Australian Government
Department of Defence
Defence Security and Vetting Service

Security Risk Management Workshop

Resource Guide

Version: 1.5

Defending Australia and its National Interests
www.defence.gov.au

Document Administration

DS&VS Building Security Capability Department of Defence
CP3-3 Campbell Park Offices
Po Box 7910
CANBERRA ACT 2610
Contact: 1800 DEFENCE

Version Control

Name	Security Risk Management Workshop Resource Guide
Version Number	1.5
Issue Date	August 2020
Author	Philippa Davidson & Nadine Hellawell
Review Date	February 2021

Change History

Version	Issue Date	Author	Reason for Change
1.0	July 2016	Charlie Marshall	Development
1.1	November 2016	Charlie Marshall	Pilot Amendments
1.2	February 2017	Charlie Marshall	Minor Amendments
1.3	March 2017	Charlie Marshall	Structural Change
1.4	March 2017	Charlie Marshall	Minor Amendments
1.5	August 2020	P Davidson & N Hellawell	Minor Amendments and Cosmetic Update

Contents

Document Administration 2
Introduction 4
Why are we here? 4
Pitfalls of Risk Management 5
Decision making 5
Defence Values 6
Quick thinking vs. slow thinking 6
SRM Processes 9
Security Risk Assessment 13
Establishing the Context 13
Assets and the Asset Register 15
Threat 17
Vulnerability Assessment 20
Security Risk Event Likelihood Descriptors 23
BILs 25
Asset Criticality rating scheme 25
Business Continuity 27
Security Risk Event Consequence Descriptors 29
Security Risk Events 30
Security Risk Event 6x6 Rating Matrix 31
Security Risk Management 32
Risk Register (RR) 32
Risk Evaluation 35
Risk Treatment 35
Security Controls 38
Reporting Residual Intolerable Risks 40
Security Risk Action Plan 41
Communicate and Consult with Stakeholders 42
Monitor and Review 43
Further Considerations 44
Further Resources 45

Introduction

Why are we here?

The Government has directed all Departments and Agencies to make decisions that are transparent, accountable and defensible. A Government-wide approach to risk management supports good decision-making.

Under legislation the Government's requirements are embodied under the *Public Governance, Performance and Accountability Act* (PGPA). The Government's policy guidance is outlined in the Protective Security Policy Framework (PSPF). While the PSPF stipulates security risk management as a mandatory requirement, it does not detail how Defence will undertake Security Risk Management (SRM).

This workshop provides an introduction to Defence methodology, tools and templates to assist the security practitioner to fulfil these requirements.

The Defence Security Principles Framework (DSPF) is focused on principles, risk management and effects. Under a principles-based approach, risk and control owners will have latitude to manage risks according to their context.

Risk managers and control owners are supported by tools that inform decision making. These tools enable and empower them, as accountable managers of security risk, to make informed risk decisions and meet the outcomes required by Defence – we will step through these concepts and tools today.

The Defence Security and Vetting Service website provides advice and templates that will assist you with most aspects of Security Risk Management

Defence Risk Management Policy

Defence will promote and maintain a positive risk culture in which all personnel have a shared understanding of risk. Defence personnel are expected to engage with and manage risk by considering risk management in all activities. They are to integrate risk management into all planning, approval, review and implementation processes.

For more information about the policy read the Defence Risk Management Framework

Pitfalls of Risk Management

"Risk assessment is a subjective, unpredictable blend of logic and gut feeling, generally with the latter dominating the former. On the surface, risk management might appear to be a simple, straight forward process. But in practice, people turn out to be astonishingly bad at both assessing and managing risks, and they are rarely equipped with the knowledge and skills to carry it out. Perception of risks is shaped by many personal factors, including experience, current agenda, personality, gender, age, culture and religion. It must be concluded that risk management is likely to remain a flawed and inconsistent management technique. Neither future events, not their business impact, can be predicted with any degree of certainty. And the process of reducing highly complex risk scenarios to single paragraph descriptions and scores based on course scales will limit its value as a reliable indicator.

Risk management is best employed as a decision-support tool, rather than a decision-making one.
Business managers cannot be expected to make big decisions on complex issues based on output of a simple calculation. But such assessments will help to support decisions based on a richer set of considerations. Risk management provides valuable supporting evidence that a methodical analysis of known hazards and future risks has taken place."[1]

Decision making

In Defence, decision-makers often need to know the basis and the context of decision-making for both members of the ADF and APS employees.

A decision-maker is the person who makes a decision about a set of factors that leads to a result. In Security Risk Management (SRM), decisions fall into two distinct categories; those decisions that have a straightforward or mathematical basis, and; those that require a more considered approach. The former category may be surmised as objective, while the latter more subjective. Decision-makers in SRM all too often make the mistake of attempting to make all decisions based around the simplest, mathematical path, for that is the easier option in terms of thought and effort. The resulting Security Risk Assessment and Risk Action plan may then reflect this effort and not be the best outcome for your purposes and for Defence.

[1] David Lacey, (2010) "Understanding and transforming organsizational security culture", Information Management Computer Security, Vol. 18 Iss: 1. pp.4-13

Defence Values

Decisions made are all under the same framework of Defence values. The Defence Senior Leadership Group has committed to these Defence-wide Values, they are:

	Professionalism is striving for excellence in everything we do
	Loyalty is being committed to each other and to Defence
	Integrity is doing what is right
	Courage is the strength of character to honour our convictions (moral courage) and bravery in the face of personal harm (physical courage)
	Innovation is actively looking for better ways of doing our business
	Teamwork is working together with respect, trust and a sense of collective purpose

Quick thinking vs. slow thinking

Daniel Kahneman is his text 'Thinking Fast and Slow', differentiates decision making into two distinct categories he describes as System 1 and System 2, but in essence are:

a) Decisions made in quick time, based on intuition with no questioning of assumptions
b) Decisions made in slow time, based on available evidence and fully reasoned and defensible.

He explores the difference between the systems and their importance, and tellingly concludes that the intuitive System 1 is 'more influential than your experience tells you, and is the secret author of many of the choices and judgements you make'.

An example of quick (thoughtless) thinking is demonstrated with the following question:

A bat and ball cost $1.10.
The bat costs one dollar more than the ball.
How much does the ball cost?

Using System 1, the immediate answer is easy $0.10. But this answer is wrong, highlighting the need to take decision making and apply a more considered approach.

Try the following other examples:

- How much dirt is there in a 14x12x10 metre hole?
- If you are in a race, and overtake the person in the second place, what place are you in now?
- Say “Silk” five times. Spell SILK. What do cows drink?
- Before Mount Everest was discovered, what was the tallest mountain in the world?
- How does Bill go eight days without sleep?
- What five letter word becomes shorter when you add two letters to it?

Unconscious Bias

Bias is a particular tendency / trend / inclination / feeling / opinion that is preconceived or unreasoned. When we make decisions, often our unconscious bias comes into play. There are four main categories of bias:

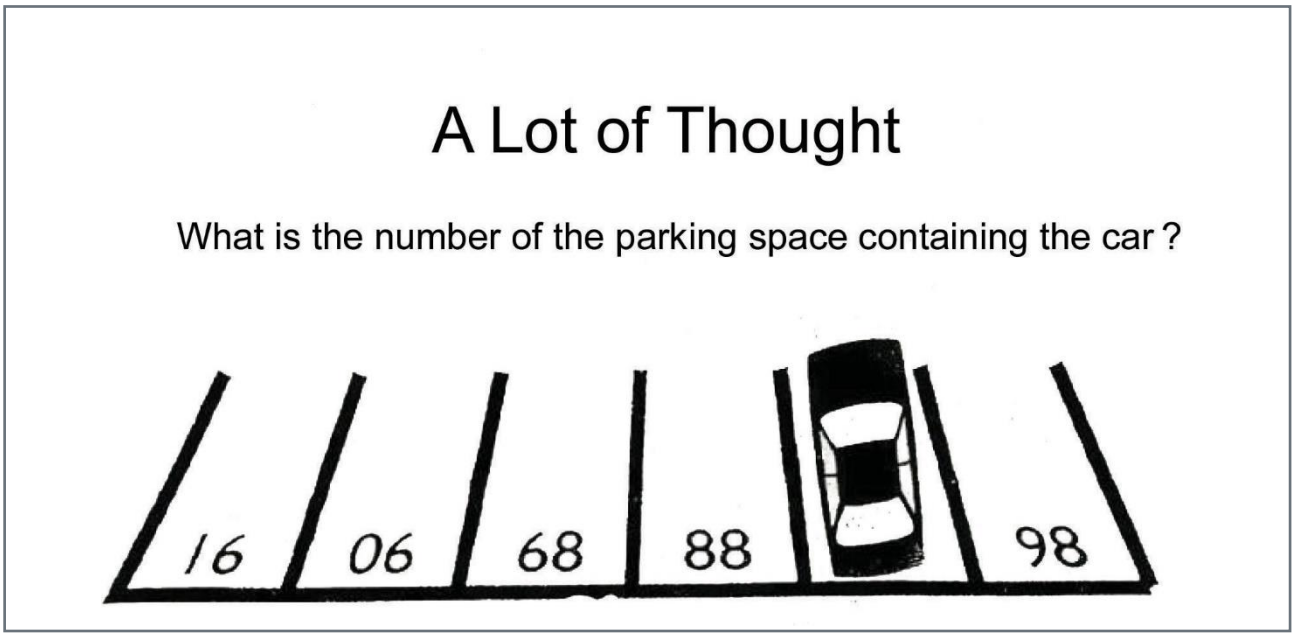
a) Cognitive Bias – where mental ‘short-cuts’ impact decisions
b) Situational Bias – where situations impact decisions
c) Personal Bias – where factors that have helped shape your life impact your decisions
d) Confirmation Bias – where evidence that support your decisions becomes the only evidence sought

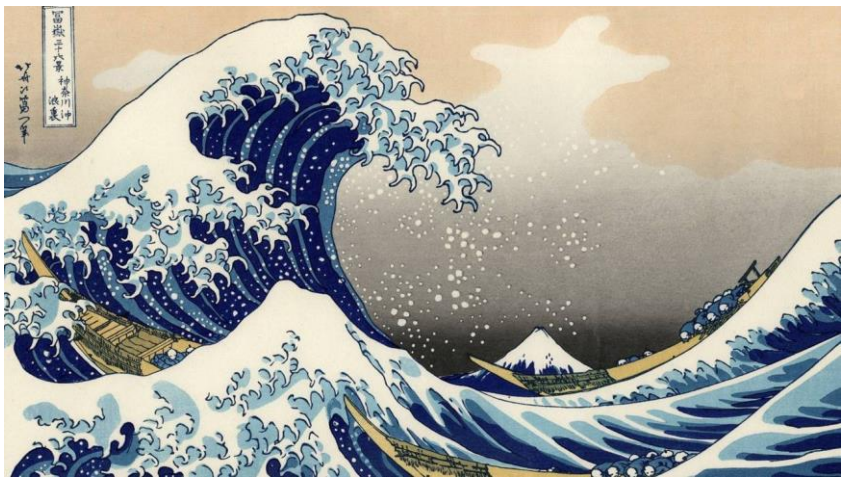
Managing Bias

Three aids in managing bias:

a) Acknowledge the bias
b) Application of critical thinking to assumptions / past thinking
c) Perspective shifting

An example of shifting perspective is illustrated here:





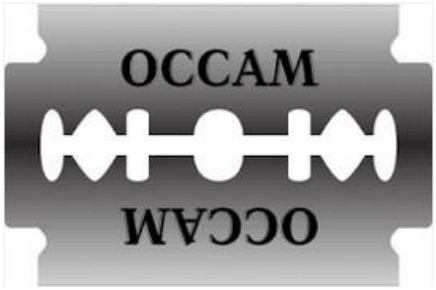
Decision making process

a) The framework: decision-making tools and processes are determined *prior* to undertaking decision based work.
b) Understanding biases / becoming situationallyaware
c) Applying critical thinking / be willing to challenge assumptions
d) Gather and utilise available information

MINDSET: In decision theory, a mindset is a set of assumptions, methods or notations held by one or more people (or group of people) that is so established that it creates a powerful incentive within these people or groups to continue of adopt (or accept) prior behaviours, choices or tools.

Other decision-making considerations

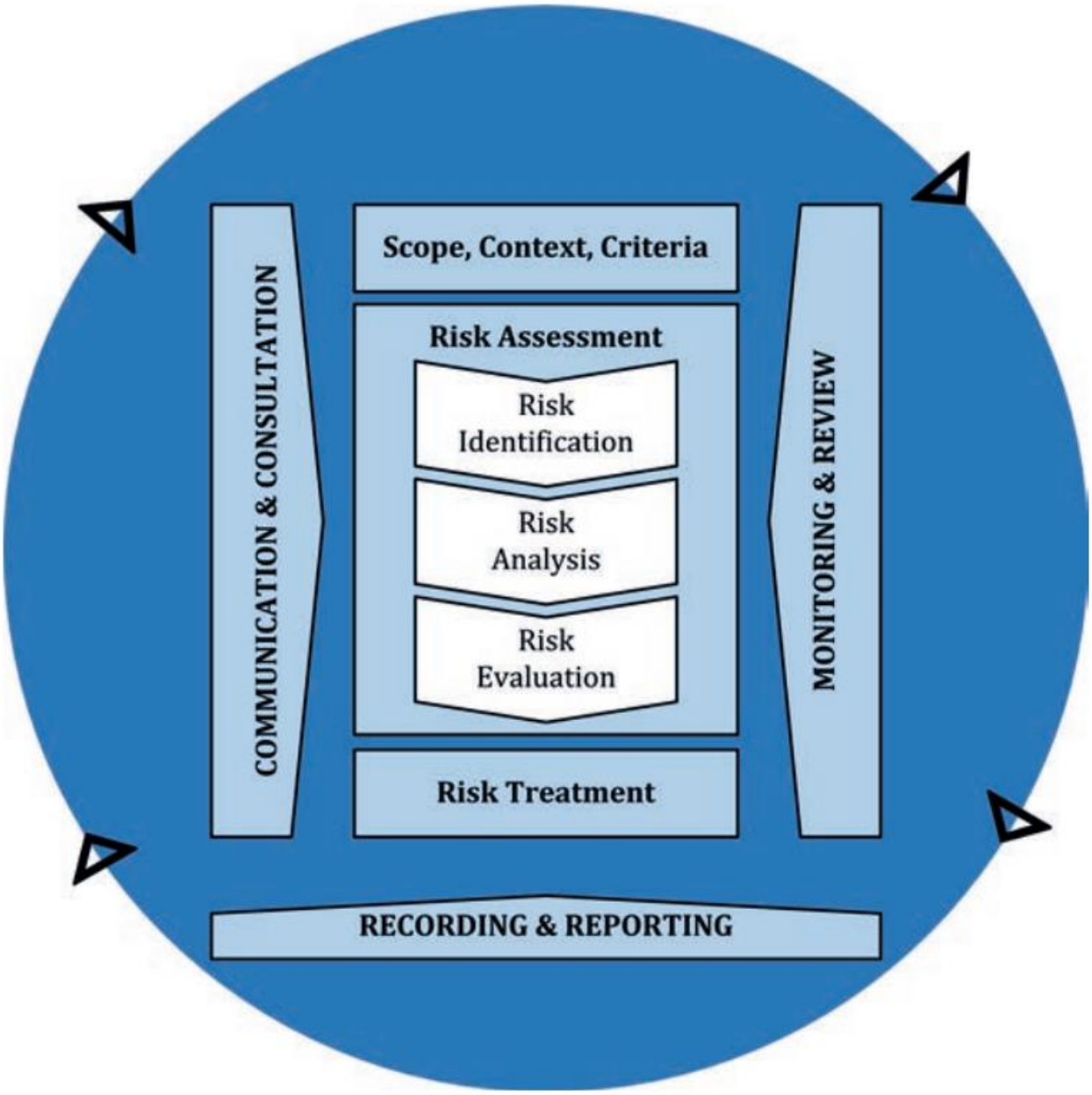
Keep Occam's Razor in mind:
"Among competing hypotheses, the one with the fewest assumptions should be selected" and please note how this differs from the KISS principle.



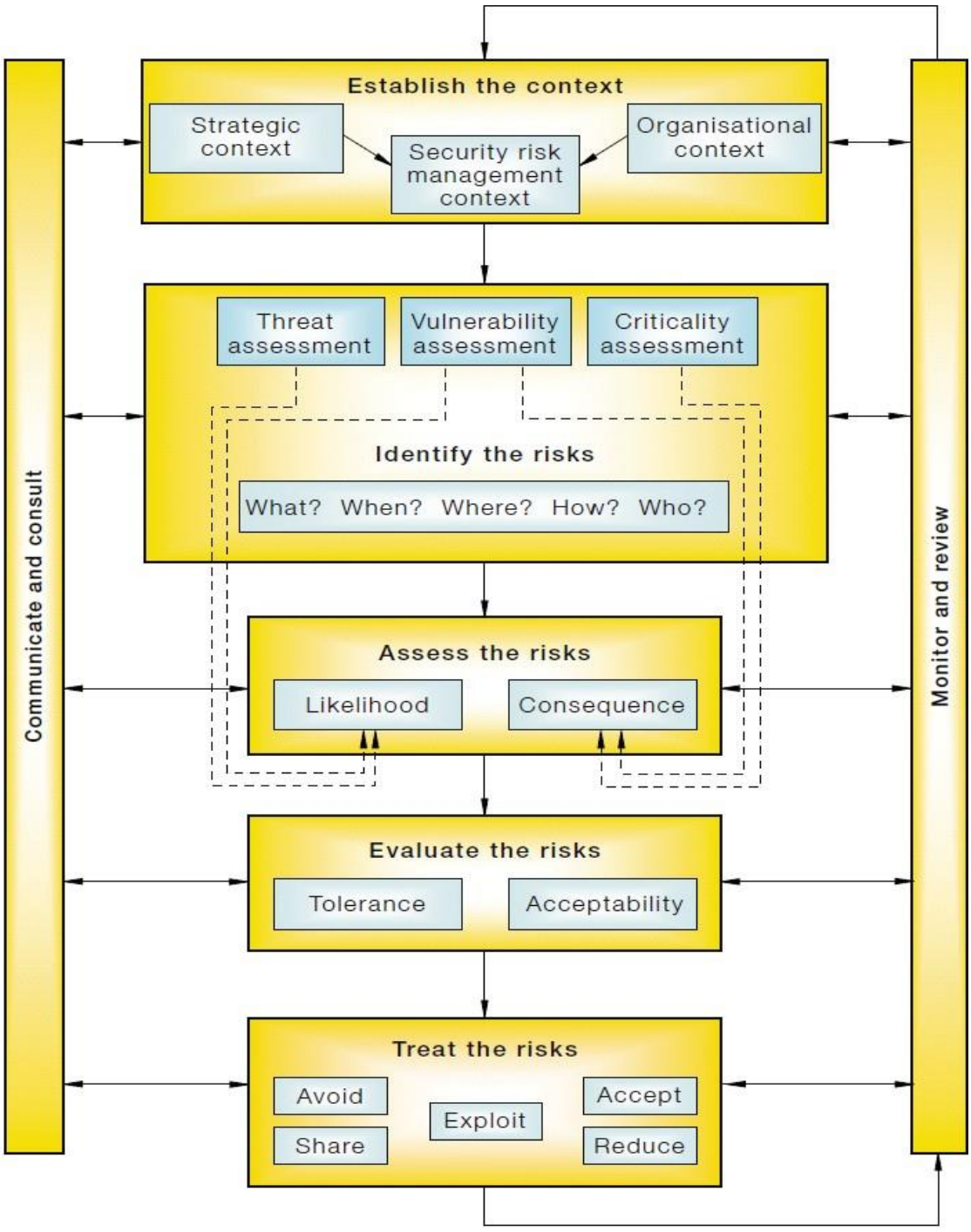
Beware decisionparalysis
"A good plan, executed now, is better that a perfect plan executed next week."

SRM Processes

ISO31000:2018

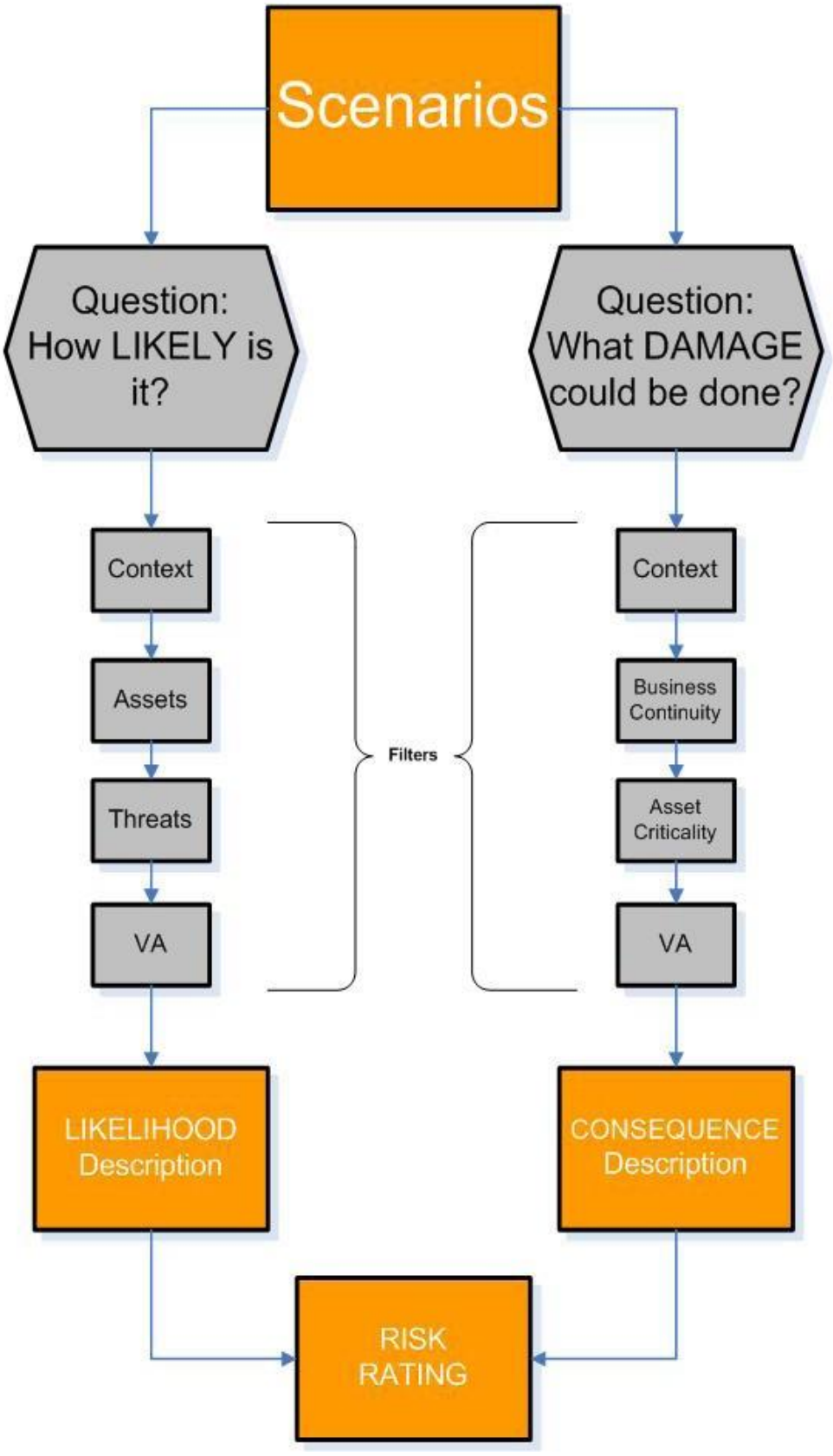


HB 167:2006

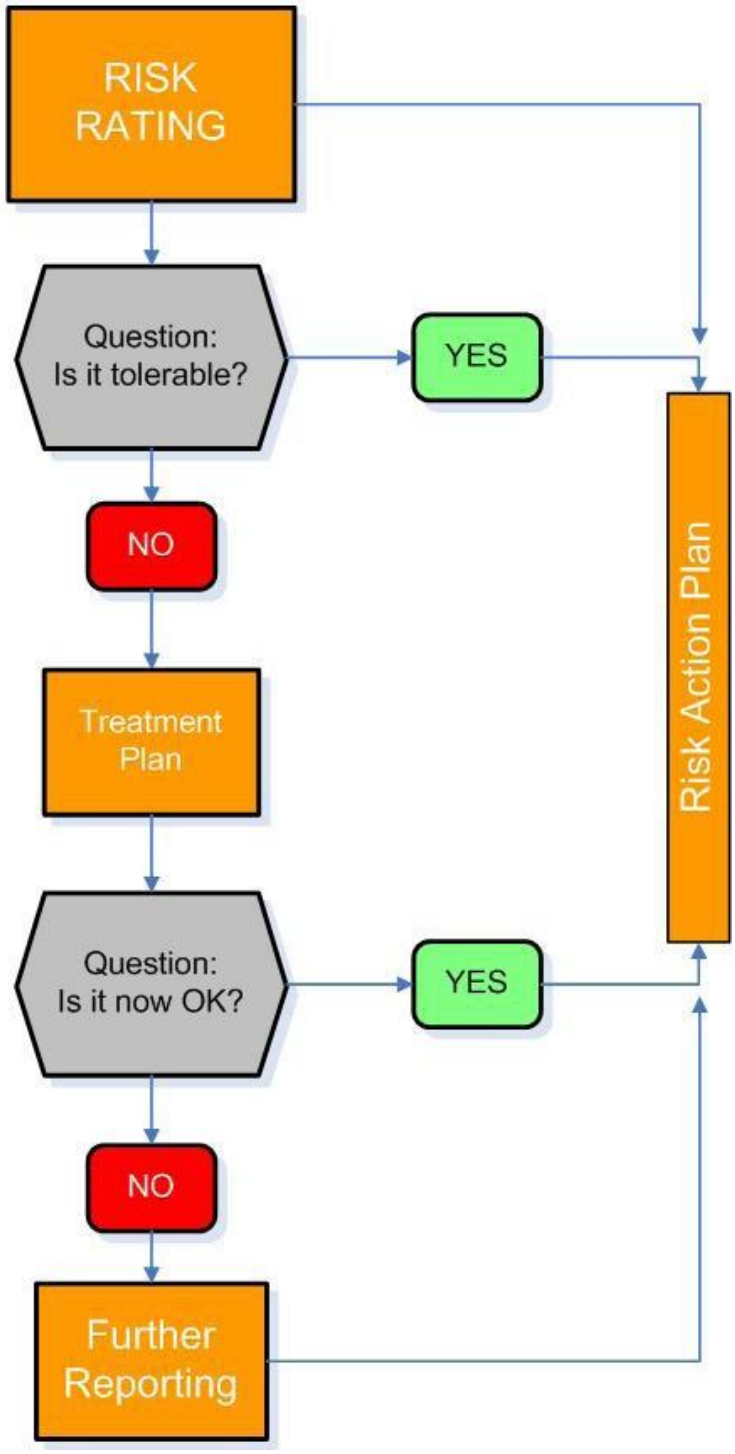

Establish the context
Strategic context
Security risk management context
Organisational context
Threat assessment
Vulnerability assessment
Criticality assessment
Identify the risks
What? When? Where? How? Who?
Assess the risks
Likelihood
Consequence
Evaluate the risks
Tolerance
Acceptability
Treat the risks
Avoid
Exploit
Accept
Share
Reduce
Communicate and consult
Monitor and review

Security

Risk Assessment



Security
Risk Management



Security Risk Assessment

Establishing the Context

Establishing the context is a starting point to the development of the security plan. The Security Practitioner will outline what the organisation does, the environment within which it operates, and the reasons why the security plan is being developed.

HB 167:2006 outlines a detailed plan for establishing the context, and breaks down the context into three major elements:

- Establishing the external context within which the organisation operates;
- Establishing the internal context of the organisation;
- Establish the security risk management context for the organisation.

The Establishing the Context section of the security plan works best when it is a simple and direct document that can be read and understood by all stakeholders.

Part I: Strategic (External) context

This part of the context refers to the 'larger picture' around Defence and may (or may not) be independent of the Security Practitioner's organisation's context. "The term 'external context' refers to gaining an understanding of the external environment in which the organisation is operating or may be operating in the future."

The scope of this context is simply to identify what environment the organisation is currently operating in (or will do so in the future): the important concept here is to limit the context to the security risk context.

Practical Strategic Context Questions

The following are provided to the Security Practitioner as a guide to navigating the contextual requirements of security planning:

Are there any relevant political concerns that could affect the organisation's operations? Examine the larger political position of the Federal, State or Local government as required. Is there Government (in) stability that may affect the organisation's ability to function fully? What group may wish to disrupt any function that the organisation has (ie Terrorist or Crime group)?

Are there any legislative concerns that may arise due to the organisation's operations? Reflect on whether the Government, be it Federal, State or Local, has affected changes that will in turn affects the organisation. Has any legislative stance from these Government bodies affected changes, adverse or otherwise, on the population that in turn would affect the organisation?

How does the organisation fit into the existing social environment (both nationally and locally)? Reflect on the social aspects on the environment surrounding the organisation; how demonstrations affect operations, whether there are local tensions that come into play and whether these tensions have been address by Government at all.

What socio-economic groups exist around local operations? In regards to local operations surroundings: what socio-economic conditions surround the operating areas; are there any implications for having an economic environment of this sort?

What levels of social infrastructure exist in the operating environment? Investigate the various aspects of infrastructure – police and response times, hospitals/clinics and medical response times, Emergency Services and their response abilities and times. Other considerations include operational logistics and access as well ingress/egress from the organisation.

What neighbouring factors (Groups, land use etc) must be taken into consideration? Investigate the area(s) surrounding the organisation(s). Does the surrounding area contain any community meeting / rally points; are there areas where illegal activities are known to occur? Are there action groups that are interested in the organisation's operations?

Who are the key external stakeholders and what relationship does your organisation have with them? Consider the broader picture; community groups, the make-up of the community itself, union organisations, the media; are there any new or emerging groups to consider as well? Significant developments between these groups that relate to interdependency and redundancies may need to be considered.

Part II: Organisational (Internal) context

This part of the context refers to the organisation itself. The purpose of the Organisational context is to "…create an agreed understanding of the organisation's internal environment and issues that may influence the nature of the security risk exposures or the activities being undertaken to manage them."

Practical Organisational Context Questions

What does the organisation do? This asks for situational and operational awareness; the Security Practitioner may be aware of what an individual unit is doing, but what about bases that have many Resident Units; how does the base fall into the larger picture of Defence?

Why does the organisation do it? Be aware not only the immediate work of the base/unit, but also the larger picture of how that work fits into Defence's operational requirements, i.e. how does it fit into Defence capability.

What does the organisation use/need to do it? This takes into consideration not only items, people and places required in order to be operational currently but also any developments that may be occurring that would influence the security context into the future. It also includes the notion that operations may be affected by the inability of another area to operate.

Who are the stakeholders and what are their interests? Look at the key participants and those with an interest in the security planning process. It is important to note, however, that stakeholders can make judgements about risk based on their perceptions of risk; these perceptions can vary due to differences in values, needs, assumptions, concepts and concerns of stakeholders. As their views can have a significant impact on the decisions made, the stakeholders' perceptions should be identified, recorded and taken into account in the decision making process.

What affects the immediate working environment? What is the nature of the organisation, what are its physical assets and protection systems, what comprises its personnel, what asset appreciation exists, and what are the personnel protection systems in place, what ICT systems does the organisation work with and what are the ICT protection systems?

Part III: Security Risk Methodology Context

Prior to undertaking the SRM process, endorsement of SRM tools, processes and terminology should be gained. It is important that this is done at this stage of the security risk methodology in order to avoid conflicts and confusion later in the SRM process.

There are many different evaluative tools that require defining, however to aid the Security Practitioner, there are many tools available that have already done this work. Such tools are available on the DSVS intranet portal, on the DPN or the DSVS presence on the DSN. Whichever definitional statements are used, it is paramount that the Security Practitioner engages key stakeholders in agreeing to terms prior to undergoing the SRM process.

The provided workshop tools are indicative and are included as examples for Security Practitioners.

Assets and the Asset Register

Understanding what you hold and what you are trying to protect is a good place to start your security risk managing. When compiling a list of risk events (scenarios) of how threats attempt to interact with assets, it's good to remind yourself of what assets you actually have – and while this may sound like common sense there can be difficulties in achieving this:

- Your resident units may not have assessed their assets
- Your event may be managed by an external organization
- Your project may not have identified all the external dependencies

What are we securing?

Defence owns a wide variety of assets that require some form of protection against the threats. For a threat to harm Australian Government or Defence assets (including people, information, physical assets, capability and/or reputation), there must be some kind of value or importance attached to the asset beyond its dollar value. If there was no other value, there would be no ideological basis for the threat, and therefore no requirement to apply additional protective security.

This gives us the concept of a 'security-protected asset' - an asset that requires more than just standard 'fire and theft' protection.

What are our assets worth?

Security-protected assets are 'graded' to show how valuable they are to the Australian Government or Defence. The grading is based on the consequence to Defence capability or the National interest if the assets were to be compromised, lose integrity or become unavailable for use. The grading of an asset is represented by a Business Impact Level and if required, a classification (consequence of compromise).

Assets are identified as being people, information, physical assets, capability and/or reputation (the last two being difficult to define from a Security Risk Management point-of-view).

Asset Register

A simple Asset Register collects together the types of assets across your particular unit (or equivalent) and any additional date you may feel is relevant. EIG are responsible for base planning and resulting documentation. Check with your Base Planning Staff (in the BSM's office) for the base's asset register location. For Projects, check with the Project Manager and the Project Security Working Group, and for Activities, check with previous documentation and the applicable participating Units involved.

In the following example, sample column headings are used:

	Asset Number (if available)	Asset Title	Asset Description	Asset Type[1]	Asset Importance[2]	Asset Location	Remarks
A1							
A2							
A3							
A3							
A4							
A5							
A6							
A7							
A8							
A9							
A10							
A11							
A12							

[1] Expressed as either people, information, physical assets, capability and/or reputation
[2] Expressed as: BIL 1-5

Threat

An understanding of threats to your security will allow you, and other decision makers, to plan against credible risk scenarios. A threat picture directly affects how likely something is to occur, and is collated from historic, objective and available information – not from 'gut feel' or perceived information.

The Threat Concept:

Desire + Expectation of Success = INTENT
Resources + Knowledge = CAPABILITY
INTENT + CAPABILITY = THREAT

Desire: An agenda, active history, current activities or merely inimitable interests that indicate the desire to create harm to Defence interests.

Expectation of Success: The threat's perception of its ability to overcome the security controls already in place to protect Defence.

Resources: This includes resources available to the threat including from its own organisation, the presence and location within Australia.

Knowledge: The threat's knowledge includes not only availability of information of intelligence value, but also modus operandi in terms of overt/covert, human/technical or even professional/ unprofessional knowledge.

INTENT: Is the degree to which the threat source has demonstrated its role, aims, intelligence collection requirements and history of even minimal activity inimical to Defence interests.

CAPABILITY: Is defined as a combination or resources and knowledge. It encompasses the adequacy of the structure, size, organisation, modus operandi, disposition and finances of the threat source as well as the opportunities available to it.

Sources of Threat:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

Threat Context understanding questionnaire

The following questions may help guide your thinking as to your current threat picture. It is meant as an aid tool only, and is required to be considered along with DS&VS developed threat material.

PART 1 - Introduction	
Where do you work?	
Why do you require an understanding of the Threat Context?	
PART 2 - Facility	
Describe the facility.	
What is the function(s) of the facility?	
What assets are located at your facility?	
What is the highest classification of material handled at your facility?	
What is the highest classification of communications systems located at your facility?	
Is there a plan layout of the facility available freely?	
Does the facility's security controls and procedures meet minimum standards?	
Are there any Dispensations for your facility?	
Do any staff require extra protection due to their duties?	
Do you have any VIPs working at your facility?	
PART 3 – Activity	
What activity is taking place?	
What is the location of the activity?	
What is the reason for the activity?	
Who is participating in the activity?	
Is there foreign participation in the activity?	
Is there an expectation of disruption caused by the event?	

PART 4 – Threats	
Do you envisage any interest from a threat source?	
Is there foreign participation in the facility/ activity/project?	
What security incidents have previously been noted?	
Have any acts of vandalism / malicious damage occurred?	
Has the facility / activity been subject to any demonstration activity?	
Have there been any known information leaks?	
Have any incidents adversely affected the security culture?	
Are there issues that have led to disgruntlement?	
Have there been known issues of clashing with security policy?	
Have there been any unauthorised disclosures to the media?	
How would you rate morale at the workplace?	
General Comments	
Details of person completing Threat Context understanding	

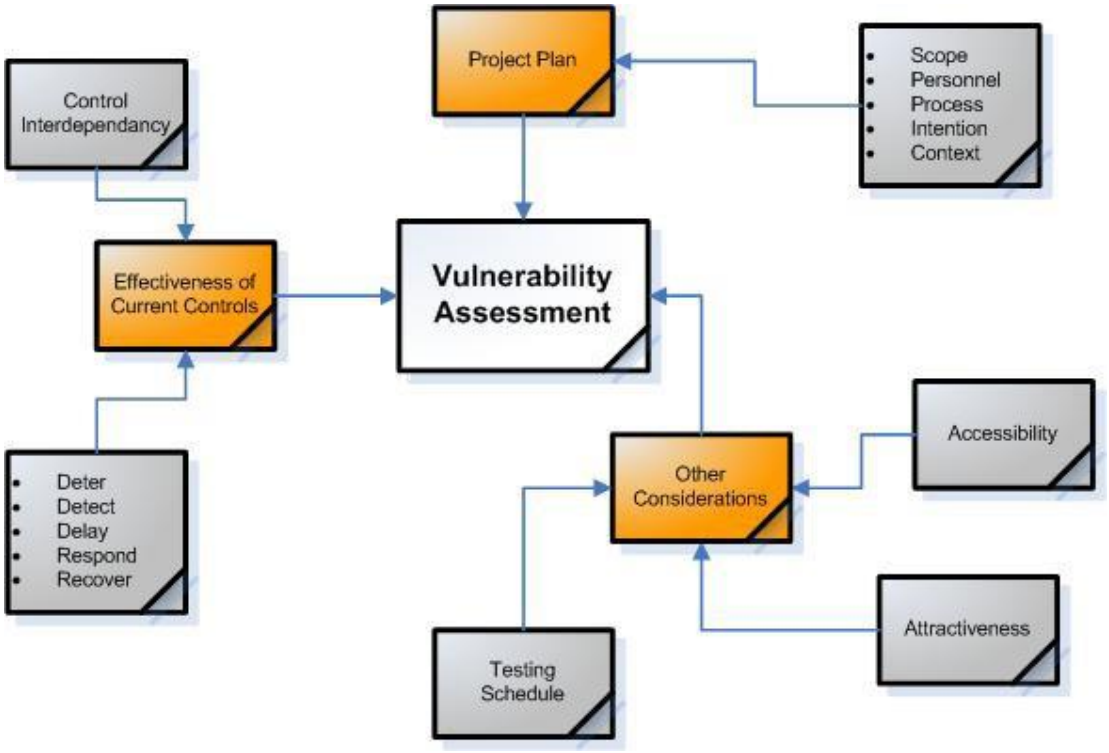
For more information on threats see Defence Security Threat Environment

Vulnerability Assessment

A Vulnerability Assessment (VA) is an attempt to understand what current security controls you have and how effective they are at doing the job you expect of them.
This is important because there may be security controls that:

- You are unaware of (such as sub-contractor's own security protocols)
- You have not considered (such as evacuation and lock down procedures)
- Are improperly maintained (such as the alarm system has never been tested)

The fundamental output of the Vulnerability Analysis (VA) is a better understanding of the potential interaction of the threat with the critical assets of the organisation, community, or individual. Such information will inform both the subsequent identification and assessment of security risk. At times some measurement of vulnerability may be required.



Depending on the complexity of Vulnerability Assessment required, the starting point for the VA should be a Project Plan that identifies key components and outcomes expected by conducting the VA.

No matter the complexity of VA, an assessment of the effectiveness of the current controls (ECC) in managing the threat's interaction with the critical asset is a key component of understanding vulnerability. While traditionally the existing controls are measured against their ability to deter, detect, delay, respond and recover, an additional consideration must be given to how the controls depend upon each other.

Vulnerability exists where controls are easily accessed and/or where the facility / asset is particularly attractive (in value terms). Vulnerability exists where controls have not been tested; types of testing may include desk-top or penetration testing.
Penetration Testing: If penetration testing is to be used, then prior approval must be sought, clear outcomes and terms-of-reference drawn up.

Effectiveness of Current Controls

ECC must include information and analysis on the: deterrence ability of the control; degree of hardness of the control; the control's ability to withstand an attack. In Defence this is portrayed as the control's ability to deter, detect, delay, respond and recover. In a spreadsheet it might look like this:

Control:					
Ability to:	Deter	Detect	Delay	Respond	Recover

Other considerations:

- Currency of the control
- Test schedule of the control
- Last time the control was tested
- Has the control been modified from its intended purpose

Please note that security controls are not simply physical controls (such as locks and alarms) but include other considerations (such as Security Standing Orders and the security culture of an organisation)

Interdependency

Consideration must be given to each control's dependency and support for other security controls. For example, the access control point for an organisation incorporates a swipe card (DCAC) access point linked to an alarm system. If one of those controls is compromised in some way (the alarm system has not been adequately tested and is faulty) this will compromise the effectiveness of the whole access control. To be effective, both the swipe and the alarm controls must be working properly and tested regularly.

Vulnerability Matrix

A table that uses definitional statements to supply a vulnerability level such as:

Vulnerability Level	Assessment Criteria
Very high/Extreme	• Controls are non-existent, critical and urgent improvements have been identified. • it is almost certain that controls will be breached or fail. • There is recent evidence of widespread control failures. • There are no contingencies in place, severe disruptions to the business are likely.
High	• Controls are largely ineffective, significant areas for improvement are identified. • There is an increasingly likely probability of the controls being breached. • There is recent evidence of significant numbers of controls being breached. • Few contingencies are in place and significant disruptions to the business are expected.
Moderate	• The majority of controls are functioning, but a number of areas for improvements are identified. • There is a moderate probability of the controls being breached. • There is recent evidence of a small number of controls being breached. • Contingencies are in place for only a few key areas of the business to manage potential disruptions.
Low	• Controls are effective, but small improvements could be made. • There is a low probability of the controls being breached in the future. • There are no recent examples of controls being breached. • Adequacy of the controls is assessed on a regular (minimum annual) basis. • Contingencies are in place for key areas of the business to manage potential disruptions to the business.
Very Low	• Controls are optimum and are sustainable. • There is an extremely low probability of the controls being breached in the future. • There are no previous incidents of the controls being breached. • Adequacy of the controls is assessed on a regular and frequent basis. • Comprehensive contingencies are in place to manage most potential disruptions to the business.

Security Risk Event Likelihood Descriptors

Likelihood Descriptor	Definition
Extreme	Credible Specific intelligence indicates a current intention, capability and planning to conduct action against <insert subject>. Action is almost certain. Could happen within days to weeks.
High	Credible intelligence indicates a current intention and capability to conduct action against <insert subject>. Action is assessed as likely. Could happen within weeks to months.
Medium	Credible intelligence indicates that <insert subject> is a potential target of threat vectors with an intention and capability to undertake action. Action is assessed as feasible and could well occur. Could occur within about a year.
Low	Credible intelligence indicates that <insert subject> is a possible target of threat vectors who have either limited intent or limited capability or both. Action is assessed as possible, but is not expected. Could happen in the next several years.
Very Low	Credible intelligence indicates that threat vectors currently have little capability or intent to target <insert subject>. Action is assessed as unlikely. Unlikely even in the medium term.
Negligible	There is no indication of any threat to <insert subject>. Action is assessed as very unlikely. Almost impossible even in the long term.

Likelihood Language Confusion

Australian Government

Australian National Security

Search...

Home | Media and publications | Security and your community | Terrorist organisations | What Australia is doing

You are here > > **Australian National Security** > > **Security and your community** > > National Terrorism Threat Advisory System

Security and your community

- Australia's Strategy for Protecting Crowded Places from Terrorism
- Active Armed Offender Guidelines for Crowded Places
- Chemical Security
- Frequently asked questions
- Improvised Explosive Device Guidelines for Crowded Places
- National Terrorism Threat Advisory System
- What I can do

Related links

- National Security Hotline
- States and territories
- National Security Campaign
- Newsroom
- Publications
- 26 November 2015—New National Terrorism Threat Advisory System—Minister Assisting the Prime Minister on Counter Terrorism and Attorney-General joint media release

Related websites

National Terrorism Threat Advisory System

Australia's current National Terrorism Threat Level is PROBABLE.

PROBABLE

- Current advice to the public
- Video—Overview of the National Terrorism Threat Advisory System

The National Terrorism Threat Advisory System is a scale of five levels to provide advice about the likelihood of an act of terrorism occurring in Australia:

When the threat level changes, the Australian Government provides advice on what the threat level means, where the threat is coming from, potential targets and how a terrorist act may be carried out.

The National Terrorism Threat Level is regularly reviewed in line with the security environment and intelligence.

It is important to be aware of the current threat level and to report any suspicious incidents to the National Security Hotline on 1800 1234 00.

More information is available in the following fact sheet:

- National Terrorism Threat Advisory System fact sheet [PDF 216KB]
- National Terrorism Threat Advisory System fact sheet [DOCX 287KB]

CERTAIN

EXPECTED

PROBABLE

POSSIBLE

NOT EXPECTED

The Australian security environment

Australia's National Terrorism Threat Level remains **PROBABLE.** Credible intelligence, assessed by our security agencies, indicates that individuals or groups continue to possess the intent and capability to conduct a terrorist attack in Australia. The public should continue to exercise caution and report any suspicious incidents to the National Security Hotline by calling 1800 123 400. Life-threatening situations should be reported to the police by calling Triple Zero (000).

International terrorist groups have proven adept at using their extremist ideology to motivate lone actors and small groups to use violence in their home countries. Individuals in Australia can be influenced directly by overseas-based extremists as well as by a wide range of

The National Terrorism Threat Level is a scale of five levels that tells the public about the likelihood of an act of terrorism occurring in Australia. Whenever the Government makes a change to the National Terrorism Threat Level it will explain why there is a change. The National Terrorism Threat Advisory System will inform Australians about the likelihood of an act of terrorism occurring in Australia and enable authorities, businesses and individuals to take appropriate measures for their own safety and security as well as that of their family, friends and associates. The National Terrorism Threat Level also provides an indicator to government agencies enabling them to respond appropriately with national threat preparedness and response planning. This ensures that an appropriate level of precaution and vigilance is maintained to minimise the threat of a terrorist incident.

The Australian Government regularly reviews the security environment and the Threat Level.

BILs

Business Impact Levels (BILs) are Defence's way to categorise assets in ascending order of importance, using a five point scale (where the higher the number, the more important the asset). BILs measure the impact to the national interest and Defence capability arising from:

- Confidentiality (unauthorized disclosure of information)
- Integrity (improper modification)
- Availability (it's been lost or ceases to function)

Use Table 1 Business Impact Levels tool from the PSPF to assist you in categorising your assets.

Asset Criticality rating scheme

Some assets are not assigned a BIL, but are still to be considered in how mission-critical assets are. This consideration is so decision makers can assess the consequence of all assets in relation to confidentiality, integrity and availability

A table that uses definitional statements to supply a criticality rating such as:

Criticality	Impact on organisation	Impact on groups (e.g. stakeholders/community)	Impact on individuals (e.g. employees, guests, residents etc)
Extreme	Loss of asset results in: • complete cessation of all functions. • no short term recovery capability. • serious prolonged reputational loss (extending for many months). • Financial loss >30% of NOPBT/EBITDA	Loss of asset results in: • severe prolonged loss of amenity (extending several months). • severe community outrage at loss of service. • extreme financial distress (e.g. loss of >30% revenue potential of businesses or local government.	Loss of asset results in: • catastrophic safety incidents (multiple serious casualties, fatalities). • long term major financial loss (e.g. loss of employment).
High	Loss of asset results in: • complete cessation of one or more key functions. • no short term recovery capability. • serious prolonged reputational loss (extending for weeks to months). • Financial loss >10% of NOPBT/EBITDA	Loss of asset results in: • severe prolonged loss of amenity (extending weeks). • community outrage at loss of service. • >10% revenue potential of businesses or local government.	Loss of asset results in: • multiple serious safety incidents (several serious casualties, or a fatality). • mid to long term major financial loss (e.g. prolonged stand down of employment - over several months).
Significant	Loss of asset results in: • cessation of one or more key functions. • limited short term recovery capability. • reputational loss on specific operations (extending for weeks to months). • Financial loss >5% of NOPBT/EBITDA	Loss of asset results in: • loss of amenity (extending days to weeks). • community upset at loss of service. • >5% revenue potential of businesses or local government.	Loss of asset results in: • major safety incidents (multiple injuries requiring medical attention). • financial losses extending over several weeks (e.g. contracts put on hold).
Moderate	Loss of asset results in: • reduced effectiveness of one or more key functions. • short term recovery capability is possible. • reputation loss (extending for days to weeks). • Financial loss >2% of NOPBT/EBITDA	Loss of asset results in: • partial or temporary loss of amenity (days). • community disquiet at loss of service. • >2% revenue potential of businesses or local government.	Loss of asset results in: • safety incidents requiring first aid treatment). • long term major financial loss (e.g. loss of employment).
Low	Loss of asset results in: • little impact on functions. • recovery is possible immediately. • little measurable reputational loss. • Financial loss <2% of NOPBT/EBITDA	Loss of asset results in: • little loss of amenity. • little negative reaction arising from loss of service. • <2% revenue potential of businesses or local government.	Loss of asset results in: • insignificant safety implications. • no appreciable financial loss.

Business Continuity

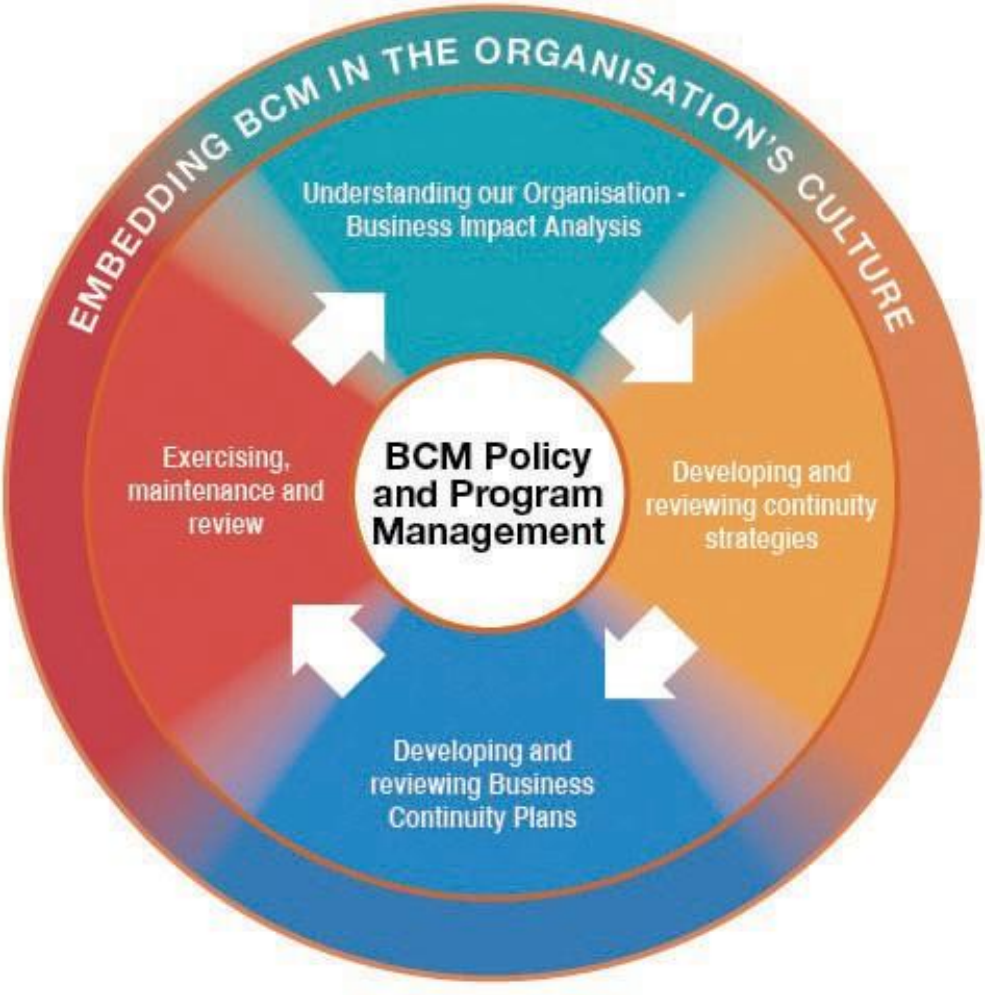
From the DS&VS website:

Business Continuity Management (BCM) is a holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience and the capability for an effective response that safeguards its critical functions and interests.

Continuity of essential Defence processes and decision making capabilities during emergencies or incidents that disrupt normal operations is critical. To ensure that Defence has the capability to continue to deliver essential functions during an incident, business continuity plans and other continuity arrangements must be in place.

BCM forms a fundamental mission of managers and commanders at all levels.

Continuity plans affect consequence ratings in Security Risk Management. For example, if your health unit relies on a generator for conducting its main business, and a risk event is considered that affects the generator, the continuity plan that accounts for the use of a back-up generator must be taken into account.



The Following is the title page from E&IG's Base Planning Documentation.

BUSINESS CONTINUITY PLAN [INSERT BASE/PRECINCT NAME]

Business Continuity Plan Approval:

Endorsed by:

Name: *[Insert Base Support Manager]*

Title:

Organisation:

Date:

Approved by:

Name: *[Insert Senior ADF Officer]*

Title:

Organisation:

Date:

[Insert base/precinct] Business Continuity Plan Version Control

BCP Name	
BCP Status	*[Draft or final version]*
Version Number	
Issue Date	
Author	
Review Date	

Change History

Version	Issue Date	Author	Reason for Change

Distribution List

Security Risk Event Consequence Descriptors

Consequence considers what **the most likely outcome** of a Risk Event might be. This is **not the best or worst case scenario**.

	Minimal	Minor	Moderate	Major	Severe	Catastrophic
People	Injuries requiring first aid treatment with little or no impact on organisational performance.	Moderate injuries with limited impact on organisational performance.	Serious injuries resulting in the reduction of business performance and ability to achieve outcomes.	Extensive injuries, possibility of deaths, resulting in reduction of organisational performance and /or ability to achieve Defence's outcomes.	Multiple deaths and injuries impacting on organisational performance and /or ability to achieve Defence's outcomes.	Mass fatalities or casualties sufficient to stop Defence's ability to achieve its outcomes.
Assets	Damage to physical assets or infrastructure resulting in inconvenience but no impact on achievement of organisational objectives.	Damage to physical assets or infrastructure resulting in manageable delays in achieving organisational objectives.	Damage to physical assets or infrastructure impacting on delivery of Defence's outcomes.	Destruction or damage of physical assets or infrastructure causing significant impact on delivery of Defence's outcomes.	Destruction or damage to physical assets or infrastructure sufficient to prevent delivery of a Defence outcome for a protracted period.	Destruction or damage to physical assets or infrastructure sufficient to prevent Defence's continued operation.
Information	Loss or compromise of classified or other Defence information. No impact on routine business.	Loss or compromise of classified or other Defence information. Limited impact on routine business.	Loss or compromise of classified or other Defence information reducing Defence's ability to achieve its outcomes.	Loss or compromise of classified or other Defence information that significantly impacts on Defence's ability to deliver its outcomes.	Loss or compromise of classified or other Defence information resulting in the inability to deliver Defence's outcomes for a protracted period.	Loss or compromise of classified or other Defence information resulting in permanent loss of Defence's capacity to deliver its outcomes.
Capability	No effect on capability. Impacts handled within local resources.	Limited effect on capacity to carry out a Defence function.	Damage reducing but not denying availability of a function.	Partial loss of, or damage to, a capability for which alternative solutions are readily available.	Substantial loss or damage to a key capability which cannot be replaced for protracted period.	Loss of key operational capability sufficient to disrupt Defence's delivery of outcomes for a protracted period.
Reputation	Limited impact involving minor local issues. Freedom to operate unimpaired. Handled within local resources.	Local impact only. Freedom to operate unimpaired. Handled within local resources.	Internal inquiry required. Short term adverse media attention handled by existing business practice.	Persistent national concern requiring external independent scrutiny or protracted internal inquiry. Special arrangements required to manage impacts.	Loss of confidence in Defence affecting access to information or assets of domestic or international partners. Special arrangements required to manage impacts.	Significant damage to Government and/or international confidence in Defence's ability to deliver its outcomes and in Australia's ability to maintain its national security.

Security Risk Events

What are they?

ISO31000 and the HB167 defines an event as an 'occurrence or change of a particular set of circumstances'.

This is not a very useful definition to the topic for the security practitioner. A Security Risk Event can be considered a 'scenario', where the THREAT interacts with an ASSET somehow. There are many different 'scenarios' that can occur to your base, project or event, and so there should be an equal number Security Risk Events in the SRA. As every base, project, event differs, so should the amount of Security Risk Events.

How do I write a Security Risk Event?

Security Risk Events are a Security Practitioners way of describing how Threats could possibly interact with Defence Assets in a consequential way. These events could be actual (historical proof of them happening) or perceived (projecting a way that they could interact).

Examining the security risk management CONTEXT and considering the THREAT, CRITICALITY and VULNERABILITY assessments will enable credible potential Security Risk Events to be identified and described.

Follow this template of four factors when writing Security Risk Events:

Someone does something to an asset for the purpose of…

For example, A Maverick Individual uses a knife to stab an employee due to their disgruntlement with Defence.

Defence has a list of Security Risk Events.

Please note that the list of Defence level Security Risk Events is OFFICIAL: Sensitive.

The list supplied contains 32 Security Risk Events. These can be used by the security practitioner as a guide. Add or subtract risk events as the do/do not suit. If you are unsure of your resulting list of Security Risk Events, have DSVS local office or SSA check them for you.

Security Risk Event 6x6 Rating Matrix

A Risk Rating Matrix is comprised of an x and y axis table. The words used to fill each axis have specific definitions so as to avoid confusion (for example one person's understanding of the word 'moderate' may differ from others).

Likewise, the words that are in the table (the word found when you have combined the Likelihood Rating with the Consequence Rating, must be defined due to the same reason. The definitions of each Likelihood, Consequence, Rating and the Rating table (Matrix) itself, must be agreed upon and endorsed by the decision makers PRIOR to the commencement of the security risk assessment - this avoids any confusion.

Likelihood	Consequence					
	Minimal	Minor	Moderate	Major	Severe	Catastrophic
Extreme	Moderate	Significant	High	Extreme	Extreme	Extreme
High	Low	Significant	High	High	Extreme	Extreme
Medium	Low	Moderate	Significant	Significant	High	Extreme
Low	Low	Low	Moderate	Moderate	Significant	High
Very Low	Low	Low	Low	Moderate	Moderate	Significant
Negligible	Low	Low	Low	Low	Low	Moderate

Security Risk Management

Risk Register (RR)

DS&VS have a Risk Register Template which can be accessed on the intranet.

The following is a further example of a RR with seven fields that captures all the key information gathered during the risk identification stage:

Risk event	Assets at risk	Assets criticality	Threat source	Likelihood	Consequence	Risk rating

The following is an example of a more complex RR with thirty fields:

Complex Security Risk Register (Example)										
Security Risk Event (SRE) #	Endorsed SRE	Threat source	Raw Risk (without Treatment)	Site Credible SRE	DS&VS STA	Physical ECC	People ECC	Policy & Process ECC	Technology ECC	Adjusted STA
People	Property	Information	Capability	Reputation	SRE Specific Consequence Rating Explanation	Overall Consequence Rating Explanation	Consequence Rating	High Risk Rating	Alarm Rating	Risk Assessment
Recommended Treatments		Acknowledged Resourced - Acknowledged Not Resourced		Risk Treatment Plan (RTP) Number		RTP Steward	RTP Key Timing	RTP Monitoring	Treatment Priority	Residual Risk Rating

Security Risk Event Register

1	2	3	4	5	6	7	8	9	10
Risk Event Description	Asset at Risk[1]	Asset Criticality[2]	Threat Source[3]	Risk Event Likelihood	Risk Event Consequence	Risk Event Rating	Treatment	Risk Event Rating after Treatment	Prioritisation

[1] Expressed as either Information, People, Asset, Reputation, or Capability
[2] Expressed as either a security classification, BIL or other
[3] Expressed as either FIS, Trusted Insider, Terrorism, Criminal Elements, Protest and Issue Motivated Groups or Maverick Individuals

Security Risk Event Narrative

RiskEvent#		Threat Source		Asset Category	
Description of Risk (Risk Event)					
Security Risk Assessment					
	With Current Controls		Post Treatment		
Risk Event Likelihood					
Risk Event Consequence					
Risk Event Risk Rating					
Vulnerability Assessment					
Identified Vulnerabilities					
Current Controls Change of these controls may impact the risk rating of the risk event. The assessment of the effectiveness of controls may vary from risk event to risk event based on the effectiveness of a particular control in relation to the risk event.	Control		Assessment of Effectiveness		
Additional comments and/ or observations					

Risk Evaluation

Risk evaluation involves two stages; prioritising risks into an agreed upon priority list for treatment, and; utilising the tolerance level of risks to accept risks that are below that agreed threshold.

Prioritising Tasks

Using the tools that key stakeholders have agreed upon in the Context stage, Security Practitioners will be able to prioritise risks objectively.

Prioritisation is predominately affected though the establishment of risk tolerance (which will be addressed shortly) and the use of risk rating descriptors e.g. Extreme to Low against all intolerable risks. Subsequent prioritisation mechanisms can be agreed to locally and could include metrics, likelihood or consequence preference and asset criticality preference.

Risk Treatment

Risk Treatment involves a number of steps for the Security Planner to follow in order to ensure that this important phase in the Security Risk Assessment process is followed correctly. The following information is principally sourced from ISO 31000:2018 and HB 167:2006.

Prioritise unacceptable risks

Risks assessed as intolerable require treatment to ensure the appropriate controls are applied to reduce either the likelihood of risk being realised or the consequence of it should it happen. The priority order for treatments has already been determined earlier in the process.

Establish treatment objectives

By directly addressing the objectives of the security risk treatments, the Security Practitioner can remain focused on the purpose of the treatments, rather than the treatments themselves.

An example of a treatment objective could be: to shift, where possible, through the application of treatments, intolerable risks into the tolerable zone, while understanding that any one treatment may affect one (or more) risks.

It is important for the Security Practitioner to note that any treatment used may affect more than just one risk.

Identify and develop treatment options

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived. A number of treatment options can be considered and applied either individually or in combination. The organisation can normally benefit from the adoption of a combination of treatment options.

Broadly speaking, options for the treatment of security risk will involve one or a combination of the following treatment strategies (this table is derived from HB167:2006).

Treatment Option	Risk Treatment Description
ACCEPT the risk	Although the risk is unacceptable, resourcing and capability is not available to treat the risk. The only option may be to retain the risk and to continue monitoring it until changes allow action to be taken
AVOID the risk	Where practicable, avoid specific activities
SHARE the risk	Use a third party or stakeholder to provide resources and capability where applicable to reduce likelihood or consequence of a risk (some responsibility and all accountability remain with the Risk Owner)
REDUCE the risk	Implement new controls to remove vulnerabilities. This could include asset hardening or improve the response and recovery efforts
ELIMINATE the risk	Where possible remove the source of threat or hazard
SUBSTITUTE the risk	Employ a different process
ISOLATE the risk	Disperse the assets or place the asset within controls where it cannot be compromised
Engineering controls	Introduce physical or technological protection systems or improve levels of preventative or reactive maintenance to current systems
Administrative controls	Implement instructions, policy, procedures, training and data collection systems

The DSPF makes the observation that minimum compliance with the DSPF forms the vast majority of risk treatments available to managers.

Evaluate treatment options

Mandatory Minimum Standards

Risk assessed as acceptable may still require some level of treatment, and the treatments themselves must meet minimum security standards.

All too often security risk management, and the treatment step in particular, deals with each risk event in isolation. In particular, insufficient attention is given to the causal factors of risk and their interaction. This is turn tends to produce treatment options that are focused on managing individual risks, with an inadequate consideration of how other risks will be affected… A more holistic view therefore needs to be taken when evaluating treatment options.

Comparative Benefit Analysis (CBA)

The most important outcome of any CBA is the provision of sufficient information to the Risk Owner to enable a fully informed decision to be made about the value of implementing a particular treatment strategy.

A CBA can be conducted either as a formal or informal process and should consider as wide a range of issues as possible, not just be restricted to financial considerations. The analysis should consider issues such as:

- direct benefits, arising from reduction in the likelihood or consequences of the security risk

- direct costs, of implementing the proposed treatment, and/or that could arise if the risk eventuates
- indirect benefits, arising from collateral effects of the treatment such as improved management and staff confidence, enhanced reputation
- indirect costs, arising from the loss of productivity, business disruption, diversion of management attention, loss of reputation or brand value.

Detailed design of treatment options

Once an appropriate treatment has been selected, a detailed design of that treatment is necessary before undertaking that treatment. This is required to ensure that the treatment is well planned and rolled out, and they best way to achieve this goal is for the Security Practitioner to involve the key stakeholders that will be involved in its implementation or end use. The detailed design phase should always be conducted with the agreed treatment objectives in mind.

Review of the treatment's design

Prior to beginning the treatment, the Security Practitioner should ensure that the detailed design meets to the treatment's objectives. The process of this evaluation may be a simple checking procedure or a more complex and formal one involving key stakeholders. At a minimum the review should:

- Meet the security objectives
- Be able to be practically implemented in the current and/or anticipated operating environments (including with the available resources)
- Provide for sustainability or maintenance for the required life span of the treatment
- Allow required monitoring to be practically undertaken
- Not introduce new collateral risk

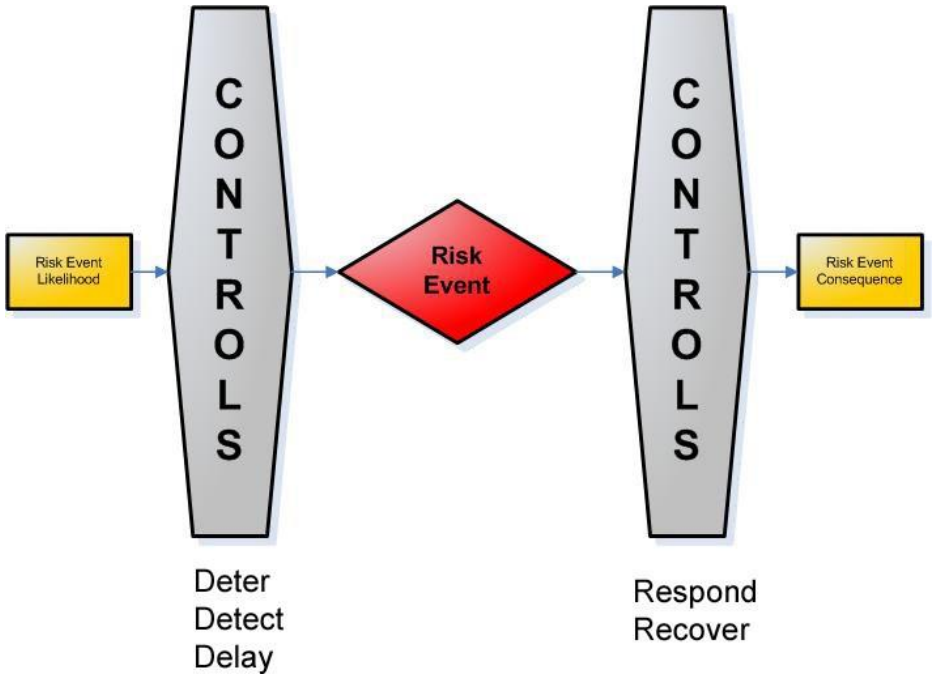
Communicate and implement treatment options

When selecting risk treatment options, the organisation should consider the values and perceptions of stakeholders and the most appropriate ways to communicate with them. Where risk treatment options can impact on risk elsewhere in the organisation or with stakeholders, these should be involved in the decision. Though equally effective, some risk treatments can be more acceptable to some stakeholders than others.

Decision makers and other stakeholders should be aware of the nature and extent of the residual risk after risk treatment. The residual risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

Security Controls

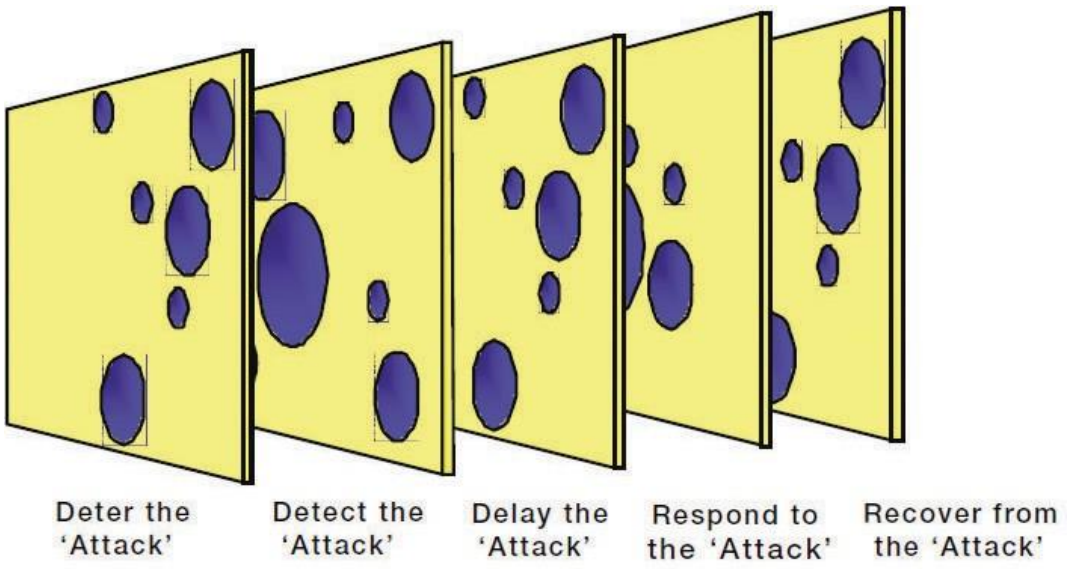
Their Relationship to Risk Event Likelihood and Risk Event Consequences



Security controls can reduce the likelihood of risk events occurring. These are called **Preventative Security Controls** and examples of which include access controls measures, physical security controls.

Security controls can also reduce the consequence of the risk event once it's occurred. These are called **Preparedness Security Controls** and examples of which include Base Security Instructions and Security Protocols.

Control Interdependency



Risk Treatment Plan

Risk Description:	Risk Serial #: Risk Priority #:
RTP Owner:	RTP Serial #:
Treatment Actions and Intended Effect: 1. 2. 3. 4.	
Treatment Resource Requirements: 1. 2. 3. 4.	
Treatment Responsibilities: 1. 2. 3. 4.	
Key Timings:	
Reporting- Monitoring – KPI Requirements:	
Approved By: Signature: Date:	

Reporting Residual Intolerable Risks

Escalating Risk: Security risks are to be resolved at the lowest possible level. Where serious residual risks cannot be resolved, they are to be reported to an appropriate decision maker, in accordance with the DSPF. 'Escalation thresholds', established by Control Owners, determine the level (rank or position title) at which Defence personnel can manage risks at varying risk ratings.

> Contractors, Consultants and Outsourced Service Providers cannot manage or escalate risks except through Defence personnel.
>
> *- DSPF Governance – paragraph 35*

Escalation thresholds can be found in each DSPF Principle and Controls document.

Example of escalation thresholds from DSPF Control – *Overseas Travel*

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	AS SPS
High	Defence Security Committee (DSC) – through AS SPS
Extreme	DSC – through AS SPS

Security Risk Action Plan

The Risk Events (scenarios) have been evaluated via the Likelihood of the event occurring and the Consequence of the event occurring. Some Risk Events become intolerable after this evaluation and required further controls to be put in place in order to make them tolerable. A Risk Action Plan tells the story of how the Risk Event is intolerable, what new control is being suggested (and maintained) and what new level the Risk Event will have post-treatment.

This is the stage of the SRM process where;

- risk events have been identified, and
- mitigations have been considered that lower the rating to an acceptable level.

Mitigations now must be employed / monitored to ensure that they are treating the risk event as the plan states. NOTE: the Risk Action Plan may very well have already been incorporated as part of the Risk Event Narrative, the Risk Event Register or even the Risk Event Treatment Plan. It does not matter where the following details are captured, as long as the stakeholders are aware of the results and that commanders or managers have assessed, endorsed, and monitor the results.

An example of a Risk Action Plan could be thus:

Risk event	Existing Controls	Risk Rating	New Controls	Risk Rating after new control	Comparative Benefit Analysis[1] Considered	Testing Schedule[2]	Monitoring Schedule[3]

[1] A Comparative Benefit Analysis is a systemic process for calculating and comparing benefits of a project.
[2] A Testing Schedule may include frequency of testing and expected outcomes, personnel or organisations conducting the testing, policy/plans updated, as well as Commander/Manager sign off of the testing schedule.
[3] A Monitoring Schedule should be included to ensure the overall management of the system is operating correctly and that all stages are considered for the efficacy, application and oversight.

Communicate and Consult with Stakeholders

Communication and consultation with stakeholders is continuous and is meant to be applied during and after every stage of the SRM process.

In the SRM process, identifying, communicating and consulting with stakeholders is paramount to ensuring that the security plan is fully informed.
Stakeholders may provide insight to an issue that may not be evident to the Security Planner, or might be able to validate the Security Planner's perceptions of an issue. Whatever the level of involvement, stakeholders are essential in developing the best product.

Engagement

The security planning process is often perceived as esoteric, overly arduous and technical by many, including those undertaking the process. Engaging with stakeholders who hold this view requires a communications strategy to be planned, agreed and acted upon.

Communications strategy

Different organisations within Defence operate with different terminology and have different specialisations. Communicating with such a wide variety of people requires the Security Risk practitioner to exhibit clear communications skills and to be able to ensure information is shared not only in a timely manner but also without misunderstandings or ambiguity.

As a result the Security Risk practitioner is encouraged to have a communications strategy. Any strategy implemented will ultimately be decided by the stakeholders involved in the Security Risk Assessment, however all communications strategies address the following:

- What are the SRA's objectives?
- Who requires certain pieces of information in order to contribute effectively?
- Who are the key stakeholders?
- How and when should the stakeholders communicate?
- What are the timeframes of the SRA?
- What resources are available to the stakeholders and security risk practitioner?

Stakeholders in the security planning process

For security planning purposes, stakeholders can be anybody affected or potentially affected by security risk. While there are numerous people who can provide input into the security plan, the key stakeholders that require engagement include:

- BSM / SADFO
- SEMC
- BMF
- HRUs
- SOs (be it for a facility or unit or both)
- SSAs
- Civilian and Service Police
- DS&VS Security Operations regional advisor(s)
- E&IG for the region
- Key contractor personnel

This list is by no means exhaustive.

Communicating with stakeholders

In developing the communications strategy, security risk practitioners should seek opportunities to engage key stakeholders, in particular the risk owners and risk controllers, at various points throughout the process to ensure engagement.

It is important that all stakeholders adhere to the appropriate lines of communication / chain of command in conveying security information. The Base Management Forum (BMF) allows for coordinated discussion and centralised security planning. Engagement of external security stakeholders in relation to whole-of-base security should be via the BSM or delegate only.

Bases will normally establish a security specific group to engage in the security planning process, for instance the Security Emergency Management Committee (SEMC).

Dispute Resolutions

Given the scope of the BMF and its intended objectives across multiple stakeholders, it is not surprising that at times disputes may occur. In such instances the appropriate parties are expected to resolve the issues themselves. This may or may not be chaired by the SADFO. If resolution cannot be sought, it is then elevated through to a regional level, then again through to the Associate Secretary Group

Resources and Further Information

The HB 167:2006 outlines strategies for engaging with staff and stakeholders, and addresses their perception of risk. It also outlines what must be considered in the communications strategy as well as issues that commonly arise. It is recommended that the Security Planner become familiar with this knowledge and incorporate relevant information into their security plan.

Monitor and Review

This is not a stage of Security Risk Management, but a continual process itself. After every decision is made, after every template completed, after ever document submitted, take the time to ask yourself is the product/decision could use another set of eyes, a different perspective. The purpose of SRM is to make clear, defensible and objective security decisions to protect your assets; the process of monitoring and reviewing achieves this.

Further Considerations

Further reading: Learning to Swim with Sharks

Further Resources