Introduction to the PSPF

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

STARTING SOON

SRMBOK

Security Risk Management Body Of Knowledge

Introduction to the PSPF

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

Julian Talbot

SRMBOK

Security Risk Management Body Of Knowledge

Agenda and Breaks

- Background to the PSPF
- Overview of the 16 policies
- 16 Policies in detail
- Control Effectiveness Assessment
- Issues and Challenges

Timings (approximate)

- 9:00 to 10:45
- 11:00 to 12:30
- 1:30 to 3:00
- 3:15 to 4:45

Introductions

- Name, role, and employer
- What brought you to this course
- What would you like to gain from it
- Any specific areas of interest

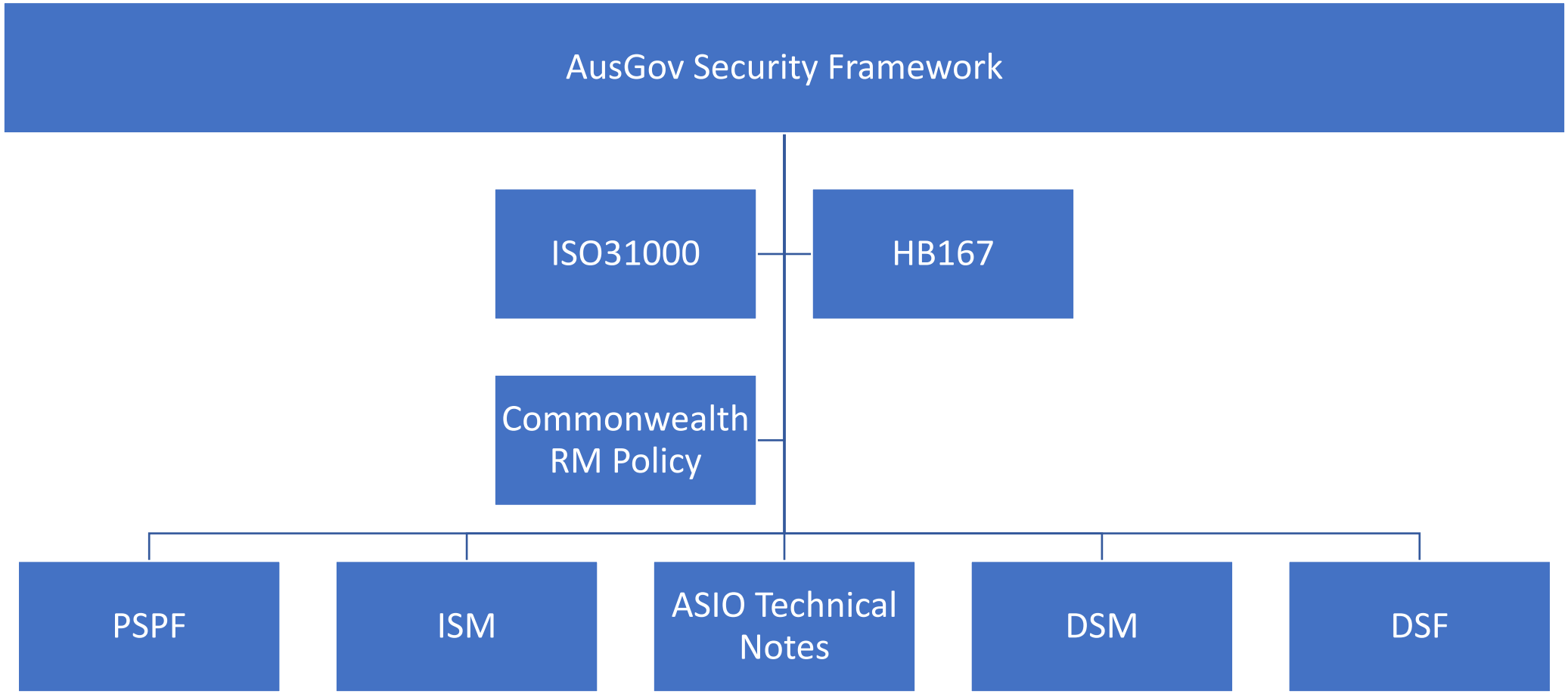
The PSPF

- 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

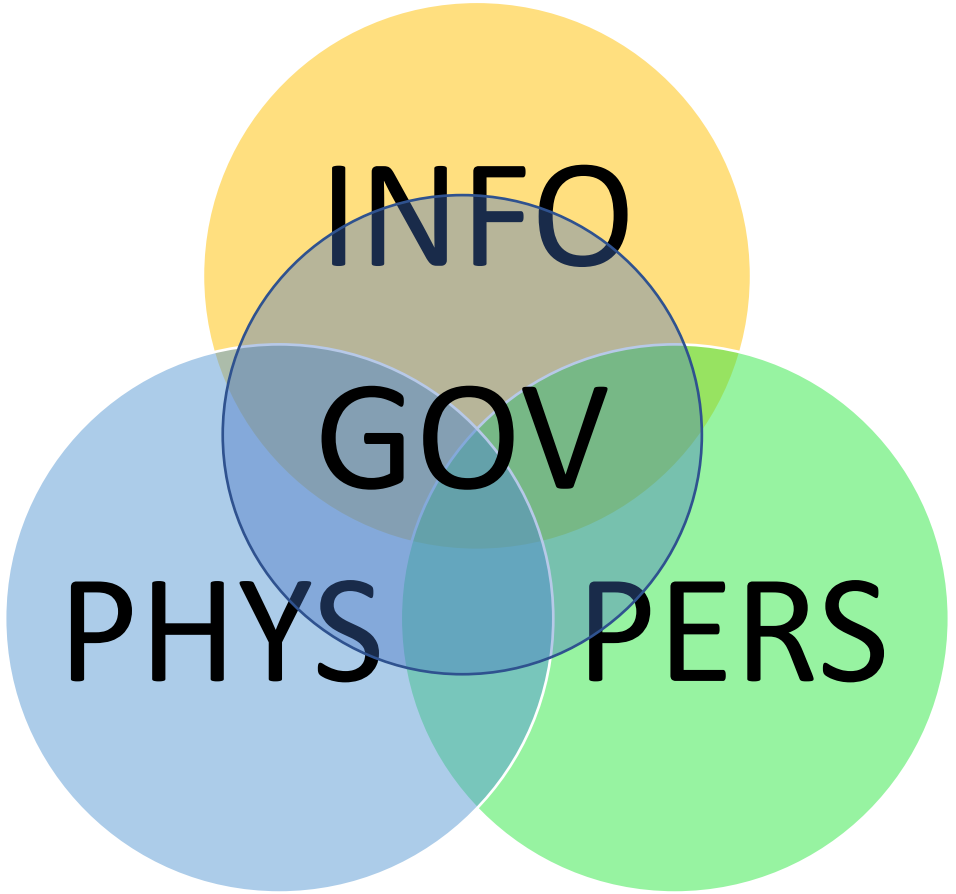
Background to the PSPF

- 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)

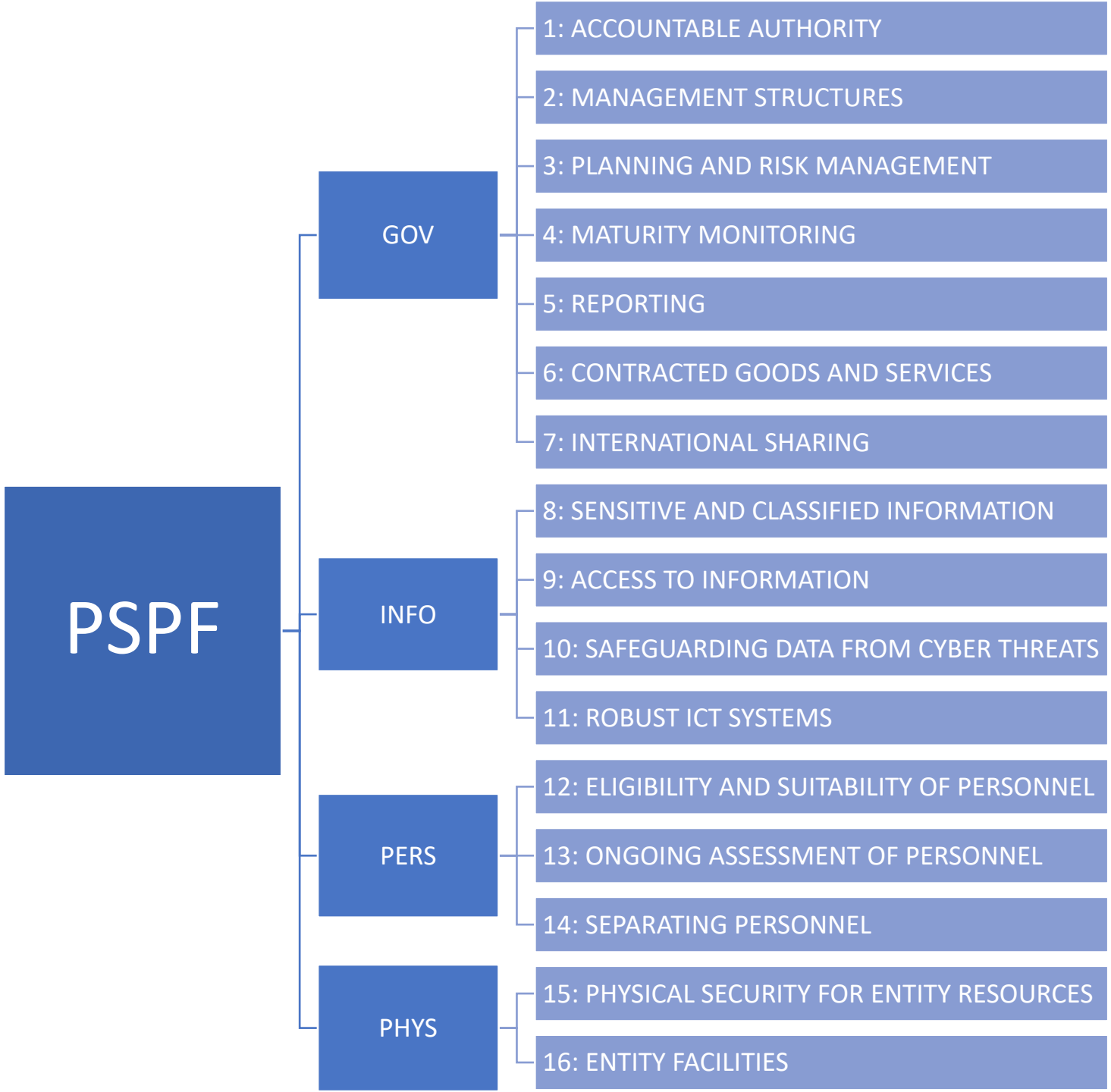
The PSPF Family



PSPF Components



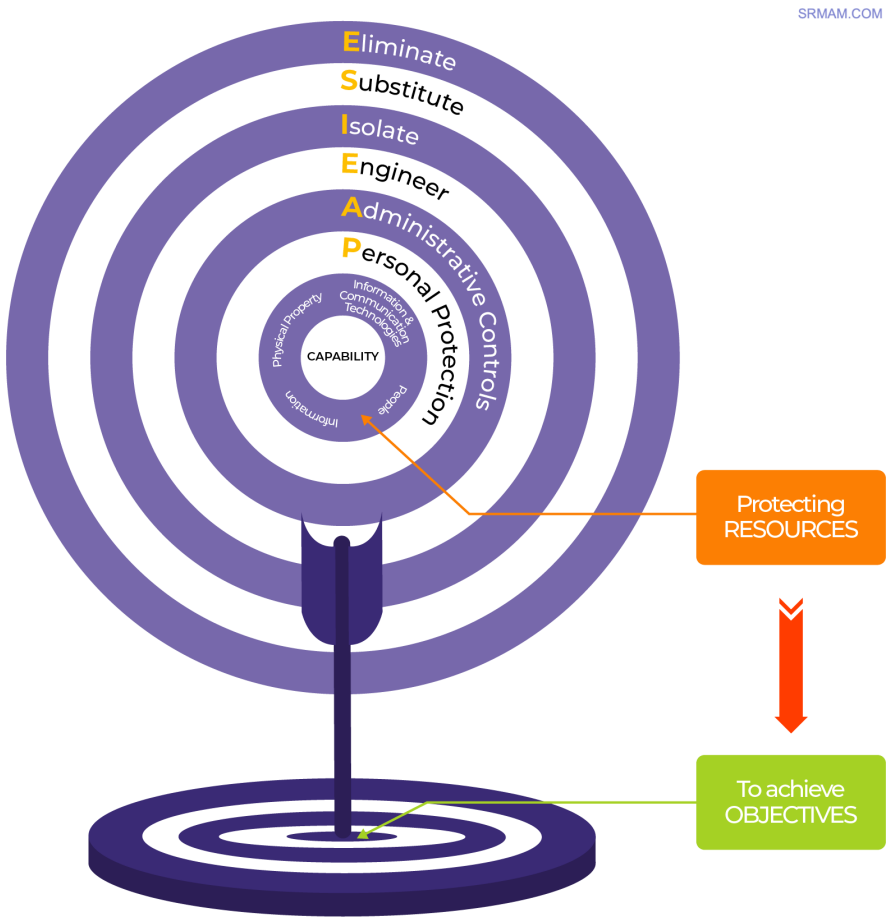
Cybersecurity?


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

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

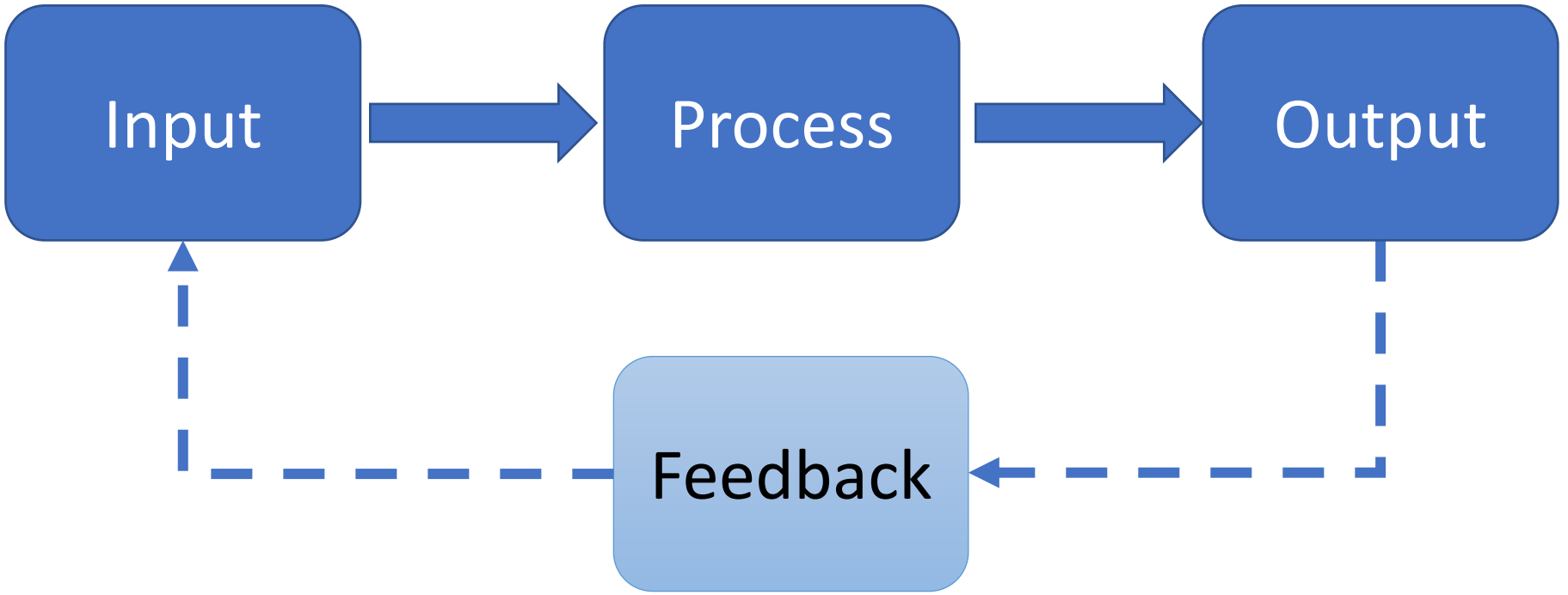
- Attorney-General's Department
- Australian Secret Intelligence Service
- Australian Signals Directorate
- Department of Foreign Affairs and Trade
- National Archives of Australia
- Digital Transformation Agency
- Department of the Prime Minister and Cabinet
- Australian Federal Police (AFP)
- Australian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

Protection in Depth

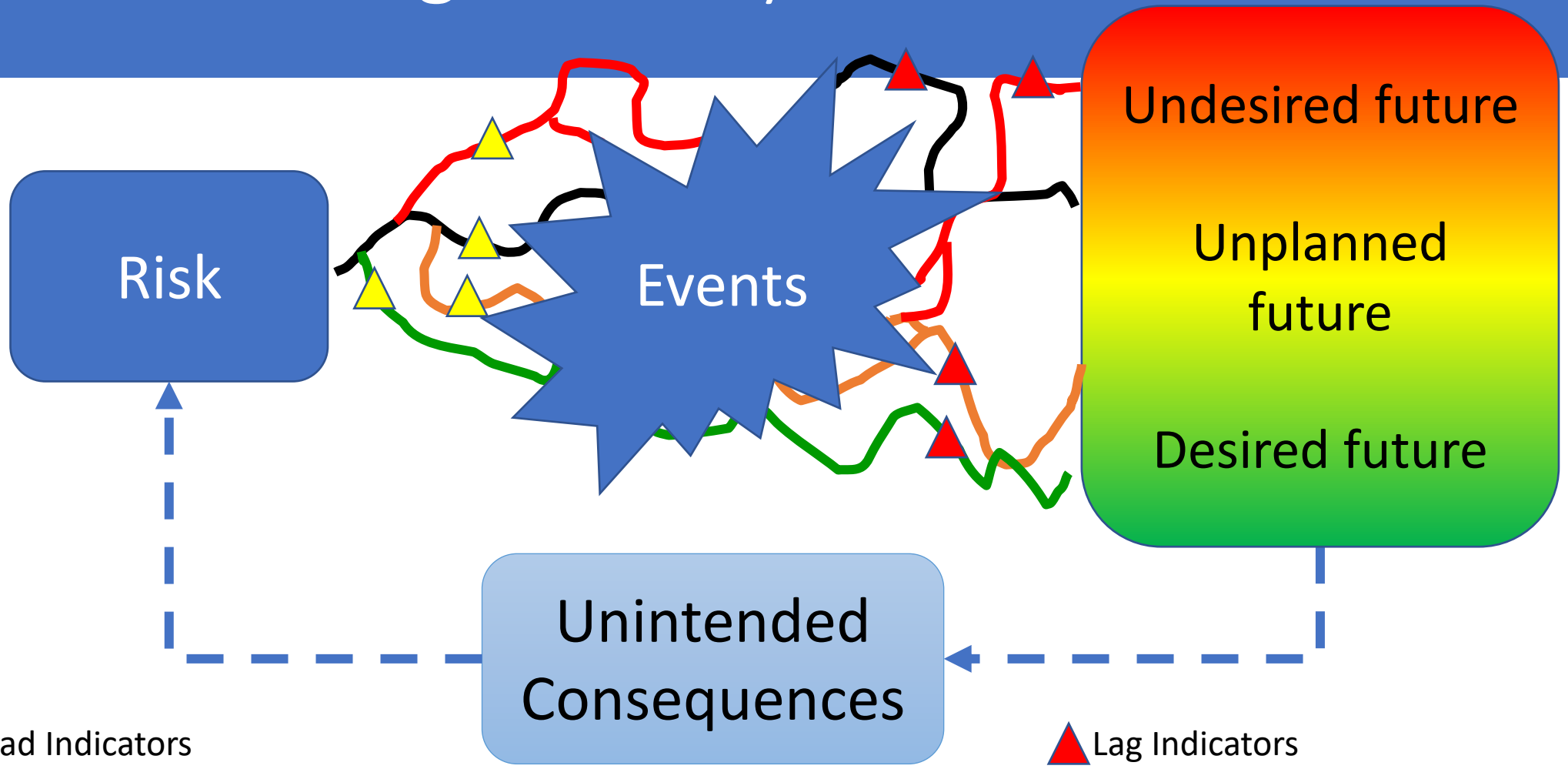


SRMBOK
Security Risk Management Body Of Knowledge

How Management Systems Work



How Risk Management Systems Work



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.

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

Accountable Authorities

- What does this mean to you?
- Who are they in your organisation?

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.

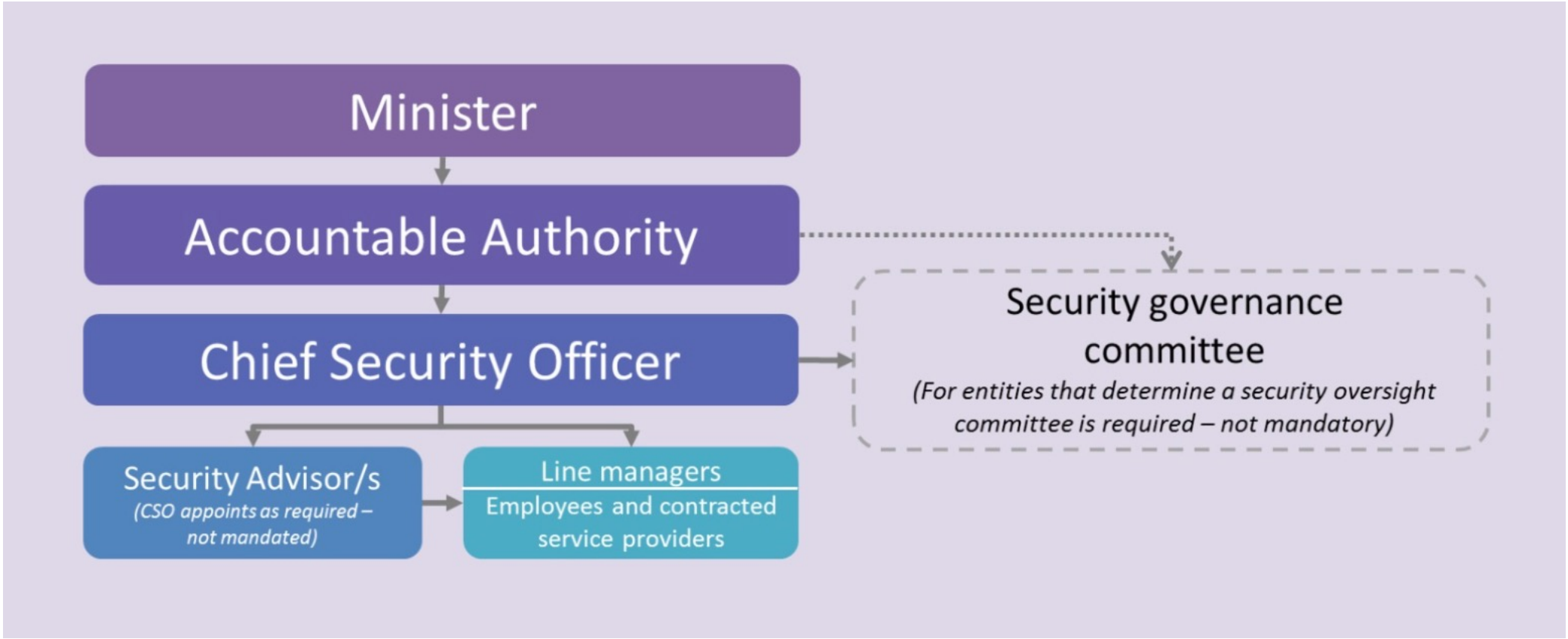
B2. Supporting Requirements

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

Management Structures

- What does this mean to you?
- Who are they in your organisation?

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.

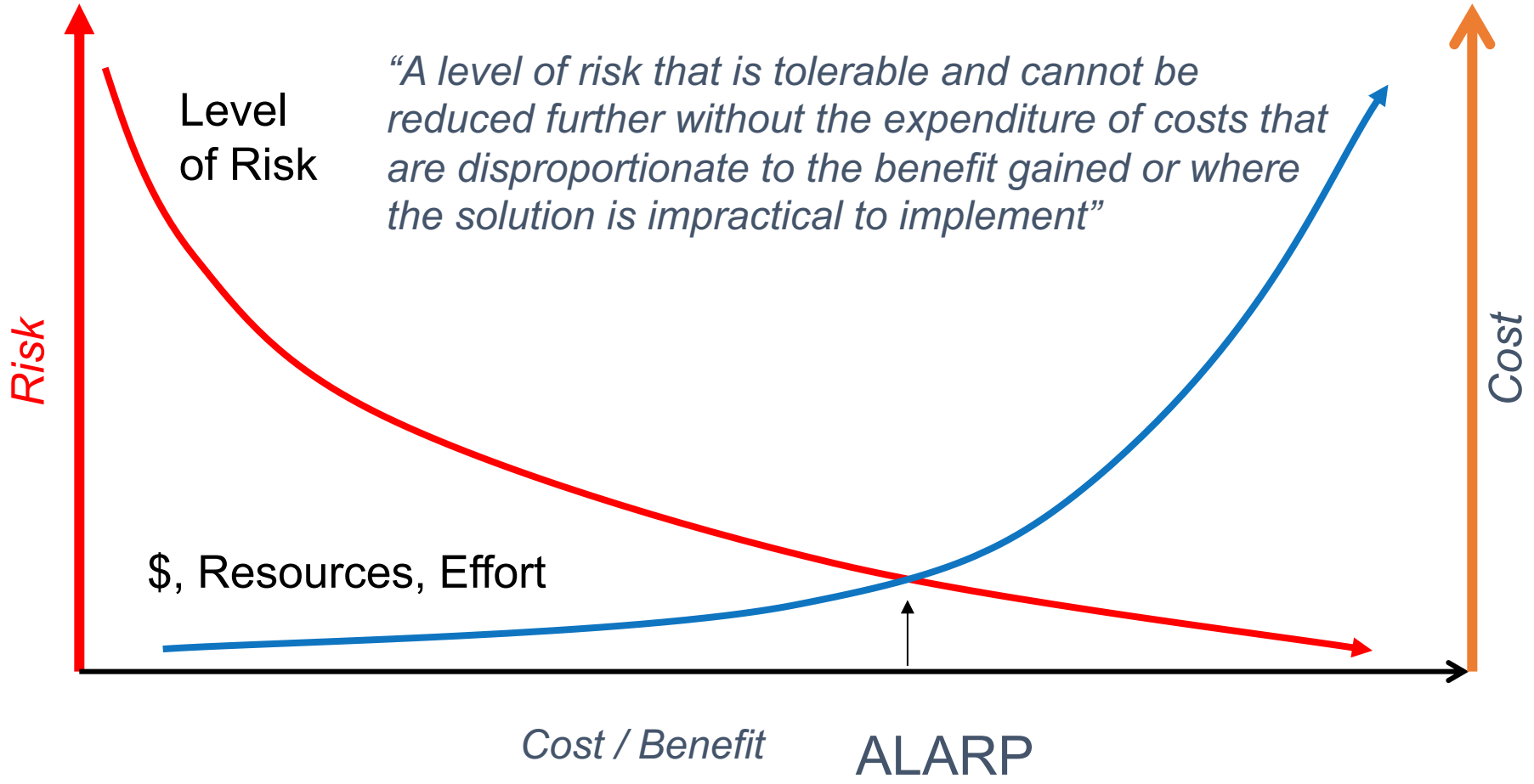
Policy 3: Risk Management Process

Identifying risks and vulnerabilities

Assessing likelihood and impact

Prioritizing and mitigating risks

Cost/Benefit of Mitigation



SRMBOK
Security Risk Management Body Of Knowledge

Source: Security Risk Management Body of Knowledge (SRMBOK)

Policy 3: Security Planning

Developing a security plan

Aligning security goals with organizational objectives

Regularly reviewing and updating plans

Policy 4: Security Maturity Monitoring

- Core:
  - 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.
- Supporting:
  - Entities must document and evidence their assessment of the entity's security maturity.

Policy 4: Monitoring Progress

Tracking security improvements

Identifying areas for improvement

Conducting regular assessments

Policy 4: Guidance

- Security capability maturity
- Security risk culture
  - entity's system of values and its personnel’s behaviours, attitudes and understanding
- Monitoring security maturity

Maturity of security capability considers how holistically and effectively each entity:

- implements and meets the intent of the PSPF core and supporting requirements
- minimises harm to the government's people information and assets
- fosters a positive security culture
- responds to and learns from security incidents
- understands and manages its security risks
- achieves security outcomes while delivering business objectives.

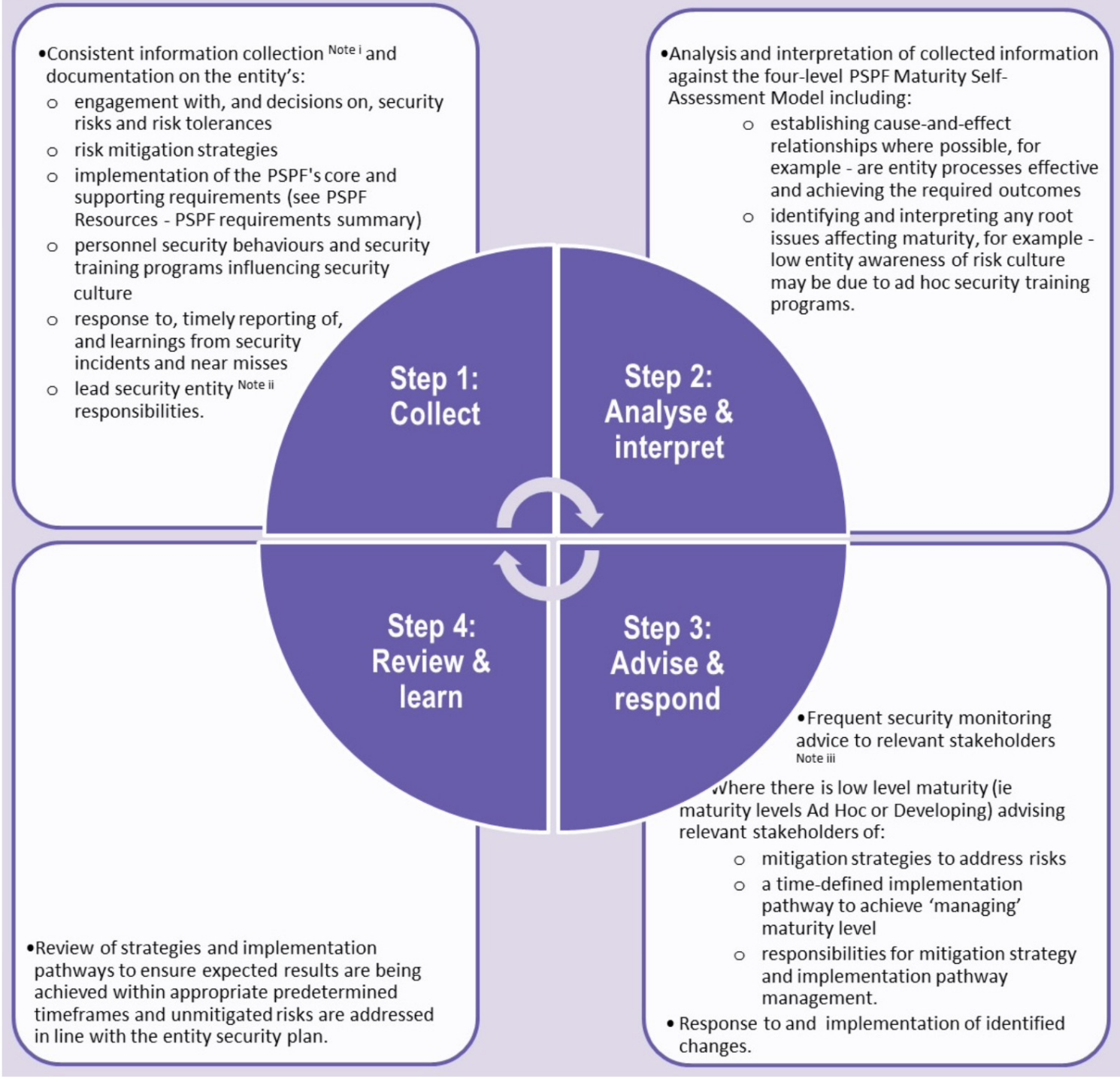
An entity with a mature security risk culture is one where the leadership team and personnel:

- comprehensively understand security risks
- appropriately manage security risks in their operational environments
- prioritise security risk management in their everyday practices
- make informed decisions on risks within agreed entity security risk tolerances
- react and respond to changes in the security risk environment.

Security maturity monitoring plan as part of overarching security plan

- Using security maturity indicators as detailed in the PSPF Maturity Self-Assessment
- Setting goals and objectives and identifying the impact on security of any goals and objectives detailed in the entity security plan
- Developing methodologies to manage the collection, measurement and analysis of data in relation to the entity's security maturity indicators
- Determining the frequency of security monitoring advice to be given to the accountable authority, Chief Security Officer, audit committee
- 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
- Where applicable, identifying the responsible area and timeframes to:
  - Manage implementation of PSPF core and supporting requirements
  - Implement strategies that achieve improvements in security culture.

Security Maturity Monitoring Cycle

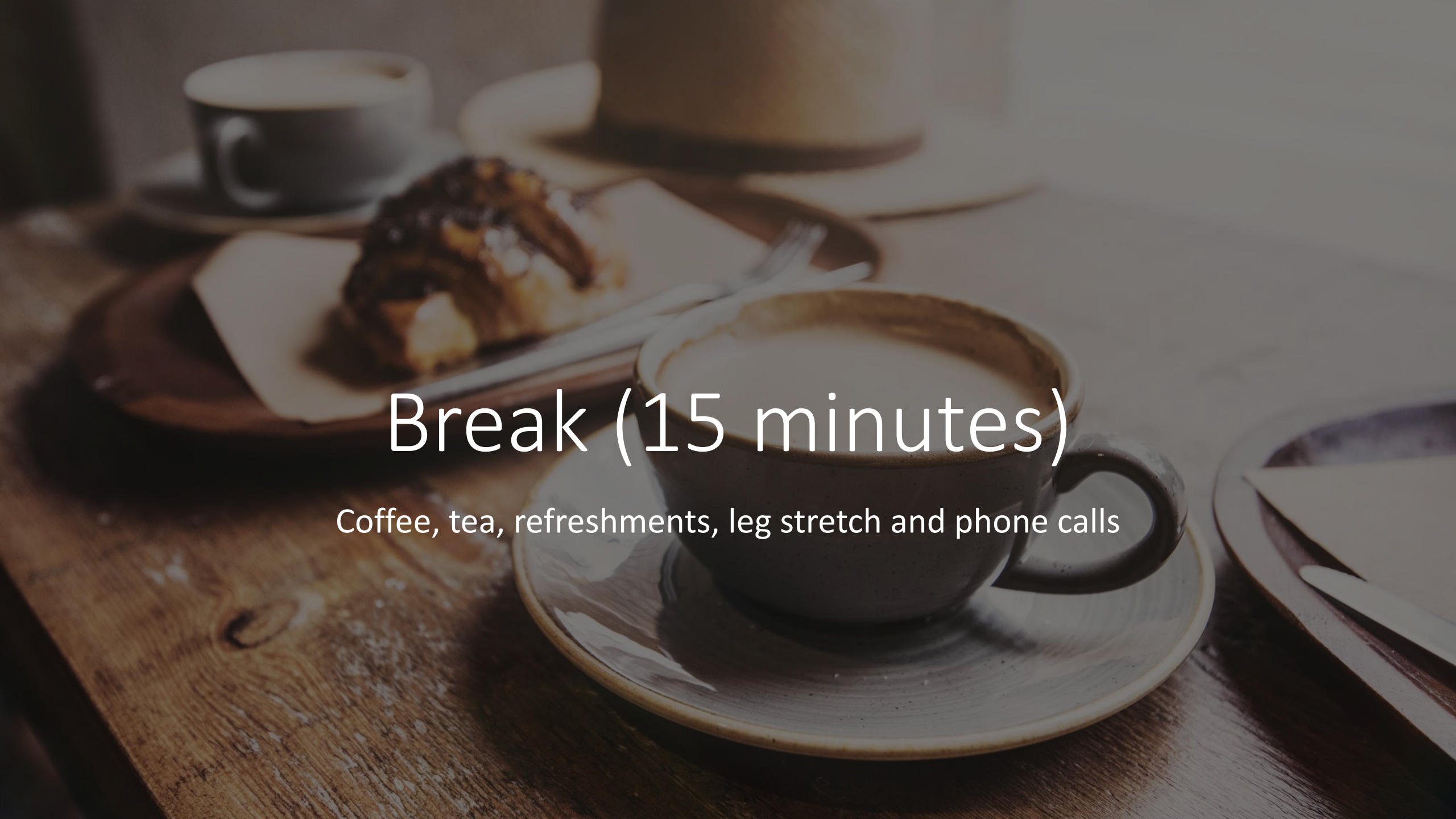


Policy 4: Key Performance Indicators

Selecting relevant KPIs

Monitoring KPIs over time

Adjusting security measures based on KPI results



Break (15 minutes)

Coffee, tea, refreshments, leg stretch and phone calls

Review

- What were the key points from the morning session
  - POLICY 1: ROLE OF ACCOUNTABLE AUTHORITY (GOV)
  - POLICY 2: MANAGEMENT STRUCTURES AND RESPONSIBILITIES (GOV)
  - POLICY 3: SECURITY PLANNING AND RISK MANAGEMENT (GOV)
  - POLICY 4: SECURITY MATURITY MONITORING (GOV)

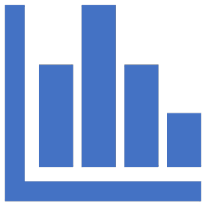
Exercise 1: Risk assessment & control selection

- In small groups conduct a hypothetical risk assessment scenario.
- Each group to use a different scenario, identify associated risks and develop a plan to mitigate them.
- Objective: Select and implement appropriate controls to mitigate risks.

SRMBOK
Security Risk Management Body Of Knowledge

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.

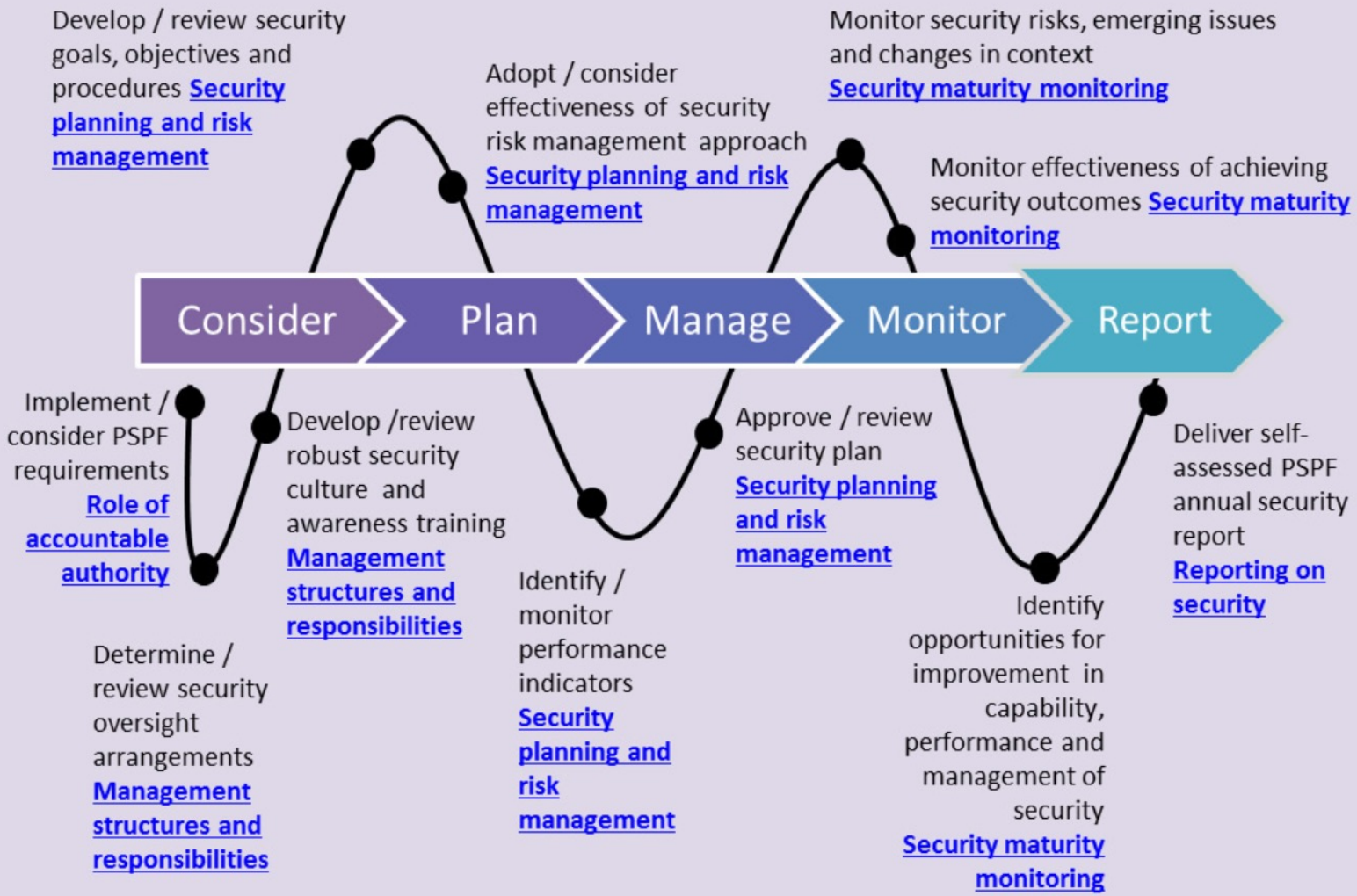
Policy 5: Supporting Requirements

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

Policy 6: Security Governance for Contracted Goods and Service Providers

- Outsourcing considerations
- Contractor requirements
- Monitoring security performance

Policy 6: Core Requirement

- Each entity is accountable for the security risks arising from procuring goods and services, and must ensure contracted providers comply with relevant PSPF requirements.

Policy 6: Supporting Requirements

Requirement 1. Assessing and managing security risks of procurement	When procuring goods or services, entities **must** put in place proportionate protective security measures by identifying and documenting: a. specific security risks to its people, information and assets, and b. mitigations for identified risks.
Requirement 2. Establishing protective security terms and conditions in contracts	Entities **must** ensure that contracts for goods and services include relevant security terms and conditions for the provider to: a. apply appropriate information, physical and personnel security requirements of the PSPF b. manage identified security risks relevant to the procurement, and c. implement governance arrangements to manage ongoing protective security requirements, including to notify the entity of any actual or suspected security incidents and follow reasonable direction from the entity arising from incident investigations.
Requirement 3. Ongoing management of protective security in contracts	When managing contracts, entities **must** put in place the following measures over the life of a contract: a. ensure that security controls included in the contract are implemented, operated and maintained by the contracted provider and associated subcontractor, and b. manage any changes to the provision of goods or services, and reassess security risks.
Requirement 4. Completion or termination of a contract	Entities **must** implement appropriate security arrangements at completion or termination of a contract.

Policy 6: Outsourcing Considerations

Identifying and balancing risks associated with outsourcing

Assessing potential contractors

Ensuring proper security measures are in place

Policy 6: Contractor Requirements

Establishing clear security expectations

Monitoring contractor compliance

Annex A. Developing contract clauses on security matters

Policy 6: Contractor Requirements (continued)

Addressing security breaches or non-compliance

Periodic reviews of contractor performance

Ensuring ongoing communication and collaboration

Policy 7: Security Governance for International Sharing

- International collaboration
- Sharing guidelines and restrictions
- Examples and case studies

Policy 7: Core Requirement

- Each entity must adhere to any provisions concerning the security of people, information and assets contained in international agreements and arrangements to which Australia is a party.

Policy 7: Supporting Requirements

Requirement 1. Sharing information with a foreign entity	a. When an entity shares sensitive or security classified Australian Government information or assets with a foreign entity there **must** be an explicit legislative provision, an international agreement or an international arrangement in place for its protection. b. The following limitations apply, even when an international agreement or international arrangement is in place: i. entities **must not** share Australian Government information bearing the Australian Eyes Only (AUSTEO) caveat with a person who is not an Australian citizen, and ii. entities, other than members of the National Intelligence Community or the Department of Defence **must not** share Australian Government information bearing the Australian Government Access Only (AGAO) caveat with a person who is not an Australian citizen.
Requirement 2. Safeguarding foreign information	Where an international agreement or international arrangement is in place, entities **must** safeguard sensitive or security classified foreign entity information or assets in accordance with the provisions set out in the agreement or arrangement.

Policy 7: International Collaboration

- Establishing international partnerships
- Benefits and risks of international collaboration
- Managing sensitive information in cross-border sharing
- Treaty or less-than-treaty-status arrangements provide for equivalent to AusGov security requirements

Australian Government information and asset classification equivalencies

Australian classification	French equivalent [Note ii]	US equivalent	EU equivalent	Japanese equivalent
TOP SECRET	TRÈS SECRET	TOP SECRET	TRÈS SECRET UE / EU TOP SECRET	Kimitsu 機密 Bouei Himitsu (Kimitsu) 防衛秘密(機密)
SECRET	SECRET	SECRET	SECRET UE	Gokuhi 極秘 Bouei Himitsu 防衛秘密
CONFIDENTIAL [Note iii]	To be handled as SECRET [Note iv]	CONFIDENTIAL	CONFIDENTIEL UE	Hi 秘
PROTECTED	No equivalence established [Note v]			
No equivalence established	No equivalence established	No equivalence established	RESTREINT UE [Note vi]	No equivalence established

Policy 7: Sharing Guidelines

- Identifying types of information to share
- Handling classified information
- Maintaining security during international exchanges

- The Australian Eyes Only (AUSTEO)
  - security cleared Australian citizens exclusively (includes Australian citizens who also hold other nationalities, such as dual nationals)
  - cannot be shared with a person who is not an Australian citizen, even when an international agreement or arrangement is in place
  - Foreign access to AUSTEO caveated information is a security incident requiring Chief Security Officer investigation, response and reporting
- The Australian Government Access Only (AGAO)
  - information that is restricted to appropriately security cleared Australian officers or
  - representatives of foreign governments from Five Eyes countries who are on exchange, long-term posting or attachment to the National Intelligence Community (NIC) or the Department of Defence
  - For other entities, information caveated AGAO is to be handled as AUSTEO

Policy 8: Sensitive and Classified Information

- Classification levels
- Handling sensitive information
- Examples and case studies

Policy 8: Core Requirement

Each entity must:

a. identify information holdings

b. assess the sensitivity and security classification of information holdings, and

c. implement operational controls for these information holdings proportional to their value, importance and sensitivity.

Policy 8: Supporting Requirements

Requirement 1. Identifying information holdings	The originator **must** determine whether information being generated is official information (intended for use as an official record) and whether that information is sensitive or security classified.
Requirement 2. Assessing sensitive and security classified information	a. To decide which security classification to apply, the originator **must**: i. assess the value, importance or sensitivity of official information by considering the potential damage to government, the national interest, organisations or individuals, that would arise if the information's confidentiality was compromised (refer to the following table), and ii. set the security classification at the lowest reasonable level. b. The originator must assess the information as OFFICIAL: Sensitive if: i. a security classification does not apply, and ii. compromise of the information's confidentiality may result in limited damage to an individual, organisation or government generally.

			Sensitive information	**Security classified information**		
	UNOFFICIAL	**OFFICIAL**	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
	No business impact	1 Low business impact	2 Low to medium business impact	3 High business impact	4 Extreme business impact	5 Catastrophic business impact
Compromise of information confidentiality would be expected to cause ➔	**No damage**. This information does not form part of official duty.	**No or insignificant damage.** This is the majority of routine information.	**Limited damage** to an individual, organisation or government generally if compromised.	**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.

Policy 8: Supporting Requirements

Requirement 3. Declassification	The originator **must** remain responsible for controlling the sanitisation, reclassification or declassification of the information. An entity **must not** remove or change information's classification without the originator's approval.
Requirement 4. Marking information	The originator **must** clearly identify sensitive and security classified information, including emails, using applicable protective markings by: a. using text-based protective markings to mark sensitive and security classified information (and associated metadata), unless impractical for operational reasons b. if text-based protective markings cannot be used, using colour-based protective markings, or c. if text or colour-based protective markings cannot be used (eg verbal information), applying the entity's marking scheme for such scenarios. Entities **must** document a marking scheme for this purpose and train personnel appropriately.
Requirement 5. Using metadata to mark information	Entities **must** apply the Australian Government Recordkeeping Metadata Standard to protectively mark information on systems that store, process or communicate sensitive or security classified information: a. for security classified information, apply the 'Security Classification' property (and where relevant, the 'Security Caveat' property) b. for OFFICIAL: Sensitive information, apply the 'Dissemination Limiting Marker' property c. where an entity wishes to categorise information content by the type of restrictions on access, apply the 'Rights' property.
Requirement 6. Caveats and accountable material	a. Caveats **must** be marked as text and (with the exception of the NATIONAL CABINET caveat) only appear in conjunction with a security classification. The NATIONAL CABINET caveat can appear in conjunction with either the OFFICIAL: Sensitive marking or a security classification. b. Entities **must** ensure that accountable material: i. has page and reference numbering ii. is handled in accordance with any special handling requirements imposed by the originator and caveat owner, and iii. has an auditable record of all incoming and outgoing material, transfer, copy or movements. c. For all caveated information, entities **must** apply the protections and handling requirements established by caveat owners in the Australian Government Security Caveats Guidelines.
Requirement 7. Storage	Entities **must** ensure sensitive and security classified information is stored securely in an appropriate security container for the approved zone in accordance with the minimum protection requirements set out in **Annexes A to D**.
Requirement 8. Transfer	Entities **must** ensure sensitive and security classified information is transferred and transmitted by means that deter and detect compromise and that meet the minimum protection requirements set out in **Annexes A to D**.
Requirement 9. Disposal	Entities **must** ensure sensitive and security classified information is disposed of securely in accordance with the minimum protection requirements set out in **Annexes A to D**. This includes ensuring sensitive and classified information is appropriately destroyed when it has passed minimum retention requirements or reaches authorised destruction dates.

Policy 8: Classification Levels

- Understanding classification categories
- Determining appropriate classifications
- Ensuring proper access controls

Policy 8: Handling Sensitive Information

- Secure storage and transmission of sensitive data
- Training employees on proper handling
- Reporting breaches and incidents

Policy 8: Minimum protection requirements for:

- TOP SECRET information
- SECRET information
- PROTECTED information
- OFFICIAL: Sensitive information
- OFFICIAL information

Minimum protections and handling requirements for TOP SECRET information

BIL 5	TOP SECRET—exceptionally grave damage to the national interest, organisations or individuals
Protective marking	Apply text-based protective marking **TOP SECRET** to documents (including emails). It is recommended that text markings be in capitals, bold text, large fonts and distinctive colours (red preferred) and located at the centre top and centre bottom of each page. If text-based markings cannot be used, use colour-based markings. For TOP SECRET a red colour is recommended. If text or colour-based protective markings cannot be used, apply the entity's marking scheme for such scenarios. If marking paragraphs, it is recommended that TOP SECRET is written in full or abbreviated to (TS) and placed either in brackets at the start or end of the paragraph or in the margin adjacent to the first letter of the paragraph.
Access	The need-to-know principle applies to all TOP SECRET information. Ongoing access to TOP SECRET information requires a Negative Vetting 2 security clearance or above. Any temporary access must only be provided to personnel with at least a Negative Vetting 1 security clearance and must be supervised.
Use	TOP SECRET information can only be used in Zones 3-5. **Outside entity facilities (including at home)** **Do not** use outside entity facilities (including at home).

Minimum protections and handling requirements for TOP SECRET information

Storage	**Do not** leave TOP SECRET information, or a mobile device that processes, stores or communicates TOP SECRET information, unattended. Store securely when unattended. When storing TOP SECRET information, or a mobile device that processes, stores or communicates TOP SECRET information: a. inside entity facilities: i. Zone 5, store in Class B container ii. Zones 3-4, store in exceptional circumstances only for a maximum of 5 days, Zone 4 (in Class B container) or Zone 3 (in a Class A container). b. outside entity facilities: **do not** store TOP SECRET information, or a mobile device that processes, stores or communicates TOP SECRET information, outside entity facilities (including at home).
Carry	When carrying physical TOP SECRET information **always retain it in personal custody** a. inside entity facilities: i. Zones 3-5, in an opaque envelope or folder that indicates classification ii. Zones 1-2, **not recommended**, if required, in an opaque envelope or folder that indicates classification and place in a security briefcase, pouch or satchel. b. outside entity facilities (including external meetings) and between entity facilities: **not recommended**, if required: i. obtain written manager approval, and ii. place in tamper-evident packaging within a security briefcase, pouch or satchel. Mobile devices that that process, store or communicate TOP SECRET information require explicit approval by the Australian Signals Directorate (ASD). When carrying an approved TOP SECRET mobile device **always retain it in personal custody** a. inside entity facilities: i. Zones 3-5, carry in secured state; if in an unsecured state apply entity procedures ii. Zones 1-2, carry in a secured state; if in an unsecured state, place inside a security briefcase, pouch or satchel. b. outside entity facilities (including external meetings) and between entity facilities – **not recommended**, if required: i. obtain written manager approval, and

Minimum protections and handling requirements for TOP SECRET information

	ii. carry in a secured state; if in an unsecured state, place in tamper-evident packaging within a security briefcase, pouch or satchel.
Transfer	When transferring physical TOP SECRET information a. inside entity facilities i. Zones 3-5, transfer by hand or entity safe hand and apply requirements for carrying; can be uncovered if in close proximity and the office environment presents low risk of unauthorised viewing ii. Zones 1-2, transfer by hand or entity safe hand and apply requirements for carrying with written manager approval. b. to another officer in a different facility i. obtain written manager approval ii. apply requirements for carrying outside entity facilities (including using tamper evident packaging), and iii. transfer by hand, entity safe hand, safe hand courier rated BIL 5, or DFAT courier. Any transfer requires a receipt.
Transmit	When transmitting electronically, communicate information over TOP SECRET secure networks. Use ASD's High Assurance Cryptographic Equipment to encrypt TOP SECRET information for any communication that is not over a TOP SECRET network.

Minimum protections and handling requirements for TOP SECRET information

Official travel	TOP SECRET information and mobile devices that process, store or communicate TOP SECRET information **must not** be stored or used outside appropriate entity facilities. **Travel in Australia** Travelling domestically with physical TOP SECRET information is **not recommended**, if required: a. obtain written manager approval b. apply requirements for carrying outside entity facilities and any additional entity procedures, and c. for airline travel, retain as carry-on baggage and **do not travel** if the airline requires it to be checked at the gate. **Do not** leave TOP SECRET information unattended. **Do not** store while travelling (eg in a hotel room). If storage required, store in an Australian entity facility. Travelling domestically with a mobile device that processes, stores or communicates TOP SECRET information is **not recommended**, consider alternative options to access information at destination. If required: a. obtain written manager approval b. apply requirements for carrying outside entity facilities and any additional entity procedures, and c. for airline travel, retain as carry-on baggage; if airline requires carry-on baggage to be checked at the gate, try to observe entering and exiting the cargo hold and reclaim as soon as possible. **Do not** leave device unattended. **Do not** store device while travelling (eg in a hotel room). If storage required, store in an Australian entity facility. **Travel outside Australia** **Do not** travel overseas with TOP SECRET information or a mobile device that processes, stores or communicates TOP SECRET information, seek DFAT advice on options to access information or mobile devices at overseas destination. If access to TOP SECRET information or mobile device provided at overseas destination: a. apply requirements for carrying outside entity facilities and any additional entity procedures, and b. retain in personal custody or store in an Australian entity facility. **Do not** leave TOP SECRET information unattended. **Do not** store while travelling (eg in a hotel room). If storage required, store in an Australian entity facility.
Disposal	Dispose of TOP SECRET information using a Class A shredder – supervise and document destruction

Policy 8: Handling Sensitive Information

Annex G. Email protective marking standard (12 pages)

Policy 9: Access to Information

- Information access controls
- Clearance requirements
- Sharing information
- Temporary access

Policy 9: Access Controls

- Identifying and managing user access
- Establishing role-based access controls
- Regularly reviewing and updating access permissions

Policy 9: Core Requirement

Each entity must enable appropriate access to official information. This includes:

- sharing information within the entity, as well as with other relevant stakeholders
- ensuring that those who access sensitive or security classified information have an appropriate security clearance and need to know that information, and
- controlling access (including remote access)to supporting ICT systems, networks, infrastructure, devices and applications

Policy 9: Supporting Requirements

Requirement 1. Formalised agreements for sharing information and resources	When disclosing security classified information or resources to a person or organisation outside of government, entities **must** have in place an agreement or arrangement, such as a contract or deed, governing how the information is used and protected.
Requirement 2. Limiting access to sensitive and classified information and resources	To reduce the risk of unauthorised disclosure, entities **must** ensure access to sensitive and security classified information or resources is only provided to people with a need-to-know.
Requirement 3. Ongoing access security classified information and resources	a. Entities **must** ensure that people requiring ongoing access to security classified information or resources are security cleared to the appropriate level:

	Security classified information		
	PROTECTED	**SECRET**	**TOP SECRET**
Personnel security clearance for ongoing access	Baseline security clearance or above.	Negative Vetting 1 security clearance or above.	Negative Vetting 2 security clearance or above.

Note l Some Australian office holders are not required to hold a security clearance.

b. In addition, entities **must** ensure that people requiring access to caveated information meet all clearance and suitability requirements imposed by the originator and caveat owner.

Policy 9: Supporting Requirements

Requirement 4. Temporary access to classified information and resources	Entities may provide a person with temporary access to security classified information or resources on the basis of a risk assessment for each case. In such cases, entities **must**: a. limit the duration of access to security classified information or resources: i. to the period in which an application for a security clearance is being processed for the particular person, or ii. up to a maximum of three months in a 12-month period b. conduct recommended employment screening checks (see the PSPF policy: Eligibility and suitability of personnel) c. supervise all temporary access d. for access to TOP SECRET information, ensure the person has an existing Negative Vetting 1 security clearance, and e. deny temporary access to classified caveated information (other than in exceptional circumstances, and only with approval of the caveat owner).
Requirement 5. Managing access to information systems	To manage access to information systems holding sensitive or security classified information, entities **must** implement unique user identification, authentication and authorisation practices on each occasion where system access is granted.

Policy 9: Clearance Requirements

- Determining clearance levels for personnel
- Ensuring proper clearance for accessing sensitive data
- Ongoing monitoring and evaluation of clearances

Policy 10: Safeguarding Data from Cyber Threats

- Cybersecurity measures
- Incident response
- Examples and case studies

Policy 10: Core Requirement

Each entity must mitigate common cyber threats by:

- implementing the following mitigation strategies from the Strategies to Mitigate
- Cyber Security Incidents:
  - application control
  - patch applications
  - configure Microsoft Office macro settings
  - user application hardening
  - restrict administrative privileges
  - patch operating systems
  - multi-factor authentication
  - regular backups
- considering which of the remaining mitigation strategies from the Strategies to Mitigate Cyber Security Incidents need to be implemented to achieve an acceptable level of residual risk for their entity.

The Essential, Excellent, and Very Good

- Strategies to mitigate cyber security incidents
- The Australian Cyber Security Centre (ACSC) has prioritised mitigation strategies to help cyber security professionals in all organisations mitigate cyber security incidents caused by various cyber threats

Policy 10: Supporting Requirements

Transacting online with the public

- Entities must not expose the public to unnecessary security risks when they transact online with government

Policy 10: Cybersecurity Measures

- Implementing layers of defense
- Monitoring for potential threats
- Regularly updating security protocols

Policy 10: Incident Response

- Identifying and responding to security incidents
- Communication and escalation plans
- Learning from incidents and adjusting security measures


Lunch
Meet back here at …

Review

- Key points from the last section
  - POLICY 5: REPORTING ON SECURITY (GOV)
  - POLICY 6: SECURITY GOVERNANCE FOR CONTRACTED GOODS AND SERVICE PROVIDERS (GOV)
  - POLICY 7: SECURITY GOVERNANCE FOR INTERNATIONAL SHARING (GOV)
  - POLICY 8: SENSITIVE AND CLASSIFIED INFORMATION (INFO)
  - POLICY 9: ACCESS TO INFORMATION (INFO)
  - POLICY 10: SAFEGUARDING DATA FROM CYBER THREATS (INFO)

Exercise 2 - Incident response planning

- Work in small groups to develop an incident response plan based on a hypothetical scenario.
- Pick a scenario and develop a plan based on PSPF guidelines and principles.
- Objective: Learn how to apply incident response planning principles in practice.

SRMBOK
Security Risk Management Body Of Knowledge

Policy 11: Robust ICT Systems

ICT SYSTEM REQUIREMENTS

RISK ASSESSMENT AND MANAGEMENT

SRMBOK
Security Risk Management Body Of Knowledge

Policy 11: Core Requirement

Each entity must ensure the secure operation of their ICT systems to safeguard information and the continuous delivery of government business by applying the Australian Government Information Security Manual's cyber security principles during all stages of the lifecycle of each system.

Policy 11: Supporting Requirements

Requirement 1. Authorisation of ICT systems to operate	Entities **must** only process, store or communicate information on ICT systems that the determining authority (or their delegate) has authorised to operate based on the acceptance of the residual security risks associated with its operation. When establishing new ICT systems, or implementing improvements to existing systems, the decision to authorise (or reauthorise) an ICT system to operate **must** be based on the *Australian Government Information Security Manual*'s six step risk-based approach for cyber security.
Requirement 2. Secure internet gateways	Entities **must** protect internet-connected ICT systems, and the information they process, store or communicate, by implementing a secure internet gateway that meets Australian Signals Directorate requirements.

Policy 11: ICT System Requirements

- Ensuring systems meet security standards
- Regular maintenance and updates
- Addressing vulnerabilities in a timely manner

Policy 11: Risk Assessment

- Identifying and assessing ICT-related risks
- Prioritizing risks and implementing mitigations
- Ongoing monitoring of ICT risk landscape

Policy 12: Eligibility and Suitability of Personnel

- Pre-employment screening
- Eligibility requirements
- Examples and case studies

Policy 12: Core Requirement

- Each entity must ensure the eligibility and suitability of its personnel who have access to Australian Government resources (people, information and assets).
- Entities must use the Australian Government Security Vetting Agency (AGSVA) to conduct vetting, or where authorised, conduct security vetting in a manner consistent with the Personnel Security Vetting Standards.

Policy 12: Supporting Requirements

Too many to list

Page 2 of the Policy

Policy 12: Pre-employment Screening

Background checks and vetting processes

Ensuring personnel meet eligibility criteria

Balancing security and privacy concerns

Policy 12: Eligibility Requirements

- Establishing criteria for personnel access
- Verifying qualifications and credentials
- Monitoring ongoing eligibility and suitability

Policy 13: Ongoing Assessment of Personnel

- Regular evaluations
- Employee support and development
- Examples and case studies

Policy 13: Core Requirement

- Each entity must assess and manage the ongoing suitability of its personnel and share relevant information of security concern, where appropriate.
  - Accountable authorities are responsible for determining their entity's risk tolerance and managing the security risks of their entity, including as they relate to the ongoing suitability of personnel to access Australian Government resources.
  - Sponsoring entities and authorised vetting agencies play a critical role in assuring ongoing suitability of personnel occupying positions that require access to security classified resources or additional levels of assurance. The supporting requirements detail the respective responsibilities of sponsoring entities and vetting agencies for assessing the ongoing suitability of security cleared personnel.

Policy 13: Supporting Requirements

Requirement 1. Security clearance maintenance Note **i**	a. Sponsoring entities **must** actively monitor and manage the ongoing suitability of their security cleared personnel, including by: i. collecting, assessing and sharing information of security concern ii. conducting annual security checks with all security cleared personnel iii. monitoring compliance with, and managing risk in relation to, clearance maintenance requirements for security clearance holders granted a conditional security clearance and reporting non-compliance to the authorised vetting agency iv. reviewing eligibility waivers at least annually, before revalidation of a security clearance, and prior to any proposed position transfer v. implementing the TOP SECRET-Privileged Access Standard in relation to the ongoing assessment and management of personnel with TOP SECRET-Privileged access security clearances. b. Vetting agencies **must**: i. share information of security concern about security clearance holders with sponsoring entities ii. assess and respond to information of security concern about security clearance holders, which includes reports from sponsoring entities iii. for conditional security clearances, review conditions annually iv. review the clearance holder's eligibility and suitability to hold a security clearance, where concerns are identified (review for cause), and v. implement the TOP SECRET-Privileged Access Standard in relation to the ongoing assessment and management of personnel with TOP SECRET-Privileged Access security clearances.

Policy 13: Supporting Requirements

Requirement 2. Security clearance revalidation	Vetting agencies **must** reassess a clearance holder's eligibility and suitability to hold a security clearance by: a. for Baseline, Negative vetting 1, Negative Vetting 2 and Positive Vetting security clearances, considering their integrity (ie the character traits of maturity, trustworthiness, honesty, resilience, tolerance and loyalty) in accordance with the Personnel Security Adjudicative Guidelines (see the PSPF policy: Eligibility and suitability of personnel Annex A) b. for TOP SECRET-Privileged Access security clearances, assessing their trustworthiness and commitment to Australia, its values and its democratic system of government (ie honesty and integrity, maturity and judgement, stability and reliability, tolerance and acceptance, loyalty and commitment, vulnerability to improper influence or coercion) in accordance with the TOP SECRET-Privileged Access Standard [Note ii] c. revalidating minimum personnel security checks for a security clearance outlined below, and d. resolving any doubt in the national interest.

Policy 13: Supporting Requirements

Minimum requirements for revalidation of security clearances

Check	Security Clearance Level				
	Baseline Vetting	**Negative Vetting 1**	**Negative Vetting 2**	**Positive Vetting**	**TOP SECRET-Privileged Access** Note iii
Revalidation Note iv undertaken at least every:	15 years	10 years	5 to 7 years	5 to 7 years	7 years
Updated personal particulars	✓ Required	✓ Required	✓ Required	✓ Required	✓ Required
	Entities **must** confirm any changes to a clearance holder's personal particulars using identification documents verified with the issuing authority by using the Document Verification Service for Australian-issued primary identification documents.				
Background assessment covering period since the initial clearance or last revalidation	✓ Required	✓ Required	✓ Required	✓ Required	✓ Required
Referee checks covering period since the initial clearance or last revalidation	✓ Required	✓ Required	✓ Required	✓ Required	✓ Required
Digital footprint check covering period since the initial clearance or last revalidation	✓ Required	✓ Required	✓ Required	✓ Required	✓ Required
National police check/criminal history check	✓ Required, no exclusion	✓ Required, full exclusion	✓ Required, full exclusion	✓ Required, full exclusion	✓ Required, full exclusion
Financial history assessment	✓ Required	✓ Required	✓ Required	✓Required	N/a
Financial statement	Not required	✓ Required	✓ Required	✓Required with supporting documents	N/a
Financial probity assessment	Not required	Not required	Not required	✓ Required	N/a
Comprehensive financial assessment	N/a	N/a	N/a	N/a	✓ Required
ASIO assessment	Not required	✓ Required	✓ Required	✓ Required	✓ Required
Security interview	Not required	Not required	✓ Required	✓ Required	✓ Required
Psychological security assessment	Not required	Not required	Not required	✓ Required	✓ Required

13 Ongoing assessment of personnel 3

ity Policy Framework

Supporting requirements					
Overseas travel check	N/a	N/a	N/a	N/a	✓ Required

irements notes:

SRMBOK
Security Risk Management Body Of Knowledge

Policy 13: Regular Evaluations

01

Conducting periodic performance reviews

02

Assessing ongoing suitability for roles

03

Addressing issues and concerns as they arise

Policy 13: Employee Support

01

Providing resources and training for development

02

Encouraging a culture of security awareness

03

Supporting employees through changes and challenges

Policy 14: Separating Personnel

- Offboarding processes
- Security measures during employee

Policy 14: Core Requirement

Each entity must ensure that separating personnel:

- have their access to Australian Government resources withdrawn, and
- are informed of any ongoing security obligations.

Policy 14: Supporting Requirements

Requirement 1. Sharing security relevant information, debriefs and continuing obligations	Prior to personnel separation or transfer, entities **must:** a. notify the Chief Security Officer, or relevant security advisor, of any proposed cessation of employment resulting from misconduct or other adverse reasons b. debrief all separating personnel who have access to sensitive or security classified information, including advising them of their continuing obligations under the Commonwealth Criminal Code and other relevant legislation, and obtain the person's acknowledgement of these obligations c. for personnel transferring to another Australian Government entity, provide the receiving entity with relevant security information, including the outcome of pre-employment screening checks and any periodic employment suitability checks, and d. report any security (as defined in the in the *Australian Security Intelligence Organisation Act 1979*) concerns to the Australian Security Intelligence Organisation (ASIO).
Requirement 2. Withdrawal of access	On separation or transfer, entities **must** remove personnel's access to Australian Government resources, including: a. physical facilities, and b. ICT systems.
Requirement 3. Risk assessment	Where it is not possible to undertake required separation procedures, entities **must** undertake a risk assessment to identify any security implications.
Requirement 4. Security clearance actions	Following the separation of security cleared personnel: a. sponsoring entities **must** advise the relevant authorised vetting agency of: i. the separation of a clearance holder, including any relevant circumstances (eg termination for cause) and any details, if known, of another entity or contracted service provider the clearance holder is transferring to, and ii. any identified risks or security concerns associated with the separation, including as a result of **Requirement 3**. b. authorised vetting agencies **must**: i. manage and record changes in the security clearance status of separating personnel, including a change of sponsoring entity, and ii. transfer personal security files where a clearance subject transfers to an entity covered by a different authorised vetting agency, to the extent that their enabling legislation allows.

Policy 14: Offboarding Processes

- Ensuring a smooth transition during employee separation
- Handling sensitive information and access rights
- Conducting exit interviews and debriefings

Policy 14: Security Measures

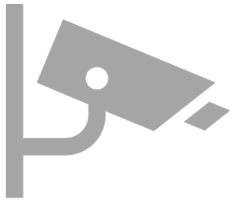
REVOKING ACCESS TO SYSTEMS AND FACILITIES

ENSURING PROPER DISPOSAL OF SENSITIVE INFORMATION

ADDRESSING POTENTIAL SECURITY RISKS DURING SEPARATION

Policy 15: Physical Security for Entity Resources

Asset protection



Security zones

Processes

Policy 15: Core Requirement

Each entity must implement physical security measures that minimise or remove the risk of:

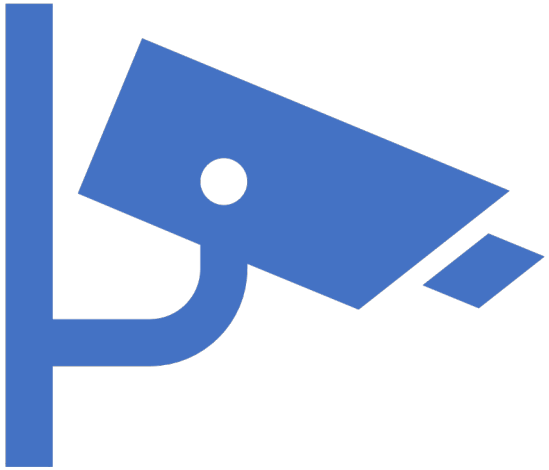
- harm to people, and
- information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.

Policy 15: Supporting Requirements

Requirement 1. Physical security measures	Entities **must** put in place appropriate physical security measures to protect entity resources, commensurate with the assessed business impact level of their compromise, [Note i] loss or damage.
Requirement 2. Security containers, cabinets and rooms	Entities **must** assess security risks and select the appropriate containers, cabinets, secure rooms and strong rooms to protect entity information and assets.
Requirement 3. Disposal	Entities **must** dispose of physical assets securely.

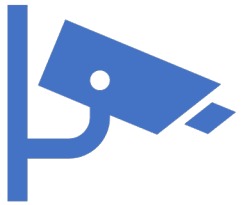
Policy 15: Asset Protection

- Identifying and prioritizing critical assets
- Implementing physical security measures
- Monitoring and maintaining asset security



Policy 15: Security Zones

Establishing and maintaining secure areas



Access control measures for security zones

Regular reviews of zone effectiveness

Policy 16: Entity Facilities

Facility requirements

Access control

Guns, Guards, Gates

and more

Policy 16: Core Requirement

Each entity must:

- ensure it fully integrates protective security in the process of planning, selecting, designing and modifying its facilities for the protection of people, information and physical assets
- in areas where sensitive or security classified information and assets are used, transmitted, stored or discussed, certify its facility's physical security zones in accordance with the applicable ASIO Technical Notes, and
- accredit its security zones.

Policy 16: Supporting Requirements

Requirement 1. Design and modify facilities

When designing or modifying facilities, entities **must**:

a. secure and control access to facilities to meet the highest risk level to entity resources, and
b. define restricted access areas as detailed below.

Zone name	Zone definition
Zone One	Public access.
Zone Two	Restricted public access. Unrestricted access for authorised personnel. May use single factor authentication for access control.
Zone Three	No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel. Single factor authentication for access control.
Zone Four	No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel with appropriate security clearance. Single factor authentication for access control.
Zone Five	No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel with appropriate security clearance. Dual factor authentication for access control.

Requirement 2. Building construction

Entities **must** ensure:

a. facilities for Zones Two to Five that store sensitive or security classified information and assets are constructed in accordance with applicable sections of:
   i. ASIO Technical Note 1/15 – Physical Security Zones, and
   ii. ASIO Technical Note 5/12 – Physical Security Zones (TOP SECRET) areas
b. security zones are constructed to protect against the highest risk level in accordance with the entity security risk assessment in areas:
   i. accessed by the public and authorised personnel, and
   ii. where physical assets, other than sensitive and security classified assets, are stored.

Requirement 3. Hardware

Entities must, in areas that store sensitive and security classified information, ensure perimeter doors and hardware are:

a. constructed in accordance with ASIO Technical Notes in Zones Two to Five, and
b. secured with SCEC-approved products rated to Security Level 3 in Zones Three to Five.

Requirement 4. Security alarm systems

Entities **must**:

a. for Zone Three, use either:
   i. a Type 1 security alarm system [Note i], or
   ii. a Class 5 commercial security alarm system, or
   iii. guard patrols performed at random intervals and within every four hours.
b. for Zone Four and Zone Five, use:
   i. SCEC-approved Type 1A or Type 1 security alarm system in accordance with the Type 1A security alarm system transition policy [Note i] with SCEC-approved detection devices and
   ii. a SCEC-endorsed Security Zone Consultant to design and commission the SCEC-approved Type 1A alarm system.
c. in Zones Three [Note ii] to Five:
   i. use sectionalised security alarm systems
   ii. security alarm systems are:
      A. directly managed and controlled by the entity
      B. maintained by appropriately cleared contractors
      C. monitored and responded to in a timely manner, and
   iii. privileged alarm systems operators and users are appropriately trained and security cleared

Policy 16: Supporting Requirements

Requirement 5. Access control	a. Entities **must** control access to Zones Two to Five within the entity's facilities by only allowing access for authorised personnel, visitors, vehicles and equipment and apply the following

#	Supporting requirements
	controls: i. for Zones Two to Five, use: A. electronic access control systems where there are no other suitable identity verification and access control measures in place. ii. for Zones Three to Five, use: A. identity cards with personal identity verification B. sectionalised access control system with full audit C. regular review of audit logs for any unusual or prohibited activity iii. for Zone Four and Zone Five, ensure access control systems are: A. directly managed and controlled by the entity B. maintained by appropriately cleared contractors C. privileged operators and users are appropriately trained and security cleared to the level of the security zone, and iv. for Zone Five, use dual authentication access control. b. When granting ongoing (or regular) access to entity facilities for people who are not directly engaged by the entity or covered by the terms of a contract or agreement, the entity's accountable authority or CSO **must** ensure the person has: i. the required level of security clearance for the facility's security zones, and ii. a business need supported by a business case and risk assessment, which is reassessed on a regular basis at least every two years.
Requirement 6. Technical surveillance counter-measures	Entities **must** ensure a technical surveillance countermeasures inspection is completed for facilities where: a. TOP SECRET discussions are regularly held, or b. the compromise of discussions may have a catastrophic business impact level.
Requirement 7. Security zone certification	CSOs or delegated security advisers **must**, before using a facility operationally: a. certify the facility's Zones One to Four in accordance with the PSPF and ASIO Technical Notes b. for Zone Five facilities, obtain: i. ASIO-T4 physical security certification for security areas used to handle TOP SECRET sensitive and security classified information, sensitive compartmented information (SCI) or aggregated information where the compromise of confidentiality, loss of integrity or unavailability of that information may have a catastrophic business impact level.
Requirement 8. Security zone accreditation	CSOs or delegated security advisers **must**, before using a facility operationally: a. accredit Zones One to Five when the security controls are certified and the entity determines and accepts the residual risks, and b. for Zone Five facilities, obtain: i. Australian Signals Directorate security accreditation for areas used to secure and access TOP SECRET sensitive compartmented information.
Requirement 9. ICT facilities	Entities **must**: a. certify and accredit the security zone for ICT sensitive and security classified information with an extreme business impact level b. ensure that all TOP SECRET information ICT facilities are in compartments within an accredited Zone Five area and comply with Annex A – ASIO Technical Note 5/12 – Compartments within Zone Five areas, and c. before using outsourced ICT facilities operationally obtain ASIO-T4 physical security certification for the outsourced ICT facility to hold information that, if compromised, would have a catastrophic business impact level.

Policy 16: Facility Requirements

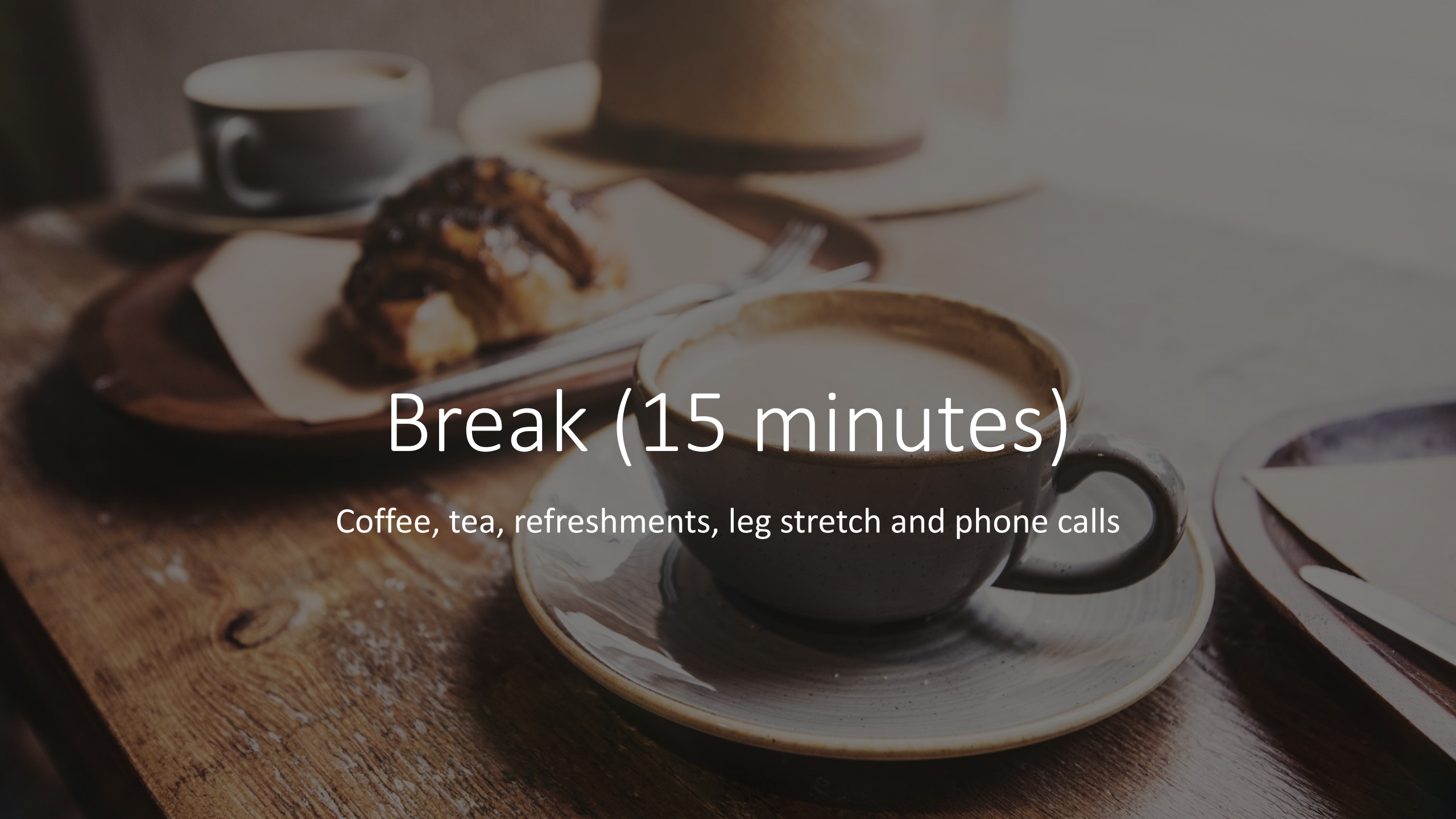
- Ensuring facilities meet security standards
- Maintaining physical infrastructure
- Addressing facility-related risks

Policy 16: Access Control

IMPLEMENTING ACCESS CONTROL SYSTEMS

MONITORING AND MANAGING ACCESS TO FACILITIES

ADAPTING ACCESS CONTROLS AS NEEDED



Break (15 minutes)

Coffee, tea, refreshments, leg stretch and phone calls

Review

- Key takeaways from the previous section
  - POLICY 11: ROBUST ICT SYSTEMS (INFO)
  - POLICY 12: ELIGIBILITY AND SUITABILITY OF PERSONNEL (PERS)
  - POLICY 13: ONGOING ASSESSMENT OF PERSONNEL (PERS)
  - POLICY 14: SEPARATING PERSONNEL (PERS)
  - POLICY 15: PHYSICAL SECURITY FOR ENTITY RESOURCES (PHYS)
  - POLICY 16: ENTITY FACILITIES (PHYS)

Exercise 3 - Security awareness training

- Work in small groups to develop a security awareness training program for a hypothetical Australian Government entity.
- Use your entity, or a hypothetical entity, identify risks and develop a training program to educate staff.
- Objective: Practice identifying and addressing security risks through effective security awareness training.

SRMBOK
Security Risk Management Body Of Knowledge

Control Effectiveness Assessment

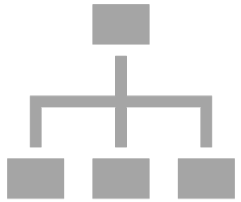
Methodology

Key factors in assessing control effectiveness

How some organisations do it

Control Effectiveness Assessment - Methodology

Overview of assessment methodologies



Choosing the right approach for your organization

Conducting and analyzing assessments

Control Effectiveness Assessment - Key Factors

IDENTIFYING IMPORTANT FACTORS IN CONTROL EFFECTIVENESS

BALANCING SECURITY AND OPERATIONAL NEEDS

RECOGNIZING AND ADDRESSING GAPS

Alternative Assessment Models

- Overview of different assessment approaches
- Pros and cons of each model
- Choosing the right model for your organization

SECURITY RISK MANAGEMENT CONTROLS

POLICY

- Policies, Procedures, Protocols, Guidance, Forms, Standards, Codes of Practice
- The why, what, when, who, where and how

ASSURANCE

- Training, capability, competency, resources, communication,
- Ensuring there is a capability to execute

COMPLIANCE

- Audits, Photos, Certifications, ICT logs, Incident reports
- Validation and monitoring of management and assurance

Some Concerns

Issues with current assessment methods

Improvement opportunities

The reporting process

Issues with Current Assessment Methods

CHALLENGES IN ASSESSING PSPF

BENCHMARKING

ADDRESSING AND OVERCOMING ISSUES

Improvement Opportunities

- Recognizing areas for improvement
- Training needs analysis
- Return on Investment
- Monitoring the impact of improvements

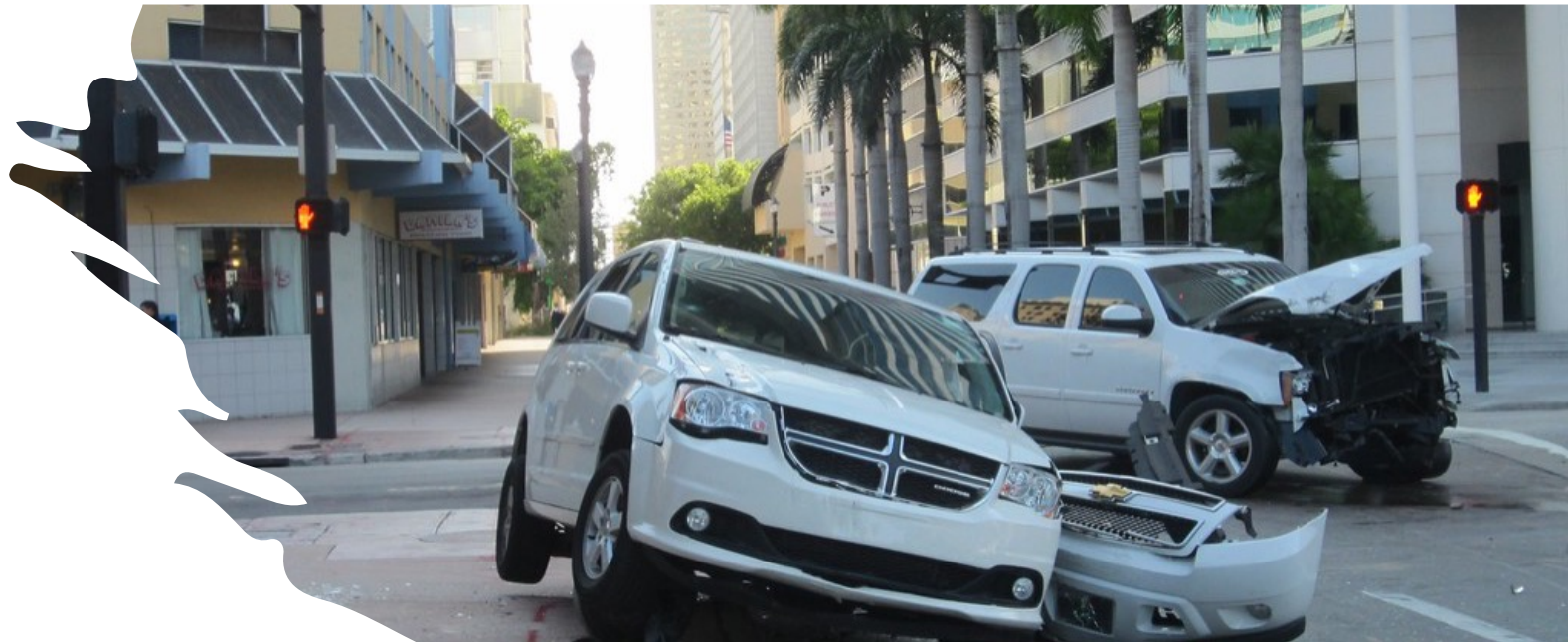
Some Recommendations

Best practices for PSPF assessment

Organisational capability / competence

Cyber security

- Risk assessment (GOV)
- Social engineering (PERS)
- Source code (INFO)
- User logon (ICT)
- Server room (PHYS)



SRMBOK
Security Risk Management Body Of Knowledge

Best Practices

IMPLEMENTING PROVEN PRACTICES FOR PSPF ASSESSMENT

ADAPTING PRACTICES TO FIT YOUR ORGANIZATION'S NEEDS

LEARNING FROM THE EXPERIENCES OF OTHERS

Implementation Guidance

Step-by-step guidance for PSPF assessment

Bottlenecks and influencers

Ongoing support and resources

The Problem with Annual Reporting

Challenges of annual reporting

Solutions for more effective reporting

Lag Indicators

Establishing a Reporting Structure

DESIGNING AN EFFECTIVE MONTHLY REPORTING FRAMEWORK

ALIGNING REPORTING WITH ORGANIZATIONAL OBJECTIVES

ADAPTING THE FRAMEWORK TO EVOLVING NEEDS

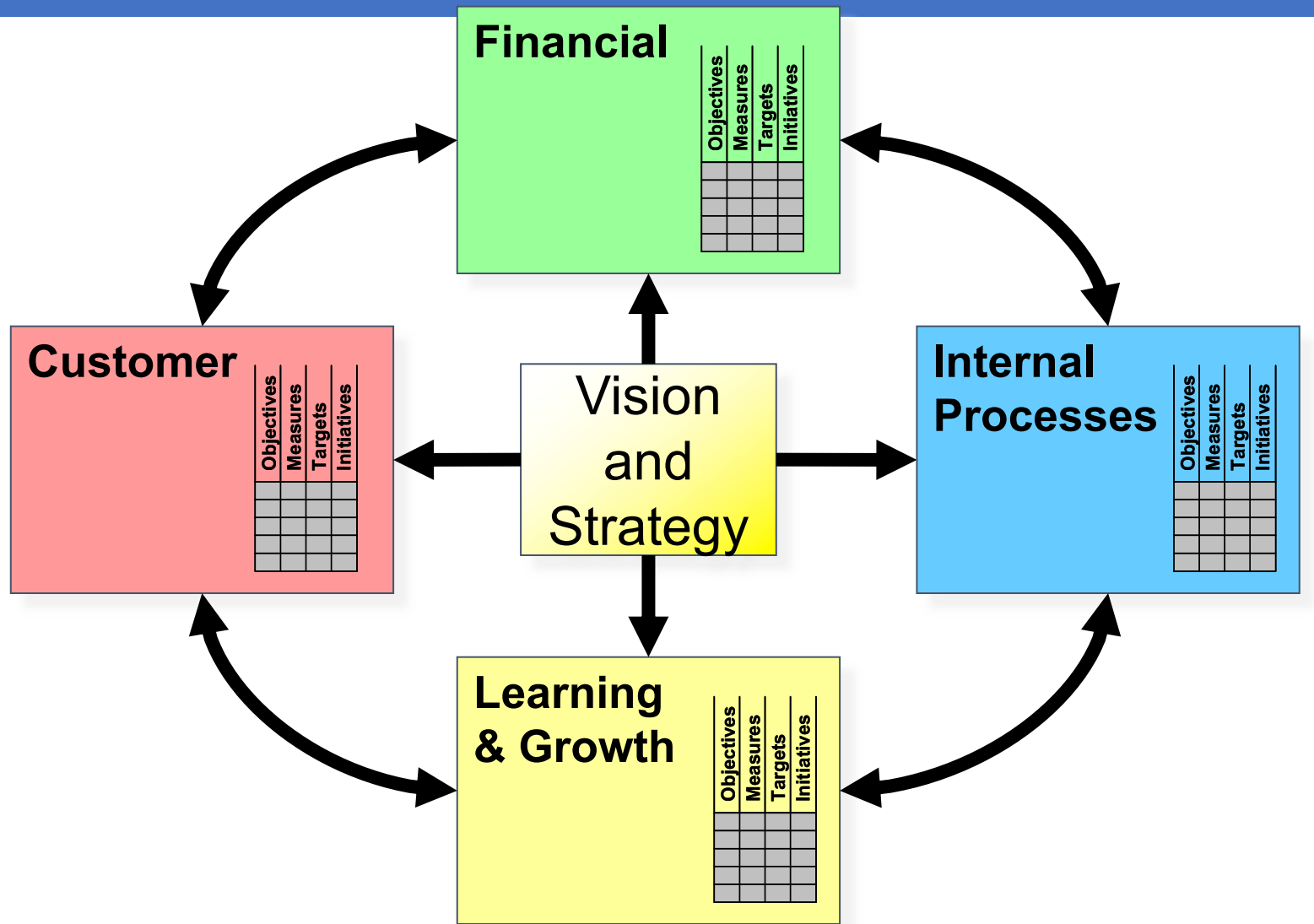
A Monthly Reporting Framework - Overview

Establishing a reporting structure

Key performance indicators (KPIs)

Balanced ScoreCard

Balanced ScoreCard (Kaplan Norton)



SRMBOK
Security Risk Management Body Of Knowledge

Monthly Report Headings

Financial

- Efficiency and Cost Management

Customer

- Customer Satisfaction

Internal Processes

- Continuous Improvement
- Security & Risk
- Security Promotion & Participation
- Access Control
- Disaster Management & Planning
- Security Equipment Management

Internal Processes

- Security System and Log Audits
- Legal Requirements
- Contractual Requirements
- Processes & Incident Management
- Management Leadership and Commitment
- Human Resources

Learning & Growth

- Training and Competency
- Staff Development

Challenges of Monthly Reporting

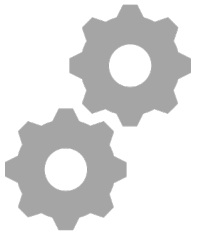
IDENTIFYING ISSUES WITH FREQUENT REPORTING

UNDERSTANDING THE IMPACT ON RESOURCE ALLOCATION

BALANCING REPORTING FREQUENCY WITH ACCURACY

Solutions for Effective Reporting

Adapting reporting practices for your organization



Implementing tools and processes to streamline reporting

Continuously improving reporting effectiveness

Key Performance Indicators (KPIs)

Identifying KPIs for PSPF compliance

Tracking and analyzing KPI data

Using KPIs to drive improvement

A Granular Control Assessment Framework

DIVING DEEPER INTO CONTROL ASSESSMENTS

MONITORING AND ADJUSTING CONTROL EFFECTIVENESS

Diving Deeper into Control Assessments

Detailed examination of controls and their effectiveness

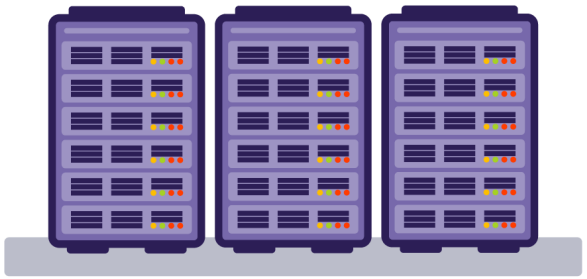
Identifying areas for further analysis and improvement

Prioritizing resources based on risk and impact

Swiss Cheese Theory

Swiss-Cheese Example

In this example, intelligence agents gain physical access to corporate servers and steal corporate data.



Government or commercial intelligence operatives discover the physical location of servers in a shared data facility

They enter server room as potential clients or technicians for co-located company

Management practices routinely allow visitors and 3rd parties to remain unsupervised in server room

Cost saving measures mean that not all server cabinets have locks on cabinet doors

Hardware or software intercept placed on client servers.

Customer and corporate records compromised.

NOTE: Most data breaches occur remotely via software vulnerabilities but a) this is a lot easier example for non-IT people and b) it is (sadly) a real world example.

4C’s of Risk Findings & ObserVations

CONDITION

- What is happening?
- Observable artefacts.

CRITERIA

- What should be happening?
- The policy, procedure, requirement or best practice.

CONSEQUENCE

- What is, or will be, the outcome?
- The impact on objectives

CAUSE

- What is the cause of this situation?
- The underlying systemic root cause.

4As of Recommendations

ACTIONABLE

- Is it clear what to do?
- Specific, measurable and time bound.

ACHIEVABLE

- How will you know when you have done it?
- Metrics for success, ideally binary with a yes/no gate.

APPROPRIATE

- Does it address the root cause?
- Address underlying cause, not the immediate issue.

AGREED

- Do the review team and risk owner support this?
- Supported by management and adequate resources.

Monitoring and Adjusting Control Effectiveness

Regularly reviewing control performance

Making adjustments as needed to maintain effectiveness

Ongoing improvement through a proactive approach

Software to Assess Control Effectiveness

Benefits

- Streamlined control assessment and reporting
- Enhanced visibility and analytics
- Improved communication and collaboration

Wrap-up and Q&A

- Recap of the day's content
- Time for questions and answers
- Next steps and resources