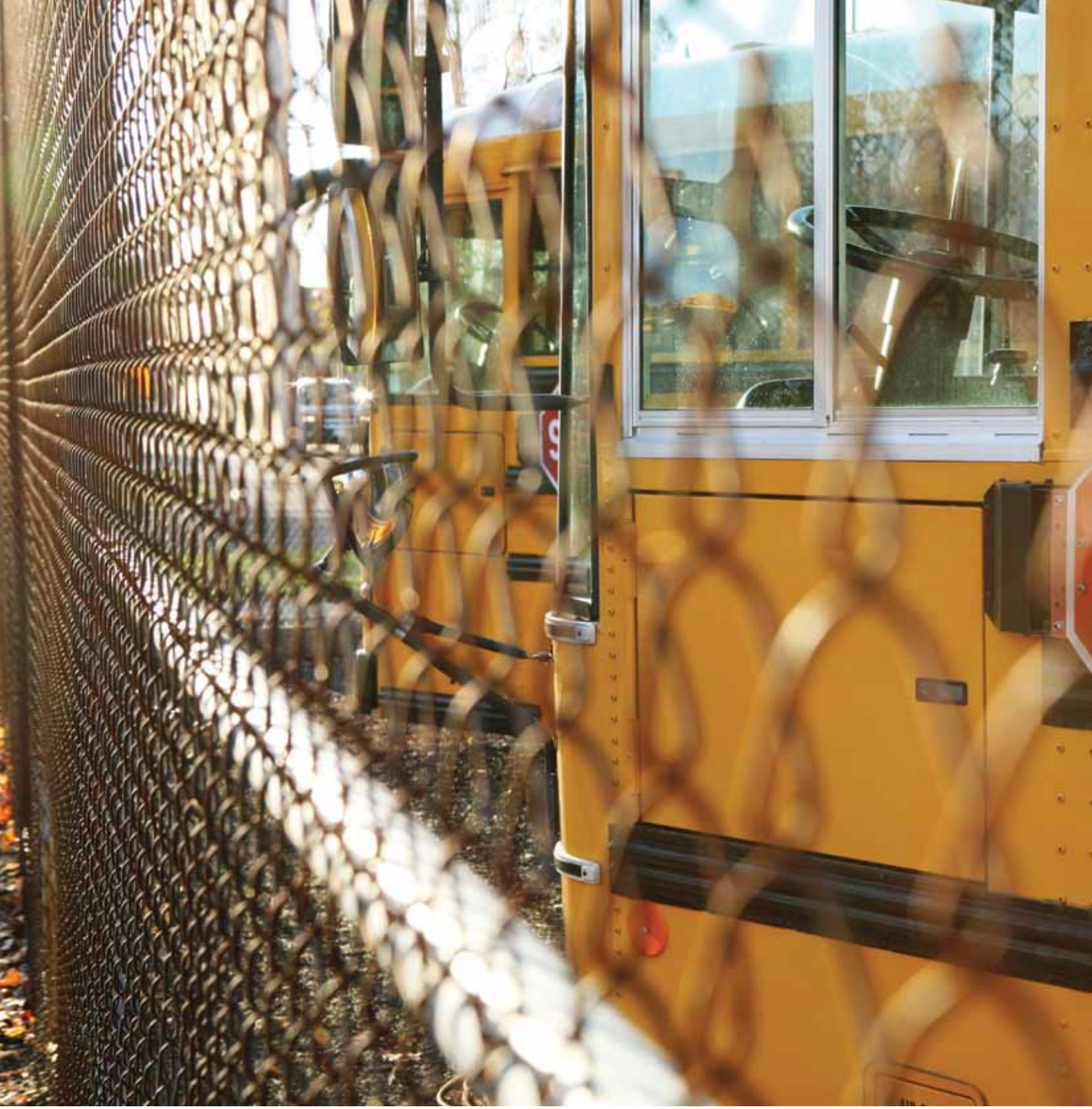
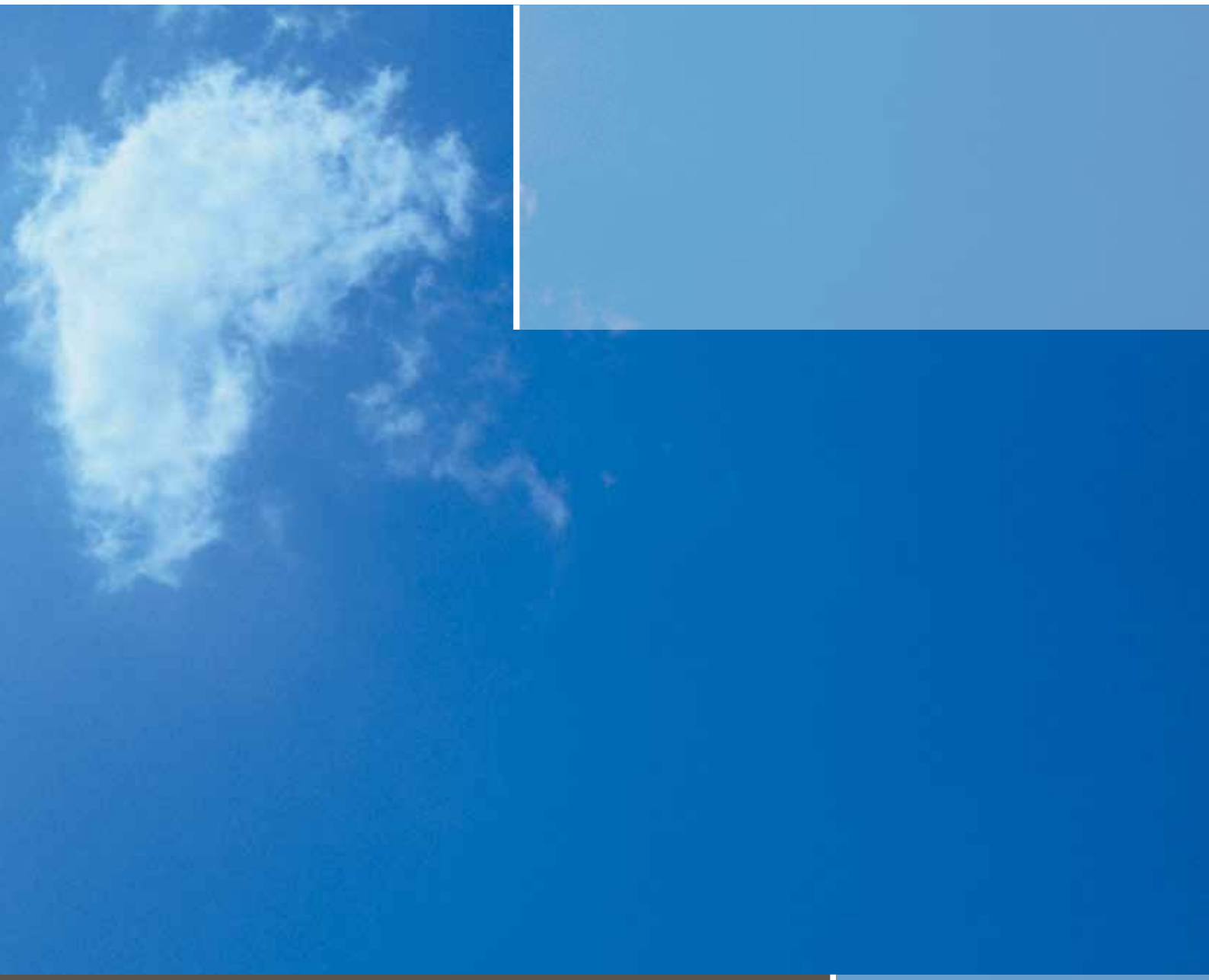


Security Risk Assessment for Transport Operators

A practical guide for small to medium-sized organisations

www.transport.vic.gov.au

State Government Victoria



ISBN 0 7311 8789 X

Authorised by the Victorian Government, 121 Exhibition St, Melbourne Victoria 3000.

If you would like to receive this publication in an accessible format, such as large print or audio please telephone Public Affairs Branch, Department of Transport on (03) 9655 6000.

Contents

Foreword

Security risks can come in many forms and have a major impact on your business. Transport operators that plan for risks recover more quickly than those who do not.

While many larger transport operators have dedicated security and risk management sections, many smaller and medium sized operators do not and may be less prepared to meet the challenges of security risks when they occur.

Under the Victorian Government's Framework for Critical Infrastructure Protection from Terrorism, the two Security and Continuity Network groups dedicated to transport and made up of industry and government representatives, are tasked with collating and disseminating good practice to the industry.

This document draws together current best practice in risk assessment from the members of these groups. It aims to be a valuable resource for those members of the transport industry who have limited resources or expertise currently dedicated to understanding their security risk environment.

By using this risk assessment tool and anticipating potential future events, transport operators will be helping to ensure the future viability and success of their services, as well as keeping the community mobile.

Donovan Croucamp

Chair, Transport Security and Continuity Network
Security and Emergency Management Division
Department of Transport, Victoria

The document

Purpose

There are a wide range of security-related risks that can affect transport operators. Organisations that anticipate and prepare for these risks can recover to normal service levels faster and in a more cost effective manner than those that do not.

A security risk assessment can be a powerful tool for identifying and prioritising these risks. It does not need to be overly complicated or time consuming. This guide offers a simple-to-use methodology for small to medium-sized transport operators who are seeking to undertake a security risk assessment, based on current industry best practice.

Key themes

There are a number of themes in this guide you should keep in mind to better understand and use this document:

- You can adapt and amend the guide where appropriate to meet the organisation's requirements.
- You should revisit the risk assessment process regularly, rather than as a one-off exercise.
- It is vital that you discuss and consult widely with stakeholders, to ensure that the assessment is accurate and communicated effectively.
- Conducting a security risk assessment is only the start. The steps you take afterwards will ensure that you gain tangible benefits.

Reliance and disclaimer

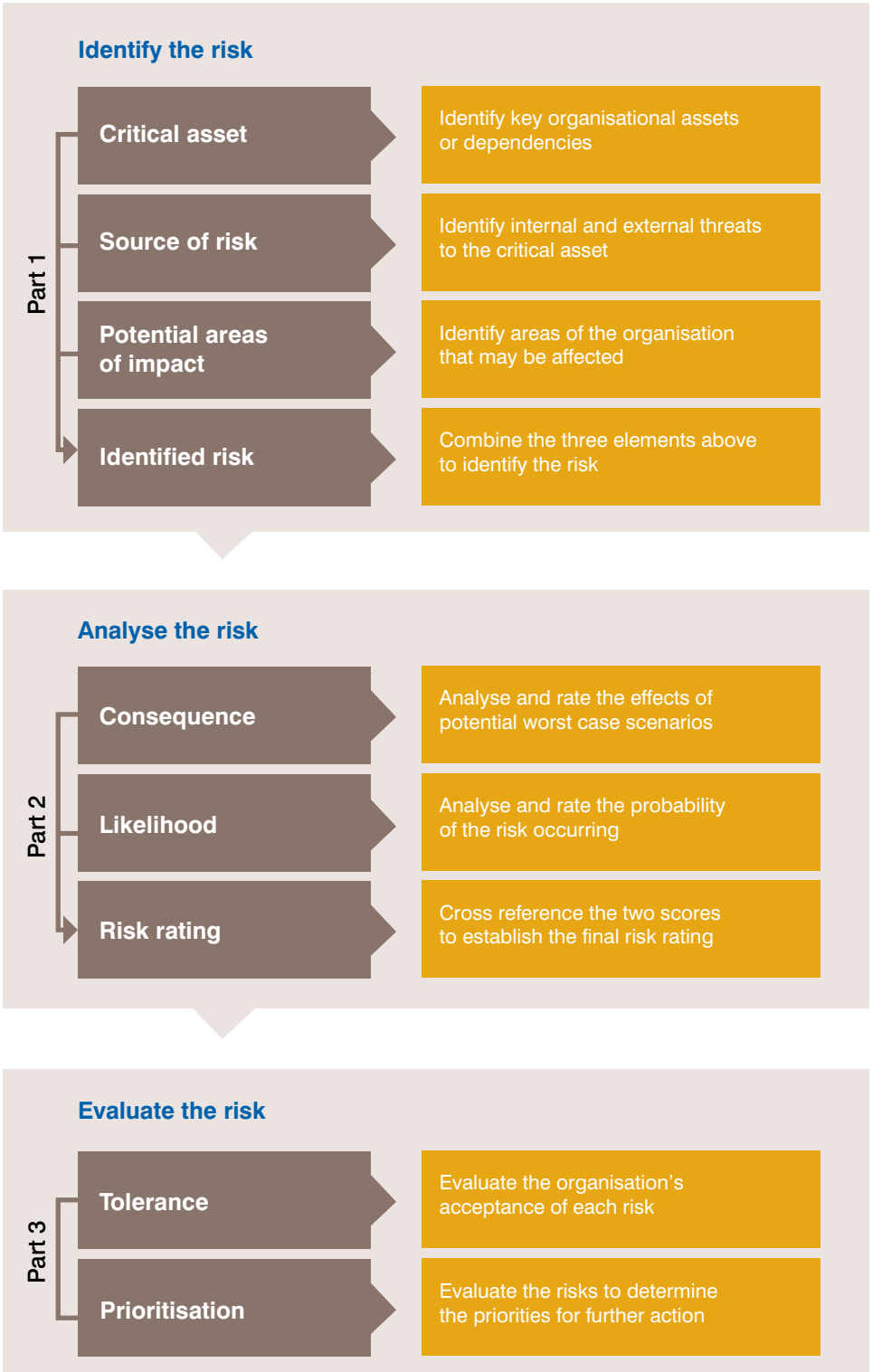
This guide is intentionally focussed on risk assessment. While it touches on other elements of the risk management cycle as referred to in the ISO 31000 standard, it does not go into specific detail on these elements to retain its ease to use. The language used in the document is largely in line with the standard.

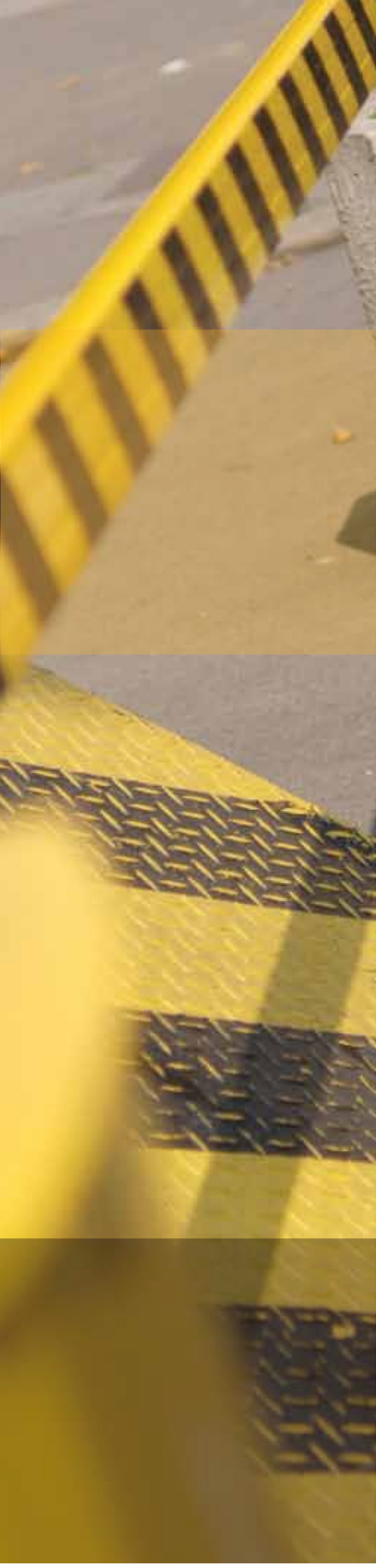
A number of amendments however have been made to reflect current use by risk management professionals within the transport sector.

Any reliance by any third party on this guide is that party's sole responsibility. The Department of Transport accepts no liability to any person, entity or organisation for any loss or damage sustained or incurred by any party as a result of that party's use or reliance upon this guide. This includes, but is not limited to, costs, indirect special or consequential loss or damage (including but not limited to negligence) arising out of the information in this guide.

The risk assessment process

Figure 1: The risk assessment process





Glossary of terms

Areas of impact	Areas of the organisation that may be impacted if a critical asset is affected by a source of risk e.g. financial.
Consequence	The potential effects on the organisation if the risk occurs. This takes into account the most plausible worst-case scenario and current controls.
Controls	Measures that are put in place to protect a critical asset against a source of risk.
Critical asset	Assets and dependencies which if lost or interrupted, would significantly impact on the organisation's ability to deliver its key objectives.
Current controls	Measures that are in place now to protect a critical asset against a source of risk.
Dependencies	Assets or services not directly under the control of the operator.
Identified risk	The final risk identification statement that combines the three elements of critical asset, source of risk and potential areas of impact.
ISO 31000	The international standard for risk management.
Level of risk	The level attributed to a risk, found by cross referencing the levels of consequence and likelihood (also known as the 'risk rating').
Likelihood	The probability of the identified risk occurring, taking into account current controls.
Residual risk	The level of risk that remains after additional treatment measures have been put in place.
Risk analysis	The process of analysing a risk's consequence and likelihood to determine its risk rating.
Risk appetite	The organisation's attitude towards which levels of risk may be acceptable (or otherwise).
Risk assessment	The overall process combining risk identification, analysis and evaluation.
Risk evaluation	The process of determining the level of risk that is acceptable and prioritising the treatment of all risks.
Risk identification	The process of identifying the security risks relevant to the organisation.
Risk rating	The level attributed to a risk, found by cross referencing the levels of consequence and likelihood (also known as the 'level of risk').
Risk register	The principal record for all of the identified security risks and associated elements of the risk assessment process.
Security risk	Identified risks to the organisation that are security related.
Source of risk	Internal and external threats which have the potential to affect an organisation's critical assets.
Tolerance	Determines what level of risk is acceptable to the organisation.
Treatment	The process of adding controls to protect a critical asset.

Part 1

Risk identification

Optional advanced techniques:

While the basic approach in Sections 1.2 to 1.5 will allow you to identify and provide an accurate picture of the relevant security risks, the optional and more detailed approaches detailed in Appendix A ('Further Techniques') on page 30, will allow you to rate the various elements of the risk and create a better understanding of your risk environment.

1.1 Introduction to risk identification

Identifying the risks that are relevant to your organisation is a key component of any security risk assessment. Any risks that are not identified at this stage will not be considered for further analysis and as such will not be treated, potentially leaving your organisation vulnerable if those risks occur.

From a security perspective, there are three primary elements that should be examined to identify risks that are relevant to your organisation:

- Establish the **critical assets** of the organisation. This will allow you to focus on the assets or dependencies that are essential for the organisation to function and achieve its objectives.
- Identify appropriate **sources of risk** (traditionally referred to as threats), to better understand the range of potential factors that may affect your critical assets.
- Determine the **potential areas of impact** on the organisation, if the sources of risk occur against your critical assets.

Security risks for the purposes of this document are therefore identified as:
Critical assets *that may be affected by* ***sources of risk*** *resulting in* ***potential impacts*** *to areas of the organisation.*

The following sections will look at each element in turn, allowing you to build a comprehensive understanding of the security risks faced by your organisation.

1.2 Identifying critical assets

1.2.1 What are critical assets?

All organisations have critical assets without which they would not be able to operate effectively or deliver their key services. By identifying these assets, you will be able to apply the risk assessment process more rigorously to those elements that are of greater importance to the running of your operations.

You should be realistic when identifying your critical assets to prevent the risk assessment process becoming too cumbersome. You should also take into consideration any key dependencies not directly under the organisation's control that it relies upon.

In general terms you should be asking:
Which assets and dependencies if lost or interrupted, would significantly impact on the organisation's ability to deliver its key objectives?

1.2.2 Methodology

When identifying critical assets, you should consider grouping elements under the headings of people, information and physical assets. Thought should also be given under these headings to identifying key dependencies.

Table 1: Examples of critical assets

	Operator assets	Dependencies
People	Drivers/pilots, CEO, technical experts	Supply of contractors
Information	Electronic databases, records	Third-party hosted servers, telephone network
Physical	Rolling stock, signal boxes, key stations/ terminals, depots, navigation beacons	Supply of power/ fuel, availability of spare parts

1.3 Identifying sources of risk

1.3.1 What are sources of risk?

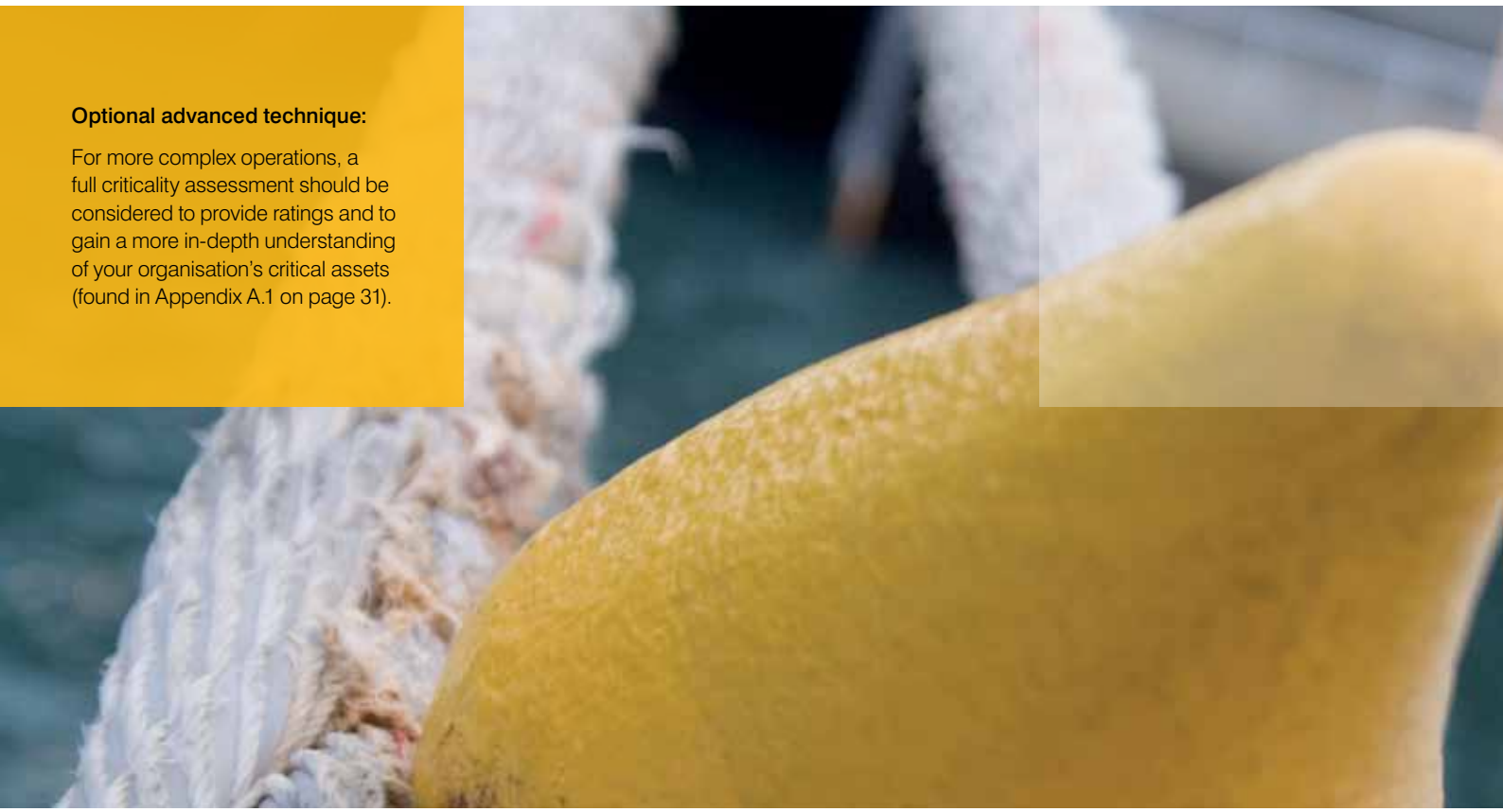
Traditionally referred to as 'threats' within a security context, you should seek to identify both internal and external potential sources of risk to your organisation.

When identifying sources of risk, it is important to look for those that have the potential to affect the organisation. At this stage, you do not need to identify the possible impacts.

For the purpose of this guide, sources of risk are defined as:
Internal and external threats which have the potential to affect the organisation's critical assets.

Optional advanced technique:

For more complex operations, a full criticality assessment should be considered to provide ratings and to gain a more in-depth understanding of your organisation's critical assets (found in Appendix A.1 on page 31).



Sources of security risk can be looked at both in terms of the potential perpetrator and method (such as the threat from an arson attack *[method]* by animal rights activists *[perpetrator]*). To avoid over complicating the assessment and to incorporate the threat from a range of groups, the method is often however referred to on its own (i.e. the threat from an arson attack).

Table 2: Example sources of risk

Potential sources of risk		
arson	cyber attack	armed assault
hijacking	sabotage	rioting and civil unrest
surveillance	suicide bomber	car bomb
chemical attack	biological attack	radiological attack
piracy	package bomb	hostage taking

1.3.2 Methodology

When identifying sources of risk, it is useful to think both strategically and operationally to ensure that all potential sources are considered. You may want to refer to the list of critical assets identified in Section 1.2 to assist the process.

Table 3: Suggested methods for identifying sources of risk

	Detail	Example
Pools of experts	A collection of experts from different fields	For a rail company, a representative group may consist of a driver, manager and engineer
Past knowledge	A review of past incidents to identify previously realised threats	Reviewing historical attacks against other vessels globally, may assist a ferry operator identify potential threats that may be enacted domestically
Staff	Reviewing staff reports of suspicious activity	Encouraging depot managers to report any threats they encounter, will assist in identifying potential trends
Horizon scanning	Anticipating future threats	A major international event such as a G20 Summit, may bring additional threats not previously present
Threat experts	Harnessing the knowledge of subject matter experts	Cyber attack may be identified as a threat, but experts will be able to drill down to establish further detailed elements such as malware or viruses
Workshop	Group discussion	At a business unit level, participants may wish to consider which threats may affect their ability to deliver on the unit's key objectives

Optional advanced technique:

For companies looking to gain a better understanding of their sources of risk, a more thorough threat assessment may be needed. Further detail on conducting a threat assessment can be found in Appendix A.2 on page 33.

Example 1: Identifying sources of risk

Whilst undertaking a horizon scan for upcoming events, a bus company notes that a soccer match between teams from countries with historical political tensions is due to take place at a location serviced by the operator.

As relations between the two countries have recently deteriorated, an extremist group in Australia associated with one team has threatened violence against fans from the other.

The company will be transporting the threatened team's supporters. As a result, 'political violence' is identified as a source of risk which has the potential to affect the bus company's critical assets.

1.4 Identifying potential areas of impact

Once you have identified the organisation's critical assets and sources of risk, you need to look at the potential areas of impact to the organisation. A non-exhaustive list of headings for consideration may include finance, health and safety, operations, reputation, people, legal and environment (for further definitions see Table 4 on page 16).

In essence, you are identifying:
Potential areas of the organisation, which may be impacted by sources of risk affecting its critical assets.

To avoid the final risk being too specific, it is important for you to keep the impacts identified broad at this stage. For example, rather than identifying an impact as 'three people seriously injured', the potential impact should be 'serious injuries'.

You should consider your organisation's critical assets and potential sources of risk when identifying areas of impact. The example below shows how this might be performed:

Example 2: Identifying potential areas of impact

A ferry company has designated its vessels as critical assets and a car bomb as a potential source of risk.

After consideration, the potential areas of impact are identified as:

- Fatalities or serious injuries
- Damage to vessel
- Financial loss

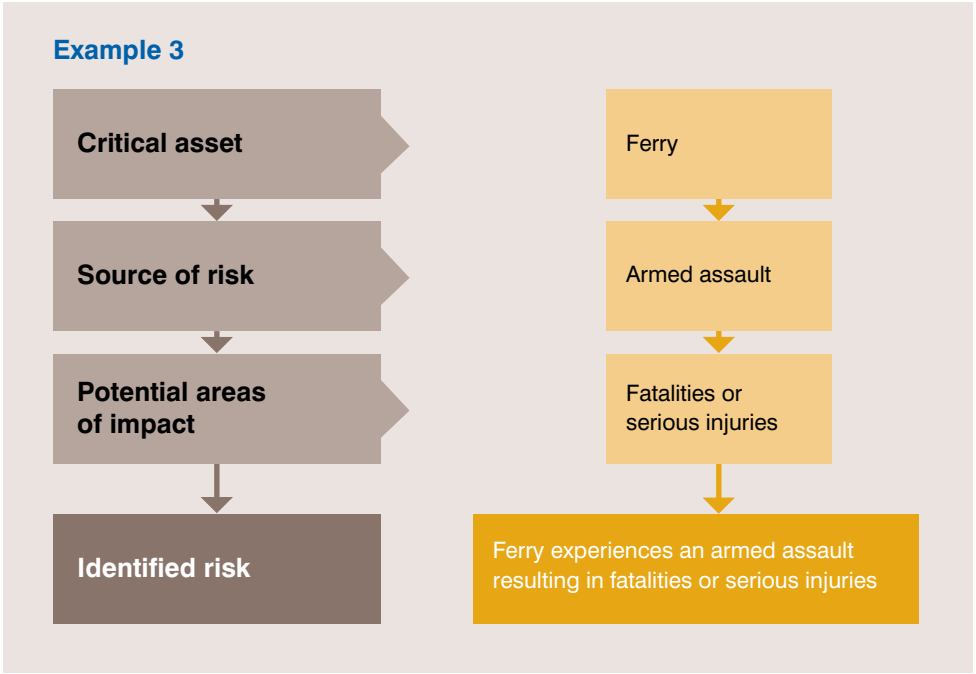
Optional advanced technique:

To gain a better understanding of the effectiveness of the company's current security measures, you can undertake a vulnerability assessment. More information on conducting a vulnerability assessment can be found in Appendix A.3 on page 34.

1.5 Identifying the risk

Once you have established the three principal elements of the risk, you now combine them to identify the final risk statement. The following flow diagram shows this process at work:

Figure 2: Risk identification



In the above example the operator's identified risk is: '*Ferry experiences an armed assault resulting in fatalities or serious injuries*.'

As discussed in Example 2 (Identifying potential areas of impact), the source of risk associated with a critical asset may have multiple potential areas of impact. These can be combined as a single risk but it may be more beneficial to break them down into separate statements to allow each risk to be treated in its own right. The example risk register on page 28 gives a practical demonstration of how this might be achieved to deliver two risks:

'Depot suffers an arson attack resulting in *damage to rolling stock*', and

'Depot suffers an arson attack resulting in *fatalities or serious injuries*'

1.6 Part 1 checklist

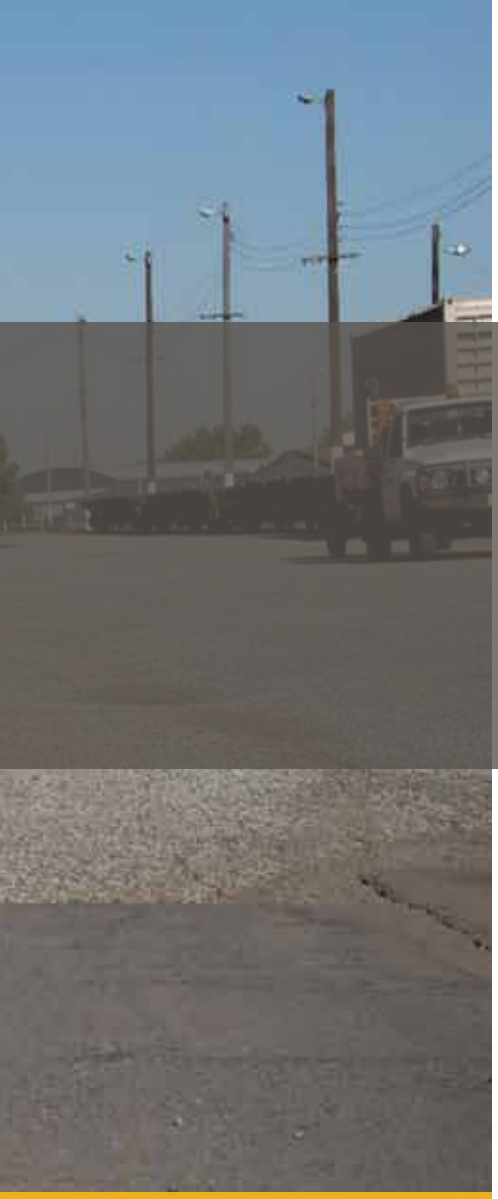
When you have completed Part 1, you should have:

- Identified critical assets
- Identified sources of risk
- Identified potential areas of impact
- Finalised a list of identified risks

Once you have completed these steps, you should move on to the risk analysis process outlined in Part 2.

Part 2

Risk analysis



Optional advanced technique:

Undertaking vulnerability and criticality assessments (outlined in Appendix A 'Further Techniques', page 30), may help you get a better understanding of the effectiveness of current controls that are in place to protect an asset.

2.1 Introduction to risk analysis

Once you have identified the risks to your organisation, the next stage of the assessment process is to work out the level of risk (or 'risk rating') attached to each. By carrying out this analysis, you will be in a better position to identify the risks that are of a higher priority to the organisation.

To establish the level of risk, the following formula is used:
*The **level of risk** is determined by rating the potential **consequences** of the risk occurring and its **likelihood.***

The analysis process is completed in three stages to establish levels of consequence, likelihood and risk. The tables included throughout this document should only be used as a guide and where possible, should be tailored to reflect your individual requirements.

2.2 Consequence

2.2.1 Rating consequence

You must now rate each identified risk in terms of its potential consequences (should it occur), considering a number of key points:

- The most plausible worst case scenario should be taken into account.
- A single risk may have multiple consequence categories.
- When analysing the potential consequences, you should take into consideration the measures that are currently in place to protect the asset (known as 'current controls').

2.2.2 Consequence categories

The categories below and in the table on the next page, represent those that are often used by transport operators in determining the consequences of a particular risk. These categories are intended as a guide and you should look to use (and develop) categories which suit your circumstances.

Table 4: Consequence categories

Category	Notes
Financial	As the financial position of operators can vary considerably, the levels for each category should be amended to reflect this. Includes infrastructure replacement costs i.e. physical assets such as buildings and IT networks.
Health & Safety	Health and safety of staff and customers, where the operator could be held culpable.
Operational	The ability to deliver key services.
Reputational	Should include political considerations alongside traditional public, media and investor relations issues.
People	Availability of workers (including losses due to strike action, pandemics etc.).
Legal	Incorporating compliance and other liability considerations.
Environmental	Considering the physical environment, wildlife and pollution.

Table 5: Rating consequence

Consequence Categories

Rating	Descriptor	Financial [1]	Health & Safety	Operational	Reputational	People	Legal	Environmental
5	**Catastrophic**	Extreme financial loss to the organisation e.g. more than $2m	Single or multiple fatalities	Loss of ability to deliver the majority of services for over one month	Extreme negative media coverage and public outcry lasting longer than a month; negative public comments by a minister	Affects enough personnel to severely impact the organisation	Severe breach of contract or law resulting in loss of operating licences; or criminal liability with extreme fine	Irreversible widespread damage
4	**Major**	Major financial loss to the organisation e.g. $501k – $2m	Severe injuries to multiple personnel	Loss of ability to deliver the majority of services for up to one month	Extensive negative media coverage lasting over a number of weeks; sustained negative state level political discussion	Affects enough personnel to severely impact a division	Major breach of contract or law resulting in additional monitoring by licensor; or criminal liability with major fine	Major damage to the environment requiring long-term recovery
3	**Moderate**	Moderate financial loss to the organisation e.g. $101k – $500k	Injuries requiring hospitalisation	Loss of ability to deliver a significant level of services for up to two weeks	Significant negative media coverage lasting for several days; negative state level political discussion	Affects a significant amount of personnel, requiring careful management	Breach of contract or law resulting in closer oversight, a significant fine or damages	Significant damage to the environment requiring medium-term recovery
2	**Minor**	Minor financial loss to the organisation e.g. $10k – $100k	Injuries requiring attention by a medical professional	Some minor reductions in operational service levels	Minor negative media coverage lasting for single day; negative local council discussion	Affects a small number of personnel and requires some management attention	Minor breach of contract or law that can be resolved with dialogue between parties	Minor damage to the environment requiring short-term action
1	**Insignificant**	Insignificant financial loss to the organisation e.g. less than $10k	Injury requiring only minor first aid	Negligible operational impact	Internal issue only, no scope for media interest; negative customer feedback	Affects a small number of personnel but requires little management attention	Technical breach of contract or law with no material consequence	Short-term impact requiring negligible action

1 Financial consequence figures should always be amended to reflect an operator's individual circumstances

Example 4: Rating consequence

A large road-haulage company that transports livestock has identified a risk from, 'Truck experiences sabotage by animal rights activists, resulting in damage to vehicle.'

The company has a number of controls already in place for the security of vehicles, including robust locks and procedures to check the vehicle after each stop.

If the risk is realised, (taking into account current controls and assuming a most plausible worst case scenario), the company has identified that there will potentially be financial and operational consequences:

- Financial – replacement cost of truck ($150,000)
- Operational – minor reduction in operational service levels

The company uses Table 5 on page 17 and as such, the consequences are rated as: *'moderate'* for financial and *'minor'* for operational.

When determining the overall level of consequence for the identified risk, the highest level is taken. The consequence rating for this risk is therefore level '3' *(moderate)*.

2.3 Likelihood

You now need to work out the likelihood of the identified risk occurring. Primarily this will be achieved by reviewing the source of risk (see Section 1.3 on page 10), however the vulnerability of the asset itself may also be taken into account (including consideration of the current controls in place to protect it).

The table here shows how likelihood may be rated and contains a range of benchmarks that can be used. While some, or all, of the criteria below might be suitable for your organisation, you may need to tailor these to suit your requirements.

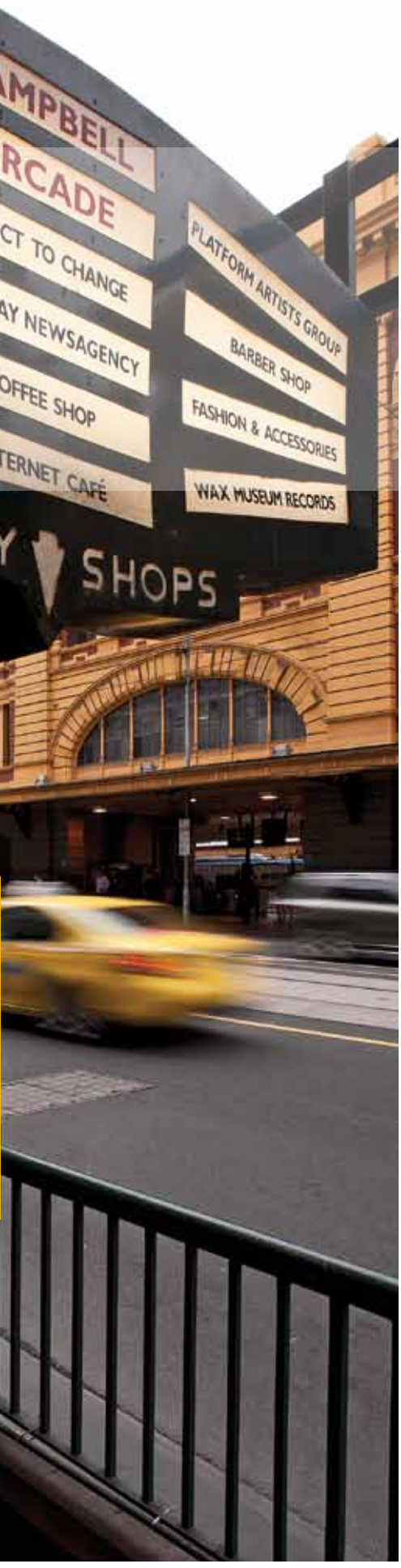
Table 6: Rating likelihood

Rating	Descriptor	Probability	Frequency
A	Almost Certain	Greater than 95%	Occurs every month
B	Likely	From 65% to 95%	Occurs once every few months
C	Possible	From 15% to less than 65%	Occurs once every year
D	Unlikely	From 5% to less than 15%	Occurs once every 10 years
E	Rare	Less than 5%	Occurs once every 100 years

When determining likelihood, you should consider both previous occurrences and future considerations. Statistically for example, an arson attack against a train operator's depots may occur once every year and therefore attract a 'C' (*possible*) rating. On the other hand, a ferry operator may have never before been affected by civil unrest but due to a heated political environment, there is a 70 per cent future chance of a riot occurring at the operator's shore facilities, therefore attracting a 'B' (*likely*) rating.

Optional advanced technique:

Undertaking threat and vulnerability assessments (outlined in Appendix A 'Further Techniques', page 30), may help you gain a better understanding of the probability of the risk occurring and the current controls that are in place to protect an asset.



Example 5: Rating likelihood

A freight train operator has identified a risk as, 'The payroll system is affected by a computer virus, resulting in the loss of employee information.'

While this type of attack has never before happened to the company, attacks have been seen against other organisations and the government is warning of a heightened threat from computer viruses against infrastructure operators.

Given this information and taking onboard security measures that are already in place ('current controls'), the operator's risk committee considers that there is a 20 per cent chance of a computer virus affecting the payroll system, which would result in the loss of employee information.

Using Table 6 on page 18, the likelihood of the risk occurring is therefore rated as 'C' (*possible*).

*Note: a computer virus can form part of a wider targeted cyber attack, as identified in Table 2 on page 11.

2.4 Rating risk

Once you have identified the appropriate levels of consequence and likelihood for the risk, you now need to allocate an overall risk rating. As with both the consequence and likelihood tables, you can alter the risk rating matrix to better represent your organisation's individual requirements.

Use Table 7 to establish the overall level of risk by cross referencing the ratings for consequence and likelihood:

Table 7: Rating the risk

Likelihood		Consequence				
		Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
		(1)	(2)	(3)	(4)	(5)
Almost Certain	(A)	Significant	High	High	Extreme	Extreme
Likely	(B)	Medium	Significant	High	High	Extreme
Possible	(C)	Medium	Medium	Significant	High	High
Unlikely	(D)	Low	Medium	Medium	Significant	High
Rare	(E)	Low	Low	Medium	Medium	Significant

Example 6: Rating risk

A bus company has identified a risk that, 'Staff members experience an armed assault by a disgruntled employee, leading to injuries or fatalities.'

Having taken into account current security measures, the operator concludes that the most plausible worst case scenario is multiple fatalities and injuries. Using the consequence Table 5 on page 17, the level of consequence (health and safety) is accordingly rated as '*catastrophic*' (5).

Given that the company has recently laid off a fifth of its staff, it is assessed that the probability of the risk occurring has risen to about 5 per cent. Using Table 6 on page 18, the likelihood is therefore assessed as '*unlikely*' (D).

Using the risk rating matrix, the levels of consequence (5) and likelihood (D) are cross-referenced to determine the final level of risk.

The risk that, 'Staff members experience an armed assault by a disgruntled employee, leading to injuries or fatalities' is therefore rated as *'high'*.

Likelihood		**Consequence**				
		Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
		(1)	(2)	(3)	(4)	(5)
Almost Certain	(A)	Significant	High	High	Extreme	
Likely	(B)	Medium	Significant	High	High	
Possible	(C)	Medium	Medium	Significant	High	
Unlikely	(D)					High
Rare	(E)	Low	Low	Medium	Medium	Significant

2.5 Part 2 checklist

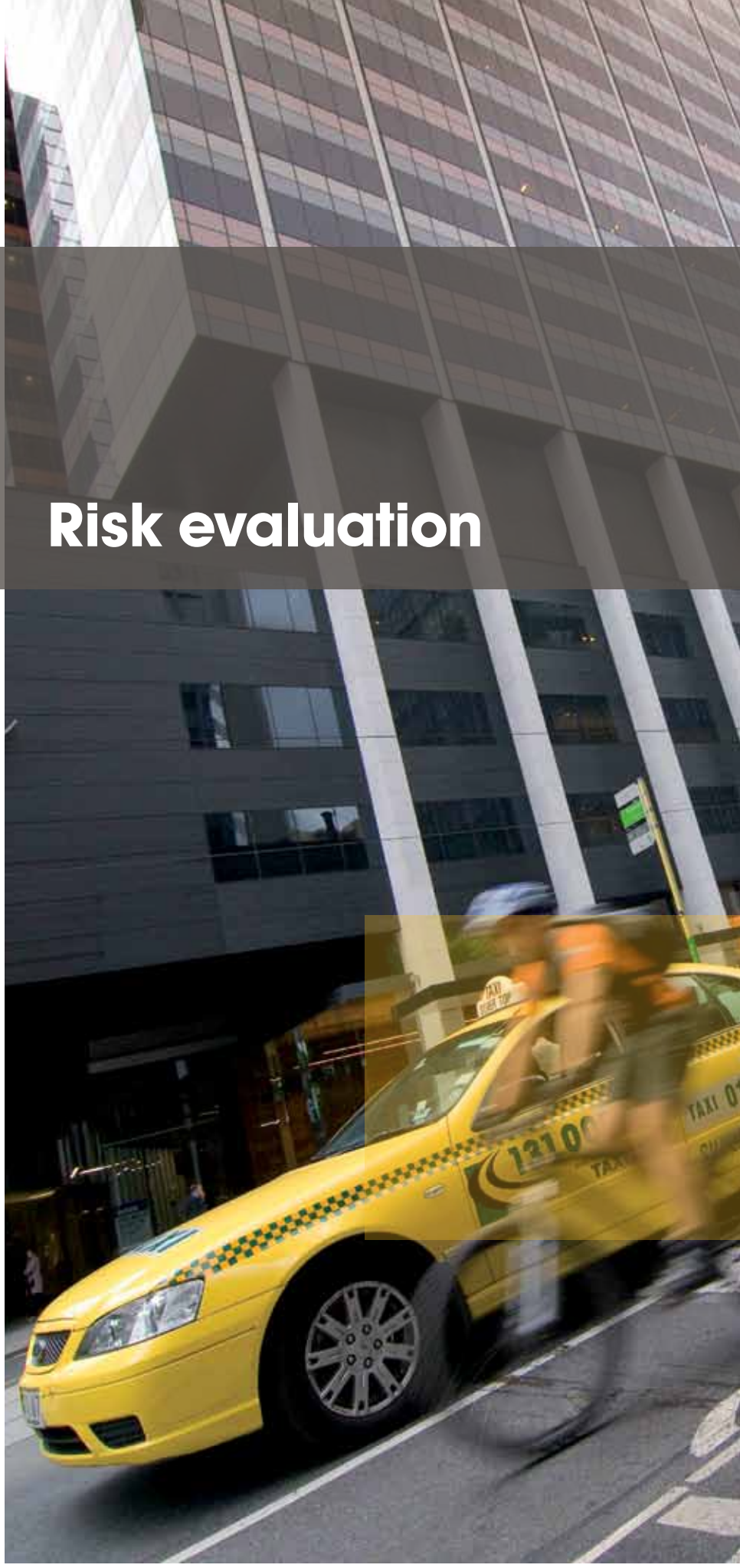
When you have completed Part 2, you should have:

- Rated the potential consequences from the identified risks occurring
- Rated the likelihood of the identified risks occurring
- Rated the risks by cross referencing consequence and likelihood

Once you have completed these steps, you should move on to the risk evaluation process outlined in Part 3.

Part 3

Risk evaluation



3.1 Introduction to risk evaluation

After you have identified and analysed your risks, you should now evaluate which risks are rated at an acceptable level and which need to be prioritised for further action.

The evaluation of tolerance and prioritisation is a key component in determining the next steps required in allocating additional controls, in order to bring the risks to levels that are considered acceptable by the organisation.

Good governance of the identified risks becomes increasingly important at this stage and the use of a risk register (see page 28) is recommended to track your progress, allocate accountability and encourage a perpetual cycle of monitoring and review.

3.2 Tolerance

The level of risk that is acceptable to your organisation (often referred to as its 'risk appetite') will vary from organisation to organisation and should be considered on a risk-by-risk basis.

You may however choose to identify a default level above which risks must be attended to more urgently, and where increasingly more senior levels of management need to be kept up-to-date on progress. For example, policy may dictate that risks rated as '*high*' or '*extreme*' must be addressed immediately, with the organisation's most senior person or body notified.

In an ideal world, the acceptable level of risk would be the lowest available rating but due to cost restrictions and other considerations, this may simply not be practical. When you consider what level would be acceptable for each risk, you should take into account what is reasonably practical to achieve.

Example 7: Tolerance

A railway operator has identified one of its risks as, 'Train intentionally rammed by car at a crossing, resulting in damage to one or more units.'

Due in part to the lack of current controls, the risk is rated as *'high'*.

As company policy states that risks rated *'high'* or above require immediate attention with notification to the Board of Directors, this is done.

For this particular risk, the operator considers a level of risk of *'medium'* to be acceptable and as such, the risk requires further treatment.

3.3 Prioritisation

To determine with what urgency risks should be addressed, they must first be prioritised. Risks with the highest risk rating are normally attended to first. So if your organisation has five risks rated as *'extreme'* and six risks rated as *'significant',* those rated as *'extreme'* would be prioritised above those rated as *'significant'.*

With the risks divided into blocks based on their risk rating, further criteria now need to be considered in order to prioritise them further. Typically additional considerations may include:

- **Safety** – what are the implications if the risk is not addressed?
- **Cost** – how much will it cost to reduce the risk (and will the benefits outweigh the expenditure)?
- **Reputation** – what is the likely affect on reputation if the risk is not treated?
- **Legal obligations** – is the organisation likely to be unable to meet its legal obligations if the risk is left in its current state?

Example 8: Prioritisation

A regional bus operator has rated three risks:

- Driver suffers assault resulting in injury: *'high'*
- Bus suffers vandalism resulting in damage to the vehicle: *'high'*
- Call centre operator endures verbal abuse from customer resulting in distress: *'medium'*

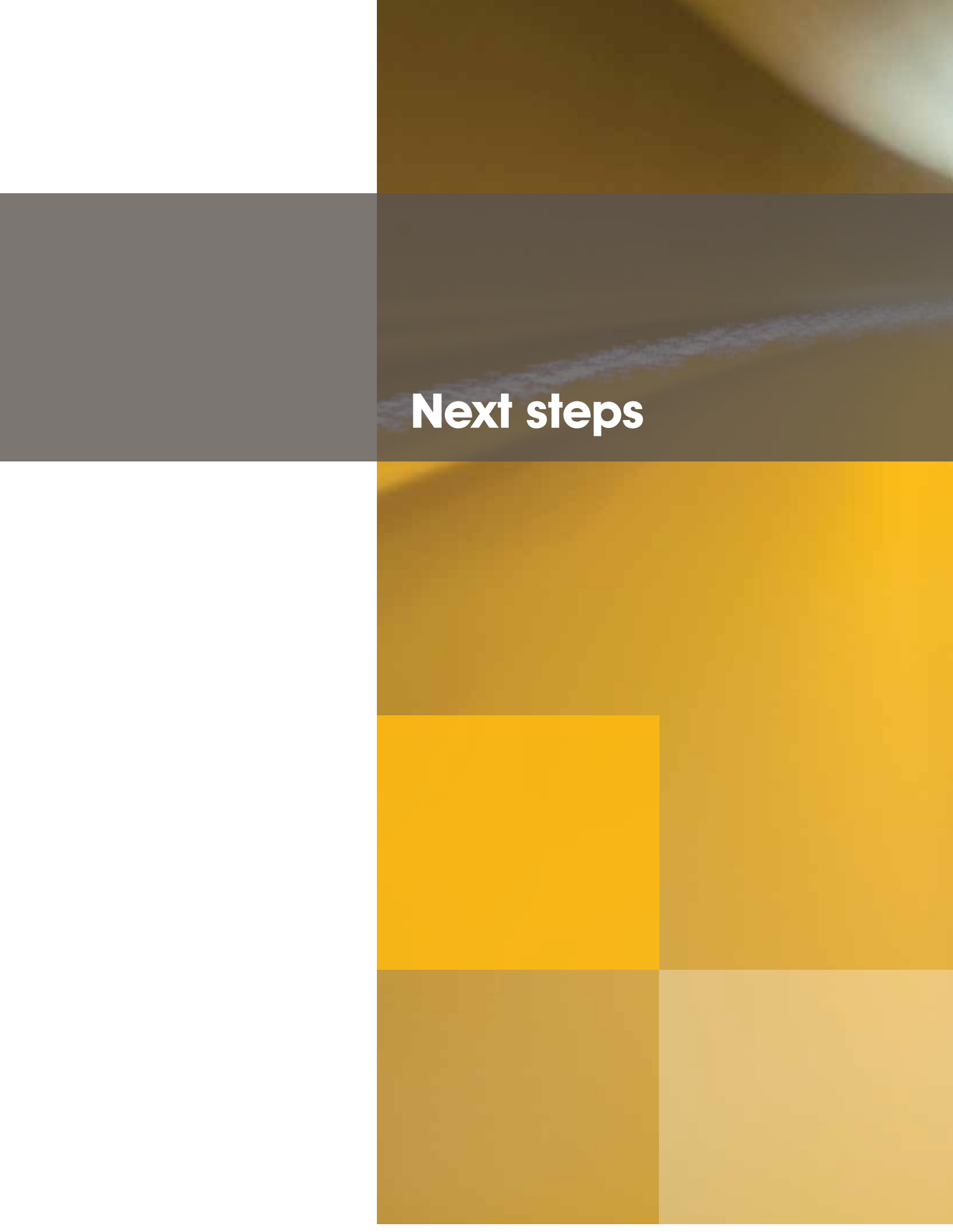
With risks first prioritised by rating, the call centre risk is therefore ranked third.

As the company considers safety to be its next priority, the assault related risk is therefore ranked first, with the vandalism related risk ranked second.

3.4 Part 3 checklist

When you have completed Part 3, you should have:

- Established the organisation's tolerance of each risk
- Prioritised risks for further action



Next steps

Considering treatment options

Once you have rated and prioritised the risks, you need to make decisions on the next steps that are required. Essentially, there are four potential options for treating each risk:

- **Retain** – If the risk is at an acceptable level, then ongoing monitoring will be the primary requirement.
- **Share** – Elements of the risk can be transferred to a third party (such as through insurance or additional contracts), although overall ownership of the risk will remain with the operator.
- **Reduce** – You can attempt to minimise the risk by introducing additional measures to reduce the consequence and/or likelihood of the risk; typically by seeking to limit the effects of the risk should it occur, or by preventing it from taking place.
- **Avoid** – If an activity produces a risk that is higher than the organisation is willing to tolerate and it cannot be treated by other means, you may cease that activity altogether in order to avoid the risk.

The four options above can be applied across all areas of organisational resilience, including preventative measures, preparation for response, and arrangements for business continuity and recovery.

Monitoring and review

All identified risks should be subject to ongoing monitoring and review. The frequency and depth of attention you give each risk should reflect its rating and priority. You should allocate an owner to each identified risk to ensure it is reviewed with an appropriate frequency and that any additional actions and measures that are required are undertaken within a designated timescale.

The risk register

The risk register aims to capture the information and ratings identified in the risk assessment process. This allows you to accurately track progress against each risk. Security risk assessments are often location or asset specific so it may simplify the process to look at the identified risks broken down into their component parts.

Table 8: Sample risk register

Identified Risk[1]			Current Controls						Future Controls				Governance	
Asset[2]	Source of risk[3]	Area of impact[4]	Current Controls[5]	C[6]	L[7]	Current Risk Rating[8]	Accept Risk?[9]	Priority[10]	Additional Actions & Controls[11]	C[12]	L[13]	Residual Risk Rating[14]	Risk Owner[15]	Action Due Date[16]

1. The identified risk as outlined in Section 1.5 'Identifying the risk' on page 13
2. The critical asset segment of the identified risk, as outlined in Section 1.2 'Identifying critical assets' on page 9
3. The source of risk segment of the identified risk as outlined in Section 1.3 'Identifying sources of risk' on page 10
4. The potential area of impact segment of the identified risk as outlined in Section 1.4 'Identifying potential areas of impact' on page 12
5. A list of the measures that are currently in place to address the risk
6. The rating for the consequence of the risk occurring, as found in Section 2.2 'Consequence' on page 15 (taking current controls into consideration)
7. The rating for the likelihood of the risk occurring, as found in Section 2.3 'Likelihood' on page 18 (taking current controls into consideration)
8. The current risk rating for the identified risk, as found in Section 2.4 'Rating risk' on page 19
9. A 'Yes/No' rating for whether the level of risk is acceptable to the organisation, as discussed in Section 3.2 'Tolerance' on page 23
10. A numbered priority for each risk, as discussed in Section 3.3 'Prioritisation' on page 24
11. A list of the additional controls for an unacceptable risk, that will be put in place in order to attempt to reduce the risk rating
12. The anticipated rating for the consequence of the risk occurring once future controls have been taken into consideration, as found in Section 2.2 'Consequence' on page 15
13. The anticipated rating for the likelihood of the risk occurring once future controls have been taken into consideration, as found in Section 2.3 'Likelihood' on page 18
14. The anticipated residual risk rating for the identified risk, after additional controls are put in place, as found in Section 2.4 'Rating risk' on page 19
15. Designates who is responsible for the risk and accountable for the delivery of any additional controls
16. The date by which additional actions and controls need to be undertaken

Example 9: Risk register

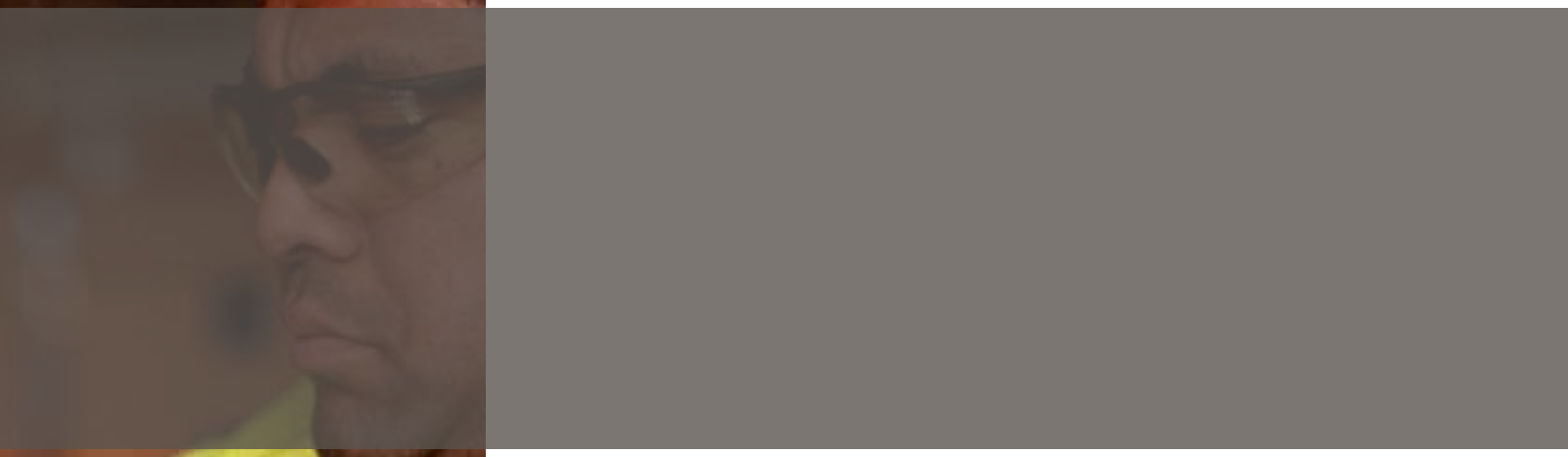
Identified Risk[1]			Current Controls						Future Controls				Governance	
Asset[2]	Source of risk[3]	Area of impact[4]	Current Controls[5]	C[6]	L[7]	Current Risk Rating[8]	Accept Risk?[9]	Priority[10]	Additional Actions & Controls[11]	C[12]	L[13]	Residual Risk Rating[14]	Risk Owner[15]	Action Due Date[16]
Depot	Arson	Damage to rolling stock	Manual fire alarms Extinguishers	5	D	High	No	2	Automatic sprinkler system to be installed	3	D	Medium	Depot Manager	Within six months
		Fatalities or serious injuries	Manual fire alarms Extinguishers	5	D	High	No	1	First aid training to be delivered to all depot staff	4	D	Significant	Depot Manager	Within six months
	Vandalism	Disruption to operations	CCTV and patrols in place	2	C	Medium	Yes	3	n/a	n/a	n/a	n/a	Depot Manager	Review in one year

NB: The explanatory notes below refer to the first of the three identified example risks in the table above

1. The first risk is identified as, 'Depot suffers an arson attack resulting in damage to rolling stock'
2. The critical asset is identified as a 'depot'
3. The source of risk is identified as 'arson'
4. The potential area of impact is identified as 'damage to rolling stock'
5. To mitigate against the risk, manual fire alarms and extinguishers are available
6. Consequence is rated as 5 (*catastrophic*) as an arson attack on the depot may impact operations for over one month (using Table 5 on page 17)
7. Likelihood is rated as D (*unlikely*) as arson attacks on the depot happen once every ten years or so (using Table 6 on page 18)
8. The current risk rating is '*high*', found by cross referencing the scores for consequence and likelihood (using Table 7 on page 19)
9. The rating of '*high*' for this risk is deemed not acceptable to the organisation and therefore requires further treatment
10. Whilst the current risk rating demands a high priority, health and safety is the next criteria and 'damage to rolling stock' is therefore rated behind 'fatalities or injuries'
11. The addition of an automatic sprinkler system is suggested as an additional treatment measure
12. The anticipated rating for consequence has changed to 3 (*moderate*), as the planned measures should reduce the impact on operational delivery (by preserving rolling stock)
13. The anticipated rating for likelihood remains the same, as the planned additional measures would not affect the probability of arson attacks occurring at the depot
14. The remaining (residual) level of risk is reassessed and whilst the likelihood remains the same, the change of consequence level means the risk rating is now '*medium*'
15. The depot manager is allocated responsibility for the risk and is accountable for the delivery of any additional controls
16. The additional measures that have been outlined are due in place within six months of this risk review


BUS LANE
AND
LEFT TURN
LANE
7AM - 9-30AM
MON - FRI
TOW AWAY
CLEARWAY TIMES
6 30-9 30 AM
MON - FRI
BUS
ZONE
Route To
316 City (Russell St)
319 City (Queen St)
340/
350 City (Flinders St)
Hail Bus Here
246
313
315

Appendix A
Further techniques



Optional advanced technique:

For operators with few assets, it may be enough to discuss and review the elements of the organisation that you consider critical. Conducting a criticality assessment may however assist those with a wide range of assets, in determining which are the most critical.

The more advanced techniques in Appendix A are optional and can be used if you wish to gain a greater understanding of your risk environment.

A.1 Conducting a criticality assessment

A criticality assessment is designed to identify and rank your organisation's critical assets and should be an enterprise-wide endeavour. Responsibility should be delegated, where appropriate, to relevant divisions or sections.

In order to accurately assess criticality, the loss of assets and dependencies should be evaluated against the most plausible worst case impact on the organisation.

You should consider what level of criticality qualifies an asset or dependency as a critical asset before you conduct an assessment. The elements that reach the required level should then be taken forward for inclusion in the remainder of the risk identification process.

Assets may be ranked firstly by level of criticality and secondly, by the depth of range of potential worst-case scenario impacts.

The following table provides an example of how criticality could be rated and identifies potential impact headings. It should be read only as a guide, as critical assets and impacts differ from operator to operator and as such, it is important for your organisation to establish a level of tolerance it is comfortable with.

Please note that the criticality table may where appropriate, be derived from the consequence table found in Section 2.2 on page 17.

Table 9: Assessing the criticality of an asset

Criticality	Most plausible worst case impact from loss of asset			
	Operational	**Health and Safety**	**Financial**	**Reputational**
Extreme	Loss of ability to deliver the majority of services for over one month	Single or multiple fatalities	Extreme financial loss to the organisation e.g. more than $2m	Extreme negative media coverage and public outcry lasting longer than a month; negative public comments by a minister
High	Loss of ability to deliver the majority of services for up to one month	Severe injuries to multiple personnel	Major financial loss to the organisation e.g. $501k – $2m	Extensive negative media coverage lasting over a number of weeks; sustained negative state level political discussion
Significant	Loss of ability to deliver a significant level of services for up to two weeks	Injuries requiring hospitalisation	Moderate financial loss to the organisation e.g. $101k – $500k	Significant negative media coverage lasting for several days; negative state level political discussion
Medium	Some minor reductions in operational service levels	Injuries requiring attention by a medical professional	Minor financial loss to the organisation e.g. $10k – $100k	Minor negative media coverage lasting for single day; negative local council discussion
Low	Negligible operational impact	Injury requiring only minor first aid	Insignificant financial loss to the organisation e.g. less than $10k	Internal issue only, no scope for media interest; negative customer feedback

Example 10: Conducting a criticality assessment

Asset
A local ferry company has one pier at each end of its only route, with no alternatives identified.

Impact from worst case scenario
The most plausible worst case scenario is complete physical loss of the pier, which would lead to services being terminated for at least two months.

Methodology
The company uses Table 9 to assess criticality and rates as *'extreme'*, the loss of any asset or dependency which leads to a complete cessation of services for at least one month (operational).

The criticality of each pier is therefore rated as *'extreme'*.

As the company treats anything rated as *'high'* or *'extreme'* as a critical asset, each pier is added to the list of critical assets.

The company's criticality assessment now states:

Asset	Impact from worst case scenario	Criticality rating	Critical asset?
Pier	Termination of services for a period of at least two months	Extreme	Yes

Optional advanced technique:
For smaller operators, identifying individual sources of risk may be all that is required. For others, gaining a greater understanding and rating factors that drive the threat may be desirable.

A.2 Conducting a threat assessment

Understanding the composition of threats and allocating them a rating, can be of substantial use in gaining a deeper understanding of the overall threat environment in which you operate. A more in-depth knowledge can be of benefit in the later stages of the risk assessment process, particularly in establishing the likelihood of risks and prioritising.

For the purposes of this document:
***Threat** is determined by assessing **intent** and **capability**.*

Table 10: Intent and capability descriptors

	Detail	Example
Intent	Focuses on an individual or group's motivation and objectives.	To take vengeance on an organisation for previous actions (such as supporting a particular cause).
Capability	Considers an individual or group's knowledge, skills and access to resources.	An insider's knowledge of security procedures, access and ability to use a range of firearms.

In order to rate the threat, the intent and capability of the attacker should be assessed then cross-referenced to determine a threat rating.

Table 11: Example threat matrix

		Intent		
		Low	**Moderate**	**High**
Capability	**High**	Significant	High	Extreme
	Moderate	Medium	Significant	High
	Low	Low	Medium	Significant

Example 11: Conducting a threat assessment

A militant group has publicised that is wishes to carry out an armed assault on a particular target and is assessed to have a *'high'* level of intent.

However, the group has no access to weaponry and therefore has a *'low'* capability.

Using Table 11, the overall level of threat is rated as *'significant'*.

A.3 Conducting a vulnerability assessment

A vulnerability assessment can be used to determine how effective current controls for a particular asset or dependency are against a specific threat. This may be useful in Part 2 to determine the possible consequences of any attack and its potential likelihood of success.

You may be tempted to make recommendations on potential additional controls after you have completed a vulnerability assessment. This should be avoided however until the risk evaluation stage of the process, to ensure that efforts and expenditure are prioritised and allocated efficiently across the organisation.

A matrix can be used to rate the vulnerability of an asset or dependency.

Table 12: Example vulnerability matrix

Vulnerability level	Criteria description
Very high	Controls are ineffective
High	Controls have minor effectiveness
Medium	Controls are moderately effective
Low	Controls are largely effective
Negligible	Controls are completely effective

Example 12: Conducting a vulnerability assessment

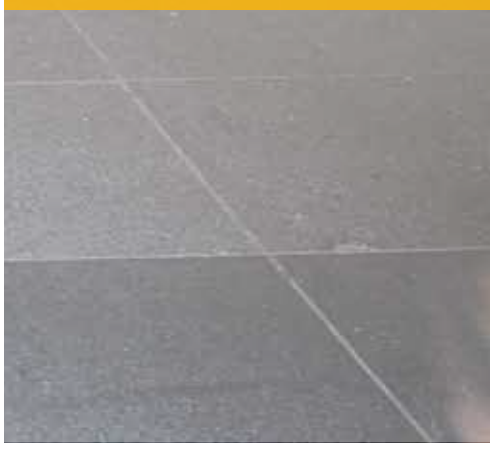
A rail operator has identified that their depot is critical for ongoing operations but may suffer vandalism.

Following a review of the current security measures in place for that asset, it is assessed that as the controls only have minor effectiveness, the vulnerability level for that asset is '*high*'.

Critical asset	Source of risk	Current control measures	Vulnerability level
Depot	Vandalism	Fencing in place around permitter No overnight guards Minimal staff security training	High

Optional advanced technique:

In order to gain a fuller understanding of the interaction between an asset and the threats that may affect it, a vulnerability assessment will assist in identifying the effectiveness of current controls.



Acknowledgements

The department wishes to thank the following members of the Security and Continuity Network Risk Working Group for their contribution to this guide:

- Pete Halvorsen — Port of Melbourne Corporation
- Murray Keen — ConnectEast
- Ron Hamilton — Ventura Group
- Trevor Greer — Yarra Trams
- Paul Roadley — Metro Trains
- Annette Bury — Department of Transport, Victoria
- Katie Clydesdale — Department of Transport, Victoria
- Rachael McIntosh — Department of Transport, Victoria
- Andrew Taylor-Gammon — Department of Transport, Victoria

For any questions with regards to this document or to obtain a hard copy version, please contact the Security and Emergency Management Division of the Victorian Department of Transport on 03 9095 4053.

Version 1, May 2012

For further information in your language please call:

Arabic	عربي	9280 0758
Cantonese	廣東話	9280 0759
Croatian	**Hrvatski**	9280 0760
Dinka	**Dinka**	9280 0776
Greek	**Ελληνικά**	9280 0761
Italian	**Italiano**	9280 0762
Macedonian	**Македонски**	9280 0763
Mandarin	普通話	9280 0771
Polish	**Polski**	9280 0764
Russian	**Русский**	9280 0765
Serbian	**Српски**	9280 0766
Spanish	**Español**	9280 0767
Turkish	**Türkçe**	9280 0768
Vietnamese	**Việt-ngữ**	9280 0769
English		1800 078 387

www.transport.vic.gov.au

Authorised by the Victorian Government, 121 Exhibition Street, Melbourne.

State Government Victoria

DOT6787/12