Framework specific report

ISO/IEC 27001 v2022

MyCISO Demo Account 1

Prepared by: Jack Hedges

27 February 2024

The ISO/IEC 27001 v2022 report breaks down your maturity score into three levels. Each level measures your current maturity plus your goal maturity. Looking at the gap between these scores forms the maturity uplift required to meet your cyber security goals.

Included in this report are the control mappings back to the original framework, this helps you locate the control within the framework for compliance or further detail purposes.

Deficient controls are listed on this page under the overall control effectiveness section. The framework deficient controls are considered to be any control that sits below a maturity score of 2. Note that sometimes the framework controls can be mapped to multiple MyCISO control questions resulting in an averaged score between the mapped control questions.

Within this report you will find the framework controls broken into the following tiers:

- **Group level -** Our top level, this is the easiest way to get an overall idea of security maturity by section of the original framework.
- **Sub group 1 -** One level down this typically is a security domain, the numbering will help you identify the section within the original framework.
- **Sub group 2 -** Is typically a direct mapping between MyCISO control questions and the actual controls from the original framework.

Overall control effectiveness

When calculating your overall control effectiveness we take your current average maturity level plus your average goal maturity level. Your control effectiveness is then calculated as a percentage of your goal.

100%
80%
60%
40%
20%
0%

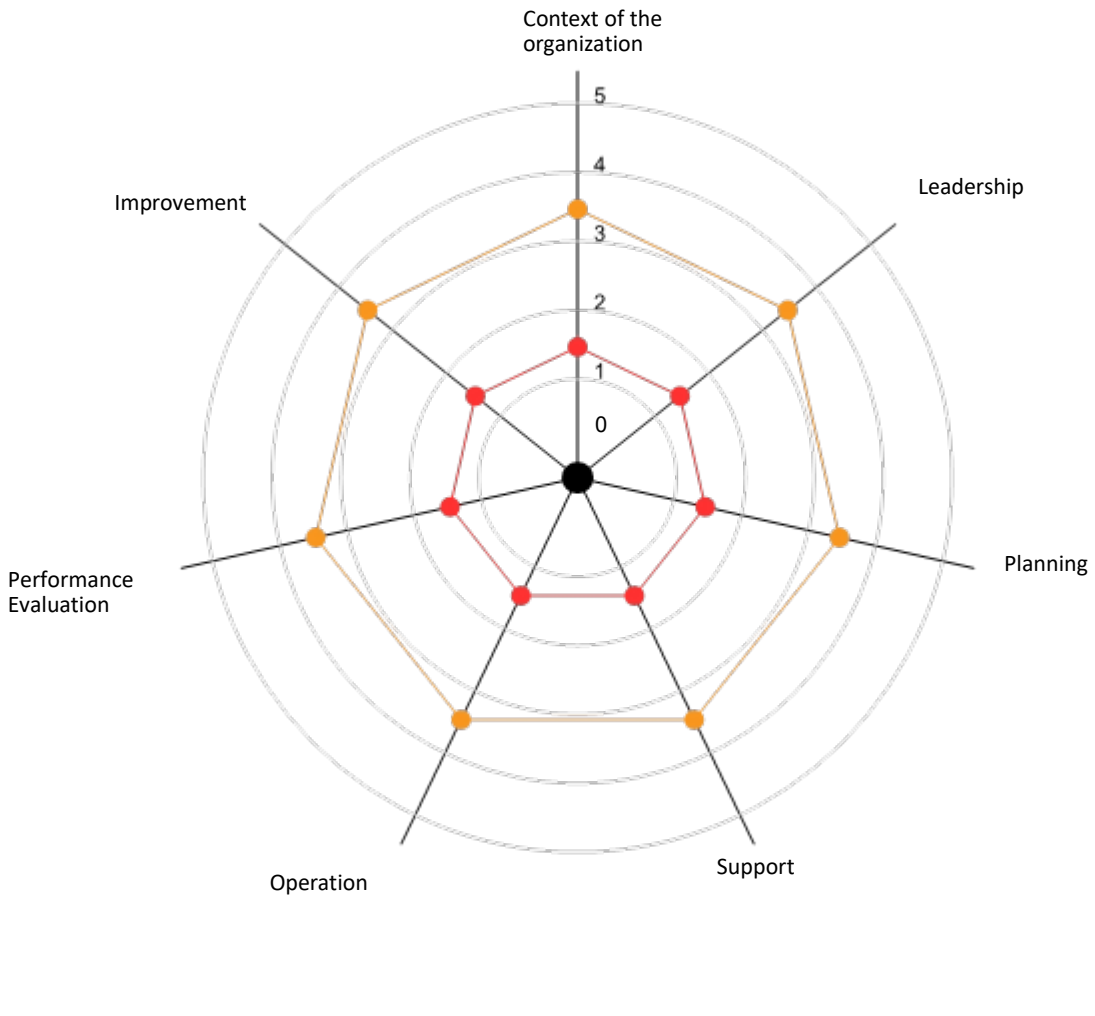
1.84 **Average maturity**

61% **Of goal maturity**

13 **Deficient controls**

The ISO/IEC 27001 v2022 spider graph below takes the top level groupings from the framework and plots them out with an average maturity of all the grouped controls underneath compared to your target maturity.

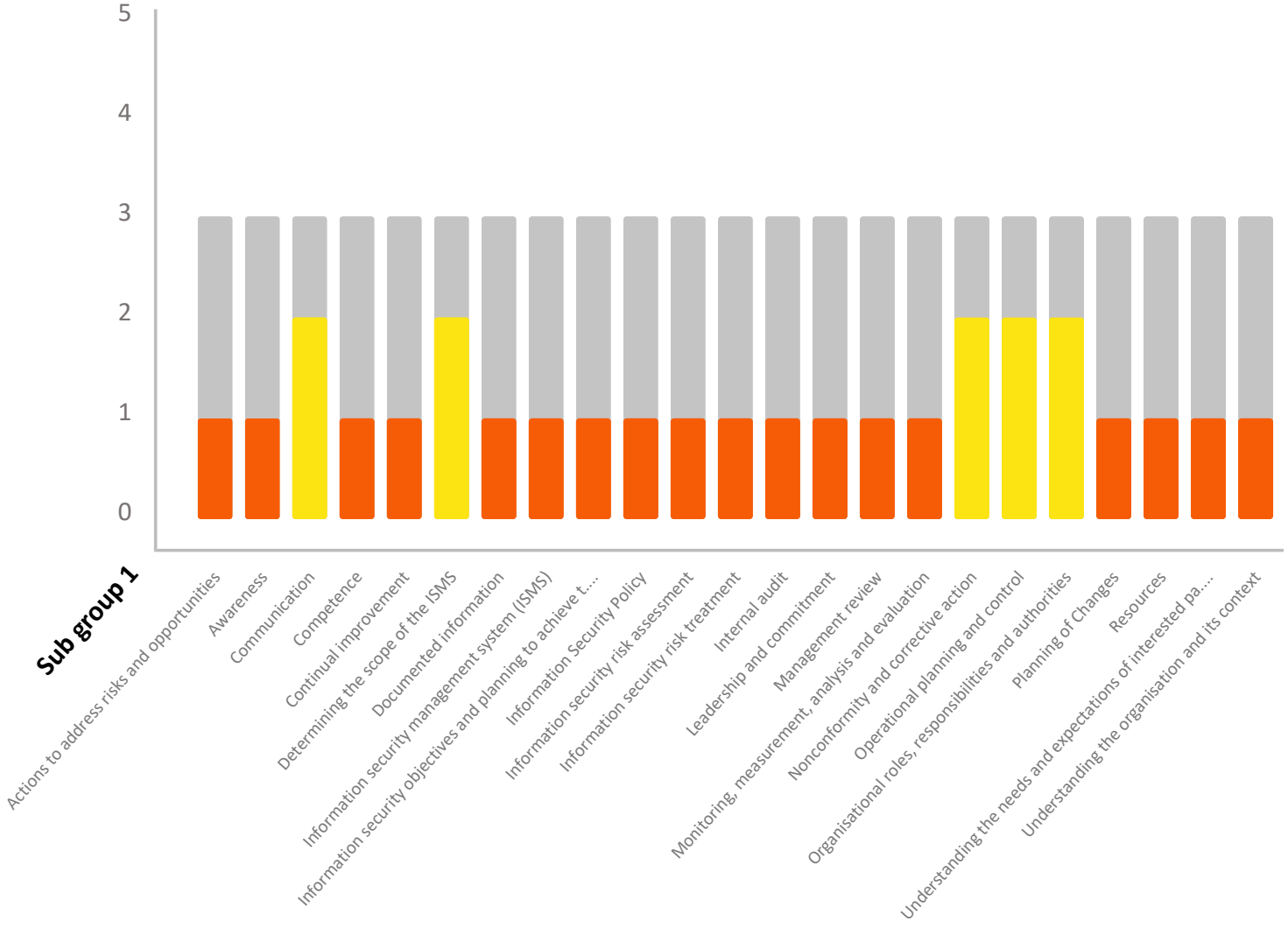
Group level current & goal maturity



This table displays your maturity per sub group 1 as it relates to the ISO/IEC 27001 v2022 framework. The grey bar behind your maturity represents your set goal maturity level.

The colours used on the graph represent whether your current maturity is: Low <33% RED, Moderate 34-66% YELLOW, High>67% GREEN.

ISO/IEC 27001 v2022 Maturity



This table displays the framework control with the mapping into MyCISO domains and control questions underneath.

ID	Group	Sub group 1	Sub group 2	Current	Goal
10.1	**Improvement**	**Continual improvement**	**Suitability, adequacy, and effectiveness of the information security management system**	**1.76**	**3**
	MyCISO Domain: Compliance	**Control:** Internal Audit Function **Recommendation to comply:** Annual audit of key governance controls and present report to senior management		2	3
	MyCISO Domain: Compliance	**Control:** Security Assessments **Recommendation to comply:** Annual review of the information security responsibility matrix		2	3
	MyCISO Domain: Compliance	**Control:** Independent Assessors **Recommendation to comply:** Annual security audit of key security control by an independent assessor		2	3
	MyCISO Domain: Compliance	**Control:** Functional Review Of Security Controls **Recommendation to comply:** Regularly review assets for compliance with cybersecurity and privacy policies and standards.		2	3
	MyCISO Domain: Compliance	**Control:** Audit Activities **Recommendation to comply:** Annual review of the information security audit program to ensure minimal interruption to business		1	3
	MyCISO Domain: Continuous Monitoring	**Control:** Continuous Monitoring **Recommendation to comply:** Implement enterprise-wide monitoring		1	3
	MyCISO Domain: Continuous Monitoring	**Control:** Monitoring Reporting **Recommendation to comply:** Generate and review periodic log report for intrusion detection		3	3
	MyCISO Domain: Incident Response	**Control:** Root Cause Analysis (RCA) & Lessons Learned **Recommendation to comply:** Annual review of the incident response process to incorporate lessons learnt		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Management Program **Recommendation to comply:** Annual review of the Risk Management Framework		1	3
	MyCISO Domain: Risk Management	**Control:** Risk Assessment **Recommendation to comply:** Perform annual risk assessment on the likelihood and magnitude of harm from cyber incidents		1	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Key Performance Indicators (KPIs) **Recommendation to comply:** Develop, report, and monitor Key Performance Indicators (KPIs) regularly, using KPI management tools, observing performance trends in cybersecurity.		2	3
	MyCISO Domain: Capacity & Performance Planning	**Control:** Performance Monitoring **Recommendation to comply:** Implement a monitoring tool to collect and analyse data from systems, applications and services to ensure continuous operation and performance.		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Monitoring **Recommendation to comply:** Incorporate risk monitoring into your daily operations with dashboarding tools, using a continuous improvement methodology. Metrics include control effectiveness and compliance levels.		2	3
10.2	**Improvement**	**Nonconformity and corrective action**	**Appropriateness and effects of nonconformities encountered and corrective actions taken**	**2**	**3**
	MyCISO Domain: Compliance	**Control:** Statutory, Regulatory & Contractual Compliance **Recommendation to comply:** Perform annual risk assessment to identify relevant legislative statutory, regulatory and contractual obligations		2	3
	MyCISO Domain: Compliance	**Control:** Non-Compliance Oversight **Recommendation to comply:** Perform annual audit to identify non-compliance with relevant legislative statutory, regulatory and contractual obligations		2	3

This table displays the framework control with the mapping into MyCISO domains and control questions underneath.

ID	Group	Sub group 1	Sub group 2	Current	Goal
	MyCISO Domain: Human Resources Security	**Control:** Personnel Sanctions **Recommendation to comply:** Security awareness training covering Appropriate Use Policy and potential disciplinary actions		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Remediation **Recommendation to comply:** Annual review of the risk register and remediation plan		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Response **Recommendation to comply:** Annual review of current audit findings and status of remediation plans		2	3
	MyCISO Domain: Third-Party Management	**Control:** Third-Party Deficiency Remediation **Recommendation to comply:** Annual compliance review of Third Party Supplier Contract		2	3
	MyCISO Domain: Vulnerability & Patch Management	**Control:** Continuous Vulnerability Remediation Activities **Recommendation to comply:** Regularly update and patch software, conduct vulnerability assessments, and implement intrusion detection systems to protect assets from known and emerging threats.		2	3
	MyCISO Domain: Vulnerability & Patch Management	**Control:** Time To Remediate / Benchmarks For Corrective Action **Recommendation to comply:** Track remediation operations effectiveness bi-monthly using reporting tools and a metric-driven approach. Success measured by the timeliness and effectiveness of corrective actions.		2	3
4.1	**Context of the organization**	**Understanding the organisation and its context**	**Issues, purpose, and achieving information security management system**	**1.5**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Security & Privacy Governance Program **Recommendation to comply:** A consistent ISMS (Information Security Management System) policy set applied across all business processes		1	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Defining Business Context & Mission **Recommendation to comply:** Organisation mission statement aligns with its business model		2	3
4.2	**Context of the organization**	**Understanding the needs and expectations of interested parties**	**Determining interested parties and their requirements**	**1.75**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Security & Privacy Governance Program **Recommendation to comply:** A consistent ISMS (Information Security Management System) policy set applied across all business processes		1	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Steering Committee **Recommendation to comply:** A security steering committee appointed by and accountable to the board		2	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Assigned Security & Privacy Responsibilities **Recommendation to comply:** The CISO manages the enterprise wide cybersecurity and privacy program		2	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Contacts With Authorities **Recommendation to comply:** A register of all applicable legal and regulatory requirement for cybersecurity and the assigned contact person		2	3
4.3	**Context of the organization**	**Determining the scope of the ISMS**	**Determining the boundaries and applicability of the information security management system**	**2**	**3**
	MyCISO Domain: Security &	**Control:** Assigned Security & Privacy Responsibilities **Recommendation to comply:** The CISO manages the enterprise wide cybersecurity		2	3

This table displays the framework control with the mapping into MyCISO domains and control questions underneath.

ID	Group	Sub group 1	Sub group 2	Current	Goal
	Privacy Governance	and privacy program			
	MyCISO Domain: Security & Privacy Governance	**Control:** Defining Business Context & Mission **Recommendation to comply:** Organisation mission statement aligns with its business model		2	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Define Control Objectives **Recommendation to comply:** Establish control objectives as a basis for the internal control system annually, using a systematic approach, measuring alignment with organisational goals.		2	3
	MyCISO Domain: Information Assurance	**Control:** Assessment Boundaries **Recommendation to comply:** Define the scope of assessments on a quarterly basis using system assessment tools, including people, processes, and technology impacting data security.		2	3
4.4	**Context of the organization**	**Information security management system (ISMS)**	**Requirements of the ISMS in acordance to the International Standard**	**1.57**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Security & Privacy Governance Program **Recommendation to comply:** A consistent ISMS (Information Security Management System) policy set applied across all business processes		1	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Steering Committee **Recommendation to comply:** A security steering committee appointed by and accountable to the board		2	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Publishing Security & Privacy Documentation **Recommendation to comply:** A comprehensive security awareness training covering the ISMS (Information Security Management System) policy set		1	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Assigned Security & Privacy Responsibilities **Recommendation to comply:** The CISO manages the enterprise wide cybersecurity and privacy program		2	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Measures of Performance **Recommendation to comply:** Key Risk Indicators (KRI) for cybersecurity and privacy management are development and tracked		1	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Contacts With Authorities **Recommendation to comply:** A register of all applicable legal and regulatory requirement for cybersecurity and the assigned contact person		2	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Defining Business Context & Mission **Recommendation to comply:** Organisation mission statement aligns with its business model		2	3
5.1	**Leadership**	**Leadership and commitment**	**Demonstration of leadership and commitment**	**1.66**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Steering Committee **Recommendation to comply:** A security steering committee appointed by and accountable to the board		2	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Measures of Performance **Recommendation to comply:** Key Risk Indicators (KRI) for cybersecurity and privacy management are development and tracked		1	3
	MyCISO Domain: Compliance	**Control:** Security Controls Oversight **Recommendation to comply:** Annual audit of key security controls		2	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Data Governance **Recommendation to comply:** Oversee data governance to ensure sensitive data management compliance, conducting regular audits, measuring compliance rates.		1	3

This table displays the framework control with the mapping into MyCISO domains and control questions underneath.

ID	Group	Sub group 1	Sub group 2	Current	Goal
	MyCISO Domain: Privacy	**Control:** Chief Privacy Officer (CPO) **Recommendation to comply:** Appoint a Chief Privacy Officer with appropriate resources, tracking successful implementation of privacy requirements and risk management.		2	3
	MyCISO Domain: Privacy	**Control:** Data Protection Officer (DPO) **Recommendation to comply:** Appoint a Data Protection Officer based on professional qualities, tracking effectiveness in protecting personal data.		2	3
5.2	**Leadership**	**Information Security Policy**	**Establishment of an Information Security Policy**	**1.4**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Security & Privacy Governance Program **Recommendation to comply:** A consistent ISMS (Information Security Management System) policy set applied across all business processes		1	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Publishing Security & Privacy Documentation **Recommendation to comply:** A comprehensive security awareness training covering the ISMS (Information Security Management System) policy set		1	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Periodic Review & Update of Security & Privacy Program **Recommendation to comply:** A consistent ISMS(Information Security Management System) policy set implemented by the CISO (Chief Information Security Officer)		1	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Defining Business Context & Mission **Recommendation to comply:** Organisation mission statement aligns with its business model		2	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Define Control Objectives **Recommendation to comply:** Establish control objectives as a basis for the internal control system annually, using a systematic approach, measuring alignment with organisational goals.		2	3
5.3	**Leadership**	**Organisational roles, responsibilities and authorities**	**Assignment and communication of responsibilities and role authorities**	**2**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Steering Committee **Recommendation to comply:** A security steering committee appointed by and accountable to the board		2	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Assigned Security & Privacy Responsibilities **Recommendation to comply:** The CISO manages the enterprise wide cybersecurity and privacy program		2	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Contacts With Authorities **Recommendation to comply:** A register of all applicable legal and regulatory requirement for cybersecurity and the assigned contact person		2	3
	MyCISO Domain: Privacy	**Control:** Chief Privacy Officer (CPO) **Recommendation to comply:** Appoint a Chief Privacy Officer with appropriate resources, tracking successful implementation of privacy requirements and risk management.		2	3
6.1	**Planning**	**Actions to address risks and opportunities**	**Determining issues and actions to address risks and opportunities**	**1.5**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Measures of Performance **Recommendation to comply:** Key Risk Indicators (KRI) for cybersecurity and privacy management are development and tracked		1	3
	MyCISO Domain: Risk Management	**Control:** Risk Management Program **Recommendation to comply:** Annual review of the Risk Management Framework		1	3
	MyCISO Domain: Security &	**Control:** Key Risk Indicators (KRIs) **Recommendation to comply:** Regularly develop, report, and monitor Key Risk Indicators (KRIs),		2	3

This table displays the framework control with the mapping into MyCISO domains and control questions underneath.

ID	Group	Sub group 1	Sub group 2	Current	Goal
	Privacy Governance	employing risk management tools, and observing risk trends in cybersecurity.			
	MyCISO Domain: Risk Management	**Control:** Compensating Countermeasures **Recommendation to comply:** Implement biannual compensating countermeasures for threat reduction using risk assessment tools and a risk-based approach. Success evaluated by reduction in risk and threat exposure.		2	3
6.1.1	**Planning**	**Actions to address risks and opportunities**	**General planning to address risks and opportunities**	**1.72**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Measures of Performance **Recommendation to comply:** Key Risk Indicators (KRI) for cybersecurity and privacy management are development and tracked		1	3
	MyCISO Domain: Risk Management	**Control:** Risk Management Program **Recommendation to comply:** Annual review of the Risk Management Framework		1	3
	MyCISO Domain: Risk Management	**Control:** Risk Framing **Recommendation to comply:** Implement a risk management framework to identify assumptions, constraints, risk tolerance, and priorities for managing risk.		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Identification **Recommendation to comply:** Perform annual risk assessment		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Assessment **Recommendation to comply:** Perform annual risk assessment on the likelihood and magnitude of harm from cyber incidents		1	3
	MyCISO Domain: Risk Management	**Control:** Risk Register **Recommendation to comply:** Annual review of the risk register		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Ranking **Recommendation to comply:** Develop a process to assess and classify newly found security vulnerabilities using industry-recognised practices.		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Remediation **Recommendation to comply:** Annual review of the risk register and remediation plan		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Response **Recommendation to comply:** Annual review of current audit findings and status of remediation plans		2	3
	MyCISO Domain: Risk Management	**Control:** Business Impact Analysis (BIA) **Recommendation to comply:** Develop a BIA process to assess potential impacts of cyber incidents on business operations. Document findings and update regularly.		2	3
	MyCISO Domain: Risk Management	**Control:** Supply Chain Risk Assessment **Recommendation to comply:** Annual review of the Supply Chain Risk Management (SCRM) Policy and update of supplier risk assessment		2	3
6.1.2	**Planning**	**Actions to address risks and opportunities**	**Planning information security risk assessment**	**1.8**	**3**
	MyCISO Domain: Risk Management	**Control:** Risk Management Program **Recommendation to comply:** Annual review of the Risk Management Framework		1	3
	MyCISO Domain: Risk Management	**Control:** Risk Framing **Recommendation to comply:** Implement a risk management framework to identify assumptions, constraints, risk tolerance, and priorities for managing risk.		2	3

This table displays the framework control with the mapping into MyCISO domains and control questions underneath.

ID	Group	Sub group 1	Sub group 2	Current	Goal
	MyCISO Domain: Risk Management	**Control:** Risk Identification **Recommendation to comply:** Perform annual risk assessment		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Assessment **Recommendation to comply:** Perform annual risk assessment on the likelihood and magnitude of harm from cyber incidents		1	3
	MyCISO Domain: Risk Management	**Control:** Risk Register **Recommendation to comply:** Annual review of the risk register		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Ranking **Recommendation to comply:** Develop a process to assess and classify newly found security vulnerabilities using industry-recognised practices.		2	3
	MyCISO Domain: Risk Management	**Control:** Business Impact Analysis (BIA) **Recommendation to comply:** Develop a BIA process to assess potential impacts of cyber incidents on business operations. Document findings and update regularly.		2	3
	MyCISO Domain: Risk Management	**Control:** Supply Chain Risk Assessment **Recommendation to comply:** Annual review of the Supply Chain Risk Management (SCRM) Policy and update of supplier risk assessment		2	3
	MyCISO Domain: Risk Management	**Control:** Risk-Based Security Categorisation **Recommendation to comply:** Establish a biannual review, employ documentation and approval tools, and apply risk analysis approach. Evaluate based on categorisation accuracy and approval.		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Monitoring **Recommendation to comply:** Incorporate risk monitoring into your daily operations with dashboarding tools, using a continuous improvement methodology. Metrics include control effectiveness and compliance levels.		2	3
6.1.3	**Planning**	**Actions to address risks and opportunities**	**Planning information security risk treatment**	**1.66**	**3**
	MyCISO Domain: Risk Management	**Control:** Risk Management Program **Recommendation to comply:** Annual review of the Risk Management Framework		1	3
	MyCISO Domain: Risk Management	**Control:** Risk Remediation **Recommendation to comply:** Annual review of the risk register and remediation plan		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Response **Recommendation to comply:** Annual review of current audit findings and status of remediation plans		2	3
6.2	**Planning**	**Information security objectives and planning to achieve them**	**Establishment of information security objectives at relevant functions and levels**	**1.83**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Security & Privacy Governance Program **Recommendation to comply:** A consistent ISMS (Information Security Management System) policy set applied across all business processes		1	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Steering Committee **Recommendation to comply:** A security steering committee appointed by and accountable to the board		2	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Defining Business Context & Mission **Recommendation to comply:** Organisation mission statement aligns with its business model		2	3

This table displays the framework control with the mapping into MyCISO domains and control questions underneath.

ID	Group	Sub group 1	Sub group 2	Current	Goal
	MyCISO Domain: Project & Resource Management	**Control:** Strategic Plan & Objectives **Recommendation to comply:** Establish a strategic cybersecurity and privacy business plan, tracking achievement of plan objectives.		2	3
	MyCISO Domain: Security Operations	**Control:** Service Delivery (Business Process Support) **Recommendation to comply:** Define business processes and implement service management based on industry standards for technology capabilities supporting business functions, measured by business process efficiency and customer satisfaction.		2	3
	MyCISO Domain: Project & Resource Management	**Control:** Security Portfolio Management **Recommendation to comply:** Annual review of the Privacy program		2	3
6.3	**Planning**	**Planning of Changes**	**Determining the need for changes in a planned manner**	**1**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Periodic Review & Update of Security & Privacy Program **Recommendation to comply:** A consistent ISMS(Information Security Management System) policy set implemented by the CISO (Chief Information Security Officer)		1	3
7.1	**Support**	**Resources**	**Determining and providing the resources needed**	**1.88**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Assigned Security & Privacy Responsibilities **Recommendation to comply:** The CISO manages the enterprise wide cybersecurity and privacy program		2	3
	MyCISO Domain: Human Resources Security	**Control:** Human Resources Security Management **Recommendation to comply:** Publish Information Security Policy covering personnel security requirements such as Police Check		2	3
	MyCISO Domain: Human Resources Security	**Control:** Roles & Responsibilities **Recommendation to comply:** Annual review of the information security responsibilities matrix to align with business requirements		1	3
	MyCISO Domain: Project & Resource Management	**Control:** Allocation of Resources **Recommendation to comply:** Develop a resource allocation plan that includes management, operational, technical, and privacy requirements for projects/initiatives.		2	3
	MyCISO Domain: Business Continuity & Disaster Recovery	**Control:** Transfer to Alternate Processing / Storage Site **Recommendation to comply:** Implement bi-annual redeployment drills and conduct an annual review of the continuity plan for alternate processing/storage sites, leverage effective communication tools, and assess key metrics such as downtime during transfer and personnel readiness levels.		2	3
	MyCISO Domain: Human Resources Security	**Control:** Identify Vital Cybersecurity & Privacy Staff **Recommendation to comply:** Regularly identify vital cybersecurity & privacy staff, leveraging HR management tools, observing changes in key staff.		2	3
	MyCISO Domain: Human Resources Security	**Control:** Establish Redundancy for Vital Cybersecurity & Privacy Staff **Recommendation to comply:** Establish redundancy for vital cybersecurity & privacy staff periodically, using workforce planning tools, measuring redundancy ratios.		2	3
	MyCISO Domain: Human Resources Security	**Control:** Perform Succession Planning **Recommendation to comply:** Implement a bi-annual review process that utilises succession planning tools to prepare for the continuity of critical cybersecurity and privacy roles, establishing metrics such as the number of successors identified, their readiness levels and gap closure plans.		2	3
	MyCISO Domain: Project & Resource Management	**Control:** Security & Privacy Resource Management **Recommendation to comply:** Develop a comprehensive capital planning and investment process that includes resources for security and privacy programs. Document any exceptions to this requirement.		2	3
7.2	**Support**	**Competence**	**Personnel competence in executing information security performance**	**1.83**	**3**

This table displays the framework control with the mapping into MyCISO domains and control questions underneath.

ID	Group	Sub group 1	Sub group 2	Current	Goal
	MyCISO Domain: Human Resources Security	**Control:** Competency Requirements for Security-Related Positions **Recommendation to comply:** Annual review of the information security responsibilities matrix with required qualification for each role		2	3
	MyCISO Domain: Human Resources Security	**Control:** Incompatible Roles **Recommendation to comply:** Enforce segregation of duties in the software development process and configuration management process		2	3
	MyCISO Domain: Human Resources Security	**Control:** Identify Critical Skills & Gaps **Recommendation to comply:** Evaluate critical cybersecurity and privacy skills needed and identify gaps, performing annual reviews, measuring skill gap reductions.		2	3
	MyCISO Domain: Human Resources Security	**Control:** Remediate Identified Skills Deficiencies **Recommendation to comply:** Remediate critical skills deficiencies regularly, using training tools, tracking improvements in skill gaps.		1	3
	MyCISO Domain: Human Resources Security	**Control:** Identify Vital Cybersecurity & Privacy Staff **Recommendation to comply:** Regularly identify vital cybersecurity & privacy staff, leveraging HR management tools, observing changes in key staff.		2	3
	MyCISO Domain: Project & Resource Management	**Control:** Manage Organisational Knowledge **Recommendation to comply:** Manage organisational knowledge of cybersecurity and privacy staff using knowledge management tools, tracking staff competency levels and knowledge gaps.		2	3
7.3	**Support**	**Awareness**	**Personnel awareness in performing organisational controls**	**1.81**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Publishing Security & Privacy Documentation **Recommendation to comply:** A comprehensive security awareness training covering the ISMS (Information Security Management System) policy set		1	3
	MyCISO Domain: Business Continuity & Disaster Recovery	**Control:** Contingency Training **Recommendation to comply:** The Business Continuity Plan (BCP) defines the role for all contingency personnels		2	3
	MyCISO Domain: Human Resources Security	**Control:** Human Resources Security Management **Recommendation to comply:** Publish Information Security Policy covering personnel security requirements such as Police Check		2	3
	MyCISO Domain: Security Awareness & Training	**Control:** Security & Privacy-Minded Workforce **Recommendation to comply:** Develop and implement training programs for security workforce to enhance awareness and skills in cyber security. Regularly assess and update training materials.		1	3
	MyCISO Domain: Security Awareness & Training	**Control:** Security & Privacy Awareness **Recommendation to comply:** Develop and implement a comprehensive training program for employees and contractors to ensure they have the necessary knowledge and skills for their roles.		2	3
	MyCISO Domain: Threat Management	**Control:** Threat Intelligence Feeds **Recommendation to comply:** Implement threat intelligence feeds and regularly update them to stay informed about evolving threats. Use this information to implement appropriate preventative and compensating controls.		2	3
	MyCISO Domain: Human Resources Security	**Control:** User Awareness **Recommendation to comply:** Continually communicate user roles and responsibilities using awareness programs, tracking user understanding and compliance.		2	3
	MyCISO Domain: Human Resources Security	**Control:** Formal Indoctrination **Recommendation to comply:** Formally indoctrinate individuals with access to sensitive information periodically, tracking the number of indoctrinated employees.		2	3
	MyCISO Domain: Human Resources Security	**Control:** Use of Critical Technologies **Recommendation to comply:** Govern usage policies for critical technologies regularly, using policy management tools, tracking policy violations.		2	3

This table displays the framework control with the mapping into MyCISO domains and control questions underneath.

ID	Group	Sub group 1	Sub group 2	Current	Goal
	MyCISO Domain: Security Awareness & Training	**Control:** Sensitive Information Storage, Handling & Processing **Recommendation to comply:** Monthly training sessions on sensitive data handling using e-learning tools and systematic educational methodology are recommended. Evaluate by tracking training completion rates and instances of mishandling.		2	3
	MyCISO Domain: Security Awareness & Training	**Control:** Cyber Threat Environment **Recommendation to comply:** Implement quarterly role-based security training with e-learning tools and scenario-based learning approach. Performance measured by training completion and reduction in threat incidents.		2	3
7.4	**Support**	**Communication**	**Determining internal and external communications relevant to information security management system**	**2**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Contacts With Authorities **Recommendation to comply:** A register of all applicable legal and regulatory requirement for cybersecurity and the assigned contact person		2	3
	MyCISO Domain: Incident Response	**Control:** Regulatory & Law Enforcement Contacts **Recommendation to comply:** Maintain incident response contacts with regulatory and law enforcement agencies, tracking the number and types of incidents reported.		2	3
7.5	**Support**	**Documented information**	**International Standard requirements in documenting information**	**1**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Publishing Security & Privacy Documentation **Recommendation to comply:** A comprehensive security awareness training covering the ISMS (Information Security Management System) policy set		1	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Periodic Review & Update of Security & Privacy Program **Recommendation to comply:** A consistent ISMS(Information Security Management System) policy set implemented by the CISO (Chief Information Security Officer)		1	3
7.5.1	**Support**	**Documented information**	**General documentation on policies and records**	**1**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Publishing Security & Privacy Documentation **Recommendation to comply:** A comprehensive security awareness training covering the ISMS (Information Security Management System) policy set		1	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Periodic Review & Update of Security & Privacy Program **Recommendation to comply:** A consistent ISMS(Information Security Management System) policy set implemented by the CISO (Chief Information Security Officer)		1	3
7.5.2	**Support**	**Documented information**	**Creating and updating documented information**	**1.66**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Periodic Review & Update of Security & Privacy Program **Recommendation to comply:** A consistent ISMS(Information Security Management System) policy set implemented by the CISO (Chief Information Security Officer)		1	3
	MyCISO Domain: Compliance	**Control:** Security Assessments **Recommendation to comply:** Annual review of the information security responsibility matrix		2	3
	MyCISO Domain: Compliance	**Control:** Functional Review Of Security Controls **Recommendation to comply:** Regularly review assets for compliance with cybersecurity and privacy policies and standards.		2	3
7.5.3	**Support**	**Documented information**	**Control of documented information**	**1**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Publishing Security & Privacy Documentation **Recommendation to comply:** A comprehensive security awareness training covering the ISMS (Information Security Management System) policy set		1	3
	MyCISO Domain: Security &	**Control:** Data Governance **Recommendation to comply:** Oversee data governance to ensure sensitive data management compliance,		1	3

This table displays the framework control with the mapping into MyCISO domains and control questions underneath.

ID	Group	Sub group 1	Sub group 2	Current	Goal
	Privacy Governance	conducting regular audits, measuring compliance rates.			
8.1	**Operation**	**Operational planning and control**	**Implementing and controlling the processes of information security requirements**	**2**	**3**
	MyCISO Domain: Compliance	**Control:** Security Assessments **Recommendation to comply:** Annual review of the information security responsibility matrix		2	3
	MyCISO Domain: Security Operations	**Control:** Operations Security **Recommendation to comply:** Security awareness training		2	3
	MyCISO Domain: Security Operations	**Control:** Standardised Operating Procedures (SOP) **Recommendation to comply:** Annual review of Standardised Operating Procedures (SOP) to align with Information Security Policy		2	3
	MyCISO Domain: Security Operations	**Control:** Security Concept Of Operations (CONOPS) **Recommendation to comply:** Annual review of the information security policy set		2	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Define Control Objectives **Recommendation to comply:** Establish control objectives as a basis for the internal control system annually, using a systematic approach, measuring alignment with organisational goals.		2	3
	MyCISO Domain: Security Operations	**Control:** Service Delivery (Business Process Support) **Recommendation to comply:** Define business processes and implement service management based on industry standards for technology capabilities supporting business functions, measured by business process efficiency and customer satisfaction.		2	3
	MyCISO Domain: Security Operations	**Control:** Secure Practices Guidelines **Recommendation to comply:** Provide secure use guidelines and recommendations for products/services, using knowledge management tools, and track adherence to these guidelines.		2	3
8.2	**Operation**	**Information security risk assessment**	**Performing information security risk assessments at planned intervals**	**1.76**	**3**
	MyCISO Domain: Risk Management	**Control:** Risk Management Program **Recommendation to comply:** Annual review of the Risk Management Framework		1	3
	MyCISO Domain: Risk Management	**Control:** Risk Framing **Recommendation to comply:** Implement a risk management framework to identify assumptions, constraints, risk tolerance, and priorities for managing risk.		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Identification **Recommendation to comply:** Perform annual risk assessment		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Assessment **Recommendation to comply:** Perform annual risk assessment on the likelihood and magnitude of harm from cyber incidents		1	3
	MyCISO Domain: Risk Management	**Control:** Risk Register **Recommendation to comply:** Annual review of the risk register		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Ranking **Recommendation to comply:** Develop a process to assess and classify newly found security vulnerabilities using industry-recognised practices.		2	3
	MyCISO Domain: Risk Management	**Control:** Business Impact Analysis (BIA) **Recommendation to comply:** Develop a BIA process to assess potential impacts of cyber incidents on business operations. Document findings and update regularly.		2	3

This table displays the framework control with the mapping into MyCISO domains and control questions underneath.

ID	Group	Sub group 1	Sub group 2	Current	Goal
	MyCISO Domain: Risk Management	**Control:** Supply Chain Risk Assessment **Recommendation to comply:** Annual review of the Supply Chain Risk Management (SCRM) Policy and update of supplier risk assessment		2	3
	MyCISO Domain: Third-Party Management	**Control:** Third-Party Deficiency Remediation **Recommendation to comply:** Annual compliance review of Third Party Supplier Contract		2	3
	MyCISO Domain: Vulnerability & Patch Management	**Control:** Vulnerability Remediation Process **Recommendation to comply:** Implement a vulnerability management system to identify, track, and fix vulnerabilities promptly. Regularly update and patch systems.		1	3
	MyCISO Domain: Risk Management	**Control:** Risk-Based Security Categorisation **Recommendation to comply:** Establish a biannual review, employ documentation and approval tools, and apply risk analysis approach. Evaluate based on categorisation accuracy and approval.		2	3
	MyCISO Domain: Risk Management	**Control:** Compensating Countermeasures **Recommendation to comply:** Implement biannual compensating countermeasures for threat reduction using risk assessment tools and a risk-based approach. Success evaluated by reduction in risk and threat exposure.		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Monitoring **Recommendation to comply:** Incorporate risk monitoring into your daily operations with dashboarding tools, using a continuous improvement methodology. Metrics include control effectiveness and compliance levels.		2	3
8.3	**Operation**	**Information security risk treatment**	**Implementing the information security risk treatment plan**	**1.66**	**3**
	MyCISO Domain: Risk Management	**Control:** Risk Management Program **Recommendation to comply:** Annual review of the Risk Management Framework		1	3
	MyCISO Domain: Risk Management	**Control:** Risk Remediation **Recommendation to comply:** Annual review of the risk register and remediation plan		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Response **Recommendation to comply:** Annual review of current audit findings and status of remediation plans		2	3
	MyCISO Domain: Third-Party Management	**Control:** Third-Party Deficiency Remediation **Recommendation to comply:** Annual compliance review of Third Party Supplier Contract		2	3
	MyCISO Domain: Vulnerability & Patch Management	**Control:** Vulnerability Remediation Process **Recommendation to comply:** Implement a vulnerability management system to identify, track, and fix vulnerabilities promptly. Regularly update and patch systems.		1	3
	MyCISO Domain: Vulnerability & Patch Management	**Control:** Continuous Vulnerability Remediation Activities **Recommendation to comply:** Regularly update and patch software, conduct vulnerability assessments, and implement intrusion detection systems to protect assets from known and emerging threats.		2	3
9.1	**Performance Evaluation**	**Monitoring, measurement, analysis and evaluation**	**Evaluation and effectiveness of information security performance and management system**	**1.88**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Measures of Performance **Recommendation to comply:** Key Risk Indicators (KRI) for cybersecurity and privacy management are development and tracked		1	3
	MyCISO Domain: Compliance	**Control:** Internal Audit Function **Recommendation to comply:** Annual audit of key governance controls and present report to senior management		2	3

This table displays the framework control with the mapping into MyCISO domains and control questions underneath.

ID	Group	Sub group 1	Sub group 2	Current	Goal
	MyCISO Domain: Compliance	**Control:** Security Assessments **Recommendation to comply:** Annual review of the information security responsibility matrix		2	3
	MyCISO Domain: Compliance	**Control:** Independent Assessors **Recommendation to comply:** Annual security audit of key security control by an independent assessor		2	3
	MyCISO Domain: Compliance	**Control:** Functional Review Of Security Controls **Recommendation to comply:** Regularly review assets for compliance with cybersecurity and privacy policies and standards.		2	3
	MyCISO Domain: Continuous Monitoring	**Control:** Continuous Monitoring **Recommendation to comply:** Implement enterprise-wide monitoring		1	3
	MyCISO Domain: Continuous Monitoring	**Control:** Log Reviews & Updates **Recommendation to comply:** Real time log review to detect intrusion		2	3
	MyCISO Domain: Continuous Monitoring	**Control:** Monitoring Reporting **Recommendation to comply:** Generate and review periodic log report for intrusion detection		3	3
	MyCISO Domain: Risk Management	**Control:** Risk Framing **Recommendation to comply:** Implement a risk management framework to identify assumptions, constraints, risk tolerance, and priorities for managing risk.		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Assessment **Recommendation to comply:** Perform annual risk assessment on the likelihood and magnitude of harm from cyber incidents		1	3
	MyCISO Domain: Risk Management	**Control:** Risk Response **Recommendation to comply:** Annual review of current audit findings and status of remediation plans		2	3
	MyCISO Domain: Risk Management	**Control:** Supply Chain Risk Assessment **Recommendation to comply:** Annual review of the Supply Chain Risk Management (SCRM) Policy and update of supplier risk assessment		2	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Key Performance Indicators (KPIs) **Recommendation to comply:** Develop, report, and monitor Key Performance Indicators (KPIs) regularly, using KPI management tools, observing performance trends in cybersecurity.		2	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Key Risk Indicators (KRIs) **Recommendation to comply:** Regularly develop, report, and monitor Key Risk Indicators (KRIs), employing risk management tools, and observing risk trends in cybersecurity.		2	3
	MyCISO Domain: Capacity & Performance Planning	**Control:** Performance Monitoring **Recommendation to comply:** Implement a monitoring tool to collect and analyse data from systems, applications and services to ensure continuous operation and performance.		2	3
	MyCISO Domain: Risk Management	**Control:** Risk Monitoring **Recommendation to comply:** Incorporate risk monitoring into your daily operations with dashboarding tools, using a continuous improvement methodology. Metrics include control effectiveness and compliance levels.		2	3
	MyCISO Domain: Vulnerability & Patch Management	**Control:** Time To Remediate / Benchmarks For Corrective Action **Recommendation to comply:** Track remediation operations effectiveness bi-monthly using reporting tools and a metric-driven approach. Success measured by the timeliness and effectiveness of corrective actions.		2	3
9.2	**Performance Evaluation**	**Internal audit**	**Conducting internal audits at planned intervals**	**1.5**	**3**

This table displays the framework control with the mapping into MyCISO domains and control questions underneath.

ID	Group	Sub group 1	Sub group 2	Current	Goal
	MyCISO Domain: Compliance	**Control:** Internal Audit Function **Recommendation to comply:** Annual audit of key governance controls and present report to senior management		2	3
	MyCISO Domain: Compliance	**Control:** Audit Activities **Recommendation to comply:** Annual review of the information security audit program to ensure minimal interruption to business		1	3
9.2.1	**Performance Evaluation**	**Internal audit**	**General internal audit**	**1.5**	**3**
	MyCISO Domain: Compliance	**Control:** Internal Audit Function **Recommendation to comply:** Annual audit of key governance controls and present report to senior management		2	3
	MyCISO Domain: Compliance	**Control:** Audit Activities **Recommendation to comply:** Annual review of the information security audit program to ensure minimal interruption to business		1	3
9.2.2	**Performance Evaluation**	**Internal audit**	**Internal audit program**	**1.5**	**3**
	MyCISO Domain: Compliance	**Control:** Internal Audit Function **Recommendation to comply:** Annual audit of key governance controls and present report to senior management		2	3
	MyCISO Domain: Compliance	**Control:** Audit Activities **Recommendation to comply:** Annual review of the information security audit program to ensure minimal interruption to business		1	3
9.3	**Performance Evaluation**	**Management review**	**Top management review of the information security management system at planned intervals**	**1.8**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Steering Committee **Recommendation to comply:** A security steering committee appointed by and accountable to the board		2	3
	MyCISO Domain: Security & Privacy Governance	**Control:** Periodic Review & Update of Security & Privacy Program **Recommendation to comply:** A consistent ISMS(Information Security Management System) policy set implemented by the CISO (Chief Information Security Officer)		1	3
	MyCISO Domain: Compliance	**Control:** Non-Compliance Oversight **Recommendation to comply:** Perform annual audit to identify non-compliance with relevant legislative statutory, regulatory and contractual obligations		2	3
	MyCISO Domain: Compliance	**Control:** Security Controls Oversight **Recommendation to comply:** Annual audit of key security controls		2	3
	MyCISO Domain: Compliance	**Control:** Functional Review Of Security Controls **Recommendation to comply:** Regularly review assets for compliance with cybersecurity and privacy policies and standards.		2	3
9.3.1	**Performance Evaluation**	**Management review**	**General management review**	**1.75**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Periodic Review & Update of Security & Privacy Program **Recommendation to comply:** A consistent ISMS(Information Security Management System) policy set implemented by the CISO (Chief Information Security Officer)		1	3
	MyCISO Domain: Compliance	**Control:** Non-Compliance Oversight **Recommendation to comply:** Perform annual audit to identify non-compliance with relevant legislative statutory, regulatory and contractual obligations		2	3
	MyCISO Domain: Compliance	**Control:** Security Controls Oversight **Recommendation to comply:** Annual audit of key security controls		2	3

This table displays the framework control with the mapping into MyCISO domains and control questions underneath.

ID	Group	Sub group 1	Sub group 2	Current	Goal
	MyCISO Domain: Compliance	**Control:** Functional Review Of Security Controls **Recommendation to comply:** Regularly review assets for compliance with cybersecurity and privacy policies and standards.		2	3
9.3.2	**Performance Evaluation**	**Management review**	**Management review inputs**	**1.6**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Periodic Review & Update of Security & Privacy Program **Recommendation to comply:** A consistent ISMS(Information Security Management System) policy set implemented by the CISO (Chief Information Security Officer)		1	3
	MyCISO Domain: Compliance	**Control:** Non-Compliance Oversight **Recommendation to comply:** Perform annual audit to identify non-compliance with relevant legislative statutory, regulatory and contractual obligations		2	3
	MyCISO Domain: Compliance	**Control:** Security Controls Oversight **Recommendation to comply:** Annual audit of key security controls		2	3
	MyCISO Domain: Compliance	**Control:** Functional Review Of Security Controls **Recommendation to comply:** Regularly review assets for compliance with cybersecurity and privacy policies and standards.		2	3
	MyCISO Domain: Compliance	**Control:** Audit Activities **Recommendation to comply:** Annual review of the information security audit program to ensure minimal interruption to business		1	3
9.3.3	**Performance Evaluation**	**Management review**	**Management review results**	**1.66**	**3**
	MyCISO Domain: Security & Privacy Governance	**Control:** Measures of Performance **Recommendation to comply:** Key Risk Indicators (KRI) for cybersecurity and privacy management are development and tracked		1	3
	MyCISO Domain: Compliance	**Control:** Security Controls Oversight **Recommendation to comply:** Annual audit of key security controls		2	3
	MyCISO Domain: Compliance	**Control:** Internal Audit Function **Recommendation to comply:** Annual audit of key governance controls and present report to senior management		2	3