4 Security maturity monitoring

A. Purpose

1. This policy describes how an entity monitors and assesses the maturity of its security capability and risk culture. This includes an entity's capability to actively respond to emerging threats and changes in its security environment, while maintaining the protection of its people, information and assets.

B. Requirements

B.1 Core requirement

Each entity must assess the maturity of its security capability and risk culture by considering its progress against the goals and strategic objectives identified in its security plan.

B.2 Supporting requirements

Supporting requirements for security maturity monitoring

#	Supporting requirements
Requirement 1. Security maturity records	Entities **must** document and evidence their assessment of the entity's security maturity.

C. Guidance

C.1 Security capability maturity

2. Security capability maturity refers to an entity's security position in relation to its specific risk environment and risk tolerances. This includes acknowledging the successes and effectiveness of PSPF implementation, as well as highlighting areas for improvement.
3. Maturity of security capability considers how holistically and effectively each entity:
   a. implements and meets the intent of the PSPF core and supporting requirements
   b. minimises harm to the government's people information and assets
   c. fosters a positive security culture
   d. responds to and learns from security incidents
   e. understands and manages its security risks
   f. achieves security outcomes while delivering business objectives.

C.2 Security risk culture

4. Security risk culture is the entity's system of values and its personnel's behaviours, attitudes and understanding that are related to security risk that shapes the risk decisions of the entity leadership and personnel. Having a mature risk culture is a fundamental enabler of good government business. Maturity of

risk culture is driven by the accountable authority and is underpinned by the PSPF policy: Role of accountable authority.

5. An entity with a mature security risk culture is one where the leadership team and personnel:
   a. comprehensively understand security risks
   b. appropriately manage security risks in their operational environments
   c. prioritise security risk management in their everyday practices
   d. make informed decisions on risks within agreed entity security risk tolerances
   e. react and respond to changes in the security risk environment.
6. For information see the PSPF policy: Security planning and risk management.

C.3 Monitoring security maturity

7. Monitoring security maturity is an ongoing process and involves routine assessment of the entity's security capability and risk culture against a set of indicators.
8. The benefits of effective security maturity monitoring include improved:
   a. understanding of the entity's security risks and risk mitigation strategies
   b. performance of the entity in:
      i. implementing the minimum core and supporting PSPF requirements in relation to its risk environment
      ii. driving a strong security culture through awareness of agreed security behaviours
      iii. identifying and implementing changes that achieve robust security outcomes
      iv. using resources efficiently and effectively to protect people, information and assets
   c. assurance that the entity's:
      i. people, information and assets are adequately protected consistent with government policy
      ii. security risks are managed appropriately (including security incidents) and clear lines of accountability and sound planning and proportionate reporting are undertaken.
9. The Attorney-General's Department recommends entities develop their security maturity monitoring plan as part of their overarching security plan. This includes:
   a. using security maturity indicators as detailed in the PSPF Maturity Self-Assessment Model (Annex A to the PSPF policy: Reporting on security)
   b. setting goals and objectives and identifying the impact on security of any goals and objectives detailed in the entity security plan
   c. developing methodologies to manage the collection, measurement and analysis of data in relation to the entity's security maturity indicators
   d. determining the frequency of security monitoring advice to be given to the accountable authority, Chief Security Officer, audit committee (see the PSPF policy: Management structures and responsibilities) and relevant security governance committee (if established in the entity)
   e. setting pre-determined levels of change in security maturity metrics that trigger escalation to the accountable authority, Chief Security Officer, audit committee and relevant security governance committees
   f. where applicable, identifying the responsible area and timeframes to:
      i. manage implementation of PSPF core and supporting requirements
      ii. implement strategies that achieve improvements in security culture.

10. **Requirement 1** mandates that an entity must document and evidence its assessment of its security maturity. This can be part of the security maturity monitoring plan where the entity records its progress against the goals and objectives of the security plan.

11. Figure 1 illustrates the stages of effective security maturity monitoring as a continuous improvement cycle. This can assist an entity to respond to changes in its security environment and emerging security risks. It can help entities implement the PSPF core and supporting requirements necessary to protect people, information and assets.

Figure 1 Security maturity monitoring cycle

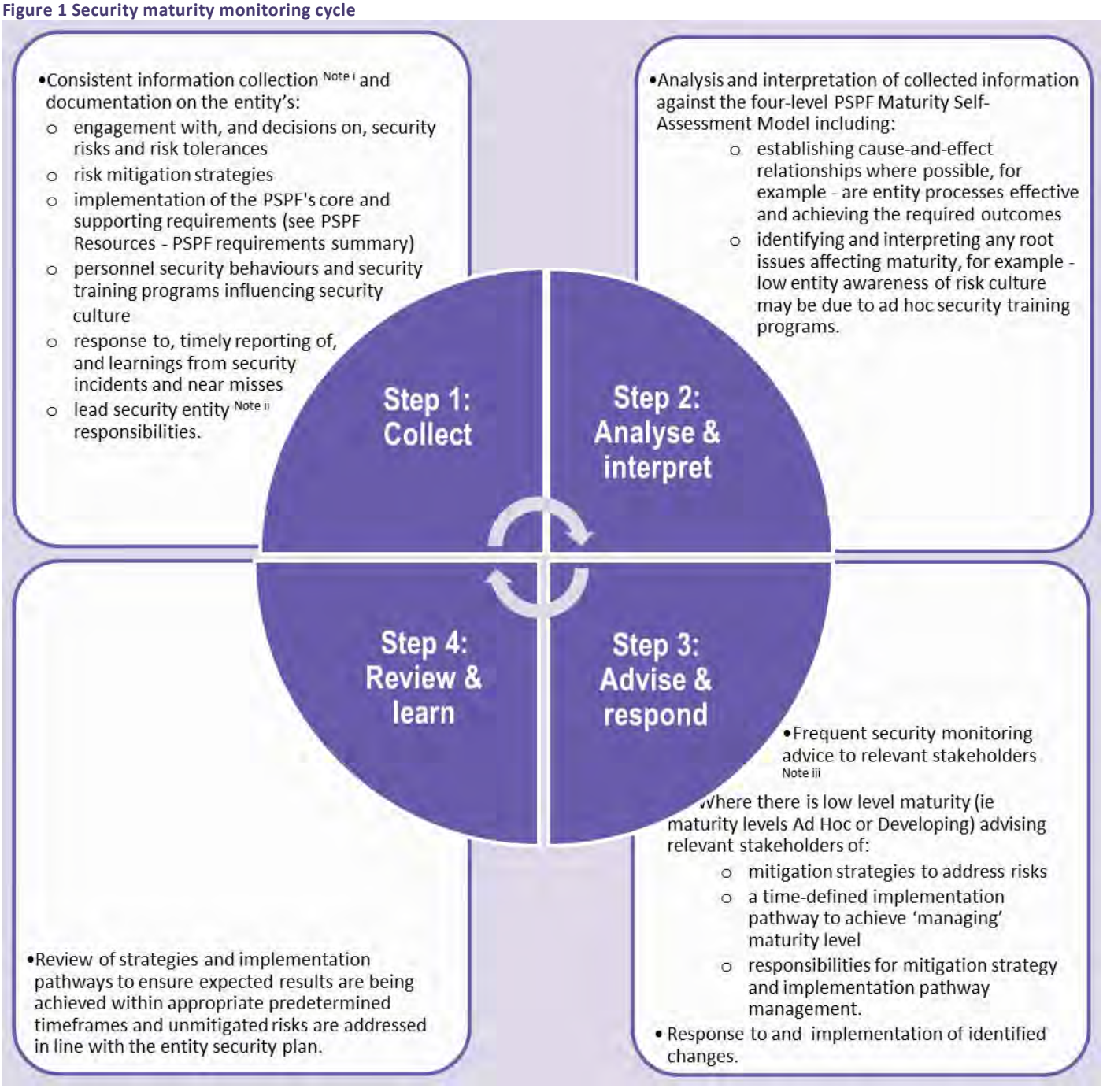

Figure 1 notes:

[i] Step 1 sources of information collection include:

a. pre-existing information
   i. systematic and routine audits of entity security practices
   ii. security incident and near miss reporting
   iii. direct observations and security facility inspections
   iv. informal and formal security networks
b. tasks to derive information
   i. reviews of entity security practices and commissioned research

ii. internal focus groups and security questionnaires
iii. stakeholder consultation
iv. horizon scanning for early identification of emerging security issues internal and external to government that may impact security maturity.

[ii] Where an entity has been identified as a lead security entity (see the PSPF policy: Management structures and responsibilities), the Attorney-General's Department recommends additional information is collected and assessed on the entity's:

a. provision of effective and timely advice, guidance and services related to the entity's area of security expertise
b. management of responsibilities and accountabilities for partnerships and security service arrangements with other entities.

[iii] Relevant stakeholders to advise under Step 3 may include the accountable authority, the Chief Security Officer, audit committee and relevant security governance committees (if established in the entity).

12. Security maturity monitoring is a continuous cycle and the information collected informs the entity security plan and the PSPF policy: Reporting on security.

D. Find out more

13. Other standards that may be relevant:

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

D.1 Change log

Table 1 Amendments in this policy

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