The Institute of
Internal Auditors
Australia

Mapping of the Cybersecurity Topical Requirement to other Frameworks

This resource reflects the 'Global Internal Audit Standards' published in 2024.

The IIA-Australia would like to thank those who voluntarily contributed to the creation of this resource.

Version 1

Introduction

The User Guide for the Cybersecurity Topical Requirement, published by IIA Global, outlines that:

> *The organisation may have its own cybersecurity efforts, using risk management and governance frameworks such as COBIT or NIST. Internal auditors may have already developed audit programs and testing procedures based on these frameworks. Internal auditors should* ***reconcile their intended cybersecurity control testing*** *to the Topical Requirement to ensure adequate coverage.*

We recognise that Australian organisations may apply Cybersecurity Frameworks other than COBIT or NIST. We have developed further mapping to assist internal auditors in identifying the coverage of these other Frameworks with the Cybersecurity Topical Requirement. This list may be refreshed over time.

Mapping:

	FRAMEWORK	
Governance Requirements:	**ISO 27001:2022**	**NSW Cyber Security Policy 2023/24**
A. A formal cybersecurity strategy and objectives are established and periodically updated. Updates on the achievement of cybersecurity objectives are periodically communicated and reviewed by the **board,** including resources and budgetary considerations to support the cybersecurity strategy.	5.1 Leadership and Commitment 6.2 Information security objectives and planning to achieve them. 9.3.1 Management Review	1.4 Develop and maintain a cyber security strategy.
B. Policies and procedures related to cybersecurity are established, periodically updated, and strengthen the control environment.	5.2 Policy 6.3 Planning of changes 7.5 Documented information	1.5 Develop and maintain formalised plans, policies and processes for cyber security practices.
C. Roles and responsibilities that support cybersecurity objectives are established, and a process exists to periodically assess the knowledge, skills, and abilities of those filling those roles.	5.3 Organisational roles, responsibilities and authorities 7.1 Resources 7.2 Competence	1.1 Allocate and perform roles and responsibilities for cyber security. 1.2 Have an executive-level governance committee with appropriate authority to make decisions about cyber security, including OT/IoT.

	FRAMEWORK	
Governance Requirements:	**ISO 27001:2022**	**NSW Cyber Security Policy 2023/24**
D. Relevant stakeholders are engaged to discuss and act on existing vulnerabilities and emerging threats in the cybersecurity environment. Stakeholders include senior management, operations, risk management, human resources, legal, compliance, vendors, and others.	5.1 Leadership and Commitment 5.3 Organisational roles, responsibilities and authorities 7.3 Awareness	1.3 Ensure that the Audit and Risk Committee (ARC) is briefed regularly on cyber security risks, related issues and corrective actions.

	FRAMEWORK		
Risk Management Requirements	**ISO 27001:2022**	**Essential 8 Maturity Model (Level 1)**	**NSW Cyber Security Policy 2023/24**
A. The organization's risk assessment and risk management processes include the identification, analysis, mitigation, and monitoring of cybersecurity threats and their effect on achievement of strategic objectives.	6.1.1 General 6.1.2 Information security risk assessment 6.1.3 Information security risk treatment 8.2 Information security risk assessment 8.3 Information security risk treatment.	-	1.9 Define risk tolerance and risk appetite, and manage cyber security risks *(indirect / implied coverage).*
B. Cybersecurity risk management is conducted across the organization, which may include the following areas: information technology, enterprise risk management, human resources, legal, compliance, operations, supply chain, accounting, finance, and others.	4.1 Understanding the organisation and its context 4.2 Understanding the needs and expectations of interested parties 6.1.2 Information security risk assessment.	-	1.10 Identify and manage third-party service provider risks, including shared ICT services supplied by other NSW Government agencies.
C. Accountability and responsibility for cybersecurity risk management is established and an individual or team is identified to periodically monitor and report how cybersecurity risks are being managed, including the resources required to mitigate risk and identify emerging cybersecurity threats.	4.3 Determining the scope of the information security management system 5.3 Organizational roles, responsibilities and authorities 6.1.2 Information security risk assessment.	-	See Roles and Responsibilities section of Policy. 1.1 Allocate and perform roles and responsibilities for Cybersecurity.

	FRAMEWORK		
Risk Management Requirements	**ISO 27001:2022**	**Essential 8 Maturity Model (Level 1)**	**NSW Cyber Security Policy 2023/24**
D. A process is established to quickly escalate any cybersecurity risk (emerging or previously identified) that rises to an unacceptable level based on the organization's established risk management guidelines or to comply with applicable legal and regulatory requirements. Both the financial and nonfinancial impacts of cybersecurity risk should be considered.	8.1 Operational planning and control 9.1 Monitoring, measurement, analysis and evaluation 9.3.2 Management review inputs 9.3.3 Management review results.	-	1.9 Define risk tolerance, risk appetite and manage cyber security risks *(indirect / implied coverage).*
E. A process is established to communicate cybersecurity risk awareness to management and employees, and for the periodic review by management of issues, gaps, deficiencies, or control failures with reporting and remediation.	7.3 Awareness 7.4 Communication.	-	3.1 Conduct awareness activities, including mandatory awareness training.
F. The organization has implemented a cybersecurity incident response and recovery process that includes detection, containment, recovery, and post-incident analysis. The incident response and recovery process is periodically tested.	8.1 Operational planning and control	Regular backups.	2.2 Maintain a cyber incident response plan and use exercises and post incident reviews to continuously improve the plan. 2.4 Include cyber security in business continuity and disaster recovery planning. 3.10 Maintain backups of important data, software and configuration settings *(indirect / implied coverage).*

	FRAMEWORK		
Control Process Requirements	**ISO 27001:2022**	**Essential 8 Maturity Model (Level 1)**	**NSW Cyber Security Policy 2023/24**
A. A process is established that ensures both internal controls and vendor-based controls are in place to protect the confidentiality, integrity, and availability of the organization's systems and data. Controls are periodically evaluated to determine they are functioning in a manner that promotes the achievement of organizational cybersecurity objectives and timely resolution of issues.	9.1 Monitoring, measurement, analysis and evaluation 9.2 Internal audit 9.3 Management review 10.1 Continual improvement. Table A.1[1] *Org Control: Information transfer,* *Information security in supplier relationships,* *Addressing information security within supplier agreements,* *Managing information security in the information and communication technology (ICT) supply chain,* *Monitoring, review and change management of supplier services,* *Protection of records,* *Privacy and protection of personal identifiable information (PII),* *Independent review of information security,* *Confidentiality or non-disclosure agreements,* *Data masking,* *Data leakage prevention,* *Information backup,* *Redundancy of information processing facilities,* *Logging.*	-	*All of Section 3 Protect of the NSW CSP could potentially be covered by this high-level requirement. Internal auditors to apply professional judgement.*
B. A talent management process is established and periodically reviewed for cybersecurity operations that includes training opportunities to develop and maintain technical competencies.	7.2 Competence *Table A.1 Org Control: Information security awareness, education and training.* *(A6) People Controls.*	-	-

[1] The controls in Annex A (Table A.1) of ISO 27001:2022 are not mandatory under this Standard, they are suggested for an organisation. They are not an exhaustive list and judgement needs to be applied in adopting these controls. More information and guidance on these can be found in ISO 27002:2022.

	FRAMEWORK		
Control Process Requirements	**ISO 27001:2022**	**Essential 8 Maturity Model (Level 1)**	**NSW Cyber Security Policy 2023/24**
C. A process is established to continuously monitor and report emerging cybersecurity threats and vulnerabilities and to identify, prioritize, and implement opportunities to improve cybersecurity operations.	*Table A.1 Org Control: Management of technical vulnerabilities,* *Threat intelligence,* *Protecting against physical and environmental threats.*	-	1.11 Establish and maintain vulnerability management processes.
D. Cybersecurity is included in the life cycle management (selection, usage, maintenance, and decommissioning) of all IT assets, including hardware, software, and vendor services.	*Table A.1 Org Control: Secure development life cycle,* *Secure system architecture and engineering principles,* *Secure coding,* *Security testing in development and acceptance,* *Outsourced development,* *Separation of development, test and production environments,* *Change management,* *Test information.*	-	1.6 Establish and maintain processes for asset inventory management and identify asset dependencies *(indirect / implied coverage).* 1.7 Assess and identify Crown Jewels and classify systems *(indirect / implied coverage).* 1.12 Ensure cyber security requirements and impacts are assessed as part of change management processes.
E. Processes are established to promote cybersecurity including configuration, end-user device administration, encryption, patching, user-access management, and monitoring availability and performance. Cybersecurity considerations are included in software development (DevSecOps).	*Table A.1 Org Control: Access control, Identity management, access rights,* *Privileged access rights,* *Information access restriction,* *Access to source code,* *Secure authentication,* *Configuration management,* *Application security requirements,* *Secure system architecture and engineering principles.*	Patch Applications. Patch operating systems. Restrict administrative privileges.	1.11 Establish and maintain vulnerability management processes. 1.12 Ensure cyber security requirements and impacts are assessed as part of change management processes. 2.1 Implement event logging and continuous monitoring to detect anomalous activity. 3.2 Implement access controls to ensure only authorised access.

	FRAMEWORK		
Control Process Requirements	**ISO 27001:2022**	**Essential 8 Maturity Model (Level 1)**	**NSW Cyber Security Policy 2023/24**
			3.3 Patch applications (Essential Eight). 3.4 Patch operating systems (Essential Eight). 3.6 Restrict administrative privileges (Essential Eight). 3.11 Establish and maintain secure configurations.
F. Network-related controls are established, such as network access controls and segmentation; the use and placement of firewalls; limited connections from and to external networks; virtual private network (VPN)/zero trust network access (ZTNA), inclusion of Internet of Things (IoT) network controls, and intrusion detection/prevention systems (IDS and IPS).	*Table A.1 Org Control: Networks security,* *Security of network services,* *Segregation of networks,* *Management of technical vulnerabilities,* *Threat intelligence,* *Protecting against physical and environmental threats.*	-	3.15 Implement network security controls.
G. Endpoint communication security controls are established regarding services such as email, internet browsers, videoconferencing, messaging, social media, cloud, and file-sharing protocols.	*Table A.1 Org Control: Authentication information,* *Information security for use of cloud services,* *Information transfer,* *User end point devices,* *Web filtering,* *Storage media,* *Clear desk and clear screen,* *Physical security monitoring,* *Physical Security Parameters,* *Physical entry,* *Securing offices, rooms and facilities,* *Data leakage prevention, Monitoring activities.*	Implement user application hardening.	3.9 Implement user application hardening. 3.12 Define and implement data security controls. 3.13 Implement email security controls. 3.14 Implement controls for endpoint protection, including mobile devices.

Related Resources

Australian Signals Directorate, 2023. *Essential Eight Maturity Model*. [Online]
Available at: https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight/essential-eight-maturity-model

Department of Customer Service, 2024. *NSW Cyber Security Policy 2023-2024 v6.0*. [Online]
Available at: https://www.digital.nsw.gov.au/sites/default/files/2024-02/NSW-Cyber-Security-Policy-2023-2024.pdf

International Organization for Standardization, 2022. *ISO 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* Geneva: International Organization for Standardization.

The Institute of Internal Auditors, Inc., 2025. Cybersecurity Topical Requirement. [Online]
Available at: https://www.theiia.org/globalassets/site/standards/topicalrequirements/cybersecurity/cybersecurity_topical_requirement.pdf

The Institute of Internal Auditors - Australia, 2025. Factsheet: Cybersecurity Topical Requirement. [Online]
Available at: https://iia.org.au/technical-resources/fact-sheet/factsheet-cybersecurity-topical-requirement