Emergency and School Security

School security

Fact sheet 1 – Conducting a security risk assessment

Introduction

The Department of Education (the department) is committed to creating and maintaining safe and secure learning environments that support the provision of high quality education for teaching and learning.

Schools face a number of security related threats and must develop appropriate strategies to manage these risks. The School security procedure outlines principal's responsibilities to conduct security risk assessments at their school.

A security risk assessment must be completed at least once per year, but should also be completed:

- in preparation for major events;
- in response to critical incidents;
- in response to changes in the school community and surrounding physical environment;
- upon completion of new security installations such as CCTV, or expansion of existing security controls such as intruder alarm systems;
- upon expansion of blocks, or completion of new blocks or facilities; and
- after installation of new information technology facilities.

This fact sheet is designed to assist principals understand the steps of conducting a security risk assessment. A Security risk assessment guide is available to assist principals complete the assessment, and develop a risk-management action plan.

What is a security risk assessment?

A risk assessment is a structured process to determine and contextualise any threats to a school's objectives. A security risk assessment means this process is specific to security related risks. The department's approach to managing risk is based on AS/NZS ISO 31000:2018: Risk management-Principles and guidelines, and is outlined in the Enterprise risk management procedure.

There are four main steps in conducting a security risk assessment:

1. Identifying security related risks
2. Analysing and assessing the identified risks
3. Evaluating the overall level of each identified risk
4. Treating the identified risks.

Step 1: Identifying security risks

Security risks at schools are not limited to common events such as vandalism and graffiti, and can affect more than physical assets. When identifying security risks, principals should consider the impact of a security incident on:

- **People** (staff, students, parents/caregivers, visitors, contractors);
- **Assets** (buildings, teaching resources, cash, equipment);
- **Information** (student records, passwords); and
- **Reputation** (goodwill of staff, parents/caregivers, school community).

There are some security risks schools cannot control. Normal school operations such as visitor access, or personal conflicts between students and external persons, will present residual risks that cannot be eliminated entirely, but can only be prepared for and managed.

Principals may wish to categorise or separate security risks to make analysis and evaluation easier. For example, a theft risk could be divided into categories (during school hours and after-hours when buildings are secure). Some of the more common school security risks and variations are in the table below:

Common Risk	Including (but not limited to)
Active armed offender	Person with intent to harm, related to personal grudge or radicalised ideals
Armed robbery	Robbery at cash collection points, personal attack for personal property
Assault	Harm to staff and students from unauthorised persons on site
Bomb threat	Threat received by phone, email, or through social media
Malicious object	Drug utensils, glass shards, flammable liquids, or weapons found on grounds
Break and enter	Unlawful forced entry to a building
Theft	Theft of school property, theft of student property
Unauthorised person on school grounds	Abduction, non-custodial parent, aggressive persons, using grounds as a shortcut, skateboarding, unauthorised access to swimming pools
Arson	Arson to buildings, facilities, school grounds, or rubbish bins
Graffiti and vandalism	Graffiti damage to buildings, fixtures, or grounds

Table 1: Common risks and variations

A security risk assessment should have consideration for the unique environment at your school. Your School Security Advisor (DoE employees only) can assist with developing strategies to manage uncommon identified risks.

Step 2: Analysing and assessing identified security risks

Analysing and assessing security risks will establish a level of severity for each identified risk. A simple but effective way to analyse risk (as outlined in the department's Enterprise risk management procedure) is the semi-quantitative method. This uses numerical rating scales for risk consequence and probability, and then combines them to produce a level of risk using a formula (the School security risk assessment guide can be used to automatically implement this formula).

Factors to consider when determining severity of an identified risk include:

- The **likelihood** of the risk occurring;
- The **consequence** of the risk (harm to persons, financial cost, damage to reputation etc.); and
- The **existing controls** that reduce the likelihood or consequence (alarm system, CCTV, security screens etc.).

Likelihood

The likelihood of any individual security risk is influenced by a wide range of factors. If it is difficult to immediately assign a likelihood to an identified risk, it can be helpful to break down the risk into a number of components for a more objective analysis. For example, the risk of a break and enter may be more prevalent at the school canteen than at a classroom.

When applying likelihood to an identified risk, existing controls should be taken into account. For example, to reduce the likelihood of a break and enter at the canteen, a school might have:

- placed a security camera looking at the roller shutters;
- reinforced the entry and secure store room doors; and/or
- increased the alarm system component to include a contact switch on the entry door.

A likelihood rating is applied once all factors have been considered, using the probability scale of five likelihood descriptors (shown below in Table 2). The table also provides examples of how likelihood might be calculated for common risks based on historical data.

Likelihood Descriptor	Description	Example 1: Vandalism	Example 2: Break and enter
Almost certain	Expected to occur in most circumstances	1+ times per month	7+ times per year
Likely	Will probably occur in most circumstances	Once per month	5-6 times per year
Possible	Might occur at some stage	Once per 1-2 months	3-4 times per year
Unlikely	Could occur once or twice	3-4 times per year	1-2 times per year
Rare	May occur in exceptional circumstances	Once per year	Almost never

Table 2: Likelihood descriptors

Consequence

A range of consequences can result from a security incident, with not all being immediately apparent. They can include financial loss, or interruptions to classes. A longer-term consequence might be damage to reputation in the school and wider community. Similar to the likelihood of an identified risk, existing controls which may reduce the consequences should be considered.

Use the five descriptors shown in the three tables below to determine the level of consequence associated with each identified risk. As several direct and indirect consequences may arise, it is recommended to determine consequences within relevant contexts and assign a descriptor to each (examples shown in the tables below).

Table 3 below gives an example of consequence descriptors for **financial** harm that may be caused if an event were to affect a planned function at a school:

Consequence Descriptor	Description (examples only)
Critical	No possible recovery of funding
Major	Major impact on budget/external recovery funding
Moderate	Serious impact on budget and/or resource reallocation
Minor	Minor impact on budget and/or some resources diverted
Insignificant	Managed within existing budget

Table 3: Financial consequence descriptors

Table 4 gives an example of consequence descriptors for **personal** harm that may be caused if an event were to affect a planned function at a school:

Consequence Descriptor	Description (examples only)
Critical	Loss of life
Major	Extensive injuries
Moderate	Medical treatment required
Minor	First aid required
Insignificant	No injuries

Table 4: Personal consequence descriptors

Table 5 gives an example of consequence descriptors for **reputational** harm that may be caused if an event were to affect a planned function at a school:

Consequence Descriptor	Description (examples only)
Critical	Total loss of confidence in the school community
Major	Public confidence is affected but not lost
Moderate	Control/response plan required to be implemented
Minor	Some media attention, no response plan required
Insignificant	No external facing impact

Table 5: Reputational consequence descriptors

Step 3: Evaluating the overall level of risk

After completing Steps 1 and 2, the likelihood and consequence of each identified risk will have been assigned a value. These values can then be applied to a matrix in the School security risk assessment guide to determine an overall level for each identified risk. There are four descriptors for risk level: **Extreme**, **High**, **Medium** and **Low**.

Table 6 below shows how likelihood and consequence of each identified risk determines the overall risk level:

		Consequence				
		Insignificant	**Minor**	**Moderate**	**Major**	**Critical**
Likelihood	**Almost Certain**	Medium	Medium	High	Extreme	Extreme
	Likely	Low	Medium	High	High	Extreme
	Possible	Low	Medium	Medium	High	High
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Low	Low	Medium

Table 6: Risk Matrix

Example: evaluating the level of an identified risk

State School X is a school with 600 enrolled students and is based in a major regional centre. Over the past two years, the school has been broken into six times and has total losses valuing $5,000, made up of primarily teaching resources and ICT equipment. Existing control measures include an intruder detection system which covers the administration block and most classrooms but no CCTV. Physical measures at each block include security screens and standard locks on doors.

Assigning a likelihood: At three times per year on average, the likelihood (as per Table 2) was rated as 'Possible' (shown below):

Descriptor	Description	Vandalism	Break and Enter
Almost certain	Expected to occur in most circumstances	1+ times per month	7+ times per month
Likely	Will probably occur in most circumstances	Once per month	5-6 times per month
Possible	Might occur at some stage	Once per 1-2 months	3-4 times per month
Unlikely	Could occur once or twice	2+ times per year	1-2 times per month
Rare	May occur in exceptional circumstances	Once per year	Almost never

Assigning a consequence: In financial terms (Table 3), the consequence is minor and in terms of interruption to school activity (Table 5) it was assessed between moderate and minor. Therefore, overall the consequence was determined as minor (shown below):

Descriptor	Description (Financial)
Critical	No possible recovery of funding
Major	Critical impact on budget/external recovery funding
Moderate	Serious impact on budget and/or resource reallocation
Minor	Minor Impact on budget and/or some resources diverted
Insignificant	Managed within existing budget

Descriptor	Description (Reputation)
Critical	Total loss of confidence in the school community
Major	Public confidence is affected but not lost
Moderate	Control/response plan required to be implemented
Minor	Some media attention, no response plan required
Insignificant	No external facing impact

Determining the risk level: Using the Risk Matrix (Table 6), the risk of theft was rated as **Medium** (highlighted below):

		Consequence				
		Insignificant	**Minor**	**Moderate**	**Major**	**Critical**
Likelihood	**Almost Certain**	Medium	Medium	High	Extreme	Extreme
	Likely	Low	Medium	High	High	Extreme
	Possible	Low	**Medium**	Medium	High	High
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Low	Low	Medium

If the school increases buildings or purchased new ICT equipment then a new risk assessment should be conducted, including a new evaluation for risk of theft. If the school had certain blocks with more or less security measures than others, the principal may assess each block separately.

Once an overall risk level has been applied, the principal can decide on the strategy or a number of strategies to manage risks, as well as the priority for implementation.

Step 4: Treating identified risks

Treating identified security risks typically employing one or more strategies to reduce the level of risk. Strategies can include:

- Avoiding the risk by not commencing or discontinuing the activity associated with the identified risk (this will be the most severe option in most cases, and can lead to other exposure to risk);
- Accepting the risk as evaluated;
- Addressing or removing the source of the risk;
- Addressing the likelihood;
- Addressing the consequence;
- Sharing the risk with another party or organisation (this is most relevant for financial risks);
- Retaining the risk by informed decision.

Some strategies for treating risk are not always attainable or appropriate, and principals must consider the effort and cost to implement a strategy against the benefit. The school environment, budget constraints, deliverability and impact on school operations should be considered when determining the suitability of each strategy to treat risk.

Information about the types of strategies to treat identified security risks is available from the School Security Handbook, the School Security Management OnePortal page , or your School Security Advisor (DoE employees only). You can also refer to Fact sheet 2: Developing security guidelines at schools for information about locally applicable guidelines that can be implemented to mitigate security risks.

Developing a risk management plan

The School security risk assessment guide includes templates for principals to prioritise the treatment of each identified risk, based on their overall risk level, and to record how selected risk management strategies will be implemented.

For each identified risk, the school's security risk management plan should include:

- description of the selected treatment strategy;
- reason/s for selection, and the expected benefit/gain;
- person/s responsible for approval and implementation;
- any actions and resources required;
- applicable performance measures or any restrictions (target reduction in incidents, financial limitations etc.);
- applicable schedule for implementation; and
- any relevant monitoring and reporting activities.

The template for an effective Security Management Plan will vary between schools, therefore the knowledge of the school and its surroundings will be the most effective way to manage risk and implement strategies. An example of what a security management plan would include for vandalism is below:

Strategy:	• Promoting the School Watch initiative
Expected Benefit:	• Neighbours reporting unauthorised persons on school grounds after-hours • Police or security respond to reports, even when intruder alarms are not activated • Possible reduction of unauthorised persons on school grounds
Actions Required:	• Renew signage on the fence line • Include notices in newsletter and on noticeboards
Resources Required:	• New Signs - $$$ • New Flyers and magnets - $$$
Restrictions:	• Budget for new materials is limited to $$$/year
Monitoring Schedule:	• Signs and flyers to be ordered and printed in two weeks • Expected to be distributed by the end of Term 1
Responsible Officer:	• Business Manager

Strategy:	• Removing loose pavers from A block garden edge
Expected Benefit:	• Elimination possibility of pavers being used as projectiles • Reduction of broken windows at A and B blocks
Actions Required:	• Sourcing and installation of alternate garden edge • Removal and storage/dumping of pavers
Resources Required:	• New garden edging - $$$ • Allocation of Facilities Officer (date/s)
Restrictions:	• Budget for grounds maintenance is limited to $$$/year
Monitoring Schedule:	• Removal of pavers by the end of the month • Installation of new edging by the end of term
Responsible Officer:	• Facilities Officer

For more information, contact your School Security Advisor (DoE employees only) or Emergency & School Security at ISB.EmergencySecurity@qed.qld.gov.au.