Annex A. PSPF Maturity Self-Assessment Model

Security governance

Outcome: Each entity manages security risks and supports a positive security culture in an appropriately mature manner ensuring clear lines of accountability, sound planning, investigation and response, assurance and review processes and proportionate reporting.

Annex A. Table 1 PSPF Maturity Self-Assessment Model – Security governance

	Ad hoc ◑	**Developing** ◕	**Managing** ●	**Embedded** ◉
Description	**Partial:** Some PSPF core and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas.	**Substantial:** The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes.	**Full:** All PSPF core and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes.	**Excelled:** All PSPF core and supporting requirements are implemented, effectively integrated and exceeding security outcomes. Entity's implementation of better-practice guidance drives achieving high performance.
Role of accountable authority	The accountable authority is partially aware of protective security requirements across the entity. Partial understanding, assessment and management of security risks to the entity's people, information and assets. Security is dealt with in an ad hoc manner.	The accountable authority substantially applies protective security requirements across the entity. Security risks and risk tolerances are identified and are substantially managed, monitored or reassessed on a regular basis. Security risk decisions and shared risks that affect other entities are substantially managed and communicated to affected entities.	The accountable authority consistently applies protective security policy across the entity, determines the entity's tolerance for security risks, promotes sound risk management processes and ensures appropriate governance arrangements are in place to protect the entity's people, information and assets. In medium to large entities, the management committee oversees and reviews risk profile and ensures underpinning procedures are consistent and adaptable to changes in the risk environment. Security risk decisions and shared risks that affect other entities are understood and communicated in a timely manner.	The accountable authority has an integrated, continuous-improvement approach to security management across the entity. Security risk management is a significant priority for the entity and is identified and aligned to business objectives. The entity identifies and operates within agreed and defendable risk tolerances that actively inform business decisions. Formal risk management processes and initiatives to connect security risk management and operations are in place. The entity promotes inter-entity collaboration to improve management of security risk decisions and shared risks that affect other entities. Where appropriate, the entity provides best-practice advice to other entities in its area of expertise.

	Ad hoc ◐	**Developing** ◕	**Managing** ●	**Embedded** ◉
Description	**Partial:** Some PSPF core and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas.	**Substantial:** The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes.	**Full:** All PSPF core and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes.	**Excelled:** All PSPF core and supporting requirements are implemented, effectively integrated and exceeding security outcomes. Entity's implementation of better-practice guidance drives achieving high performance.
Management structures and responsibilities	Security management structures and responsibilities are partially in place. Responsibility for designated security roles, protective security planning and management of security practices are ad hoc. Incident reporting is by exception with partial staff awareness of obligations. Incident response processes are informal and not centrally managed. Security is partially prioritised by leadership with partial employee and contractor awareness.	The CSO is appointed and key security responsibilities are substantially assigned. Security risk and incident reporting is occurring across the entity and response processes are centrally managed in the majority of cases. The importance of security and developing a strong security culture is substantially recognised by the leadership. The majority of personnel attend periodic security awareness and skills development training.	The CSO is empowered to investigate, respond to and report on security incidents. Clearly defined security roles and responsibilities exist with skilled personnel appointed by the CSO and empowered to make security decisions for their entity. A governance oversight function is established (where appropriate to entity size). Entity's cycle of action, evaluation and learning is evident in response to security incidents. Personnel are knowledgeable of security incident reporting obligations with reporting processes published and accessible. Security is integral to the entity's business and informs decision-making. Leadership is actively engaged and visibly prioritises good security practices with a strong security culture evident within the entity. Personnel's attendance and understanding of regular education programs that inform and assist their understanding of security-related processes and obligations is monitored.	Role of the CSO is highly visible and central to delivering on strategic business priorities and objectives. A security governance oversight function is operational. Security is fully integrated into entity operations, actively managed, monitored and drives improvements. Security procedures and practices are robust and of proven effectiveness. The CSO ensures personnel resources are deployed to support the maintenance of effective protective security; appointing skilled personnel according to business needs. Comprehensive approach to managing security incidents including investigating to determine root causes and inform security improvements and education programs. All personnel are trained annually on security policy and procedures and take responsibility for implementation within their area of responsibility. Security culture is underpinned by continuous improvement and accountability.

	Ad hoc ◐	Developing ◕	Managing ●	Embedded ◉
Description	**Partial:** Some PSPF core and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas.	**Substantial:** The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes.	**Full:** All PSPF core and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes.	**Excelled:** All PSPF core and supporting requirements are implemented, effectively integrated and exceeding security outcomes. Entity's implementation of better-practice guidance drives achieving high performance.
Security planning	Security planning is ad hoc. The security plan is partially developed and implemented but may not be current or comprehensive.	A security plan is endorsed, captures entity's goals and strategic objectives, key threats, risks, vulnerabilities and details of security risk tolerances and risk mitigation strategies. The plan is consistently applied across the entity in the majority of instances.	A security plan is endorsed by accountable authority and captures entity's goals and strategic objectives, key threats, risks, vulnerabilities and details of security risk tolerances and risk mitigation strategies. The plan is regularly reviewed and informs entity's decision-making. The plan is used to determine the security objectives and clearly supports the broader business goals. The security plan is communicated and accessible across the entity.	The security plan is comprehensive in identifying goals, strategic objectives, key threats, risks, vulnerabilities, risk tolerances and risk mitigations. The security plan influences executive management decision-making and planning. The entity continuously adapts the security plan in response to emerging or changing risks and threat levels.
Security maturity monitoring	The entity partially monitors security maturity performance of its security capability and risk culture against the goals and strategic objectives identified in the entity security plan.	Security capability and risk culture is addressed in the security plan. The performance and progress against the security plan's goals and strategic objectives is substantially monitored regularly.	Consistent and defined approach to monitoring the entity's security performance, which is tailored to the entity's risk environment. The entity has clearly defined security goals and objectives in the security plan. Performance is tracked and measured to assess security capability and risk culture maturity.	The entity proactively engages in ongoing monitoring and improvement of security capability and culture through long-term planning to predict and prepare for security challenges. Performance data is captured analysed and informs change.

	Ad hoc ◐	**Developing** ◕	**Managing** ●	**Embedded** ◉
Description	**Partial:** Some PSPF core and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas.	**Substantial:** The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes.	**Full:** All PSPF core and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes.	**Excelled:** All PSPF core and supporting requirements are implemented, effectively integrated and exceeding security outcomes. Entity's implementation of better-practice guidance drives achieving high performance.
Reporting on security	The entity has partially met external reporting obligations to its portfolio minister, AGD, other affected entities and ASD on cyber security matters. Reporting on the entity's achievement of security outcomes, implementation of core requirements, maturity of security capability, key risks to people, information and personnel and mitigation strategies to manage identified risks is partial and ad hoc.	The entity substantially meets external reporting obligations to the portfolio minister, AGD, other affected entities and ASD on cyber security matters. The entity's achievement of security outcomes, implementation of core requirements, maturity of security capability, key risks to people, information and personnel and mitigation strategies to manage identified risks is substantially captured in the annual security report.	The entity meets all external reporting obligations within required timeframes to the portfolio minister, AGD, other affected entities and ASD on cyber security matters. The entity meets these obligations through comprehensive reporting on achievement of security outcomes, implementation of core requirements, maturity of security capability, key risks to people, information and personnel and mitigation strategies. Key findings and trends are shared within the entity.	The entity excels in meeting reporting obligations and uses annual reporting to drive improvements, strengthen security culture and inform future planning.
Security governance for contracted goods and service providers	Protective security provisions are partially included in goods and service provider contracts. The entity partially monitors service providers' adherence to contract provisions.	Appropriate security obligation clauses are included in the majority of provider contracts. The entity substantially applies processes to monitor service provider adherence to contract provisions.	Provider contracts contain explicit provisions to ensure implementation of relevant protective security requirements. The entity uses processes to monitor service providers' adherence to contract provisions and security obligations.	The entity actively monitors and audits service provider capability to fully implement contractual protective security requirements. Where appropriate, the entity supports contractors to achieve security outcomes.

	Ad hoc ◑	**Developing** ◕	**Managing** ●	**Embedded** ◉
Description	**Partial:** Some PSPF core and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas.	**Substantial:** The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes.	**Full:** All PSPF core and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes.	**Excelled:** All PSPF core and supporting requirements are implemented, effectively integrated and exceeding security outcomes. Entity's implementation of better-practice guidance drives achieving high performance.
Security governance for international sharing	The entity has access to foreign government information and assets and partially understands and implements handling and protection requirements agreed in international agreements and arrangements to which Australia is a party.	The entity has access to foreign government information and assets. There is substantial awareness, through training and accessibility of applicable agreements, of the level of handling protection requirements agreed in international agreements and arrangements to which Australia is a party.	The entity has access to foreign government information and assets and consistently applies handling protection requirements agreed in international agreements and arrangements to which Australia is a party. Alternatively, the entity is confident it does not access any information or assets that would be governed by international agreements or arrangements to which Australia is a party.	Where an entity has access to foreign government information and assets, it actively implements and monitors handling requirements agreed in international agreements and arrangements to which Australia is a party – and these are consistently applied. The entity proactively contributes to, and identifies, opportunities to evolve multilateral, bilateral agreements and arrangements to which Australia is a party on sharing and protection of information and assets.