3 Security planning and risk management

A. Purpose

1. This policy describes how entities establish effective security planning and can embed security into risk management practices. Security planning can be used to identify and manage risks and assist decision-making by:
   a. applying appropriate controls effectively and consistently (as part of the entity's existing risk management arrangements)
   b. adapting to change while safeguarding the delivery of business and services
   c. improving resilience to threats, vulnerabilities and challenges
   d. driving protective security performance improvements.

B. Requirements

B.1 Core requirement

Each entity must have in place a security plan approved by the accountable authority to manage the entity's security risks. The security plan details the:

- ***a. security goals and strategic objectives of the entity, including how security risk management intersects with and supports broader business objectives and priorities***
- ***b. threats, risks and vulnerabilities that impact the protection of an entity's people, information and assets***
- ***c. entity's tolerance to security risks***
- ***d. maturity of the entity's capability to manage security risks, and***
- ***e. entity's strategies to implement security risk management, maintain a positive risk culture and deliver against the PSPF.***

2. Where a single security plan is not practicable due to an entity's size or complexity of business, the accountable authority may approve a strategic-level overarching security plan that addresses the core requirements.

B.2 Supporting requirements

Supporting requirements for security planning and risk management

#	Supporting requirements
Requirement 1. Security plan review	The security plan (and supporting security plans) **must** be reviewed at least every two years. The review process must include how the entity will: a. determine the adequacy of existing measures and mitigation controls, and b. respond to and manage significant shifts in the entity's risk, threat and operating environment.
Requirement 2. Critical assets	Entities **must** identify people, information and assets that are critical to the ongoing operation of the entity and the national interest and apply appropriate protections to these resources to support their core business.
Requirement 3. Risk steward	Entities **must** identify a risk steward (or manager) who is responsible for each security risk or category of security risk, including for shared risks.

#	Supporting requirements
Requirement 4. Impact of risks	When conducting a security risk assessment, entities **must** communicate to the affected Commonwealth entity any identified risks that could potentially impact on the business of another entity.
Requirement 5. Threat levels	The security plan (and supporting security plans) **must** include scalable measures to meet variations in threat levels and accommodate changes in the National Terrorism Threat Level.
Requirement 6. Alternative mitigations	Where the CSO (or security advisor on behalf of the CSO) implements an alternative mitigation measure or control to a PSPF requirement, they **must** document the decision and adjust the maturity level for the related PSPF requirement.

C. Guidance

C.1 Security planning approach

3. Successfully managing entity security risks and protecting people, information and assets requires an understanding of what needs protecting, what the threat is and how assets will be protected. Security planning is designing, implementing, monitoring, reviewing and continually improving practices for security risk management.

    a. A **security plan** (see section C.2) specifies the approach, responsibilities and resources applied to managing protective security risks. The security plan allows entities to review the degree of security risk that exists in different areas of operations and take action to mitigate identified risks.

    b. A **security risk management process** (see Annex A) manages risks across all areas of security (governance, information, personnel and physical) to determine sources of threat and risk (and potential events) that could affect government or entity business. Security risk management includes:

        i. **security risk assessments**, which are structured and comprehensive processes to identify, analyse and evaluate security risks and determine practical steps to minimise the risks

        ii. **security risk treatments**, which are the considered, coordinated and efficient actions and resources required to mitigate or lessen the likelihood or negative consequences of risks.

4. Regardless of an entity's functions or security concerns, the central messages for managing security risks are:

    a. security is everyone’s responsibility and risk management is the business of all personnel (including contractors) in the entity, supported by security awareness training

    b. security is a business enabler that informs decision-making, is part of day-to-day business and is embedded into an entity’s business processes

    c. security management is logical, systematic and transparent and is part of the enterprise risk management process

    d. security processes identify changes in the threat environment and allow for adjustments to maintain acceptable levels of risk, balancing operational and security needs.

5. For information on how a risk-based approaches work with the PSPF core requirements, refer to section C.4.

C.2 Security plan

6. Entities develop a security plan to articulate how their security risks will be managed and how security aligns with their priorities and objectives. Where a single security plan is not practicable due to the entity’s size or complexity of business, the Attorney-General’s Department recommends developing an overarching security plan supported by more detailed plans (referred to as supporting security plans).

7. Each entity’s security plan will be different. The security plan reflects an entity’s protective security requirements and mitigation strategies appropriate to the levels of threat, risks to its assets and risk tolerances. Entities are encouraged to use approaches that manage risks for the Australian Government and best meet their operational environment.

8. **Requirement 1** mandates security plans (and supporting security plans) are reviewed at least every two years. A security plan is a 'living' document and requires review and adjustment to ensure the goals and management of security risks keeps pace with changes in the entity and with emerging threats. This could include, for example, a change in the National Terrorism Threat Level or an emerging threat that alters the entity's business impact level (see **Table 3**). It is recommended the security plan also be reviewed when there are significant shifts in the entity's risk or operating environment.
9. Entities determine how the review of the security plan (and supporting security plans) is conducted. Security plans may be reviewed by the CSO or appointed security advisor, an external security consultant or through a security governance oversight committee for larger or more complex business operations.
10. Security plans are best developed by a person who also has an understanding of the entity's strategic goals and objectives and the appropriate level of security risk management knowledge and expertise.
11. Entities are encouraged to make the security plan (and supporting security plans) available across the entity, particularly for those with obligations or responsibilities identified in the plan, helps to build a positive security culture based on a common understanding of security.

Table 1 Security plan overview

Sections of the plan	Suggested content coverage
Goals and objectives	The accountable authority's commitment to effective security risk management, expectations for a positive security culture, outlining the entity's security priorities, goals and objectives (see sub-section C.2.2).
Security risk environment	The environment in which the entity operates; the threats, risks and vulnerabilities effecting the entity's protection (see section C.2.3), including: a. what the entity needs to protect (via a risk assessment) being the people, information and assets assessed as critical to its ongoing operation and to the national interest (mandated in **Requirement 2**) b. what it needs to protect against (via threat assessment) c. how the risk will be managed within the entity. See **Annex A** for the security risk management process.
Risk tolerance	The entity's level of risk tolerance. Each entity's level of tolerance for risk will vary depending on the level of potential damage to the Australian Government or to the entity (see sub-section C.2.4).
Security capability	The maturity of the entity's capability to manage security risks (see sub-section C.2.5).
Security risk management strategies	Strategies to manage security, maintain a positive risk culture and deliver the PSPF requirements (see sub-section C.2.6). The entity's approach to managing security risks, including identifying how it will apply proportional and sufficient controls to deter, detect, delay and respond to threats (internal or external) that affect the security of its people, information or assets. This includes: a. establishing risk stewards and managers (mandated in **Requirement 3**) b. instigating steps that minimise risks (according to risk environment and tolerances) c. managing residual risks to ensure the protection of people, information and assets.
Supporting and evidentiary documents	Entities are encouraged to consider what, if any, evidentiary documents support the security plan (and supporting security plans).

Examples	
security risk assessment report	security alert levels
threat assessment	site security plan
vulnerability assessment	entity-specific security procedure
security risk register	entity-specific PSPF security maturity monitoring
critical asset register	security incident register/response procedure
privacy impact assessment	ICT system security plans (see ISM)
information asset register	other entity operational or compliance plans

12. The Attorney-General's Department recommends security plans be comprehensive and span all areas of protective security. This includes governance arrangements and information, ICT, personnel and physical security as outlined in **Table 2**.

Table 2 Suggested coverage for security plan

Governance arrangements	Information (including ICT) security	Personnel security	Physical security
Suggested coverage for governance arrangements: a. roles and responsibilities b. risk tolerances c. security risk management (including threat, vulnerability and criticality assessments) d. security incidents e. security culture f. security awareness training g. security monitoring h. reporting security maturity i. contracted service providers.	Suggested coverage for information security: a. classification and management arrangements for information holdings b. access to information including sharing information c. ICT access and system security d. cyber security to mitigate targeted intrusions e. information handling within the entity as well as when in transit or out of the office.	Suggested coverage for personnel security: a. personnel security provisions during recruitment in conjunction with human resource management b. security clearance maintenance plans that address risks identified by security vetting agencies c. security assessment position list d. contact reporting e. security clearance aftercare f. ongoing security awareness training g. managing the separation of personnel.	Suggested coverage for physical security: a. access control systems b. security monitoring and alarm systems c. measures to increase security if the National Terrorism Alert Level or entity-specific threats increase.

13. When developing or reviewing the security plan (and supporting security plans), entities are encouraged to seek advice and technical assistance from specialist entities such as:
    a. Australian Security Intelligence Organisation for threat assessments
    b. ASIO-T4 Protective Security for physical security advice or technical assistance
    c. local police for state and territory criminal threat information
    d. Australian Government Security Vetting Agency for security vetting procedural advice
    e. Australian Signals Directorate for ICT, cyber security and certified cloud services advice
    f. subject-matter experts.

C.2.1 Security planning for projects

14. The Attorney-General's Department recommends that security is considered during all stages of project management and planning. This is particularly important for projects that involve:
    a. major acquisitions
    b. establishment of infrastructure or major modifications to existing infrastructure
    c. information that is:
        i. sensitive in nature or security classified
        ii. proprietary in nature or
        iii. meets the financial and economic impact threshold with a business impact of low to medium (level two) or higher.

C.2.2 Security plan – goals and objectives

15. Security is everyone's responsibility, however, overall accountability for security planning and risk management rests with the entity's accountable authority, supported by the CSO.
16. Security arrangements support an entity's business objectives by identifying and managing risks that could adversely affect achieving those objectives. The accountable authority and CSO determine the security arrangements required for:
    a. vigilance, resilience and adaptability of personnel to security risks

b. capacity to function, including during security incidents, disruptions or emergencies

c. safety of personnel (including contractors) and those who have dealings with government (including visitors)

d. protection of resources, information and assets held in the entity.

17. Clear protective security goals and objectives allow effective implementation of security risk management that is consistent with the entity's operating objectives. This includes how security underpins business priorities and functions as reflected in the entity's corporate plan.

18. When setting goals, entities are encouraged to consider historical security experience and knowledge, results from previous performance indicators and past compliance with the PSPF.

19. The Attorney-General's Department recommends that entities assess their existing protective security arrangements and procedures to identify areas for improvement. This could be areas of exposure, vulnerability or 'target attractiveness'. Target attractiveness is the value of an entity or its components to an adversary when viewed as a target. Reviewing protective security arrangements also considers the entity's maturity in implementing PSPF requirements.

C.2.3 Security plan – threats, risks and vulnerabilities

20. When implementing the core requirement to detail threats, risks and vulnerabilities that affect the protection of people, information and assets, entities:

a. identify the people, information (including ICT) and assets to be safeguarded (**Requirement 2**)

b. determine specific risks (including shared risks) to its people, information and assets in Australia and abroad (risk identification)

c. identify and assess criticality of people, information and assets (criticality assessment)

d. identify the threats to people, information and assets (threat assessment)

e. assess the degree of susceptibility and resilience to hazards (vulnerability assessment)

f. assess the likelihood and consequence of each risk occurring (risk analysis)

g. determine adequacy of existing safeguards and whether current risks (or residual vulnerabilities) are acceptable or not (evaluate risks)

h. implement protective security measures to mitigate or reduce identified risks to an acceptable level (risk treatments)

i. manage residual risks (treatable and untreatable) and vulnerabilities

j. identify and accept responsibility for risks (**Requirement 3**).

21. **Requirement 2** mandates that entities must identify the people, information and assets that are critical to the ongoing operation of the entity and to the national interest.

a. Assets are items that have a value to the entity, including resources and property that are relied on to sustain operations and capabilities. These are in addition to people and information (including ICT) identified as critical to ongoing operations.

b. Critical assets (and components of an asset) are essential to the ongoing operation of the entity.

c. Asset attractiveness is how a threat source may view the asset in relation to the activity it seeks to undertake.

d. Asset attributes are the qualities that determine the nature and extent of impact on the entity operations following an event or incident.

22. **Annex A** provides details on the security risk management process. The Attorney-General's Department recommends entities ensure methodologies are appropriate, compatible with security and align with their risk management standards when developing their security risk management approach. Entities may consider:

a. Department of Finance Commonwealth Risk Management Policy

b. Australian Standards AS/NZS ISO 31000 Risk Management – Guidelines and HB 167 – Security Risk Management.

23. These standards are a non-prescriptive method of managing risk. They are applicable for all types of organisations, including government.

24. Where risks are identified that could potentially affect the operations of another government entity, **Requirement 4** mandates that entities communicate these risks to the affected entity.[1]

25. Where a risk with national security implications is identified, the Attorney-General's Department recommends the entity inform ASIO of these risks.[2]

C.2.3.1 What is a security risk?

26. A security risk is something that could result in the compromise, loss, unavailability or damage to information or assets, or cause harm to people. Security risk is the effect of uncertainty on objectives and is often measured in terms of its likelihood and consequences. The causes are generally people, systems, processes, procedures, crime, attacks or natural events. An:

    a. **effect** is a deviation from the expected and may be positive or negative

    b. **objective** has different aspects such as financial, health and safety and environmental goals, and can apply at multiple levels such as strategic, organisation-wide, project, product and process levels.

27. Entities are encouraged to consider where security risks intersect with other risks including fraud, privacy and business continuity. Entities are encouraged to treat risk holistically across its operations. For example, there may be opportunities to treat multiple risks with one mitigation control.

C.2.3.2 Shared security risks

28. Shared security risks are those that extend across entities, premises, the community, industry, international partners and other jurisdictions. They require high levels of cooperation between stakeholders to effectively understand and manage those risks.

29. Where entities share accommodation or facilities, the Attorney-General's Department recommends entities conduct a risk assessment to evaluate the security risks for the co-tenancy and apply protective security measures to address the combined risks.

30. Where an entity considers a risk is shared due to its location (eg physical boundaries, crowded public space, government precinct) and there is no identifiable other party to share the assessment and management of the risk, the entity is expected to mitigate the risk to the extent it is able to within its operations.

31. In situations where risks are shared between parties with differing risk tolerances, it is recommended that the parties identify the areas of difference and whether concerns might be alleviated by applying additional controls.

32. Where shared risks are identified, it is important to develop clear roles and responsibilities, including those mandated in **Requirement 3**.

33. For information on managing shared risks, see the Commonwealth Risk Management Policy Understanding and managing shared risks information sheet.

C.2.4 Security plan – tolerance to security risks

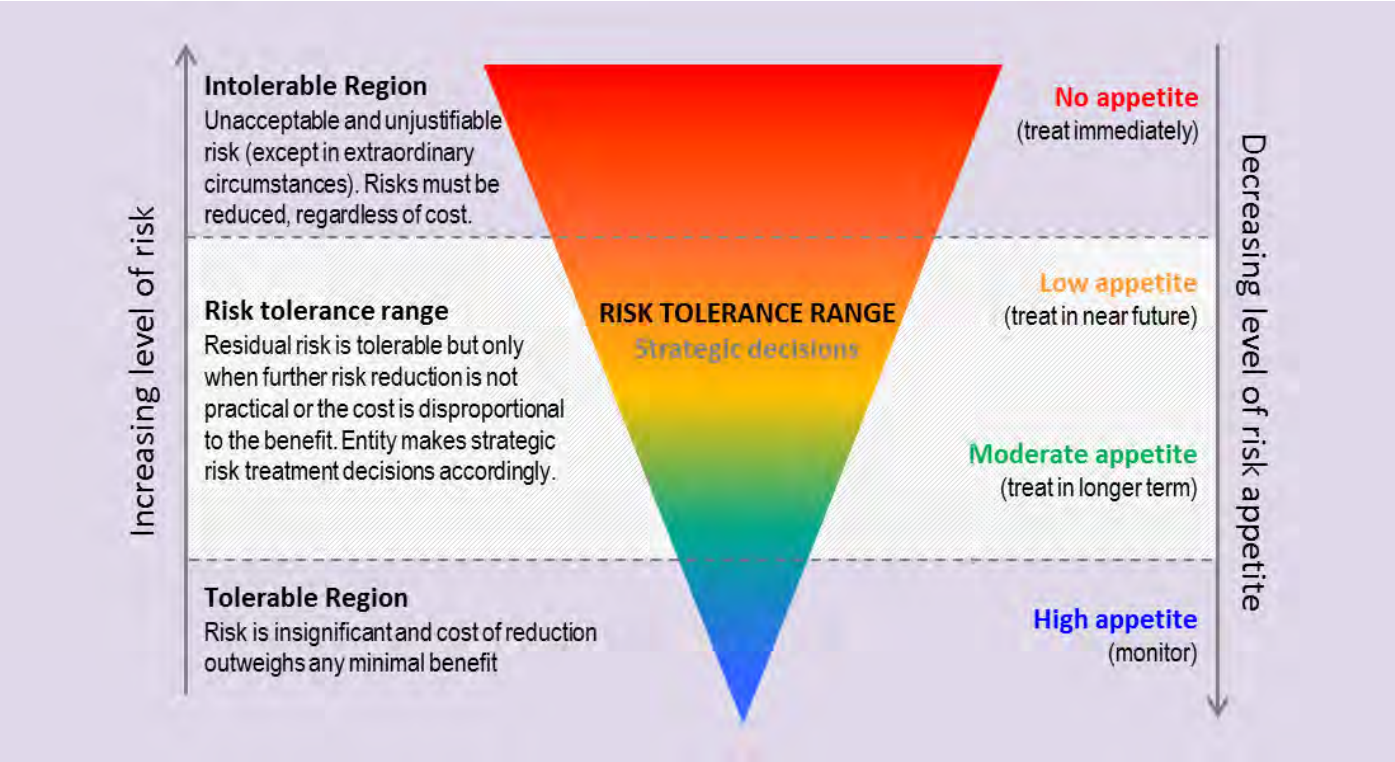
34. The PSPF policy: Role of accountable authority mandates that the accountable authority determine their entity's tolerance for security risks, supported by a transparent and justifiable process. When setting risk tolerance levels, some entities may decide to differentiate between ICT risks and other security risks.

35. Risk tolerance is an informed decision to accept a risk. It is the level of acceptable risk after risk treatment to achieve an objective or manage a category of risk. Determining whether a risk is acceptable involves judgment. It is highly dependent on the entity context and the accountable authority's approach.

[1] Refer to the Australian Government Directory for contacts.
[R] Report to the Australian Security Intelligence Organisation or call the National Security Hotline on 1800 123 400.

36. Risk tolerance is based on the principle of managing risk to a level that is as low as reasonably practicable, allowing for flexible and innovative business practices. It is a practical application of risk appetite, which is the amount of risk an entity is willing to accept or retain within its tolerance levels and the limits of PSPF requirements. Risk tolerance includes:
    a. expectations for mitigating, accepting and pursuing specific types of risk
    b. boundaries and thresholds of acceptable risk taking
    c. actions to be taken or consequences for acting beyond approved tolerances.
37. An entity's risk tolerance can be affected by changes in evaluation criteria and the accountable authority's appetite for risk. It can vary depending on:
    a. prevailing political and community sensitivities and expectations
    b. the nature of a security incident (eg terrorist act, hacking)
    c. existing or emerging security incidents (trusted insider, cyber-attacks)
    d. strategic or business priorities
    e. vigilance, resilience and adaptability of personnel and how effective they are at applying security awareness principles
    f. resource availability for treatment
    g. the ability of the government, entity or individual to absorb losses.
38. Manipulating risk assessment inputs (consequence or likelihood of a risk) to achieve a lower result is **not** an appropriate method of risk management and bypasses the intent of risk tolerance. Entities are encouraged to develop appropriate rating scales for likelihood and consequence in accordance with their risk tolerances.
39. In most cases, determining risk tolerance and levels of risk appetite can be understood as a gradient scale, where the appetite for the risk becomes progressively less tolerable as the risk level increases (see **Figure 1**).

Figure 1 Risk tolerance regions (example only)



40. For information, refer to the Commonwealth Risk Management Policy Defining risk appetite and tolerance information sheet.

C.2.5 Security plan – capability to manage security risks

41. The PSPF governance outcome is that 'each entity manages security risks and supports a positive security culture in an appropriately mature manner.' The PSPF policy: Reporting on security outlines that maturity is a meaningful scale to measure an entity's overall security position within its risk environment and risk tolerances. Maturity acknowledges the progression in achieving a security culture and highlights areas for improvement. Security capability maturity is how an entity:
    a. implements and meets the PSPF core and supporting requirements
    b. minimises harm to people and resources
    c. fosters a positive security culture
    d. responds to and learns from security incidents
    e. understands and manages security risks
    f. achieves security outcomes while delivering business objectives.

C.2.6 Security plan - strategies to implement security risk management, maintain a positive risk culture and deliver against the PSPF

42. The success of security risk management depends on the effectiveness of security planning and how well arrangements are supported by the entity's senior leadership and integrated into business processes. This includes meeting core and supporting requirements of the PSPF or adopting mitigations that are equivalent to or exceed those requirements.
43. It is important that entities foster a culture where risk management is an important and valued aspect of decision-making, where risk management processes are understood and applied appropriately; and where personnel can be confident in managing and taking risks, within defined parameters, in order to achieve objectives.
44. Effective security risk management supports better decision-making and builds positive risk culture by:
    a. identifying possible risks and opportunities in advance, lessening the potential of adverse outcomes and increasing the likelihood of desirable outcomes
    b. having processes in place to monitor risks and provide access to reliable, up-to-date information about risks
    c. providing guidance around appropriate limits through well understood risk appetite and risk tolerance statements
    d. providing transparency over the decision-making process and the achievement of entity objectives.
45. When security risk management is done well, it underpins organisational resilience and a positive risk culture because entities know their security risks, make coordinated and informed decisions in managing those risks, identify opportunities and learns from mistakes. This is reinforced with meaningful training and support across all levels of management.
46. Refer to the Department of Finance:
    a. Developing a positive risk culture information sheet
    b. Commonwealth Risk Management Policy Element Eight – Maintaining risk management capability
    c. Commonwealth Risk Management Policy Element Four – Embedding systematic risk management into business processes.

C.3 Security threat levels

47. **Requirement 5** mandates the security plan (and supporting security plans) include scalable control measures to meet increases or decreases in risk as a consequence of a change in threat to the entity. These must be able to accommodate changes in the National Terrorism Threat Level. Refer to **Table 3** for the business impact levels for consequences of threat levels.
48. Measures could include:

a. determining who needs to know about changes in the security threat level

b. outlining specific roles or responsibilities including who is responsible for determining the security alert level

c. ensuring personnel are aware of the measures employed by the entity to adapt to and mitigate emergencies and heightened threat levels

d. detailing arrangements to monitor the threat level and review the security alert level when the entity undertakes significant new projects, the risk environment changes, or after a significant incident impacting the entity's ability to operate.

Table 3 Business impact levels for consequences of threat

Business impact level	1 Low impact	2 Low to medium impact	3 High impact	4 Extreme impact	5 Catastrophic impact
Consequence of threat	Insignificant damage to the national interest, organisations or individuals.	Limited damage to the national interest, organisations or individuals.	Damage to the national interest, organisations or individuals.	Serious damage to the national interest, organisations or individuals.	Exceptionally grave damage to the national interest, organisations or individuals.

49. Developing entity security alert levels is one way an entity can ensure personnel are aware of the measures employed by the entity to adapt to and mitigate emergencies and heightened threat levels. Alert levels also allow entities to scale the controls used to mitigate risks as the risks increase or decrease.

50. The number of alert levels required for the entity will depend on its operational requirements and expected changes in risk sources. See **Table 4** for examples of security alert levels.

51. The source of security risks can be categorised into three areas:

    a. **Event** – an event is an important happening or incident impacting on the entity's ability to function such as a natural event (eg storm) or an emergency event (eg fire).

    b. **Threat** – a threat is a declared intent to inflict harm on entity personnel or property.

    c. **Activity** – an activity is an action by one or more people likely to have a negative impact on physical security (eg protest activity, filming in the vicinity of premises).

52. When determining the security alert level, entities are encouraged to monitor:

    a. National Terrorism Threat Level Advisory System advice

    b. protective security risk reviews

    c. police advice

    d. emergency management advice

    e. Bureau of Meteorology advice

    f. entity security incident reports

    g. media reports.

Table 4 Examples of security alert levels

Security alert levels	Low	Medium	High	Extreme	Catastrophic
Likelihood of threat	Applies when only general concerns exist of an event, physical activity or general threat.	Applies when an event, physical activity or threat is assessed as feasible.	Applies when an event, physical activity or threat is likely to occur.	Applies when an event, physical activity or threat is imminent or has occurred.	Applies when a severe event, physical activity or threat is imminent or has occurred.
Security measures required	Existing security measures are sufficient.	Security measures are maintainable indefinitely, with minimal impact to	Security measures are sustainable for lengthy periods without causing	Security measures will not be sustainable over the long term	Advice required from the National Security Hotline on additional

Security alert levels	Low	Medium	High	Extreme	Catastrophic
		the entity's operations.	undue hardship to personnel, affecting operational capability or aggravating relationships with the local community.	without creating hardship and affecting the entity's activities and personnel.	security measures.

C.4 Risk-based approach to the PSPF

53. Applying a risk-based approach to the PSPF is about making informed decisions on how to implement the core and supporting requirements to achieve a baseline security maturity level of 'managing'.[3] Under the CSO's direction, the entity implements PSPF requirements giving consideration to the entity's size, operations and risk environment. For example, the level of risk tolerance accepted by a national security entity may be very different to that of an administrative entity.

54. Outcomes from the entity's security planning and risk assessments inform these decisions, including whether additional protective security controls are required.

55. In the event that an entity is unable to implement a requirement, a risk-based approach allows an alternative mitigation to be implemented where it achieves a level of protection that is the same as or exceeds that afforded by the PSPF requirement. **Requirement 6** mandates that where the CSO (or security advisor) implements an alternative mitigation measure or control, they must document the decision and adjust the maturity level for the related PSPF requirement accordingly. **Requirement 1a** also applies to any alternative mitigation measures implemented by the entity.

56. Accepted variances may apply where the entity has temporarily varied the application of a PSPF requirement in response to an exceptional circumstance. These circumstances are outlined in the exceptional circumstances provision in the PSPF policy: Role of accountable authority. Variances are for a limited time and take into consideration the entity's risk tolerances. When applied appropriately, the entity may maintain a 'managing' maturity level rating during the circumstance.

D. Find out more

57. Other policies and information sources:

    a. Commonwealth Risk Management Policy available on the Security planning and risk management page on the Department of Finance website.

    b. Australian Standards:

        i. AS/NZS ISO 31000 – Risk Management – Guidelines

        ii. ISO Guide 73 – Risk management – Vocabulary

        iii. HB 167 – Security Risk Management

        iv. HB 436 – Risk management guidelines – Companion to AS/NZS ISO 31000

        v. HB 327 – Communicating and consulting about risk

        vi. HB 158 – Delivering assurance based on AS/NZS ISO 31000

    c. National Terrorism Threat Level Advisory System

58. Links to PSPF policy and guidelines include:

    a. Role of accountable authority – for accountable authority's security risk management responsibilities

[3] For guidance on security maturity levels, see the PSPF policy: Reporting on security.

b. Sensitive and classified information – for advice on business impact levels when determining the consequences of compromise, or loss of entity information or assets, or harm to its people

c. Reporting on security – for risk management reporting obligations

d. Security governance for contracted goods and service providers – for advice on security risks in contracts

e. Physical security for entity resources – for advice on physical risks.

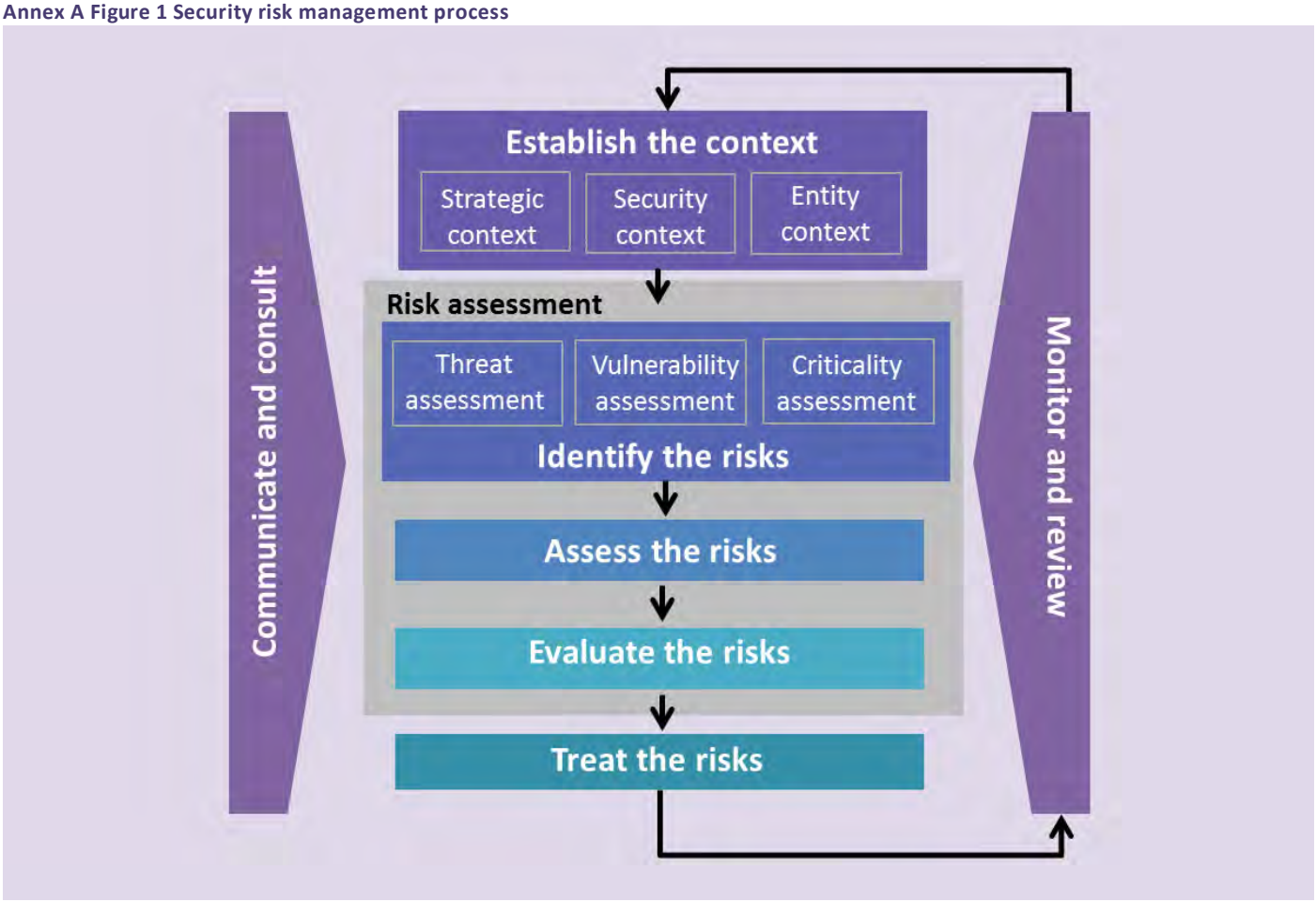
D.1 Change log

Table 5 Amendments in this policy

Version	Date	Section	Amendment
v2018.1	Sep 2018	Throughout	Not applicable. This is the first issue of this policy

Annex A. Security risk management process

Annex A Figure 1 Security risk management process



1. Elements of this guidance are based on the recommended Australian Standards: Commonwealth Risk Management Policy, AS/NZS ISO 31000 and HB 167 – Security Risk Management).
2. Risk is defined as the effect of uncertainty on objectives. An effect is a deviation from the expected—positive or negative.[4]

Communicate and consult

3. To ensure that risk management remains relevant and current, it is important to communicate and consult with stakeholders, contracted service providers and decision-makers throughout all stages of the process. This approach ensures stakeholders are properly represented, have their views taken into account in determining risk criteria and confirms that all participants understand their roles and responsibilities.
4. It is recommended that the following is documented:
   a. audience and stakeholders
   b. communication objectives and activities (what are you trying to achieve, how it will be achieved, delivery method, expectations)
   c. monitoring and review processes (noting that communication and consultation occurs at all stages of the security risk management process).
5. Refer to Commonwealth Risk Management Policy Element six – Communicating and consulting about risk.

Establish the context

6. The security risk management process addresses the strategic, operational and security risk management contexts. Defining the frame of reference provides the scope for risk management activities. The security

[4] As defined in ISO Guide 73 – Risk Management Vocabulary.

risk management process is used to determine all applicable sources of risk and potential events that could impact government or entity business.

Organisational context

7. Organisational context includes:
   a. scope and parameters of activities where risk management is applied
   b. resources (or limitations) available or required for risk treatments and activities
   c. reputational expectations or objectives
   d. logistical or locational challenges
   e. outcomes of related internal or external audit reports
   f. security risk management processes adopted
   g. processes for documenting results of risk assessments and risk treatments.

External context

8. External context includes:
   a. Regulatory environment, including legislative or policy obligations and responsibilities, foreign laws or potential jurisdictional access to information
   b. political or economic climate
   c. community sensitivities or expectations.

Security context

9. Security context includes:
   a. purpose and scope of security in supporting or achieving the entity's business objectives
   b. criteria for evaluating the significance of security risks
   c. risk appetite and tolerance criteria and threshold levels for the entity (see section C.2.4 for information on risk tolerances)
   d. threat and risk environment (areas of concern, specific threats identified, known vulnerabilities)
   e. decision-makers (when and by whom)
   f. critical asset statement (what are you looking to protect)
   g. interdependencies and links to other plans or security procedures
   h. details of any shared risk
   i. constraints and assumptions.

Security risk assessment

10. Security risk assessment is the process of risk identification, analysis and evaluation to understand the risks, their causes, consequences and probabilities. The aim is to generate a comprehensive list of threats and risks that effect the protection of the entity's people, information and assets and identify the sources, exposure and potential consequences of these threats and risks. Consideration is also given to the entity's prevailing and emerging risk environment.
11. Each risk is described as comprehensively as possible, so that decision-makers can fully understand the position. This may be in the style of a formal assessment undertaken by competent personnel, or a contracted service provider.

Identify security risks

12. Identifying security risks generates a clear, comprehensive and concise list of potential sources of risk and threats (referred to as a risk register, see example below) that could impact government, entity operations or continuous delivery of services. This is achieved by mapping the sources of risk (threat assessment), determining the importance of organisational assets (criticality of assets) and the manner in which these elements may facilitate or inhibit this interaction (vulnerability).

13. In preparing a list of security risks, consider questions like:

    a. What could happen? (potential event or incident and resulting outcomes or consequences)

    b. What is the likely outcome and impact of the risk eventuating?

    c. When could it happen? (how frequently)

    d. Where could it happen? (physical location and assets affected)

    e. How could it happen? (sources, potential threats, catalysts, triggers)

    f. How reliable is the information that the risk assessment is based upon?

    g. Why could it happen? (causes, underlying factors, vulnerabilities or inadequacies in protective security controls or mitigations)

    h. Who could be involved or effected? (individuals or groups, stakeholders or service providers)

    i. Do entity mitigation measures or activities create risk to clients or the public?

Annex A Table 1 Risk register example

Item	Description
Description	describe the risk (consider the questions above)
Category	people, information, property, reputation, financial, business operations
Event	occurrence or change of a particular set of circumstances
Source	threat or hazard that is the source of the risk
Cause	why the threat or hazard is a risk
Consequences	level of impact the risk will have on the entity
Risk criteria	determined tolerability against consequence and likelihood tables
Priority	comparing the level of risk (magnitude of risk = consequence + likelihood) with the risk criteria
Controls	adequacy of existing controls in place, or the known controls for the risk
Current risk rating	what is the current risk rating status
Risk decision	does the risk need treatment
Treatments	what action needs to be taken, by whom, with what resources and by when
Residual risk rating	once treatments have been implemented, what will be the residual risk rating
Stakeholders	who else is impacted by the risk (other entities, contractors, service providers etc)
Previous risk information	information on any previous risk, threat or vulnerability assessments

Criticality assessment

14. Criticality assessment identifies and assigns importance to all resources (something that has value to the entity including personnel, information and physical assets or processes that support them) that are critical to the ongoing operation of the entity or to the national interest. Asset identification and security risk management documents can form part of the security plan or be standalone and inform the security plan.

15. The criticality assessment will be different depending on the entity's purpose, business objectives and risk environment. Criticality assessments include:

    a. **criticality ratings** – the scale of the resources' importance to the entity (eg a numerical scale 1-5 or importance value scale such as catastrophic, significant, moderate, low, insignificant). Alternatively, a business impact level can be applied by assessing the impact on the entity if the integrity or availability of the resource was compromised (applying a business impact level to the confidentiality of an resource means applying a security classification. See the PSPF policy: Sensitive and classified information)

    b. **consequence of loss, compromise or harm** – a description of what the consequence is

c. **category** – consequences can also be expressed across categories such as people, information, property, reputation, financial, business operations or services.

Threat assessment

16. A threat assessment identifies the source of harm and is used to inform the entity's risk assessment. Threats are assessed by determining the intent to cause harm, damage or disruption and the capability (the potential that exists to actually cause harm or carry out intentions) of the threat source.

Vulnerability assessment

17. Vulnerability assessment identifies the degree of susceptibility and resilience of an entity to hazards. To understand the potential of risks, it is recommended that entities assess the possible vulnerabilities to each risk to gauge the consequence and likelihood of these risks. This process of understanding possible vulnerabilities helps entities to prioritise the risks and guides the allocation of resources in mitigating their effects.

Analyse security risks

18. Risk analysis involves assessing the likelihood and potential consequence of each identified risk, determining the level of risk rating and assessing whether additional controls are required.

19. Aims of risk analysis:

a. Determine **control effectiveness** – whether the existing control measures are adequate or effective in managing identified risks.

b. Define the likelihood and consequence of the event. This is achieved by considering the:

i. **likelihood** – the chance or probability of the event occurring,[Error! Bookmark not defined.] probability or frequency of the event (an occurrence or change in a particular set of circumstances, it can be one or more occurrences and can have several causes) occurring

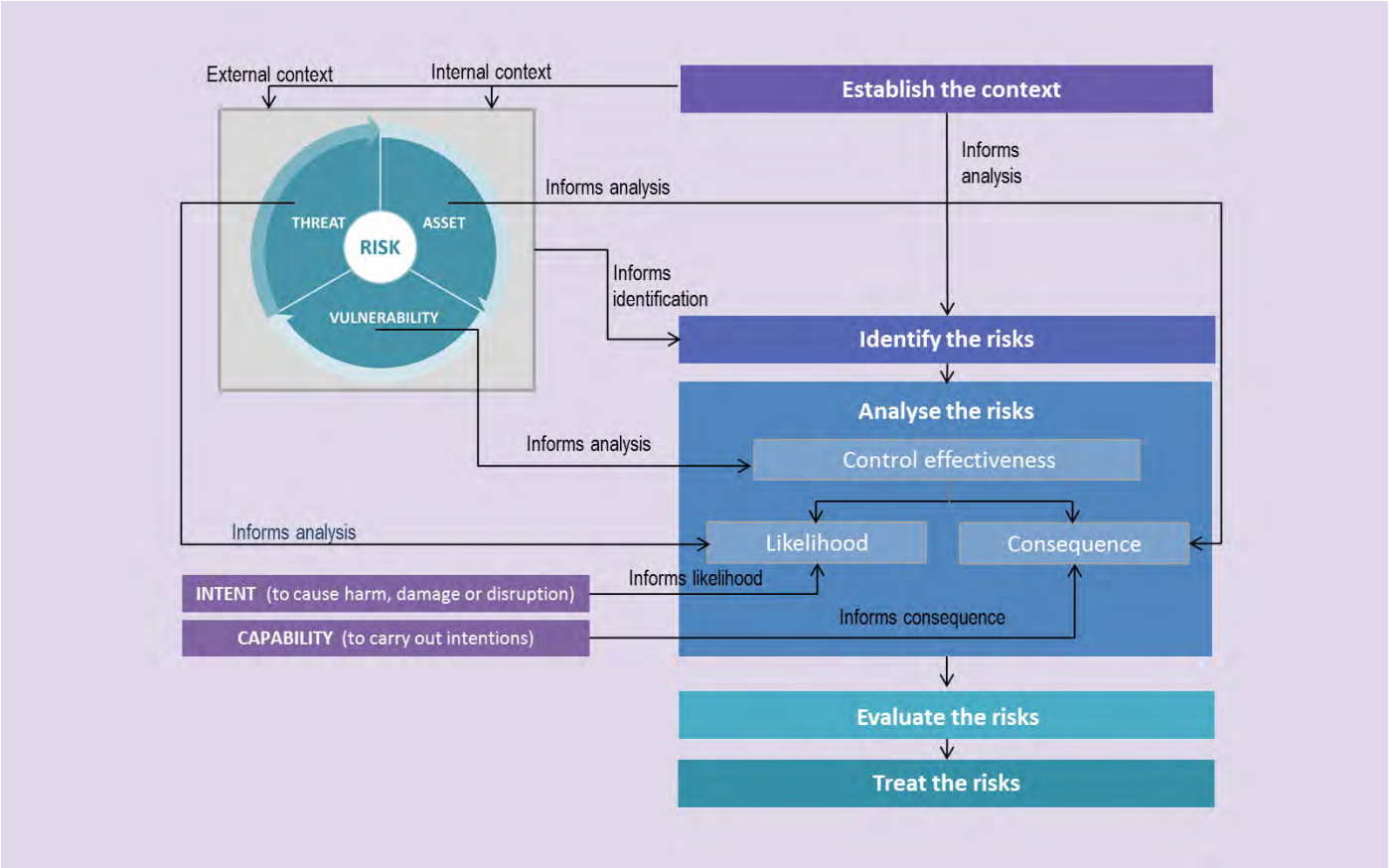
ii. **consequence** – the outcome affecting objectives if the event occurs[Error! Bookmark not defined.] (consequences can be expressed qualitatively or quantitatively and can be certain or uncertain and have positive or negative effects on objectives). There may be a number of possible outcomes associated with an event.

c. Assign the level of risk rating based on the likelihood and consequence risk matrix. The overall risk rating is determined by combining the likelihood and consequence estimations. Risk rating allows the security risk to be prioritised in order of decreasing risk levels. This helps with deciding the tolerability of risk in the evaluation step. The Attorney-General's Department recommends adopting a risk-rating-matrix approach for determining the levels of risk.

d. Prioritise risks for subsequent evaluation of tolerance or the need for further treatment.

e. Provide an improved understanding of the vulnerability of critical assets to identified risks.

Annex A Figure 2 Using threat, criticality and vulnerability to inform risk analysis



Evaluate security risks

20. Risk evaluation involves making decisions based on the outcomes of risk analysis about whether risks are:

    a. **acceptable** (tolerable) with existing controls or further treatment (risks identified as acceptable or tolerable with no further treatment still need to be documented, monitored and periodically reviewed to ensure they remain acceptable)

    b. **unacceptable** (intolerable) and need treatments (consideration is given to the criteria for determining tolerability).

21. Refer to section C.2.4 for information on risk tolerances.

Treat security risks

22. Appropriate risk mitigation treatments and controls are selected to address identified risks in accordance with the entity's security plan objectives. Efforts to treat risks will not remove them completely but aim to reduce them to a more tolerable level.

23. Risk treatments can be applied separately or in combination. When selecting treatment, the Attorney-General's Department recommends that the entity balances the cost and effort of implementing the treatment with the expected benefits and ensure the treatment is proportional to the determined risk rating level. It may not be possible or cost-effective to implement all possible risk treatments. However, it is necessary to choose, prioritise and implement the most appropriate treatment or combination of treatments.

24. Australian Standards HB 167: Security Risk Management Chapter 7 outlines strategies for risk treatment. This includes a six-step process where entities:

    a. prioritise intolerable risks

    b. establish treatment options

    c. identify and develop treatment options

    d. evaluate treatment options

e. detail design and review of chosen options, including the management of residual risks

f. communicate and implement.

25. Treatment plans:

a. prioritise the risks to be treated

b. assess current risk; the actual risk once all treatments have been implemented

c. identify gaps and residual risks that remain or require further treatment

d. capture decisions about treatments and actions to be taken to address or treat identified security risks

e. determine appropriate timeframes to implement treatment or when further consideration of mitigations is required be considered

f. identify resources, budget allocations, timeframes (defined and measurable) and responsibilities to achieve required treatment outcomes

g. establish monitoring and reviewing processes.

26. Risk treatment strategies (examples):

a. Accept the risk, where:

i. based on judgment or informed decision, the risk is considered to be tolerable (either before or after treatment)

ii. the only option is to retain the risk and continue to monitor it until the circumstances change and action can be taken

iii. taking on increased risk in order to pursue an opportunity where the benefit outweighs the risk

iv. the risk may be considered intolerable but due to capability, resources or exceptional circumstances may be accepted.

b. Avoid the risk,[5] by:

i. deciding not to start an activity that gives rise to the risk

ii. removing or reducing the activities or personnel, including contractors, that create the exposure.

c. **Exploit the risk**, by taking or increasing the risk in order to realise the benefit that an opportunity affords by ensuring the event occurs.

d. **Reduce the risk**, by changing the likelihood or consequence (or both) by:

i. implementing new treatments or controls to reduce, deter, delay or detect the threat or event

ii. improving business processes, training or practices

iii. establishing or improving audit and compliance arrangements, contractual arrangements, communication channels etc.

e. Share the risk, where:

i. the risk has no single owner but is shared with another party or parties (eg through shared services, entities co-located in the same building, inter-entity taskforce, partnership or joint venture)

ii. the risk may have no apparent owner.

27. Refer to section C.2.3.2 for information on shared security risks.

[5] Where entities have been directed to undertake the activity, they will not be able to avoid the risks. Risk treatment is preferable to risk aversion or avoidance.

Implementation

28. Implementation involves deciding on the resources required and who is responsible for implementing the risk treatments. In addition, implementation details the ongoing resources needed to maintain the required level of protective security and identifies resources that may be needed to take additional precautions if the threat level increases.

29. Refer to section C.3 for information on security alert levels.

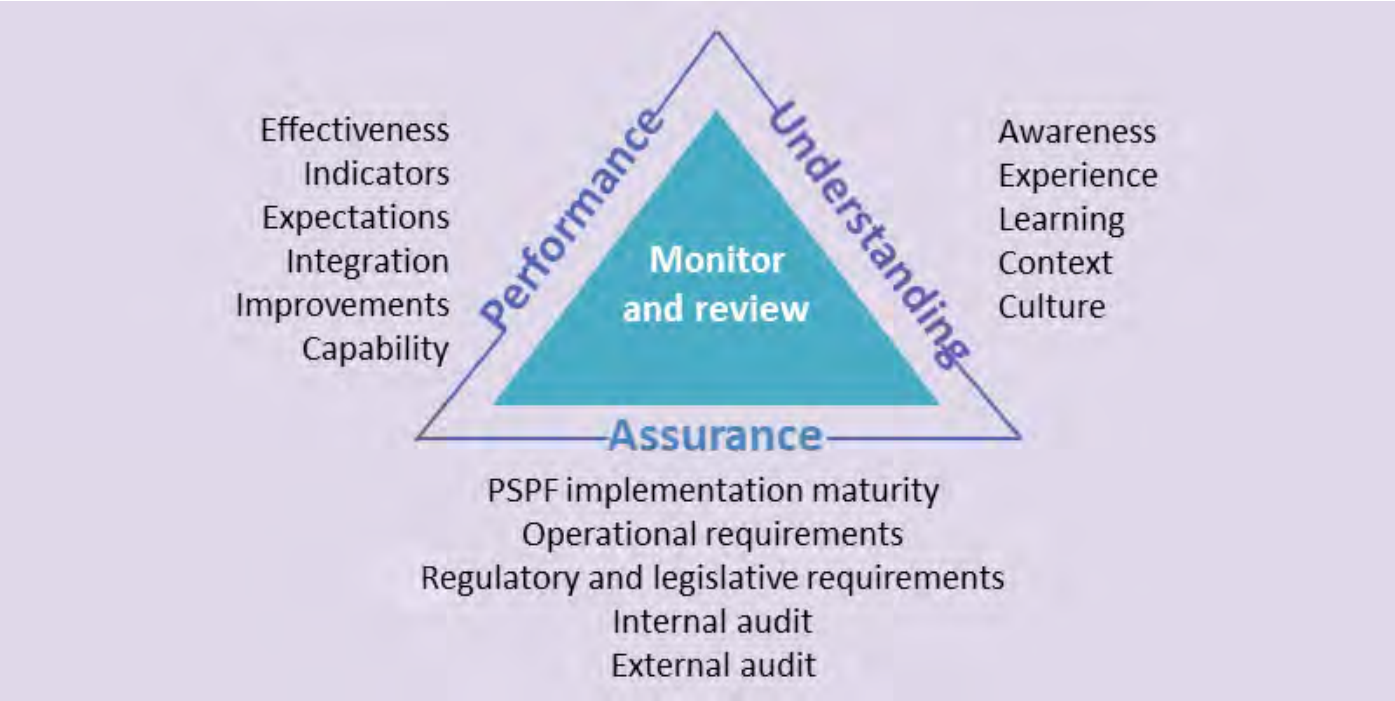
Monitoring and review performance

30. Security risk management requires monitoring to ensure the entity is able to adapt or respond to incidents and changes in their threat or risk environment, prevent further exposure to hazards, maintain a positive risk culture and deliver against the PSPF.

31. Making decisions and implementing risk treatments is not the end of risk management. The security planning cycle is continuous. Reviewing the external and internal environments and reconsidering the context allows the entity to determine how effectively their protective security controls and measures are performing and how they are achieving the objectives.

32. Australian Standards HB 167: 2006 Security Risk Management Chapter 8 outlines strategies for monitoring and review, including the following model.

Annex A Figure 3 Monitoring and reviewing security performance



33. Key questions to ask when monitoring and reviewing risk may include:

    a. Are the controls (and respective implementation strategies) effective in minimising the risks; how might improvements be made?

    b. Are the controls comparatively efficient and cost-effective?

    c. Are the assumptions made about the context/environment still valid?

    d. Do controls comply with policy requirements, legal obligations and entity procedures?

    e. Is the entity's security planning approach effective in managing security risks and achieving objectives?

34. Refer to:

    a. Commonwealth Risk Management Policy Element Five – Developing a positive risk culture

    b. Commonwealth Risk Management Policy Element Nine – Reviewing and continuously improving the management of risk

c. PSPF policy: Security maturity monitoring.