PSPF Webinar

A (brief) overview of the Australian Government's Protective Security Policy Framework (PSPF)

STARTING SOON

SRMBOK

Security Risk Management Body Of Knowledge

Julian Talbot

RegSecP, CISSP, FRMIA, FISRM

Chief Technology Officer | Director | Cofounder

Speed, Rigour, and Consistency in Security Risk Assessment

www.juliantalbot.com

SRMBOK

Security Risk Management Body Of Knowledge

www.sert.solutions - DOWNLOADS

Protective Security Policy Framework Overview

A summary of the Australian Government Protective Security Policy Framework (PSPF) and recommendations for improving self-assessment reporting.

March 2023

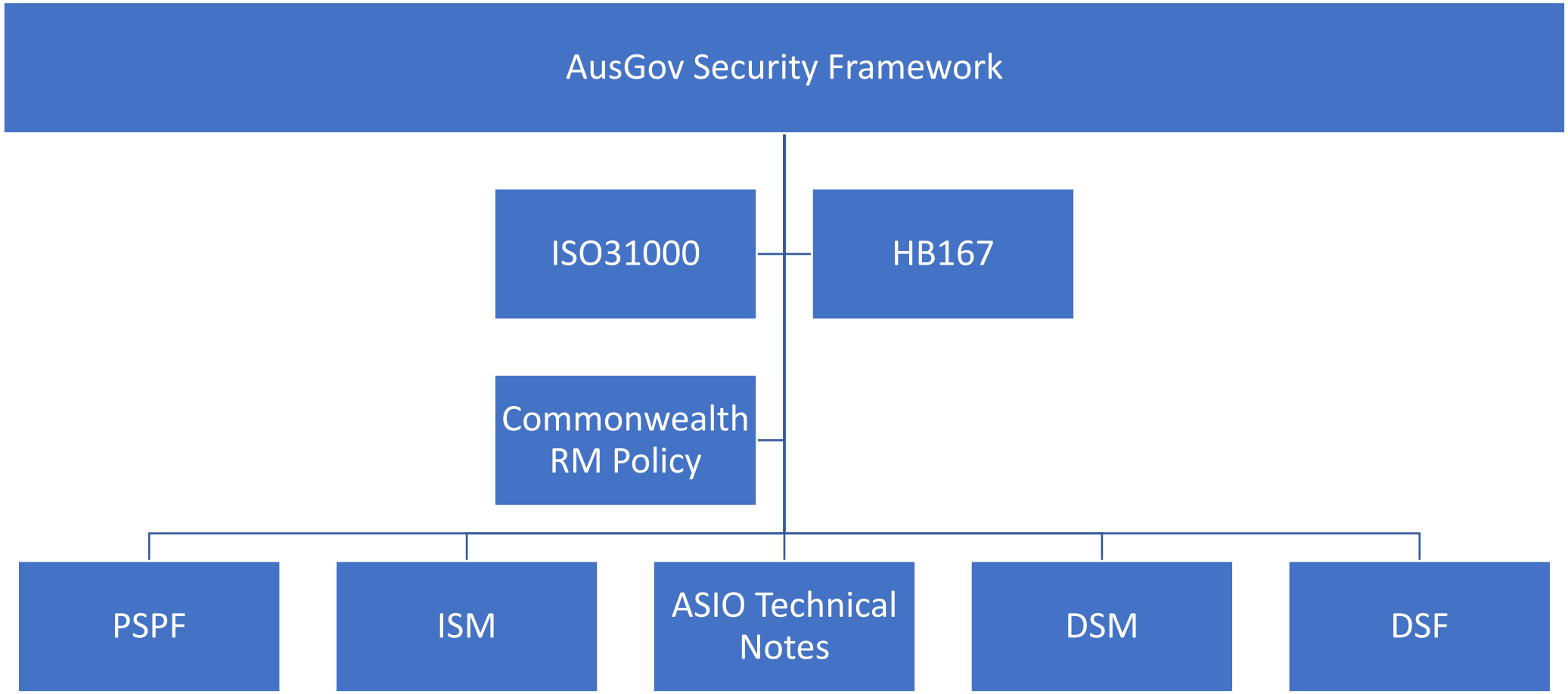
The PSPF

- Australian Government established the Protective Security Policy Framework (PSPF) to provide a comprehensive approach to security
- PSPF sets out mandatory policies and guidelines for AusGov entities to manage security risks and protect their people, information, and assets
- PSPF covers topics such as physical security, information security, personnel security, and emergency management
- PSPF also requires government entities to undertake regular security risk assessments and implement appropriate controls based on the level of risk
- Compliance with the PSPF is mandatory for all AusGov entities
- Failure to comply may result in disciplinary action or other consequences

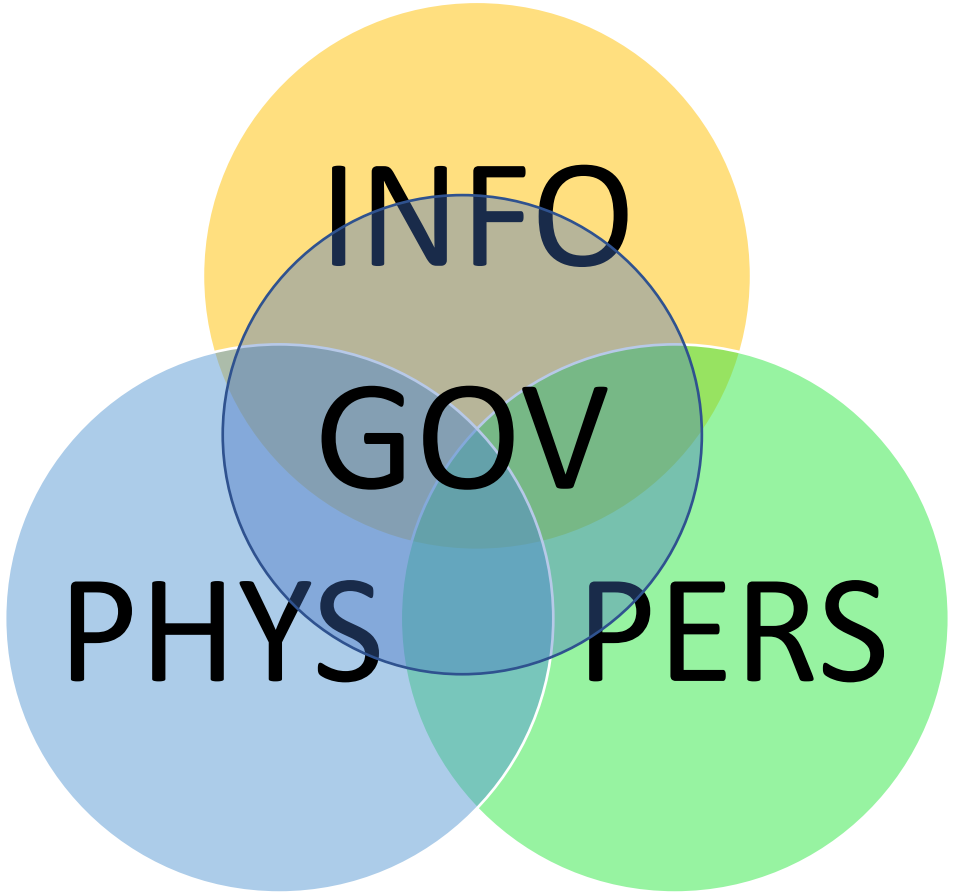
Background to the PSPF

- The ASIO Protective Security Manual (PSM)
- The Australian Government Security Manual (AGSM)
- Other relevant legislation and policies:
  - Privacy Act 1988
  - Archives Act 1983
  - The Intelligence Services Act 2001
  - The Australian Signals Directorate Act 2018
  - The Security of Critical Infrastructure Act 2018
  - The Protective Security Act 2021
  - The Australian Government Information Security Manual (ISM)

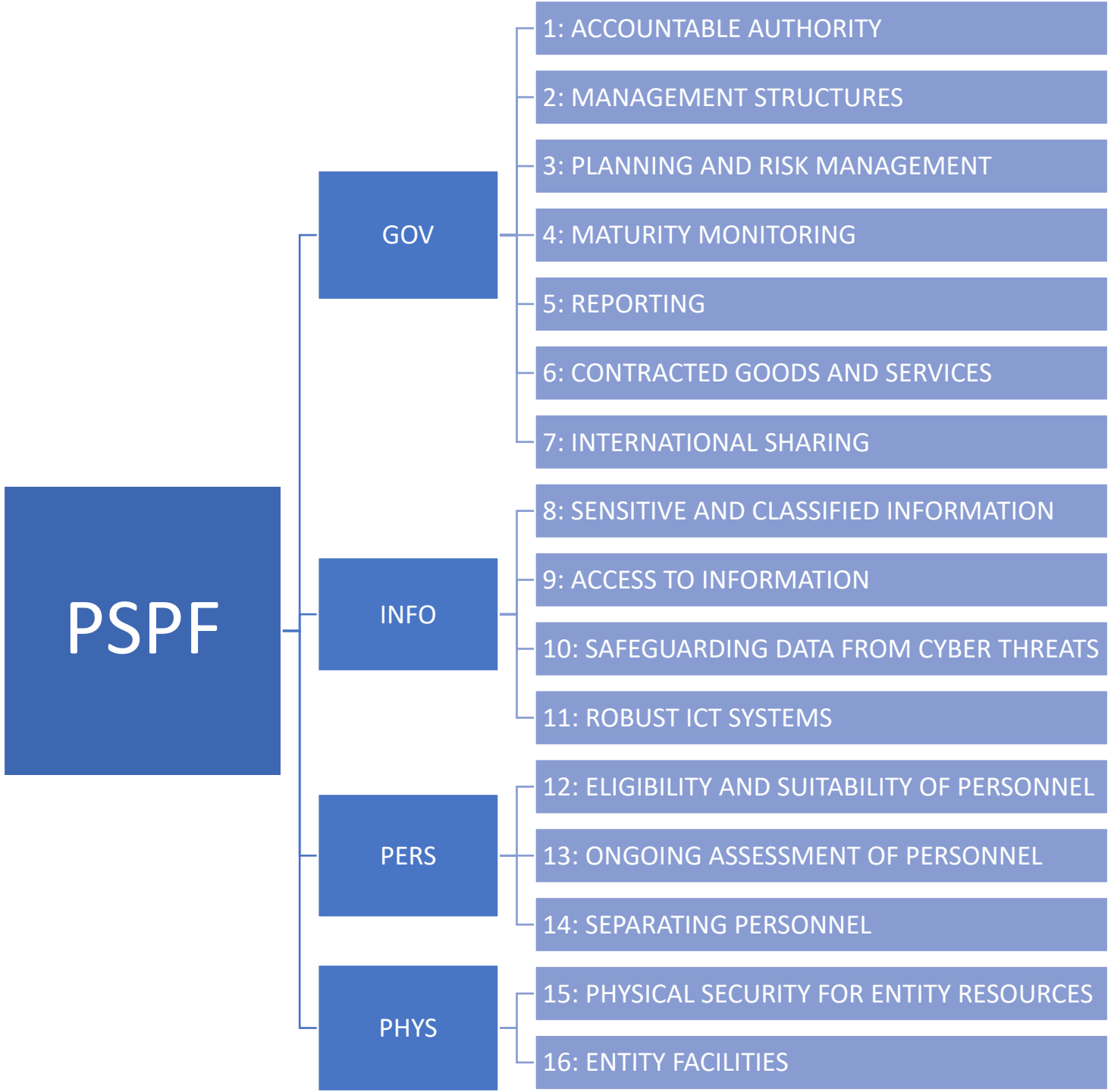
The PSPF Family



PSPF Components



Cybersecurity?


PSPF
GOV
1: ACCOUNTABLE AUTHORITY
2: MANAGEMENT STRUCTURES
3: PLANNING AND RISK MANAGEMENT
4: MATURITY MONITORING
5: REPORTING
6: CONTRACTED GOODS AND SERVICES
7: INTERNATIONAL SHARING
INFO
8: SENSITIVE AND CLASSIFIED INFORMATION
9: ACCESS TO INFORMATION
10: SAFEGUARDING DATA FROM CYBER THREATS
11: ROBUST ICT SYSTEMS
PERS
12: ELIGIBILITY AND SUITABILITY OF PERSONNEL
13: ONGOING ASSESSMENT OF PERSONNEL
14: SEPARATING PERSONNEL
PHYS
15: PHYSICAL SECURITY FOR ENTITY RESOURCES
16: ENTITY FACILITIES

Policy 1: Role of Accountable Authority

- *"The accountable authority is **answerable to their portfolio minister** for the protective security of the entity's **people, information and assets**.*
- *In meeting obligations to their portfolio minister, the accountable authority is **supported by a Chief Security Officer** and, where appropriate, a **security governance committee**."*

Core Requirement

The Accountable Authority of each entity must:

a. determine their entity's tolerance for security risks

b. manage the security risks of their entity, and

c. consider the implications their risk management decisions have for other entities and share information on risks where appropriate.

Core Requirement

The accountable authority of a lead security entity must:

a. provide other entities with advice, guidance and services related to government security

b. ensure that the security support it provides helps relevant entities achieve and maintain an acceptable level of security, and

c. establish and document responsibilities and accountabilities for partnerships or security service arrangements with other entities.

Australia's lead entities that hold key protective security accountabilities services

- Attorney-General's Department
- Australian Secret Intelligence Service
- Australian Signals Directorate
- Department of Foreign Affairs and Trade
- National Archives of Australia
- Digital Transformation Agency
- Department of the Prime Minister and Cabinet
- Australian Federal Police (AFP)
- Australian Security Intelligence Organisation
- Department of Defence
- Department of Home Affairs
- Office of National Intelligence
- Office of the Australian Information Commissioner

Supporting Requirements

Requirement 1. Exceptional circumstances	Where exceptional circumstances prevent or affect an entity's capability to implement a PSPF requirement, the accountable authority: a. **may** vary application, for a limited period of time, consistent with the entity's risk tolerance b. **must** record the decision to vary in the annual report on security to the Attorney-General's Department and advise remedial action taken to reduce the risk to the entity.

Policy 1: Accountable Authority - Key Concepts

Governance structures

Risk-based protective security

Balancing security and operational needs

Security Risk Management

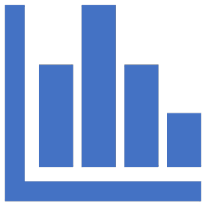
- Security risk management includes **identifying, assessing and prioritising risks** to people, information and assets. It involves the efficient and coordinated application of **protections that minimise, monitor and control the probability and effects of risks**.
  - informed decisions on priorities
  - balances the entity's capacity to deliver business objectives while maintaining a secure environment
  - determining the level of risk the entity is willing or able to accept
  - common-sense approach when setting security risk tolerance levels

Exceptional Circumstances

- Exceptional circumstances prevent or affect an entity's capability to implement a PSPF requirement
- The accountable authority may vary application (for a limited period of time) consistent with the entity's risk tolerance. E.g.: natural disasters and emergency situations
- Exceptional circumstances are not routine in nature or enduring
- Must record the decision to vary in the annual report

Policy 5: Reporting on Security

Reporting requirements for organizations



Frequency of required reports

Contents of reports

Policy 5: Core Requirement

Each entity must report on security:

a. each financial year to its portfolio minister and the Attorney-General's Department addressing:
   I. whether the entity achieved security outcomes through effectively implementing and managing requirements under the PSPF
   II. the maturity of the entity's security capability
   III. key security risks to the entity's people, information and assets, and
   IV. details of measures taken to mitigate or otherwise manage identified security risks

b. to affected entities whose interests or security arrangements could be affected by the outcome of unmitigated security risks, security incidents or vulnerabilities in PSPF implementation

c. to the Australian Signals Directorate in relation to cyber security matters.

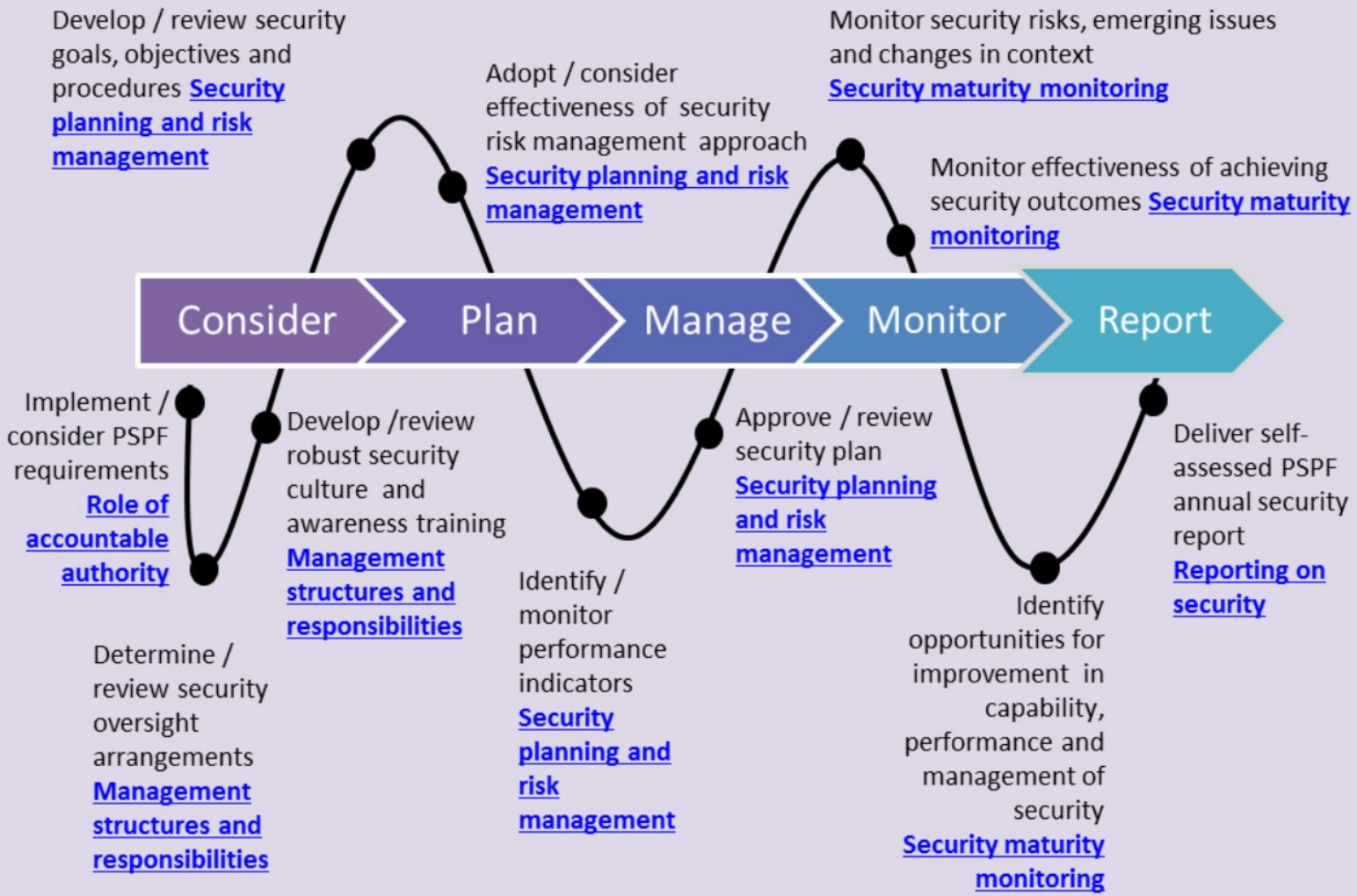
Policy 5: Supporting Requirements

Requirement 1. PSPF reporting model and template	Each entity **must** submit a report on security each financial year: a. through the PSPF online reporting portal for information up to PROTECTED or b. by submitting an offline reporting template for information classified higher than PROTECTED.
Requirement 2. Reporting security incidents	Each entity **must** report any significant or reportable security incidents at the time they occur to: a. the Attorney-General's Department b. the relevant lead security authority c. other affected entities. Table 3 provides detailed guidance on reporting security incidents.
Requirement 3. ASD cyber security survey	Each entity **must** complete the Australian Signals Directorate's annual cyber security survey.

Maturity Self-Assessment Model

- **Ad hoc:** partial or basic implementation and management of PSPF core and supporting requirements
- **Developing:** substantial, but not fully effective implementation and management of PSPF core and supporting requirements
- **Managing:** complete and effective implementation and management of PSPF core and supporting requirements-this is the baseline maturity level for reporting entities
- **Embedded:** comprehensive and effective implementation and proactive management of PSPF core and supporting requirements and excelling at implementation of better-practice guidance

Collecting Information on Security Maturity



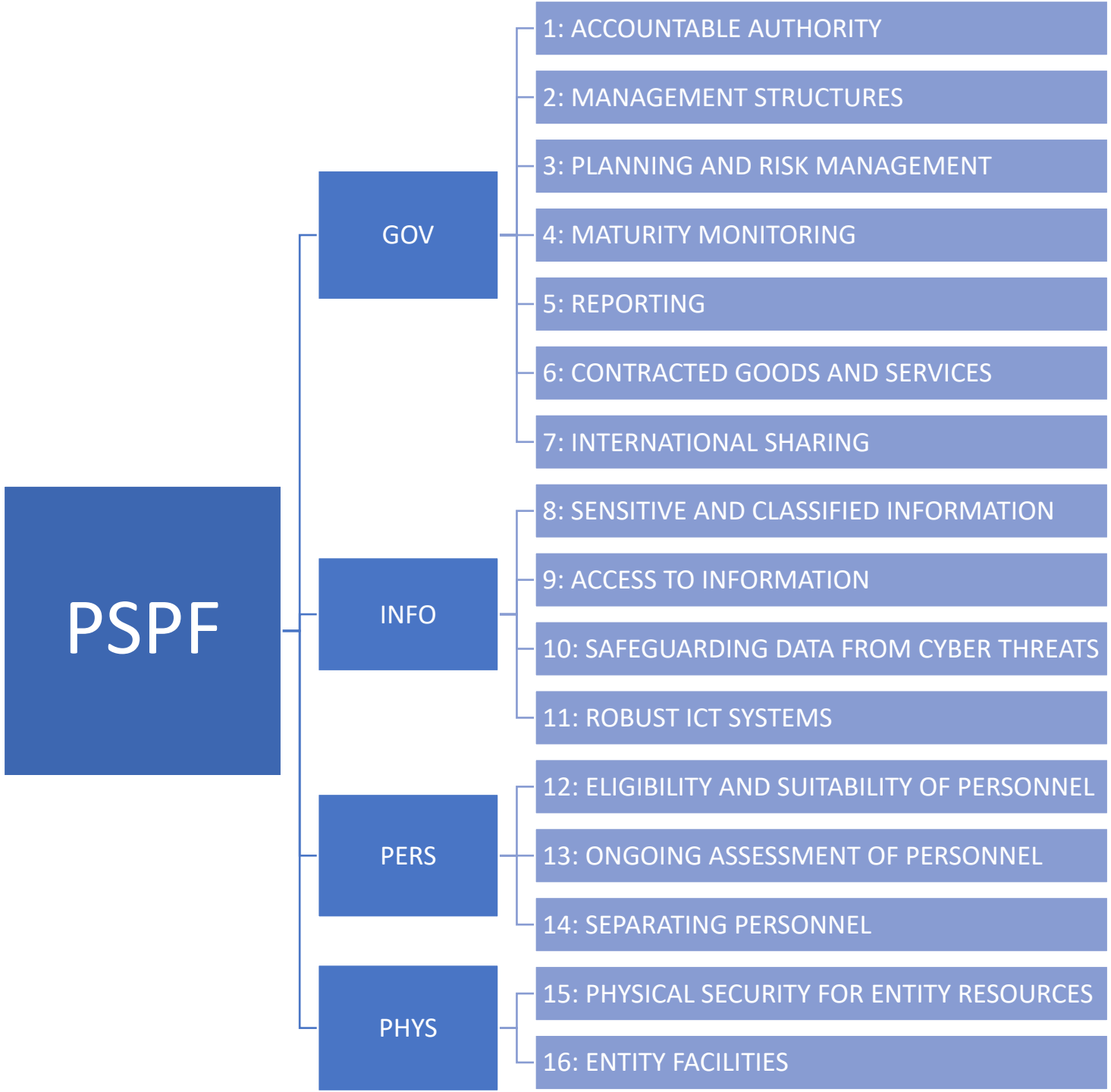
SRMBOK
Security Risk Management Body Of Knowledge

Policy 5: Reporting Frequency

Determining appropriate reporting intervals

Balancing timeliness and thoroughness

Adjusting reporting frequency as needed


PSPF
GOV
1: ACCOUNTABLE AUTHORITY
2: MANAGEMENT STRUCTURES
3: PLANNING AND RISK MANAGEMENT
4: MATURITY MONITORING
5: REPORTING
6: CONTRACTED GOODS AND SERVICES
7: INTERNATIONAL SHARING
INFO
8: SENSITIVE AND CLASSIFIED INFORMATION
9: ACCESS TO INFORMATION
10: SAFEGUARDING DATA FROM CYBER THREATS
11: ROBUST ICT SYSTEMS
PERS
12: ELIGIBILITY AND SUITABILITY OF PERSONNEL
13: ONGOING ASSESSMENT OF PERSONNEL
14: SEPARATING PERSONNEL
PHYS
15: PHYSICAL SECURITY FOR ENTITY RESOURCES
16: ENTITY FACILITIES

8 Sensitive and classified information

Protective Security Policy Framework

Table 1 Business Impact Levels tool – Assessing damage to the national interest, government, organisations or individuals

	Sensitive information		Security classified information		
	OFFICIAL	OFFICIAL: Sensitive	PROTECTED	SECRET	TOP SECRET
Sub-impact category ↓	1 Low business impact **The majority of official information created or processed by the public sector.** This includes routine business operations and services. OFFICIAL is not a security classification and compromise of OFFICIAL information would result in **no or insignificant damage to individuals, organisations or government.**	2 Low to medium business impact **OFFICIAL information that due to its sensitive nature requires limited dissemination.** OFFICIAL: Sensitive is not a security classification. It is a dissemination limiting marker (DLM), indicating compromise of the information would result in **limited damage to an individual, organisation or government.**	3 High business impact **Valuable, important and sensitive information.** Compromise of PROTECTED information would be expected to cause **damage to the national interest, organisations or individuals.**	4 Extreme business impact **Very valuable, important and sensitive information**. Compromise of SECRET information would be expected to cause **serious damage to the national interest, organisations or individuals.**	5 Catastrophic business impact **The most valuable, important and sensitive information.** Compromise of TOP SECRET information would be expected to cause **exceptionally grave damage to the national interest, organisations or individuals.**
Potential impact on individuals from compromise of the information					
Dignity or safety of an individual (or those associated with the individual)	Information from routine business operations and services. Includes personal information as defined in the *Privacy Act*.[i] This may include information (or an opinion) about an identifiable individual (eg members of the public, staff etc) but would not include information defined as sensitive information under the *Privacy Act*.	Limited damage to an individual is: a. potential harm, for example injuries that are not serious or life threatening or b. discrimination, mistreatment, humiliation or undermining an individual's dignity or safety that is **not life threatening**.	Damage to an individual is discrimination, mistreatment, humiliation or undermining of an individual's dignity or safety that leads to potentially **significant harm or potentially life threatening injury**.	Serious damage is discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to **directly threaten or lead to the loss of life of an individual or small group**.	Exceptionally grave damage is: a. widespread loss of life b. discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to directly lead to the death of a large number of people.
Potential impact on organisations from compromise of the information					
Entity operations, capability and service delivery	Information from routine business operations and services.	Limited damage to entity operations is: a. a degradation in organisational capability to an extent and duration that, while the **entity can perform its primary functions**, the effectiveness of the functions is noticeably reduced b. minor loss of confidence in government.	Damage to entity operations is: a. a degradation in, or loss of, organisational capability to an extent and duration that the **entity cannot perform one or more of its primary functions** b. major loss of confidence in government.	Serious damage to entity operations is: a. a severe degradation in, or loss of, organisational capability to an extent and duration that the **entity cannot perform any of its functions** b. directly threatening the internal stability of Australia.	Not applicable. Impacts on an entity or organisation due to compromise of information are assessed as to the level of impact to the national interest.
Entity assets and finances, eg operating budget	Information compromise would result in insignificant impact to the entity assets or annual operating budget.	Limited damage to entity assets or annual operating budget is equivalent to **$10 million to $100 million**.	Damage is: a. substantial financial loss to an entity b. **$100 million to $10 billion** damage to entity assets.	Not applicable. Impacts on an entity or organisation at this scale are considered a matter of national interest.	Not applicable. Impacts on an entity or organisation due to compromise of information are assessed as to the level of impact to the national interest.
Legal compliance, eg information compromise would cause non-compliance with legislation,[ii] commercial confidentiality or legal professional privilege	Information compromise would not result in legal and compliance issues.	Limited damage is: a. issues of legal professional privilege for communications between legal practitioners and their clients b. contract or agreement non-compliance c. failure of statutory duty d. breaches of information disclosure limitations under legislation resulting in less than two years' imprisonment.	Damage is: a. failure of statutory duty or breaches of information disclosure limitations under legislation resulting in two or more years' imprisonment.	Not applicable. Impacts on an entity or organisation at this scale are considered a matter of national interest.	Not applicable. Impacts on an entity or organisation due to the compromise of information are assessed as to the level of impact to the national interest.
Aggregated data[iii]	An aggregation of routine business information.	A significant aggregated holding of information that, if compromised, would cause limited damage to the national interest, organisations or individuals.	A significant aggregated holding of sensitive information that, if compromised, would cause damage to the national interest, organisations or individuals.	A significant aggregated holding of sensitive or classified information that, if compromised, would cause serious damage to the national interest, organisations or individuals.	A significant aggregated holding of sensitive or classified information that, if compromised, would cause exceptionally grave damage to the national interest, organisations or individuals.
Potential impact on government or the national interest from compromise of the information					
Policies and legislation	Information compromise from routine business operations and services. For example, this may include information in a draft format (not otherwise captured by higher business impact level).	Limited damage to government is impeding the development or operation of policies.	Damage to the national interest is: a. impeding the development or operation of major policies b. revealing deliberations or decisions of Cabinet, or matters submitted, or proposed to be submitted, to Cabinet[iv] (not otherwise captured by higher level business impacts).	Serious damage to the national interest is: a. a severe degradation in development or operation of multiple major policies to an extent and duration that the policies can no longer be delivered.	Exceptionally grave damage to the national interest is the collapse of internal political stability of Australia or friendly countries.
Australian economy	Information from routine business operations and services.	Limited damage to government is: a. undermining the financial viability of one or more individuals, minor Australian-based or owned organisations or companies	Damage to the national interest is: a. undermining the financial viability of a major Australian-based or owned organisation or company	Serious damage to the national interest is: a. undermining the financial viability of an Australian industry sector (multiple major organisations in the same sector)	Exceptionally grave damage to the national interest is the collapse of the Australian economy.

8a Annex. Sensitive and classified information

Protective Security Policy Framework

Message type	Example
A message containing sensitive information that is legally privileged (where the entity wishes to categorise information content)	From: neville.jones@entity.gov.au To: alice@example.gov.au Message-ID: <42113213312443432456743 5@entity.gov.au> MIME-Version: 1.0 Content-Type: text/plain; charset=ISO-8859-1 Content-Transfer-Encoding: 7bit X-Protective-Marking: VER=2018.4, NS=gov.au, SEC=OFFICIAL:Sensitive, ACCESS=Legal-Privilege, ORIGIN=neville.jones@entity.gov.au Subject: This is an example subject line This is an example message body. Bye, Neville
A message containing sensitive information prepared for National Cabinet or its subcommittees	From: neville.jones@entity.gov.au To: alice@example.gov.au Message-ID: <42113213312443432456743 5@entity.gov.au> MIME-Version: 1.0 Content-Type: text/plain; charset=ISO-8859-1 Content-Transfer-Encoding: 7bit X-Protective-Marking: VER=2018.4, NS=gov.au, SEC=OFFICIAL:Sensitive, CAVEAT=SH:NATIONAL-CABINET, ORIGIN=neville.jones@entity.gov.au Subject: This is an example subject line This is an example message body. Bye, Neville

Policy 2: Management Structures and Responsibilities

Governance in relation to the PSPF

Security roles within an organization

Must, Should, May

B1: Core Requirement

The accountable authority must:

a) appoint a Chief Security Officer (CSO) at the Senior Executive Service1 level to be responsible for security in the entity

b) empower the CSO to make decisions about:
   i. appointing security advisors within the entity
   ii. the entity's protective security planning
   iii. the entity's protective security practices and procedures
   iv. investigating, responding to, and reporting on security incidents, and

c) ensure personnel and contractors are aware of their collective responsibility to foster a positive security culture, and are provided sufficient information and training to support this.

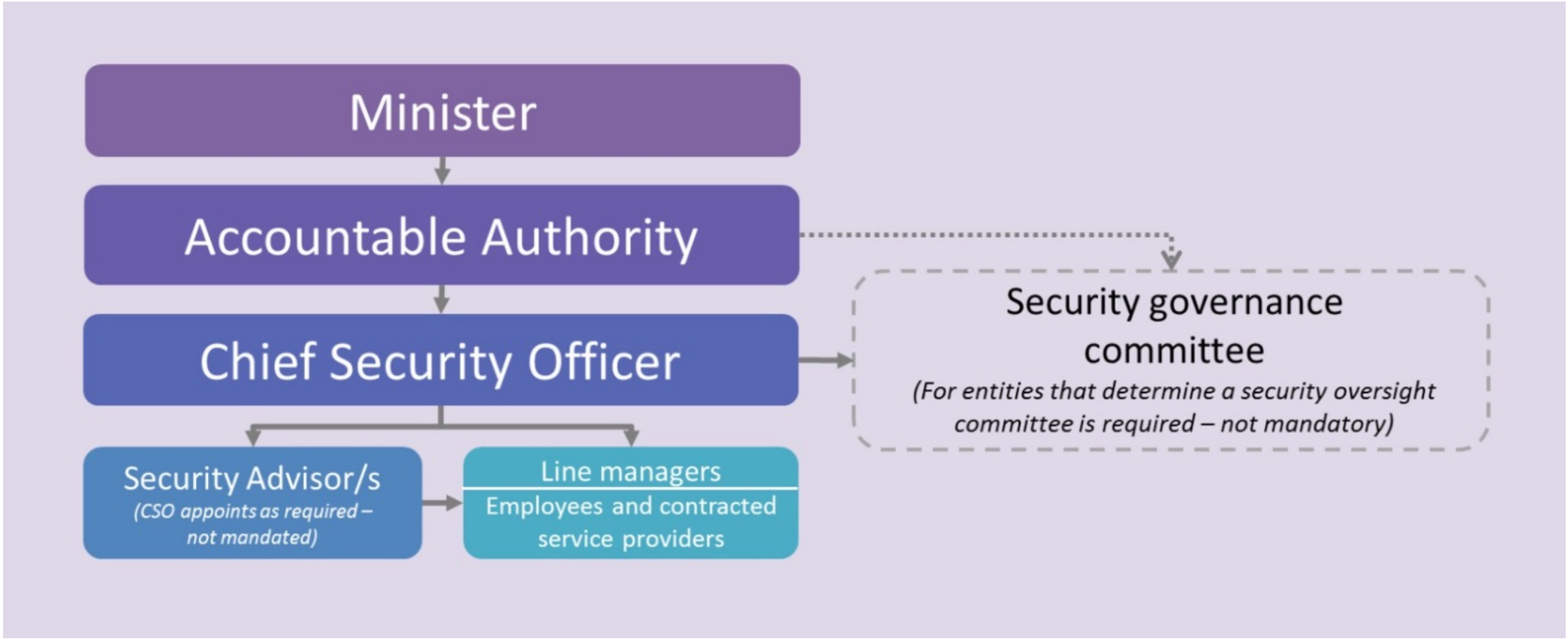
B2. Supporting Requirements

Requirement 1. Security advisors	The CSO **must** be responsible for directing all areas of security to protect the entity's people, information (including ICT) and assets. This includes appointing security advisors to support them in the day-to-day delivery of protective security and, to perform specialist services.
Requirement 2. Security procedures	Entities **must** develop and use procedures that ensure: a. all elements of the entity's security plan are achieved b. security incidents are investigated, responded to, and reported c. relevant security policy or legislative obligations are met.
Requirement 3. Security training	Entities **must** provide all personnel, including contractors, with security awareness training at engagement and annually thereafter.
Requirement 4. Specific training	Entities **must** provide personnel in specialist and high-risk positions (including contractors and security incident investigators) with specific security awareness training targeted to the scope and nature of the position.
Requirement 5. General email	Entities **must** maintain a monitored email address as the central conduit for all security-related matters across governance, personnel, information (including ICT) and physical security.

Policy 2: Management Structures - Security Roles

- Identifying necessary security roles
- Responsibilities of security roles
- Training and development for security personnel

Suggested Management Structure



Roles & Responsibilities to Support the CSO

- Planning
- Practices and procedures
- Detecting
- Managing
- Reporting
- Investigating

- Advisors may align with the four security outcomes - governance, information (including ICT), personnel and physical
- The CSO determines when a security incident is serious or significant enough to commence an investigation

Policy 3: Security Planning and Risk Management

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 must detail 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***
- ***e. entity's strategies to implement security risk management, maintain a positive risk culture and deliver against the PSPF, and***
- ***f. entity's arrangements for implementing any direction issued by the Secretary of the Attorney-General's Department under the PSPF.***

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, 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.
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.

PSPF Course | JulianTalbot.com | PSPF Overview

Introduction to the PSPF
Virtual Interactive Training

Intro to PSPF Presentation
DOWNLOADS Menu

PSPF Overview eBook
DOWNLOADS Menu

SRMBOK
Security Risk Management Body Of Knowledge

FREE RISK ASSESSMENT

https://www.juliantalbot.com/sectara

SRMBOK
Security Risk Management Body Of Knowledge