Governance Security maturity indicators

SAPSF Policy	Informal - 1	Basic - 2	Managed - 3	Enhanced - 4
GOVSEC1: Security governance **Core Requirement 1:** *The accountable authority must establish the right security governance for the agency*	• The accountable authority is at best partially aware of the SAPSF and their protective security responsibilities within the agency • Security management personnel are appointed in name only. Formal day-to-day functional security leadership has not been assigned • Good security practice is not understood or modelled by the agency's leadership or employees • There are limited or no defined reporting lines for protective security management • Security management is insufficiently resourced (no security budget) and • Security management is reactive and processes and treatments are ad hoc (e.g. security incident management) • Overall responsibility for security is unclear and employee awareness and security culture are poor • There is no security awareness training available, and the agency's employees do not understand security risk • Security is not a priority for the agency	• The accountable authority understands their security responsibilities and has basic measures in place to meet the SAPSF core and supporting requirements • An ASE has been assigned responsibility for security, however, that person has limited involvement in the delivery of the agency's security goals. • Security management is assigned to at least cover the protective security domains (information, personnel, physical) • Day-to-day security responsibilities are unstructured and not interconnected. There is limited interaction with security management • Protective security management and governance structures are occasionally reviewed to ensure responsibilities and reporting lines are appropriate and effective • Effective security relies upon individual managers or employees. There is lack of central oversight and coordination • The agency's employees view security as the responsibility of a few managers and specialists • The agency has some ability to assess its security culture • Security performance does not align with the agency's security goals • Security management is adequately resourced (limited security budget) but additional resources are required • Security is a low priority for the agency	• The accountable authority has implemented all core and supporting requirements of the SAPSF to a level that identifies, assesses, monitors and reviews the agency's security risks. • The agency's Agency Security Executive has active and effective oversight of the agency's protective security risks and arrangements. The ASE is highly aware of the agency's security goals and maturity level. • The ASE has been empowered to make decisions affecting the agency's security, including allocation of resources • Day-to-day security management responsibilities have been clearly defined and assigned across all domains of protective security, including for driving the agency's security culture and cycle of continuous improvement. • Security incidents or issues are routinely reported, assessed and managed (well-resourced) • Day-to-day security management and the agency's security governance are clearly delineated to ensure monitoring and review processes are effective • Security management and leaders are known and approachable. They lead by example and actively model good security practices • The agency's employees understand and accept their security responsibilities • Security training (including awareness training) is undertaken routinely and lessons learned are fed back for planning and policy reviews • Security performance reflects the agency's security goals	• In addition to the criteria of 'managed': • The accountable authority has implemented a protective security regime that exceeds the outcomes of the SAPSF and adopts a dynamic, risk-based approach to protective security. • Formal and connected risk management processes exist across all elements or functions of the entity • The ASE ensures the agency's Executive and Governance groups are involved in security decisions, training and planning, and are aware of how security impacts their responsibilities. • Security management and leaders drive continuous improvement to security within their business units through identifying areas for improvement • The agency's employees are central to the success of security, including actively identifying areas for improvement and driving positive cultural change • Long-term security planning has been undertaken to ensure resources and priorities are maintained • Security performance routinely exceeds the agency's security goals • Security is a significant priority for the agency.

			• Security is priority for the agency, and is factored into all decision making processes	
GOVSEC2: Security planning **Core Requirement 2:** *Maintain a security plan to manage security risks*	• Some security risks and requirements are reflected in the agency's strategy and planning, however, is not widespread or consistent • The agency does not understand security risks broadly, or how they can impact the efficient and effective delivery of government services • The is no or limited structure to risk management processes in the agency and there is little or no confidence knowing what the agency's risks are • Security planning is ad hoc. A security plan may be partially developed but may not be current or comprehensive. • There are no or limited security policies or procedures documented and in place. Application of these policies or procedures is highly variable and inconsistent • The agency's risk tolerances are unknown. • There is no documented business continuity plan • There is no or limited capability to increase security levels or resources during a security incident or event	• Agency planning considers known security risks and needs, but may not be informed by the most up-to-date or informed risk, threat, vulnerability or criticality assessments • The security plan captures the agency's security goals, strategic objectives, maturity targets, key risk, threat, vulnerability and criticality assessments and risk treatment plans. • The plan has been endorsed by the accountable authority but is reviewed no earlier than every 2 years, and may be out of date • The agency's security planning generally mitigates known or significant security risks effectively, but there are no established measures in place to confirm their effectiveness • People responsible for planning are appropriately skilled, but may not have the time or resources to ensure plans are robust • A basic business continuity plan has been developed but it is not routinely reviewed or updated • There is an ad hoc approach to increasing security levels or resources during a security incident or event	• Agency planning is comprehensive to ensure people, information and assets are protected. All areas of the agency and its function are reflected in agency planning. • The security plan supports the agency's broader business goals • The agency's plan demonstrates clear understanding of the security risks, informed by a robust risk management process. • All security risks are proactively managed to reduce the likelihood of something occurring, or the consequences if it does • The security plan is reviewed a least every 2 years to ensure it is relevant to the agency's risk profile. • Security management regularly reviews the plan and uses it to inform decision making. • The security plan is flexible and adaptable to changing or emerging risks. Security management updates the plan according to changes to risk, threat, vulnerability or criticality. • The Executive and Governance groups of the agency are aware of the security plan and are informed of progress against, and changes to, the plan • The agency's business continuity plan is regularly tested and reviewed • The security plan is communicated and available to those who need it • The security plan is scalable to account for increased security levels or need for resources during a security incident or event	• In addition to the criteria of 'managed': • Protective security is fully integrated into the agency's business strategy and objectives • Strategies, plans and processes are dynamic, well-informed and evidence based. • Data is readily available to assist risk assessments and to analyse risks, threats, vulnerabilities and criticalities • A robust security culture ensures opportunities to enhance security planning and actions are identified • The business continuity plan is regularly exercised and reviewed to ensure the agency is prepared for disruption
GOVSEC3: Security monitoring **Core requirement 3:**	• The agency has no defined monitoring structure in place and is unaware of any changes to risks, threats, vulnerabilities or criticalities	• Security planning is not centrally coordinated, so improvement is inconsistent and/or inefficiently applied (e.g. security information	• The agency reviews its security arrangements at least annually	• In addition to the criteria of 'managed' • The agency has continuous monitoring and spot-checking capability in place which can identify the breakdown or failure of critical risk

Monitor security maturity against the security plan	• The agency has limited confidence in its security arrangements as there is no central coordination of security risk management • Any security plans or processes in place are not reviewed or updated routinely • Security is not a part of the agency's business planning	needs to be re-gathered every time a review is undertaken) • There is some confidence the agency meets some of the SAPSF core and supporting requirements • Security plans and procedures are only reviewed reactively • The agency plans to implement better assurance practices but is yet to do so	• Security reporting and risk assessments contain the level of detail the agency requires to keep its plans accurate and effective • Assurance activities are undertaken on a routine basis and considered a core part of security planning and risk management • Security decisions are informed by evidence collected by the agency through routine business practices. Security maturity can be effectively measured by this evidence. Some of this information is automated. • Criteria is established to ensure each security risk, threat, vulnerability or criticality is reviewed according to the level of risk • Security policies and procedures are effective at meeting the security needs of the agency, in line with the security plan • Security performance is consistent with the agency's business plan and security goals • The agency undertakes periodic independent security reviews and the outcomes inform security planning and risk management decisions • Monitoring processes, including environmental scanning, identify changes to risk, threat, vulnerabilities or criticalities	treatments. Many of these processes are automated • The effectiveness of risk treatments not subject to continuous monitoring are routinely audited and assessed • The agency routinely reports security performance to employees, including changes to risks, threats, vulnerabilities and criticalities (where there is no reason to restrict that information) • The agency has a governance or audit committee in place to provide independent oversight of the effectiveness and efficiency of the security arrangements
GOVSEC4: Annual security attestation **Core Requirement 4:** *Provide an annual security attestation to the Department of the Premier and Cabinet on progress against the security plan*	• The agency has no defined structure in place to monitor or assess its protective security risks, the risk environment or the required security measures • Assurance measures are informal, inconsistent and lack evidence-based outcomes • Protective security is not a part of the agency's strategic risk management activities • There is limited or no audit mechanisms in place to assess the effectiveness of policies, procedures or measures	• The agency has limited confidence it meets all the requirements of the SAPSF • The agency has the ability to perform assurance activities effectively, however, the capability is reactive only • There is a lack of continuity between assurance activities meaning roles and responsibilities need to be reassigned each time and there is often duplication of effort in collecting and collating information • The protective security program is informally monitored	• The agency completes all annual assurance and assessment activities • Assurance is a routine component of the protective security performance of the agency • Evidence is used as the basis for both security performance and identifying security mitigations • Security risks are routinely considered by the agency's executive and security governance bodies • Monitoring capability it commensurate with the criticality of the security risk or agency resources	• In addition to the criteria of 'managed' • The agency has continuous monitoring in place to detect and prevent control breakdowns. This monitoring is supported by automation, at least in high-risk areas • Security measures not subject to automation are regularly checked • Performance indicators to significant security risks are captured to inform real-time responses • The agency provides periodic reporting on the security performance of the organisation to all employees, except where there is a reason to restrict the information

		• The agency obtains limited information to demonstrate the effectiveness of protective security policies, processes and measures	• The agency's security performance is linked to the strategic objectives and, as far as possible, is designed to support it • The agency periodically commissions independent assurance reviews, at least the management of significant security risks • Assurance activities automatically inform changes to security policies and measures • Ongoing monitoring can actively identify improvements to security, changes in risk levels and if security measures are being implemented correctly or appropriately • The agency routinely gathers evidence to assist in demonstrating performance and improvement, and the effectiveness of existing security measures	• The agency receives independent oversight on the effectiveness of security measures from a governance or audit committee
GOVSEC5: Managing the security of contractors and service providers **Core Requirement 5:** *Ensure contractors and service providers are compliant with all relevant agency and SAPSF requirements*	• The agency does seek clarification or visibility of the security procedures or measures of external contractors or service providers before sharing sensitive information with them • Security is not a consideration in procurement decisions	• The levels of due diligence on the security procedures or measures of external contractors or service providers is inconsistent across the agency • Procurement decisions identify requirements for people, information and assets to remain protected	• The agency conducts due diligence checks on contractors and service providers to ensure the conditions of the contract are being met • Procurement contracts include standard terms and conditions relating to security • The agency's plans and procedures include guidance for working with, or entering into contracts with, external service providers	• In addition to the criteria or 'managed' • The agency encourages and contractors and service providers to contribute to and participate in the agency's continuous improvement program, including optimising their own procedures or measures • The agency is able to identify changed or emerging risks relating to contractors and service providers and put in place mitigations to improve existing and future contracts and services • Contractors and service providers are routinely audited for compliance with the security requirements of their contract, and are held accountable for the results
GOVSEC6: Security governance for international sharing **Core Requirement 6:** *Ensure adherence to any provisions for the security of*	• The agency has access to foreign government information and assets but either does not or only partially understands and implements handling and protection requirements agreed in international arrangement to which Australia is a party.	• The agency 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 agency has access to foreign government information and assets and consistently applies handling and protection requirements agreed in international agreements and arrangements to which Australia is a party. • Alternatively, the agency is confident it does not have access to any information that would be governed by international agreements to which Australia is a party.	• In addition to the criteria of 'managed' • 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.

people, information and assets contained in international agreements and arrangements to which Australia is a party	• 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.

Information security maturity indicators

SAPSF Policy	Informal - 1	Basic - 2	Managed - 3	Enhanced - 4
INFOSEC1: Protecting official information **Core Requirement 7:** *Protect official information against compromise*	• The agency has a little or no understanding of the information assets it has and does not proactively seek to identify which assets require protection. The agency is unaware if any information assets require security classification and associated protections • Protective markings are not (or infrequently) used (including email). Any protective markings are applied manually, inconsistently and often incorrectly • There are limited or no information security measures in place to protect information assets (including ICT systems), and no understanding if any measures are effective or proportionate • Unauthorised access to the agency's information or systems is unlikely to be identified • The agency would not know how to create, access, handle or protect security classified information	• Information security is generally only practised well by those with protective security responsibilities • There are some pockets of good information security practices, but protections and understanding are generally inconsistent • Most, if not all information (including email) is protectively marked, although sometimes incorrectly. Some marking is automated, however, most relies on employees manually applying the appropriate markings • Only simple information security measures are in place for areas holding physical information assets, ICT equipment and general information access controls are basic • Unauthorised access to the agency's information can sometimes be identified retrospectively, however real-time monitoring capability is low or non-existent • The agency may have identified a need for creating, accessing or handling security classified information, but does not have the required systems or processes in place	• The agency has effective processes in place to assess, classify and protect its information assets. These processes are well understood and frequently reviewed • Changes to information security policies and procedures are consistent with the security plan and communicated effectively across the agency • The security measures in place to protect information are proportionate to the agency's information assets • All the agency's information assets are classified, protectively marked, accessed and handled in line with the South Australian Information Classification System and requirements of the SAPSF • The agency has effective measures in place to detect and deter unauthorised or inappropriate access to its information assets (including ICT) • Information security measures are all consistent and compliant with PC012 Information Privacy Principles (IPPS) Instruction and other relevant South Australian policy and legislation • All information is appropriately disposed of once it is no longer needed • Robust policies and procedures are in place to manage mobile devices and remote working arrangements	• In addition to the criteria of 'managed' • The agency actively seeks to and contributes to continuous improvement of information security internally and across government • Information security measures are highly adaptable and responsive

			• The agency has the required systems and processes in place to create, access and handle security classified information • All employees creating, accessing and handling security classified information hold security clearances at the required level	
INFOSEC2: Accessing official information **Core Requirement 8:** *Ensure official information is available to those who need it*	• There are limited or no information security measures in place to protect information assets from unauthorised access (including ICT) • There is limited or no understanding of where and how information is shared outside of the agency, including with contractors or service providers • Unauthorised access to the agency's information or systems is unlikely to be identified (including ICT) • The agency does not know if it needs security cleared personnel	• Only simple information security measures are in place for areas holding physical information assets, ICT equipment and ICT system access controls are basic • There is some understanding of where and how information is shared outside of the agency, including with contractors or service providers, and basic protections are in place to control unauthorised access • Unauthorised access to the agency's information can sometimes be identified retrospectively, however real-time monitoring capability is low or non-existent • The agency may have identified employees requiring security clearances or other positions of trust	• Robust security measures are in place to protect the agency's information assets (including ICT) and access controls are highly effective • The agency has a clear understanding of what and how information is shared outside of the agency, including with contractors and service providers. Appropriate measures (including contracts or agreements) are in place • Access permissions or rights are changed or removed routinely when employees change roles or leave the agency. • Unauthorised access to the agency's information can be identified retrospectively and often in real-time. The agency conducts scheduled and unannounced tests and audits of its controls and access to information • Security measures include segregating duties and reducing opportunities for unauthorised or unintentional access and/or misuse of information assets	• In addition to the criteria of 'managed' • The agency actively seeks to and contributes to continuous improvement of information security internally and across government • Information security measures are highly adaptable and responsive
INFOSEC3: Robust ICT and cyber security **Core Requirement 9:** *Safeguard ICT systems from compromise to ensure confidentiality, integrity and availability of official information is maintained*	• New or existing ICT systems are not certified or accredited • The agency has no security measures in place for ICT system development • There are inadequate ICT system access controls in place • There are limited or no measures in place to identify and respond to targeted cyber intrusions. Responses to cyber threats or attacks are reactive	• The agency has basic certification and accreditation processes for new and existing ICT systems, but they are inconsistently applied • Some security measures are in place for ICT system development • There are basic ICT system access controls in place • The agency understands existing and emerging cyber threats and some measures are in place to identify and mitigate targeted cyber intrusions. It would not take long for capability to be exceeded by increasing threats	• All new and existing ICT systems are certified and accredited according to the requirements of the SACSF • The agency has effective ICT and cyber security measures in place to detect and deter unauthorised or inappropriate access to its information assets • Robust ICT system access control are in place	• In addition to the criteria of 'managed' • The agency actively seeks to and contributes to continuous improvement of information security internally and across government • Information security measures are highly adaptable and responsive

Personnel security maturity indicators

SAPSF Policy	Informal - 1	Basic - 2	Managed - 3	Enhanced - 4
PERSEC1: Recruiting employees **Core Requirement 10:** *Ensure the suitability of all new employees*	• The agency performs limited or no identify or background checks to establish suitability for employment • Security measures to ensure only suitable employees are given access to sensitive information, assets or facilities are inconsistently applied • The agency does not proactively assess what it needs to protect from the insider threat or how an insider might breach security • Employees are not aware of their specific security responsibilities	• Pre-employment screening checks are in place that meet the mandatory requirements of the SAPSF • Some additional role-based, pre-employment checks are undertaken for some employees, but not on a routine basis • Roles requiring security clearances or higher-levels of suitability assurance have been identified and recorded. Some security measures are in place to minimise the risks from employees that do not hold appropriate level clearances	• The agency's pre-employment screening program meets all mandatory requirements of the SAPSF, as well as other relevant checks that help establish the suitability of new employees • All pre-employment practices are role-based and consistently applied	• In addition to the criteria of 'managed' • The agency routinely applies all non-mandatory pre-employment screening checks in addition to the mandatory checks for all employees, regardless of their role • The agency uses security clearances as a method to ensure a higher level of suitability amongst new employees, even where those employees may not access security classified material • Recruitment processes are routinely reviewed to ensure their effectiveness
PERSEC2: Maintaining employee suitability **Core Requirement 11:** *Ensure ongoing suitability of all employees*	• Agency employees are often dismissive of personnel security risks and awareness of threats and agency expectations is poor • The agency would not likely be able to determine a trusted insider breaching security requirements or procedures • There are no mechanisms in place to ensure the ongoing suitability of existing agency employees • The agency would not know if it has security cleared personnel or if they are managing those clearances appropriately	• The people responsible for personnel security generally understand the security lifecycle • There are some areas of good personnel security awareness and practices, but it is inconsistently applied • There are some mechanisms in place to assess the ongoing suitability of most agency employees • Security concerns regarding employees are sometimes reported, but the practice is not widespread and there are limited mechanisms in place to deal with such events • The agency has limited confidence that security clearance holders are managing their clearances appropriately.	• All employees understand their security expectation for maintaining their ongoing suitability and actively participate in any processes • Employees genuinely care for their colleagues and the security of the agency and contribute to detecting, reporting and managing concerning behaviours • Effective mechanisms are in place to assess, monitor and manage the ongoing suitability of all agency employees, especially those in higher-risk positions • All positions requiring security clearances have been identified and recorded, and all employees occupying those roles hold clearances as the appropriate levels • The agency has a high degree of confidence that security clearance holders are managing their clearances appropriately • Personnel security measures are consistent with the agency's risk profile and changes to policies, procedures or expectations are well communicated	• In addition to the criteria of 'managed' • Employee role changes automatically include security and suitability assessments to manage any security risks • Security incidents are routinely reviewed and assessed to improve processes and reduce any likelihood of insider threat • The agency is assured that security clearance holders are complying with all requirements and are actively monitoring suitability for changes in risk • Stakeholders who may be affected by identified security risks are communicated with in an effective and timely manner

PERSEC3: Employee separation **Core Requirement 12:** *Securely manage the separation of all employees*	• There is no formal separation/exit procedure for agency employees • There are no or limited records to identify and remove accesses to agency information or assets after separation • The agency is unaware of any ongoing security risks associated with former employees • Employees are unaware or dismissive of ongoing security obligations	• The agency follows basic separation procedures for employees exiting the agency, but ongoing security risks associated with former employees are not identified or managed • Most accesses are successfully removed following separation, however, there is only limited confidence that former employees no longer maintain any access • Majority of employees understand their ongoing security obligations	• The agency has a robust procedure in place to manage employees who separate from the agency, change roles or need to be managed for security or other reasons • Ongoing security risks arising from separating employees are identified, monitored and managed as required • Security concerns are routinely shared with relevant authorities or stakeholders • All employees are aware of their ongoing security obligations	• In addition to the criteria of 'managed' • Security incidents are routinely reviewed and assessed to improve processes and reduce any likelihood of insider threat • The agency has effective methods to communicate security concerns with relevant authorities or stakeholders, including lessons learned • The agency has mechanisms in place to be able to monitor former employees to ensure they are maintaining any security obligations

Physical security maturity indicators

SAPSF Policy	Informal - 1	Basic - 2	Managed - 3	Enhanced - 4
PHYSEC1: Physical security **Core Requirement 13:** *Implement physical security measures that minimise the risk of harm or compromise to people, information and assets*	• The agency does not proactively assess its physical security risks and does not know what assets require the most protection • Staff awareness of physical security risks is poor and behavioural expectations are unknown or inconsistent • Unauthorised access to agency facilities would likely go undetected • It is unlikely theft, or attempted theft, of agency assets or information would be detected • There is limited confidence the agency's physical security measures would reduce the risk of harm to people, information or assets • Physical security is only considered late, if at all, in the planning, selection, construction or modification of agency facilities • Existing physical security measures are simple and inconsistent across facilities and business areas. Suspicious activity or threats would likely go unnoticed.	• Employees with responsibility for physical security understand the security lifecycle • The agency's physical security forms a part of the workplace health and safety requirements, • There are pockets of good security awareness and practice across the agency, but it is generally inconsistent and difficult to assess • Some physical security measures reduce the risk of information or resources being compromise, or made inaccessible or inoperable, or being accessed or removed without proper authorisation • Physical security is generally integrated into planning, selection, construction and modification of agency facilities	• The agency has effective mechanisms in place for protecting people (including customers, visitors and members of the public), information and assets. Agency employees know and understand these mechanisms and they are updated regularly • Physical security needs are actively considered in the planning, selection, construction and modification of agency facilities and resources. • The agency is compliant with all zoning requirements for agency facilities and work areas, including design, certification and accreditation • There are proportionate measures in place to deter, detect, delay, respond and recover any attempts to attack or remove physical assets or information • The agency has robust disposal and destruction procedures in place for information and assets, including ICT equipment • Physical security measures extend to people, information and assets when they are not located within facilities or on agency premises • The agency has effective ICT and cyber security measures in place to detect and deter	• In addition to the criteria or 'managed' • The agency actively seeks to and contributes to continuous improvement of physical security internally and across government • The agency has mechanisms in place to routinely detect and monitor irregular access and controls • The agency's physical security measures are constantly monitored and audited • The agency's employees understand and respect the importance of physical security measures, and accept the consequences of repeat incidents

unauthorised or inappropriate access to its information assets

- Physical security incidents, issues or concerns are routinely identified and reported by agency employees, who actively contribute to making improvements
- Changes to physical security arrangements, including to the risk environment, are actioned promptly and communicated effectively to agency employees
- Physical security measures extend to managing the security of special events, such as conferences, including those held outside agency facilities
- Physical security measures of contractors and service providers, (including sub-contractors) are reviewed regularly to ensure compliance with the requirements of the agency
- Physical security in the agency is adaptable and agency employees understand their changing responsibilities in such circumstances