| ISO27001 - Annex A | Description | Control | NIST Cybersecurity Framework | HECVAT | QLD Health Third Party Security Questionnaire |
|---|---|---|---|---|---|
| **A.5** | **Information security policies** | | | | |
| A.5.1 | Management direction for information security | | | | |
| A.5.1.1 | Policies for information security | A set of policies for information security must be defined, approved by management, published and communicated to employees and relevant external parties. | ID.GV-1: Organizational cybersecurity policy is established and communicated | QUAL-03, QUAL-04, COMP-03, DOCU-07, APPL-10, BCPL-01-10, PPPR-01, PPPR-12, PPPR-16 | Q5 |
| A.5.1.2 | Review of the policies for information security | The policies for information security need to be reviewed at planned intervals, or if significant changes occur, to ensure their continuing suitability, adequacy and effectiveness. | | | Q5 |
| **A.6** | **Organization of information security** | | | | |
| A.6.1 | Internal organization | | | | |
| A.6.1.1 | Information security roles and responsibilities | All information security responsibilities need to be defined and allocated. | ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established<br>ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners<br>PR.AT-2: Privileged users understand their roles and responsibilities<br>PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities<br>PR.AT-4: Senior executives understand their roles and responsibilities<br>PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities<br>DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability<br>RS.CO-1: Personnel know their roles and order of operations when a response is needed | | Q31 |
| A.6.1.2 | Segregation of duties | Conflicting duties and areas of responsibility must be segregated in order to reduce the opportunities for unauthorised or unintentional modification or misuse of any of the organisation's assets. | PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | PPPR-15 | Q26, Q27, Q31, Q49, Q53, Q54, Q61 |
| A.6.1.3 | Contact with authorities | Appropriate contacts with relevant authorities must be maintained. | RS.CO-2: Incidents are reported consistent with established criteria | | Q21, Q22, Q23, Q24 |
| A.6.1.4 | Contact with special interest groups | Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained. | ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources<br>RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness<br>RC.CO-1: Public relations are managed | | |
| A.6.1.5 | Information security in project management | Information security should be addressed in project management, regardless of the type of project. | ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources<br>RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | HIPA-05-07 | |
| A.6.2 | Mobile devices and teleworking | | | | |
| A.6.2.1 | Mobile device policy | A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices. | PR.AC-3: Remote access is managed | | |
| A.6.2.2 | Teleworking | A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites. | PR.AC-3: Remote access is managed | | |
| **A.7** | **Human resource security** | | | | |
| A.7.1 | Prior to employment | | | | |
| A.7.1.1 | Screening | Background verification checks on all candidates for employment should be carried out in accordance with the relevant laws, regulations and ethics, and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. | PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions<br>PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | DOCU-08, PPPR-10, PPPR-11 | Q18, Q34, Q37, Q49, Q58, Q60, Q62 |
| A.7.1.2 | Terms and conditions of employment | The contractual agreements with employees and contractors should state their and the organisation's responsibilities for information security. | PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | | |
| A.7.2 | During employment | | | | |
| A.7.2.1 | Management responsibilities | Management should require all employees and contractors apply information security in accordance with the policies and procedures of the organisation. | ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners<br>PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities<br>PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | | Q5, Q7, Q60, Q61, Q62 |
| A.7.2.2 | Information security awareness, education, and training | All employees of the organisation and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function. | PR.AT-1: All users are informed and trained<br>PR.AT-2: Privileged users understand their roles and responsibilities<br>PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities<br>PR.AT-4: Senior executives understand their roles and responsibilities<br>PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities<br>PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)<br>DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability<br>RS.CO-1: Personnel know their roles and order of operations when a response is needed | PPPR-13, PPPR-14 | Q7 |

| | | | | | |
|---|---|---|---|---|---|
| A.7.2.3 | Disciplinary process | There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach. | PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | | Q18 |
| A.7.3 | Termination and change of employment | | | | |
| A.7.3.1 | Termination or change of employment responsibilities | Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced. | PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | | Q31, Q35 |
| **A.8** | **Asset management** | | | | |
| A.8.1 | Responsibilities for assets | | | | |
| A.8.1.1 | Inventory of assets | Assets associated with information and information processing facilities should be identified and an inventory of thes assets should be drawn up and maintained. | ID.AM-1: Physical devices and systems within the organization are inventoried<br>ID.AM-2: Software platforms and applications within the organization are inventoried | | Q55 |
| A.8.1.2 | Ownership of assets | Assets maintained in the inventory should be owned. | ID.AM-1: Physical devices and systems within the organization are inventoried<br>ID.AM-2: Software platforms and applications within the organization are inventoried | | Q55 |
| A.8.1.3 | Acceptable use of assets | Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented. | | | Q55 |
| A.8.1.4 | Return of assets | All employees and external party users should return any organisational assets in their possession upon termination of their employment, contract or agreement. | PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | | Q55 |
| A.8.2 | Information classification | | | | |
| A.8.2.1 | Classification of information | Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. | ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value<br>PR.PT-2: Removable media is protected and its use restricted according to policy | | Q55 |
| A.8.2.2 | Labeling of information | An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organisation. | PR.PT-2: Removable media is protected and its use restricted according to policy | | |
| A.8.2.3 | Handling of assets | Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organisation. | PR.DS-1: Data-at-rest is protected<br>PR.DS-2: Data-in-transit is protected<br>PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition<br>PR.IP-6: Data is destroyed according to policy<br>PR.PT-2: Removable media is protected and its use restricted according to policy | | Q42, Q43, Q44, Q45, Q46 |
| A.8.3 | Media handling | | | | |
| A.8.3.1 | Management of removable media | Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organisation. | PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition<br>PR.IP-6: Data is destroyed according to policy<br>PR.PT-2: Removable media is protected and its use restricted according to policy | DATA-19 | |
| A.8.3.2 | Disposal of media | Media should be disposed of securely when no longer required, using formal procedures. | PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition<br>PR.IP-6: Data is destroyed according to policy | | |
| A.8.3.3 | Physical media transfer | Media containing information needs to be protected against unauthorised access, misuse or corruption during transportation. | PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition<br>PR.PT-2: Removable media is protected and its use restricted according to policy | | |
| **A.9** | **Access control** | | | | |
| A.9.1 | Business requirements of access control | | | | |
| A.9.1.1 | Access control policy | An access control policy should be established, documented and reviewed based on business and information security requirements. | | APPL-01, APPL-02, APPL-09 | Q31 |
| A.9.1.2 | Access to networks and network services | Users should only be provided with access to the network and network services they have been specifically authorised to use. | PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties<br>PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | APPL-09 | Q31 |
| A.9.2 | User access management | | | | |
| A.9.2.1 | User registration and de-registration | A formal user registration and deregistration process should be implemented to enable assignment of access rights. | PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes<br>PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions<br>PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) | | Q19, Q26, Q27, Q28, Q29, Q30, Q32, Q33, Q34, Q35, Q37, Q47, Q48, Q49, Q50, Q52, Q53, Q54, Q57, Q59, Q60, Q61, Q63, Q64, Q65, Q66, Q67 |
| A.9.2.2 | User access provisioning | A formal user process should be implemented to assign or revoke access rights for all user types to all systems and services. | PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | | Q19, Q26, Q27, Q28, Q29, Q30, Q32, Q33, Q34, Q35, Q37, Q47, Q48, Q49, Q50, Q52, Q53, Q54, Q57, Q59, Q60, Q61, Q63, Q64, Q65, Q66, Q68 |
| A.9.2.3 | Management of privileged access rights | The allocation and use of privileged access rights should be restricted and controlled. | PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes<br>PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | | Q19, Q26, Q27, Q28, Q29, Q30, Q32, Q33, Q34, Q35, Q37, Q47, Q48, Q49, Q50, Q52, Q53, Q54, Q57, Q59, Q60, Q61, Q63, Q64, Q65, Q66, Q69 |

| | | | | | |
|---|---|---|---|---|---|
| A.9.2.4 | Management of secret authentication information of users | The allocation of secret authentication information should be controlled through a formal management process. | PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes<br>PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) | AAAI-14 | Q19, Q26, Q27, Q28, Q29, Q30, Q32, Q33, Q34, Q35, Q37, Q47, Q48, Q49, Q50, Q52, Q53, Q54, Q57, Q59, Q60, Q61, Q63, Q64, Q65, Q66, Q70 |
| A.9.2.5 | Review of user access rights | Asset owners should review users' access rights at regular intervals. | | | Q19, Q26, Q27, Q28, Q29, Q30, Q32, Q33, Q34, Q35, Q37, Q47, Q48, Q49, Q50, Q52, Q53, Q54, Q57, Q59, Q60, Q61, Q63, Q64, Q65, Q66, Q71 |
| A.9.2.6 | Removal or adjustment of access rights | The access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.. | PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | | Q19, Q26, Q27, Q28, Q29, Q30, Q32, Q33, Q34, Q35, Q37, Q47, Q48, Q49, Q50, Q52, Q53, Q54, Q57, Q59, Q60, Q61, Q63, Q64, Q65, Q66, Q72 |
| A.9.3 | User responsibilities | | | | |
| A.9.3.1 | Use of secret authentication information | Users should be required to follow the organisation's practices in the use of secret authentication information. | PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes<br>PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) | | Q19, Q26, Q27, Q28, Q29, Q30, Q32, Q33, Q34, Q35, Q37, Q47, Q48, Q49, Q50, Q52, Q53, Q54, Q57, Q59, Q60, Q61, Q63, Q64, Q65, Q66, Q72 |
| A.9.4 | System and application access control | | | | |
| A.9.4.1 | Information access restrictions | Access to information and application system functions should be restricted in accordance with the access control policy. | PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | | Q19, Q26, Q27, Q28, Q29, Q30, Q32, Q33, Q34, Q35, Q37, Q47, Q48, Q49, Q50, Q52, Q53, Q54, Q57, Q59, Q60, Q61, Q63, Q64, Q65, Q66, Q72 |
| A.9.4.2 | Secure log-on procedures | Where required by the access control policy, access to the systems and applications should be controlled by a secure log-on procedure. | PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes<br>PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) | | Q19, Q26, Q27, Q28, Q29, Q30, Q32, Q33, Q34, Q35, Q37, Q47, Q48, Q49, Q50, Q52, Q53, Q54, Q57, Q59, Q60, Q61, Q63, Q64, Q65, Q66, Q72 |
| A.9.4.3 | Password management system | Password management systems should be interactive and should ensure quality passwords. | PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes<br>PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) | HIPA-08, HIPA-09 | Q19, Q26, Q27, Q28, Q29, Q30, Q32, Q33, Q34, Q35, Q37, Q47, Q48, Q49, Q50, Q52, Q53, Q54, Q57, Q59, Q60, Q61, Q63, Q64, Q65, Q66, Q73 |
| A.9.4.4 | Use of privileged utility programs | The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled. | PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | | Q19, Q26, Q27, Q28, Q29, Q30, Q32, Q33, Q34, Q35, Q37, Q47, Q48, Q49, Q50, Q52, Q53, Q54, Q57, Q59, Q60, Q61, Q63, Q64, Q65, Q66, Q74 |
| A.9.4.5 | Access control to program source code | Access to program source code should be restricted. | PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | | Q19, Q26, Q27, Q28, Q29, Q30, Q32, Q33, Q34, Q35, Q37, Q47, Q48, Q49, Q50, Q52, Q53, Q54, Q57, Q59, Q60, Q61, Q63, Q64, Q65, Q66, Q75 |
| **A.10** | **Cryptography** | | | | |
| A.10.1 | Cryptographic controls | | | | |
| A.10.1.1 | Policy on the use of cryptographic controls | A policy on the use of cryptographic controls for the protection of information should be developed and implemented. | | DATA-03, DATA-04 | Q38, Q39, Q40, Q41 |
| A.10.1.2 | Key management | A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle. | | DATA-18 | Q38, Q39, Q40, Q41 |
| **A.11** | **Physical and environmental security** | | | | |
| A.11.1 | Secure areas | | | | |
| A.11.1.1 | Physical security perimeter | Security perimiters should be defined and used to protect areas that contain either sensitive or critical information or information processing facilities. | PR.AC-2: Physical access to assets is managed and protected<br>DE.CM-2: The physical environment is monitored to detect potential cybersecurity events | | |
| A.11.1.2 | Physical entry controls | Secure areas should be protected by the appropriate entry controls to ensure only authorised personnel are allowed access. | PR.AC-2: Physical access to assets is managed and protected<br>PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools<br>DE.CM-2: The physical environment is monitored to detect potential cybersecurity events | | |
| A.11.1.3 | Securing offices, rooms and facilities | Physical security for offices, rooms and facilities should be designed and applied. | PR.AC-2: Physical access to assets is managed and protected | | |
| A.11.1.4 | Protection against external and environmental threats | Physical protection against natural disasters, malicious attacks or accidents should be designed and applied. | ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)<br>PR.AC-2: Physical access to assets is managed and protected<br>PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met | DRPL-01, DRPL-02, DRPL-04, DRPL-05, DRPL-07, DRPL-08, DRPL-09, DRPL-11 | |
| A.11.1.5 | Working in secure areas | Procedures for working in secure areas should be designed and applied. | PR.AC-2: Physical access to assets is managed and protected | | |
| A.11.1.6 | Delivery and loading areas | Access points such as delivery and loading areas and other points where unauthorised persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access. | PR.AC-2: Physical access to assets is managed and protected | | |
| A.11.2 | Equipment | | | | |

| | | | | | |
|---|---|---|---|---|---|
| A.11.2.1 | Equipment siting and protection | Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and against unauthorised access. | PR.AC-2: Physical access to assets is managed and protected<br>PR.AT-1: All users are informed and trained<br>PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met | | |
| A.11.2.2 | Supporting utilities | Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. | ID.BE-4: Dependencies and critical functions for delivery of critical services are established<br>PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met | | |
| A.11.2.3 | Cabling security | Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage. | ID.BE-4: Dependencies and critical functions for delivery of critical services are established<br>PR.AC-2: Physical access to assets is managed and protected<br>PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met | | |
| A.11.2.4 | Equipment maintenance | Equipment should be correctly maintained to ensure its continued availability and integrity. | PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity<br>PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools<br>PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | | |
| A.11.2.5 | Removal of assets | Equipment, information or software should not be taken off-site without prior authorisation. | PR.AC-2: Physical access to assets is managed and protected<br>PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition<br>PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools | | |
| A.11.2.6 | Security of equipment and assets off-premises | Security controls should be applied to off-site assets, taking into account the different risks involved with working outside the organisation's premises. | ID.AM-4: External information systems are catalogued<br>PR.AC-2: Physical access to assets is managed and protected<br>PR.AC-3: Remote access is managed<br>PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools | | |
| A.11.2.7 | Secure disposal or re-use of equipment | All items of equipment including storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. | PR.AC-2: Physical access to assets is managed and protected<br>PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition<br>PR.IP-6: Data is destroyed according to policy | | |
| A.11.2.8 | Unattended user equipment | Users shold ensure that any unattended equipment has the appropriate protection. | PR.AC-2: Physical access to assets is managed and protected | | |
| A.11.2.9 | Clear desk and clear screen policy | A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted. | PR.PT-2: Removable media is protected and its use restricted according to policy | | |
| **A.12** | **Operations security** | | | | |
| A.12.1 | Operational procedures and responsibilities | | | | |
| A.12.1.1 | Documented operating procedures | Operating procedures should be documented and then made available to all users who need them. | DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed | | |
| A.12.1.2 | Change management | Changes to the organisation, business procedures, information processing facilities and systems that affect information security should be controlled. | PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)<br>PR.IP-3: Configuration change control processes are in place<br>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed | DOCU-09, CHNG-03, CHNG-10, CHNG-11, CHNG-13, CHNG-14, CHNG-15, CHNG-16, PPPR-02 | Q56 |
| A.12.1.3 | Capacity management | The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance. | ID.BE-4: Dependencies and critical functions for delivery of critical services are established | | |
| A.12.1.4 | Separation of development, testing and operational environments | Development, testing and operational environments should be separated to reduce the risks of unauthorised access or changes to the operational environment. | PR.DS-7: The development and testing environment(s) are separate from the production environment | | Q57 |
| A.12.2 | Protection from malware | | | | |
| A.12.2.1 | Controls against malware | Detection, prevention and recovery controls to protect against malware should be implemented, combined with the appropriate user awareness. | PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity<br>DE.CM-4: Malicious code is detected<br>RS.MI-1: Incidents are contained<br>RS.MI-2: Incidents are mitigated | | |
| A.12.3 | Backup | | | | |
| A.12.3.1 | Information Backup | Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy. | PR.IP-4: Backups of information are conducted, maintained, and tested | DATA-12, DATA-13, DATA-14, DATA-15, DATA-16, DATA-17 | |
| A.12.4 | Logging and Monitoring | | | | |
| A.12.4.1 | Event logging | Event logs recording user activities, exceptions, faults and information security events should be produced, kept and reviewed regularly. | PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy<br>DE.AE-2: Detected events are analyzed to understand attack targets and methods<br>DE.AE-3: Event data are collected and correlated from multiple sources and sensors<br>DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events<br>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed<br>RS.AN-1: Notifications from detection systems are investigated | AAAI-17, AAAI-18, AAAI-19 | Q8, Q9, Q10, Q11, Q12, Q13, Q14, Q15, Q16 |

| | | | | | |
|---|---|---|---|---|---|
| A.12.4.2 | Protection of log information | Logging facilities and log information should be protected against tampering and unauthorised access. | PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | | Q14, Q15 |
| A.12.4.3 | Administrator and operator log | System administrator and system operator activities need to be logged and the logs protected and regularly reviewed. | PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy<br>DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events<br>RS.AN-1: Notifications from detection systems are investigated | | Q8, Q10, Q12 |
| A.12.4.4 | Clock synchronization | The clocks of all relevant information processing systems within an organisation or security domain should be synchronised to a single reference time source. | PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | | |
| A.12.5 | Control of operational software | | | | |
| A.12.5.1 | Installation of software on operational systems | Procedures should be implemented to control the installation of software on operational systems. | ID.AM-2: Software platforms and applications within the organization are inventoried<br>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity<br>PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)<br>PR.IP-3: Configuration change control processes are in place<br>DE.CM-5: Unauthorized mobile code is detected | | |
| A.12.6 | Technical vulnerability management | | | | |
| A.12.6.1 | Management of technical vulnerabilities | Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. | ID.RA-1: Asset vulnerabilities are identified and documented<br>ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk<br>PR.IP-12: A vulnerability management plan is developed and implemented<br>DE.CM-8: Vulnerability scans are performed<br>RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks | FIDP-01-11, VULN-01-6 | |
| A.12.6.2 | Restriction on software installation | Rules governing the installation of software by users should be established and implemented. | PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)<br>PR.IP-3: Configuration change control processes are in place<br>DE.CM-5: Unauthorized mobile code is detected | | |
| A.12.7 | Information systems audit considerations | | | | |
| A.12.7.1 | Information system audit control | Audit requirements and activities involving verification of operational systems should be carefully planned and agreed on to minimise disruptions to the business processes. | PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | | Q11, Q13, Q16, Q17, Q25 |
| **A.13** | **Communications security** | | | | |
| A.13.1 | Network security management | | | | |
| A.13.1.1 | Network controls | Networks should be managed and controlled in order to protect information within systems and applications. | PR.AC-3: Remote access is managed<br>PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)<br>PR.DS-2: Data-in-transit is protected<br>PR.PT-4: Communications and control networks are protected<br>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed | FIDP-01-11 | |
| A.13.1.2 | Security of network services | Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced. | DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed | | |
| A.13.1.3 | Segregation in networks | Groups of information services, users and information systems should be segregated on networks. | PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation) | | |
| A.13.2 | Information transfer | | | | |
| A.13.2.1 | Information transfer policies and procedures | Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities. | ID.AM-3: Organizational communication and data flows are mapped<br>PR.AC-3: Remote access is managed<br>PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)<br>PR.DS-2: Data-in-transit is protected<br>PR.PT-4: Communications and control networks are protected | | Q43 |
| A.13.2.2 | Agreements on information transfer | Agreements should address the secure transfer of business information between the organisation and any external parties. | ID.AM-3: Organizational communication and data flows are mapped | | Q17, Q24, Q25 |
| A.13.2.3 | Electronic messaging | Information involved in any form of electronic messaging should to be appropriately protected. | PR.DS-2: Data-in-transit is protected | | Q43 |
| A.13.2.4 | Confidentiality or non-disclosure agreements | Requirements for confidentiality or non-disclosure agreements that reflect the organisation's needs for the protection of information should be identified, regularly reviewed and documented. | | | |
| **A.14** | **System acquisition, development and maintenance** | | | | |
| A.14.1 | Security requirements of information systems | | | | |
| A.14.1.1 | Information security requirements analysis and specification | The information security related requirements should be included in any requirements for new information systems or enhancements to existing information systems. | PR.IP-2: A System Development Life Cycle to manage systems is implemented | PPPR-04, PPPR-05 | |

| | | | | | |
|---|---|---|---|---|---|
| A.14.1.2 | Securing application services on public networks | Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification. | PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)<br>PR.DS-2: Data-in-transit is protected<br>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity | | |
| A.14.1.3 | Protecting application services transactions | Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay. | PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)<br>PR.DS-2: Data-in-transit is protected<br>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity<br>PR.PT-4: Communications and control networks are protected | | |
| A.14.2 | Security in development and support processes | | | | |
| A.14.2.1 | Secure development policy | Rules for the development of software and systems should be established and applied to developments within the organisation. | PR.IP-2: A System Development Life Cycle to manage systems is implemented | | Q57 |
| A.14.2.2 | System change control procedures | Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures. | PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)<br>PR.IP-3: Configuration change control processes are in place | | |
| A.14.2.3 | Technical review of applications after operating platform changes | When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on the organisational operations or security. | PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)<br>PR.IP-3: Configuration change control processes are in place<br>PR.IP-12: A vulnerability management plan is developed and implemented | | |
| A.14.2.4 | Restrictions on chnages to software packages | Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled. | PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity<br>PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)<br>PR.IP-3: Configuration change control processes are in place | | |
| A.14.2.5 | Secure system engineering principles | Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts. | PR.IP-2: A System Development Life Cycle to manage systems is implemented | | |
| A.14.2.6 | Secure development environment | Organisations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle. | | | |
| A.14.2.7 | Outsourced development | The organisation should supervise and monitor the activity of outsourced system development. | DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events<br>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed | | |
| A.14.2.8 | System security testing | Testing of security functionality should be carried out during development. | DE.DP-3: Detection processes are tested | | |
| A.14.2.9 | System acceptance testing | Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions. | | | |
| A.14.3 | Test Data | | | | |
| A.14.3.1 | Protection of test data | Test data should be selected carefully, protected and controlled. | | | |
| **A.15** | **Suppliers relationships** | | | | |
| A.15.1 | Information security in supplier relationships | | | | |
| A.15.1.1 | Information security policy for supplier relationships | Information security requirements for mitigating the risks associated with suppliers access to the organisation's assets should be agreed with the supplier and documented. | ID.BE-1: The organization's role in the supply chain is identified and communicated<br>ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners<br>ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders<br>ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.<br>PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | THRD-01, THRD-02 | Q47 |
| A.15.1.2 | Addressing security within supplier agreements | All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation's information. | ID.BE-1: The organization's role in the supply chain is identified and communicated<br>ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders<br>ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. | THRD-03 | |
| A.15.1.3 | Information and communication technology supply chain | Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain. | ID.BE-1: The organization's role in the supply chain is identified and communicated<br>ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders<br>ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. | | |

| | | | | | |
|---|---|---|---|---|---|
| A.15.2 | Supplier service delivery managemnt | | | | |
| A.15.2.1 | Monitoring and review of supplier services | Organisations should regularly monitor, review and audit their supplier service delivery. | ID.BE-1: The organization's role in the supply chain is identified and communicated<br>ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders<br>ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process<br>ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.<br>PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access<br>DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events<br>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed | THRD-04, THRD-05, APPL-05 | |
| A.15.2.2 | Managing changes to supplier services | Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking into account the criticality of business information, the nature of the change, the supplier type/s affected, the systems and processes involved and a re-assessment of risks. | ID.BE-1: The organization's role in the supply chain is identified and communicated<br>ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders<br>ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process<br>ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. | THRD-05 | |
| **A.16** | **Information security incident management** | | | | |
| A.16.1 | Management of information security incidents and improvements | | | | |
| A.16.1.1 | Responsibilities and procedures | Management responsibilities and procedures should be established in order to ensure a quick, effective and orderly response to information security incidents. | PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed<br>DE.AE-2: Detected events are analyzed to understand attack targets and methods<br>RS.CO-1: Personnel know their roles and order of operations when a response is needed | DRPL-01, DRPL-02, DRPL-04, DRPL-05, DRPL-07, DRPL-08, DRPL-09, DRPL-11, PPPR-06 | Q20, Q21, Q22, Q23 |
| A.16.1.2 | Reporting information security events | Information security events should be reported through appropriate management channels as quickly as possible. | DE.DP-4: Event detection information is communicated<br>RS.CO-2: Incidents are reported consistent with established criteria<br>RS.CO-3: Information is shared consistent with response plans | PPPR-07 | Q24, Q25 |
| A.16.1.3 | Reporting information security weaknesses | Employees and contractors using the organization's information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services. | PR.IP-12: A vulnerability management plan is developed and implemented<br>DE.DP-4: Event detection information is communicated | | Q21, Q23 |
| A.16.1.4 | Assessment of and decision on information security events | Information security events should be assessed and it should be decided if they are to be classified as information security incidents. | DE.AE-2: Detected events are analyzed to understand attack targets and methods<br>DE.AE-4: Impact of events is determined<br>DE.AE-5: Incident alert thresholds are established<br>RS.AN-2: The impact of the incident is understood<br>RS.AN-4: Incidents are categorized consistent with response plans | | Q22 |
| A.16.1.5 | Response to information security incidents | Information security incidents should be responded to in accordance with the documented procedures. | RS.RP-1: Response plan is executed during or after an incident<br>RS.AN-1: Notifications from detection systems are investigated<br>RS.MI-1: Incidents are contained<br>RS.MI-2: Incidents are mitigated<br>RC.RP-1: Recovery plan is executed during or after a cybersecurity incident | IH-01 | Q22 |
| A.16.1.6 | Learning from information security incidents | Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents. | ID.RA-4: Potential business impacts and likelihoods are identified<br>PR.IP-7: Protection processes are improved<br>PR.IP-8: Effectiveness of protection technologies is shared<br>DE.DP-5: Detection processes are continuously improved<br>RS.AN-2: The impact of the incident is understood<br>RS.IM-1: Response plans incorporate lessons learned<br>RS.IM-2: Response strategies are updated<br>RC.IM-1: Recovery plans incorporate lessons learned<br>RC.IM-2: Recovery strategies are updated | | Q22 |
| A.16.1.7 | Collection of evidence | The organization should define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence. | DE.AE-3: Event data are collected and correlated from multiple sources and sensors<br>RS.AN-3: Forensics are performed | | Q20, Q21, Q22, Q23 |
| **A.17** | **Information security aspects of business continuity management** | | | | |
| A.17.1 | Information security continuity | | | | |
| A.17.1.1 | Planning information security continuity | The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster. | ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)<br>PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed | DRPL-01, DRPL-02, DRPL-04, DRPL-05, DRPL-07, DRPL-08, DRPL-09, DRPL-11 | Q5 |

| | | | | | |
|---|---|---|---|---|---|
| A.17.1.2 | Implementing information security continuity | | ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)<br>PR.IP-4: Backups of information are conducted, maintained, and tested<br>PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed<br>PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | DRPL-01, DRPL-02, DRPL-04, DRPL-05, DRPL-07, DRPL-08, DRPL-09, DRPL-11 | Q5 |
| | | The organization should establish, document, implement and maintain processes, procedures, and controls to ensure the required level of continuity for information security during an adverse situation. | | | |
| A.17.1.3 | Verify, review and evaluate information security continuity | | ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers<br>PR.IP-4: Backups of information are conducted, maintained, and tested<br>PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed<br>PR.IP-10: Response and recovery plans are tested | DRPL-01, DRPL-02, DRPL-04, DRPL-05, DRPL-07, DRPL-08, DRPL-09, DRPL-11 | Q5 |
| | | The organization should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. | | | |
| A.17.2 | Redundancies | | | | |
| A.17.2.1 | Availability of information processing facilities | | ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)<br>PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | | Q46 |
| | | Information processing facilities should be implemented with redundancy sufficient to meet availability requirements. | | | |
| **A.18** | **Compliance** | | | | |
| A.18.1 | Compliance with legal and contractual requirements | | | | |
| A.18.1.1 | Identification of applicable legislation and contractual requirements | All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organization. | ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | | |
| A.18.1.2 | Intellectual property rights | Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. | ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | | |
| A.18.1.3 | Protection of records | Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements. | ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed<br>PR.IP-4: Backups of information are conducted, maintained, and tested | | Q14, Q15 |
| A.18.1.4 | Privacy and protection of personally identifiable information | | ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed<br>PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)<br>DE.DP-2: Detection activities comply with all applicable requirements | | |
| | | Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable. | | | |
| A.18.1.5 | Regulation of cryptographic controls | Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations. | ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | PPPR-03 | |
| A.18.2 | Information security reviews | | | | |
| A.18.2.1 | Independent review of information security | The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur. | | | Q6 |
| A.18.2.2 | Compliance with security policies and standards | Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. | PR.IP-12: A vulnerability management plan is developed and implemented<br>DE.DP-2: Detection activities comply with all applicable requirements | | |
| A.18.2.3 | Technical compliance review | | ID.RA-1: Asset vulnerabilities are identified and documented<br>PR.IP-12: A vulnerability management plan is developed and implemented<br>DE.DP-2: Detection activities comply with all applicable requirements | | |
| | | Information systems should be regularly reviewed for compliance with the organization's information security policies and standards. | | | |

| **NIST Cybersecurity Framework controls not immediately covered by ISO27001 Annex A** | |
|---|---|
| ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated | |
| ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated | |
| ID.GV-4: Governance and risk management processes address cybersecurity risks | Addresses clause 6 of ISO 27001 |
| ID.RA-3: Threats, both internal and external, are identified and documented | Addresses clause 6.1.2 of ISO 27001 |
| ID.RA-6: Risk responses are identified and prioritized | Addresses clause 6.1.2 of ISO 27001 |
| ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders | Addresses clause 6.1.3, 8.3, 9.3 of ISO 27001 |
| ID.RM-2: Organizational risk tolerance is determined and clearly expressed | Addresses clause 6.1.3, 8.3 of ISO 27001 |
| ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | Addresses clause 6.1.3, 8.3 of ISO 27001 |
| PR.IP-7: Protection processes are improved | Addresses clause 9, 10 of ISO 27001 |

| | |
|---|---|
| DE.CM-1: The network is monitored to detect potential cybersecurity events | |
| RS.CO-3: Information is shared consistent with response plans | Addresses clause 7.4, 16.1.2 of ISO 27001 |
| RS.CO-4: Coordination with stakeholders occurs consistent with response plans | Addresses clause 7.4 of ISO 27001 |
| RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers) | Addresses clause 10 of ISO 27001 |
| RS.IM-1: Response plans incorporate lessons learned | Addresses clause 10 of ISO 27001 |
| RS.IM-2: Response strategies are updated | Addresses clause 10 of ISO 27001 |
| RC.IM-1: Recovery plans incorporate lessons learned | Addresses clause 10 of ISO 27001 |
| RC.IM-2: Recovery strategies are updated | Addresses clause 10 of ISO 27001 |
| RC.CO-1: Public relations are managed | Addresses clause 7.4 of ISO 27001 |
| RC.CO-2: Reputation is repaired after an incident | Addresses clause 7.4 of ISO 27001 |
| RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams | Addresses clause 7.4 of ISO 27001 |