









Annex A. PSPF Maturity Self-Assessment Model

Information security

Outcome: Each entity maintains the confidentiality, integrity and availability of all official information.

Annex A. Table 1 PSPF Maturity Self-Assessment Model – information security

	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, are effectively integrated and exceeding security outcomes with better-practice guidance achieving high performance.
Sensitive and classified information	The entity has a partial understanding of its information holdings. Procedures and operational controls to protect official government information assets proportional to their value, importance and sensitivity are ad hoc.	The entity knows the value of its information holdings and has established operational controls to ensure official government information is managed in accordance with minimum protections identified in the PSPF policy: Sensitive and classified information . The entity monitors and controls classified information holdings in the context of its risk environment.	The entity knows the value of its information holdings and operational controls are in place to ensure official government information asset holdings are consistently handled in accordance with minimum protections identified in the PSPF policy: Sensitive and classified information , proportional to their value, importance and sensitivity.	The entity culture actively supports the consistent and appropriate handling of official government information asset holdings in accordance with minimum protections identified in the PSPF policy: Sensitive and classified information . In a heightened risk environment, the entity closely monitors and controls classified information holdings.
Access to information	Information access controls and security procedures are partially in place. Supporting requirements on information sharing, access to sensitive and security classified information and controlling access to supporting ICT systems, networks, infrastructure, devices, applications and data holdings are partially applied.	Processes are substantially in place to enable appropriate sharing of information with relevant stakeholders who have a need-to-know and are appropriately security cleared. Access controls are substantially implemented to limit unauthorised access to supporting ICT systems, networks, infrastructure, devices, applications and data holdings in accordance with the information access control supporting requirements.	Information holdings are accessed and shared with appropriately security cleared personnel who have a need-to-know. Access controls support the integrity of ICT systems, networks, infrastructure, devices, applications and data holdings.	The entity proactively refines and reinforces information management processes and access controls to ensure protection of information and currency of systems to protect against emerging threats and issues. Information is shared with appropriately security cleared personnel who have a need-to-know. Systems are in place to detect, monitor and respond to irregular access to information or ICT systems, networks, infrastructure, devices and applications in real-time.

	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, are effectively integrated and exceeding security outcomes with better-practice guidance achieving high performance.
Safeguarding from cyber threats	Partial implementation of Top 4 strategies to mitigate targeted cyber intrusions . Reactive approach to <u>implementing the remaining Strategies to Mitigate Cyber Security Incidents to protect the entity</u> .	The entity has implemented the majority of the Top 4 strategies to mitigate targeted cyber intrusions . The entity understands and has substantially implemented the remaining Strategies to Mitigate Cyber Security Incidents it considers necessary to protect the entity.	All Top 4 strategies to mitigate targeted cyber intrusions have been fully implemented with ongoing performance monitoring. The entity understands and has implemented the remaining Strategies to Mitigate Cyber Security Incidents it considers necessary to protect the entity.	The entity has fully implemented the Essential Eight, and other activities relevant to the entity's risk environment, to protect against harm from identified cyber threats. Processes are regularly tested to ensure real-time response to potential cyber intrusions and emerging threats.
Robust ICT systems	Partial security measures are in place for ICT system development. Management of ICT systems certification and accreditation (or assessment and authorisation) is ad hoc and partially implemented in accordance with relevant Information Security Manual technical standards when operationalised.	Security measures are substantially in place for ICT system development. Certification and accreditation (or assessment and authorisation) of ICT systems is in accordance with ISM technical standards in the majority of cases managed when operationalised.	Security measures are applied during all stages of ICT system development. ICT systems are certified and accredited (or assessed and authorised) in accordance with ISM technical standards when operationalised.	ICT security measures, including ICT systems certification and accreditation (or assessment and authorisation) are in accordance with the ISM technical standards. The entity excels in proactively exploring opportunities to further improve ICT security protections in response to ICT security threats.