Appendix two – The maturity model for the mandatory requirements

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
1	**Planning and governance**					
1.1	Allocate roles and responsibilities as detailed in this policy.	The Agency Head, CIO, CISO and Audit and Risk are not aware of their cyber security responsibilities as outlined in the policy or are not performing these responsibilities.	The Agency Head, CIO, CISO and Audit and Risk are aware of their cyber security responsibilities as outlined in this policy but are not yet performing all of them.	The CISO or equivalent is appointed responsibilities in this policy and these are assigned and undertaken. The CISO is supported by internal audit, risk and compliance teams. The Agency Head, CIO and CISO (or equivalent) are aware of their responsibilities as outlined in the policy and are performing them. The CISO (or equivalent executive) is a member or advisor of the agency's risk committee.	Maturity level 3 requirements, and in addition: • The CIO (or equivalent) is aware of who is responsible for cyber security for all information and systems including building management systems, IoT and IACS. • The agency's internal audit, risk and compliance teams are actively involved in addressing cyber risks.	Maturity level 4 requirements, and in addition: • The role of the CISO is highly visible and central to delivering on strategic business priorities and objectives. • The CISO is empowered to make security decisions for the agency/cluster.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
1.2	Ensure there is a governance committee at the executive level (dedicated or shared) to be accountable for cyber security including risks, plans and meeting the requirements of this policy. Agencies need to consider governance of ICT systems and OT (Operational Technology) to ensure no gaps in cyber security related to items such as video surveillance, alarms, life safety and building management systems that use automated or remotely controlled or monitored assets including industrial Internet of Things (IoT) devices.	There is no governance committee with a charter to cover cyber security risks, plans and policy requirements.	A governance committee is being established at the executive level but does not meet regularly, or a governance committee exists but with no executive representation or a governance committee exists but does not cover IACS/OT and IoT (if applicable).	There is a governance committee with executive level representation and agreed terms of reference that covers cyber security risks, plans, initiatives and policy requirements. The committee has governance over (or has delegated to another committee) information security as well as cyber security of OT. The governance committee meets at least quarterly to discuss cyber security.	Maturity level 3 requirements, and in addition: • Cyber security is a regular item on the agenda at the agency or cluster Risk and Audit Committees.	Maturity level 4 requirements, and in addition: • Cyber security is fully integrated into entity operations, actively managed, monitored and drives improvements. • The Agency Head understands cyber security risks to their agency.
1.3	Have an approved cyber security plan to manage the agency's cyber security risks, integrated with business continuity arrangements. This must include consideration of threats, risks and vulnerabilities that impact the protection of the agency's information and ICT assets and services.	There is no approved cyber security plan in place for the agency/cluster.	The security plan has been developed and is partially implemented but may not be current or comprehensive. The cyber security plan has been approved by the Agency Head.	A security plan is endorsed by the appropriate governance committee, captures key threats, risks, vulnerabilities and actions/initiatives to make improvements and address any gaps. The plan is linked to the agency's risk management framework and cyber security is considered in business continuity arrangements.	Maturity level 3 requirements, and in addition: • The progress of initiatives and new requirements are reviewed at least quarterly.	Maturity level 4 requirements, and in addition: • The security plan is reviewed by the governance committee at least quarterly and kept current.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
1.4	Consider cyber security threats when performing risk assessments and include high and critical risks in the agency's overall risk management framework.	Risk assessments do not consider cyber security risks.	Cyber security risk assessments are conducted on an ad-hoc basis and risks identified and managed across the IT department but are not identified across the agency.	Cyber security is included in the agency's risk management framework and cyber security risk is considered in all areas across the agency/cluster, including cyber security risks to OT. Actions are identified to mitigate cyber security risks.	Maturity level 3 requirements, and in addition: • Unmitigated cyber risks are escalated from across the agency and are visible to the Risk Committee through the agency's enterprise risk register.	Maturity level 4 requirements, and in addition: • Security risk management is a significant priority for the agency and is identified and aligned to business objectives. • Formal risk management processes to connect security risk management and operations are in place.
1.5	Be accountable for the cyber risks of their ICT service providers and ensure the providers comply with the applicable parts of this policy and any other relevant agency security policies. This must include providers notifying the agency quickly of any suspected or actual security incidents and following reasonable direction from the agency arising from incident investigations.	No consideration for cyber security in procurement processes and contracted arrangements in the agency.	Consideration for cyber security is given in all new contractual arrangements. The agency partially monitors service provider's adherence to contract provisions.	All new third party technology contracts clearly define the cyber security requirements and the responsibilities of the provider. The agency monitors compliance to security requirements in technology contracts with a security provider. There is a process for service providers to notify the agency of suspected or actual security incidents.	Maturity level 3 requirements, and in addition: • All current third party technology contracts define the cyber security requirements and responsibilities of the provider. • Service provider service delivery agreements are periodically reviewed and updated at allowable contract review/ extension periods to ensure they address any changes in business or security requirements. Standard templates for service provider agreements in contracts include clauses dealing with cyber	Maturity level 4 requirements, and in addition: • The agency actively monitors and audits technology service provider capability to fully comply with contractual arrangements.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
					security requirements.	
2	**Cyber security culture**					
2.1	Implement regular cyber security education for all employees, contractors and outsourced ICT service providers.	Cyber security education is not available to employees, contractors and outsourced ICT service providers.	Cyber security education is available for all employees but not for contractors and/or outsourced ICT service providers.	Cyber security education is available for employees, contractors and ICT service providers and completion is encouraged in all areas of the agency.	Maturity level 3 requirements, and in addition: • Cyber security education is available for employees, contractors and ICT service providers and completion is mandatory but not enforced. • Induction programs include ensuring that employees are aware of and acknowledge their security responsibilities and the agency's cyber security policies or guidelines.	Maturity level 4 requirements, and in addition: • Cyber security education is available for employees, contractors and ICT service providers and completion is mandatory and is enforced. • Completion rates are monitored to ensure they are above a defined threshold (minimum 90 per cent).
2.2	Increase awareness of cyber security risk across all staff including the need to report security risks.	Only staff within the cyber security-related teams have awareness of cyber security issues in the workplace. Responsibilities regarding cyber security are not being communicated to all staff.	All staff have been provided information regarding their responsibilities in ensuring the confidentiality, integrity and availability of data e.g. a link to the agencies Information Security Policy prior to logging in or a copy of the policy as part of onboarding. Regular communications relating to cyber security have not been sent to all staff.	Regular cyber security communications are sent to all staff including covering awareness items such as how to identify and report phishing attacks or malicious links. Phishing simulation exercises and incident response exercises (functional or discussion) have been run during the reporting period.	Maturity level 3 requirements, and in addition: • Staff in high risk roles have been identified and are appropriately trained in cyber security.	Maturity level 4 requirements, and in addition: • All staff have been made aware of cyber security threats and what they can do to detect them. • There is evidence that reports of potential malicious emails are increasing and/or improvements in results of simulations.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
2.3	Foster a culture where cyber security risk management is an important and valued aspect of decision-making and where security risk management processes are understood and applied.	Only the IT department play an active role in managing cyber security risks.	Non-IT department employees have been made aware of cyber security. Cyber security risk management is still seen as the responsibility of the IT department.	The importance of cyber security and developing a strong cyber security culture is recognised by agency executives. Cyber security risk management processes are documented, understood and followed by the relevant people across the agency.	Cyber security risk management processes are actively applied and followed by the relevant people across the agency. Leadership is aware of good cyber security practices and factor these into relevant decision-making. Residual cyber security risks are periodically reviewed and reassessed.	Maturity level 4 requirements, and in addition: • Cyber security is integral to the agency's business and clearly informs decision-making. • Secretary is briefed on cyber security risk management as part of cluster risk management reporting.
2.4	Ensure that people who have access to sensitive or classified information or systems and those with privileged system access have appropriate security screening, and that access is removed when they no longer need to have access, or their employment is terminated.	The agency has not classified their information or systems to enable suitable personnel to access the information.	Access controls are in place but removal and auditing of privileges does not occur or takes place on an ad hoc basis.	The agency has classified information or systems and has access controls and security procedures in place to enable sharing with relevant stakeholders who have a need-to-know and are appropriately security cleared. Access controls are implemented and documented to prevent unauthorised access. Access is removed within a defined period of an employee's termination or the employee no longer needing access to the information or system.	Maturity level 3 requirements, and in addition: • Routine auditing takes place to ensure that access is being removed for staff on employment termination / staff that have moved roles have not retained higher privileges (privilege creep). • A documented process is in place to ensure efficient and consistent implementation of access controls in managing all user access, which includes: – Clear identification of privileged users, which means users with access to sensitive or classified information	Maturity level 4 requirements, and in addition: • The agency has automated processes to remove access on role changes and termination of employment.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
					and users with privileged system access. – Clear identification of steps to be taken when 'Privileged Users' leave employment. In some cases, some system password needs to be reset as on any shared accounts.	
2.5	Share information and intelligence on security threats and vulnerabilities with Cyber Security NSW, as well as cooperate across NSW Government to enable management of government-wide cyber risk.	Agency does not provide any information or intelligence on security threats or vulnerabilities outside the Agency.	Agency shares information and intelligence on security threats and vulnerabilities on an ad hoc basis or only shares within its own cluster.	Agency routinely works with Cyber Security NSW to receive and/or provide information and intelligence on security threats and vulnerabilities across NSW Government. In the agency's incident management procedures, there is a defined workflow that indicates when and where information and intelligence should be shared. There is a process for receiving and acting on information and intelligence received from Cyber Security NSW.	Maturity level 3 requirements and in addition: • Agency routinely receives and/or provides information and intelligence on security threats and vulnerabilities across their cluster and with other agencies/ clusters.	Maturity level 4 requirements and in addition: • Agency receives a feed of verified Indicators of Compromise (IoCs) that can be ingested by a Security Information and Event Management (SIEM) system and actions against these IoCs are automated.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
3	**Safeguarding information and systems**					
3.1	Implement an Information Security Management System (ISMS) or Cyber Security Framework (CSF), with scope at least covering systems identified as an agency's 'crown jewels'. The ISMS or CSF should be compliant with, or modelled on, one or more recognised ICT/OT standard (see guideline for more information).	An ISMS or CSF is not in place or scope does not cover all 'crown jewels' as a minimum.	An ISMS or CSF is in place with scope covering only the 'crown jewels'. Controls are implemented to address some agency requirements.	Maturity level 3 requirements, and in addition: • The scope of the ISMS or CSF covers more than just the 'crown jewels'. • Controls are implemented based on agency requirements and current risk appetite. Control effectiveness is assessed and documented.	Maturity level 3 requirements, and in addition: • Agency risk appetite is well defined, gaps have been documented and controls have been implemented. All outstanding risks are within the current risk appetite and reviewed at least every six months. • Control effectiveness is reviewed at least every six months.	Maturity level 4 requirements, and in addition: • An ISMS or CSF is in place and scope covers all ICT and/or OT systems. • Agency executives and finance personnel are engaged by complementing cyber security risk assessment with Factor analysis of information risk (FAIR) or Value at risk (VaR) calculations.
3.2	Implement the ACSC Essential 8.	Implementation of the Essential 8 has not commenced for all mitigation strategies or implementation of the Essential 8 has not been approved by the CIO.	Implementation of the Essential 8 has not commenced for all mitigation strategies but there is a plan to begin implementation with CIO approval.	Implementation of the Essential 8 has commenced for all mitigation strategies and maturity is projected to improve year-on-year.	Priority has been given to Essential 8 implementation and uplift and the CIO is actively engaged in directing other areas of IT to prioritise this work. No mitigation strategies have a maturity level below level 1 as of August 31.	The agencies target level has been achieved and there is continuous monitoring of alignment to this maturity level.
3.3	Classify information and systems according to their importance (i.e. the impact of loss of confidentiality, integrity or availability), adhere to the requirements of the NSW Government Information Classification Labelling and	Information and systems are not classified according to the agency classification guidelines. No asset register exists for identifying agency's 'crown jewels'.	Information and systems are documented and dedicated owners with responsibilities are assigned to them. No asset register exists for identifying agency's 'crown jewels'.	Information and systems are documented and dedicated owners with responsibilities are assigned to them. 'Crown jewels' have been identified.	Information and systems are classified according to agency classification guidelines and systems are assigned business and/or IT owners. Agency has identified their 'crown jewels' and they have been approved by the	Information and systems are classified according to agency classification guidelines and systems are assigned business and/or IT owners. Appropriate controls are in place for the

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
	Handling Guidelines and: • assign ownership • implement controls according to their classification and relevant laws and regulation • identify the agency's 'crown jewels' and report them to Cyber Security NSW as per mandatory requirement 5.4.				Governance Committee.	information and systems. Agency has identified their 'crown jewels' and they have been approved by the Governance Committee.
3.4	Ensure cyber security requirements are built into procurements and early stages of projects and the system development life cycle (SDLC), including agile projects.	There are no cyber security requirements built into the agency SDLC or project assurance.	There are cyber security checks performed before a new system is implemented but not in the early stages of development. Agile projects do not have a method for verifying that cyber security requirements are being designed and built into new systems.	Security requirements are addressed in the requirements and pre-implementation procedures or checks of new projects including agile projects. The agency includes cyber security requirements in the procedures and assurance checks of the purchase/ development of new systems.	Maturity level 3 requirements, and in addition: • System acceptance includes confirmation that appropriate security controls have been applied to the system. • Internet facing applications are penetration tested before implementation. • Functional regression testing includes regression testing of security functions.	Maturity level 4 requirements, and in addition: • Access restrictions and segregation/ isolation of systems have been implemented into all infrastructure, business and user developed applications. Role based controls are implemented to ensure segregation of duties and user access privileges are revalidated at least quarterly. • Vulnerability Assessments occur on a routine basis.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
3.5	Ensure that new ICT systems or enhancements include processes for audit trails and activity logging to assess the accuracy and integrity of data including internal fraud detection.	No process exists to ensure new system or enhancements have acceptable audit and activity logging in place before implementation.	There are policies in place around auditing and logging covering log retention and alerting. Logging is enhanced for security devices such as firewalls and Intrusion Detection System (IDS) devices.	Processes (including data validity checks, audit trails and activity logging) have been established in 'crown jewels' systems to ensure development and support processes do not compromise the security of applications, systems or infrastructure. New 'crown jewel' systems or major enhancements to them have appropriate audit trails and audit logging to assess the accuracy and integrity of data. The agency has processes to confirm that these are implemented before a new system or major enhancement is implemented into production. Audit and activity logs are regularly reviewed to ensure that there are no anomalies.	Maturity level 3 requirements, and in addition: • System owners follow a process for checking logs at defined intervals to identify irregularities. A procedure is in place to act on identified anomalies. • System health checks are performed frequently to ensure that audit logs are being successfully collected as per design.	Maturity level 4 requirements, and in addition: • Logging is incorporated into a tool/system to generate automatic alerts.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
4	**Cyber incident management**					
4.1	Have a current cyber incident response plan that integrates with the agency incident management process and the NSW Cyber Incident Response Plan.	Cyber security incident management is largely manual and ad-hoc. No analysis of cyber security events or incidents.	Cyber security incident response is integrated with the agency's incident management processes but cyber security incidents cannot easily be extracted and reported.	Cyber security incident management is integrated with the agency incident management process. The agency's incident management process references the NSW Cyber Incident Response Plan. The agency's disaster recovery plan caters for cyber security incidents.	Maturity level 3 requirements, and in addition: • Analysis of cyber security events and incidents take place e.g. post incident root cause analysis, post incident review actions.	Maturity level 4 requirements, and in addition: • Cyber security incidents are reported regularly to a governance committee and are used to identify new initiatives for the agency Cyber Security Plan.
4.2	Test their cyber incident response plan at least every year, and involve their senior business and IT executives, functional area coordinators (if applicable), as well as media and communication teams.	No test of the incident response plan has ever been conducted.	No test of the incident response plan was conducted in the last reporting period, or a test was conducted involving IT only.	The agency has performed a desktop exercise in the reporting period involving the agency's senior executives and media and communications teams.	In the last reporting period, the agency tested the cyber incident response plan via a business continuity exercise (simulation) involving the senior executives, media and communications teams and any other personnel who have a role in the Business Continuity Plan (BCP). Results of the business continuity exercise have been used to update existing processes and templates including those of the media and communications teams.	Maturity level 4 requirements and in addition: • A red team assessment was held during the reporting period, covering at least the agency's 'crown jewels' and improvements have been identified from the results.

Ref	Mandatory requirement	1. Initial	2. Managed / developing	3. Defined	4. Quantitatively managed	5. Optimised
4.3	Deploy monitoring processes and tools to allow for adequate incident identification and response.	The agency does not monitor for threats.	Manual or ad hoc monitoring occurs.	Automated monitoring and alerting is in place e.g. Endpoint protection and Host or Network based Intrusion Detection Systems / Intrusion Prevention Systems (IDS/IPS). IT staff receive automated alerts from monitoring solutions. Ad hoc searching in the public domain is occurring to detect data being dumped, traded or sold.	Maturity level 3 requirements and in addition: • Events are consolidated from various sensors and correlated to actions via a SIEM. • Tools and processes exist for ongoing detection and alerting of data being dumped, traded or sold in the public domain.	Maturity level 4 requirements and in addition: • SIEM correlation events are reviewed / tuned on a regular basis to minimise false positives. • Escalation of high priority incidents is automated.
4.4	Report cyber security incidents to Cyber Security NSW according to the NSW Cyber Incident Response Plan.	The agency did not report cyber security incidents to Cyber Security NSW during the reporting period.	A percentage of cyber security incidents were reported to Cyber Security NSW during the reporting period.	All cyber security incidents and crises have been reported to Cyber Security NSW in line with the NSW Cyber Incident Response Plan during the reporting period.	Maturity level 3 requirements, and in addition: • Continual updates are provided to Cyber Security NSW on what remediation is taking place.	Automated reporting of incidents to Cyber Security NSW is in place, which includes known indicators of attack (IOAs) and/or indicators of compromise (IOCs).
4.5	Participate in whole-of-government cyber security exercises as required.	Did not send a representative to exercises held during the reporting period, or no whole-of-government cyber security exercises were held.	Representatives attended exercises but were are not part of an appropriate team.	Appropriate representatives were sent to whole-of-government cyber security exercises during the reporting period.	CIO and CISO or equivalent attended the exercises.	Maturity level 4 requirements, and in addition: • The cluster's Minister(s) and Secretary attended the exercises.

Source: Cyber Security Policy – Maturity Model Guidance (April 2020).