Appendix two – ISMS maturity model

Public sector agencies are required to rate themselves from one to five against the following 12 ‘actions’ as part of an Information Security Management System (ISMS) model. The risk matrix developed to assess this maturity is presented on the following page.

Action number	Action name
Action 1	ISMS governance is established and aligned to implementation of risk management policies.
Action 2	ISMS is reviewed in accordance to the level of risks to digital information and digital information system.
Action 3	All digital information is classified to ensure it is handled with appropriate level of protection under the NSW Government Information Classification and Labelling Guidelines.
Action 4	Access to digital information and digital information systems is monitored and controlled.
Action 5	Controls are in place and working effectively to prevent unauthorised disclosure, modification, removal or destruction of digital information.
Action 6	Security requirements are considered and implemented as part of the acquisition, development and maintenance of information systems and services.
Action 7	The security of digital information and digital information systems accessed, processed, communicated to, or managed by external parties is controlled.
Action 8	The security of digital information and software exchanged with external entities is maintained.
Action 9	Controls are in place to counteract interruptions to business activities and to ensure that IT systems support the recovery of critical business processes, and are tested at planned intervals.
Action 10	The timely resumption of business processes in the event of a major failure is ensured.
Action 11	Processes are in place for the communication of digital information security events and weaknesses associated with digital information systems within the agency and across the sector as appropriate.
Action 12	Awareness training program is implemented and maintained.

Matrix for agencies to assess their maturity scores

Key attributes

Optimised	Information owners accountable Risk-aware culture Automated controls in place and corrective action integrated within process Continuous evaluation and improvement regular reviews of risks Benchmarking in place Policies and processes are providing auditable benefits By design solution incorporated in new assets	3	4	5
Managed	Governance body established Info-centric approach Security organisation working well Effective KPIs, metrics and reporting in place Controls implemented according to risk assessment Value is promoted	3	3	4
Defined	Policies and processes defined Security organisation defined Improving user awareness Risk assessment performed	2	3	3
Developing	CISO appointed Formal program(s) initiated User awareness initiated	1	2	2
Initiated	Ad hoc activities Loosely controlled and reactive Initial Executive Awareness Policies and process not defined or only partially defined	1	1	2
		1% – 33%	34% – 66%	67% – 100%
		Only high risk assets covered	Some of the existing assets/process/ system covered	Majority of existing assets/process /system covered