the door frame A keeper plate attached to the door which is held by the magnetic field of the solenoid; When the electric current is switched off, then there is no residual magnetism in the solenoid The solenoid and keeper are moisture and dust resistant The affect of foreign objects on the performance has been considered Has a holding force between the solenoid and the keeper must exceed 223 Newtons of force at the supply voltage The system must successfully complete an endurance test of 10,000 cycles of the following activities: Energising / de-energising of the door holder Separate the keeper plate from the solenoid by opening the door Close the keeper plate to the solenoid			
No accessible louvre windows			
Ground floor – if low windows ensure openings are small. For large windows use fixed glazing with high openings			
Consider size and shape of windows to prevent access			
Use of bars or grilles on inside			
Secure window fixing to frame			
Use of plastic or film against vandalism			
System designed to: Standards Australia. (2008). AS 4145.2-2008 Locksets – Mechanical locksets for doors in buildings. Standards Australia International Ltd Standards Australia. (2001). AS 4145.3-2001 Locksets – Mechanical locksets for windows in buildings. Standards Australia International Ltd Standards Australia. (2002). AS 4145.4-2002 Locksets – Padlocks. Standards Australia International Ltd Standard Australia AS 4178-1994 Electromagnetic Door Holders			

Aide Memoir for Design of Exterior Lighting			
Security lighting supports the facility physical security system	**Comment**	**Yes**	**No**
Adequacy of lighting to illuminate critical areas and over entrances			
Separation of the protective lighting system and the working lighting system from the same power line			
Provision of an auxiliary power source for protective lighting			
Automatic or manual operation of the protective lights			
Period of operation of lighting			
An inventory of types of lights installed around the property			
Cost-effectiveness of lights			
Vandalism susceptibility of the fixtures			
Magnitude of the glare factor			
Distribution of illumination over the area			
System designed to: Standards Australia. (2008). AS 1680.3:2008 Interior lighting – Measurement, calculation and presentation of photometric data. Standards Australia. (2008). AS 1680.2.1:2008 Interior lighting – Circulation spaces and other general areas. Standards Australia International Ltd Standards Australia. (2006). AS 1680.1:2006 Interior lighting – General principles and recommendations. Standards Australia International Ltd Standards Australia. (2009). AS/NZS 1680.0:2009 Interior lighting – Safe movement. Standards Australia International Ltd Standards Australia. (2005). AS 1158.3.1:2005 Road lighting – Pedestrian areas (Cat P) lighting performance and design. Standards Australia International Ltd Standards Australia. (2001). AS 1680.4:2001 Interior lighting – Maintenance of electrical lighting systems. Standards Australia International Ltd			

Aide Memoir for Design of Buildings			
External doors	**Comment**	**Yes**	**No**
Choice of final exit doors, design and strength of doors and frames			
Choice and strength of panels: glass and wood			
Ensure hinges cannot be removed from the outside			
Choice of locks and hardware			
Use of steel doors and frames			
Elimination of exterior hardware on egress doors wherever possible			
Building line			
Lines of vision			
Elimination of hidden entrances			
Roof			
Access ways and roof pitch angle			
Skylights			
External pipes			
Flush or concealed pipes			
Podium blocks			
Access to upper windows			
Basement			
Inside and outside access			
Storage areas			
Lighting			
Number of entries to basement, stairs and elevators			
Grilles on windows			
False ceilings			
Access to/through false ceilings			
Service entrances			
Service hatches / ventilation ducts / air vent openings / service elevators			

Construction Site Security Checklist Responsibility for a facility begins at the construction site. Cost will spiral if theft is not controlled, and the business fabric may be damaged if the assets are exposed to harm. Consider the following points to ensure improved construction site security:	
Who is the contractor liaison person to work with police?	
Construction site perimeter, describe adequacy of:	
▪ Gate strength	
▪ Hinges	
▪ Locks	
▪ Chains	
▪ Lighting	
▪ Neighborhood crime rate	
▪ Perimeter fence	
Contractor's site buildings, describe:	
▪ Security of this building	
▪ Review the contractor's security procedures and controls	
▪ Internal and external lighting	
Forbid on site staff vehicle parking	
Are building materials and tools protected in a secure area?	
Are there facilities for storage/security of workers tools etc?	
Are facilities adequate for security patrols?	
Is temporary intruder alarm system needed?	
Protocol to check for fraudulent deliveries?	
Is security signage around perimeter?	
ID transportable material and property?	
Protocol established to report theft to the Local police Office Insurance or Security company?	

Crime Prevention through Environmental design (CPTED) Space Assessment Questions

This guide provides an indication of the effectiveness of the design principles for crime deterrence. The assessment uses three functions or dimensions to assess human space:

Designation – All human space has some ***designated*** purpose.

- What is the designated purpose of this space? What was it originally intended to be used for?

Definition – All human space has social, cultural, legal or physical ***definitions*** that prescribe the desired and acceptable behaviours.

- How is the space defined? Is it clear to all persons normally in the area who own it?
- Where are the borders for the space? Are there social or cultural definitions that affect how that space is used?

Design – All human space is ***designed*** to support and control the desired behaviours.

- How well does the physical design support the intended function?
- How well does the physical design support the definition of the desired or accepted behaviours?
- Does the physical design conflict with or impede the productive use of the space or the proper functioning of the intended human activity?
- Is there confusion or conflict in the manner in which the physical design is intended to control behaviour? Does the physical design match the intended use?
- Does the space clearly belong to someone or some group? Is the intended use of the space clearly defined?
- Does the design provide means for normal users to naturally control the activities, and control access and provide surveillance?

The design of the space has to ensure that the intended activity can function properly, as well as directly supporting the control of behaviour, in order to reduce the opportunity for crime. Are there:

- Clear definition of controlled space with boundaries/markings/signage?
- Clearly marked transitional zones available to indicate movement from public to semi-public to private space?
- Gathering areas positioned at locations with natural surveillance and access control?
- Unsafe activities positioned in safe spots to overcome the vulnerability of these activities with the natural surveillance and access control of the safe area?
- Is space designed to increase the perception or reality of natural surveillance?
- Do entrances, driveways, gardens and especially windows overlook adjacent spaces in order to generate enhanced opportunity for surveillance?
- Do entrances not project out from the facade to avoid obstructing the view of the building perimeter walls?
- Are buildings visible from roads or well-travelled walkways (suffer less crime due to natural surveillance)?
- Are low bushes and hedges and level ground used to increase natural vision and remove potential hiding places for intruders?
- Is the internal design of buildings vulnerable areas (includes lobbies, halls, lifts and stairwell exits which are places of high crime rate) positioned to take advantage of natural surveillance?

Writing the Report

The style and format of survey report is a matter of individual taste, but the following is a suggested format:

1. **Cover page**: this should have the name of the site surveyed, the schools name and the name of the surveyor
2. **Distribution list**
3. **Contents page**
4. **Executive summary**
    a. An introduction, brief explanation of methodology, findings, and recommendations.
5. **Introduction**
    a. Authority
    b. Purpose
    c. Define the scope and nature of the report
    d. Participants, date and time of review
6. **Description**:
    a. At this point the premises or area surveyed is described. The location, age, and condition of the premises should be included. When appropriate, the number of users and activities in the building should be included. If this information is self evident the writer may choose to omit this information.
7. **Resource appreciation/Asset analysis**
    a. A list of organisational resources and their estimated dollar value needs to be provided. The amount of detail will depend on the survey, the site, the audience and the writer.
8. **Existing security strategies**
    a. State any existing security strategies and their effectiveness.
9. **Threat assessment**
10. **Risk assessment**
    a. List the vulnerability of assets and rate in order of priority.
11. **Findings**
12. **Conclusion**
13. **Vulnerabilities**
14. **Recommendations**
15. **Annexes**
    a. These may include plans, terms of reference, charts, maps and other information relevant to the survey.
16. **Photographic supplement**
    a. This may be a separate document, depending on its size.

Security Marketing

Having conducted a Security Survey and developed appropriate Security Policies and Procedures, personnel must be made aware of these and what is expected of them. It is essential that the work force is continually educated about security and their security role as failure do so is to condemn the security plan to apathy and indifference.

Security awareness – Seeks to solicit conscious attention to the existence of a Security Management Program and convinces the individual that the program is concerned with his or her safety, welfare and behaviour as well as those of the organisation.

Why security awareness? Established Security Policies and Security Procedures will spell out in detail the requirements of all personnel to contribute to achieving an effective Security Management Program within the organisation. Issuing policies and procedures and expecting them to be followed correctly or followed at all without any further explanation will not be successful.

Aims of security awareness – to minimise resistance to and maximising personnel contribution and participation in a Security Management Program.

Strategies for security awareness

- Formal security briefings upon commencement / seminars / posters / brochures / signs / bulletins and memos / loan of property-marking equipment for home use / discussion at staff meetings and incentive schemes.

Security awareness for executives, managers, teachers and other staff Executive management Concerned with the success of the school, to executive management the Security Management Program and its associated activities must:

- Be justified by the demonstration of real benefits, benefits quantified in $ terms, and demonstrate that benefits will be proportionate to the resources allocated

Middle management – Concerned with performance of his or her area of responsibility, to middle managers the Security Management Program and its associated activities must not impede the progressive performance of their area. The positive benefits of security must be emphasised.

Teachers – Concerned with the timely completion of quality work, they will view any consequence of the Security Management Program as undesirable if it was to affect their area by slowing the work process or causing inconvenience. Teachers need to perceive the security management program as a response to genuine vulnerabilities which could affect the operations in their area.

Marketing the security function – achieve by implementing the following marketing strategies:

1. Solicit stakeholder feedback
2. Listen to what the staff are saying
3. Encourage new approaches
4. Show you care
5. Test ideas
6. Do not focus on the worst all the time
7. Be compelling, but avoid scare mongering
8. Be comprehensive and keep a good plan rolling
9. Define security's role in business terms.