Statement Of Applicability

Project Name:	ISO/IEC 27001: 2022
Version:	1
Status:	Complete
Date Created:	26/04/2024
Date Updated:	02/10/2024

Clause	Clause Description	Is Applicable?	Justification
A.5	**Organizational controls.** ...		
A.5.1	**Policies for information security.** Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	True	The organisation understands Information Security Policies are a vital component of an effective ISMS and these will be used as the foundation for the ISMS. Policies are required to set the direction, show intent and formally document the ISMS. Staff need to be aware of these policies to improve the effectiveness of the ISMS. Our policies will help us to protect Sensitive Data, Legal and Regulatory Compliance, Risk Management, Prevent Data Breaches, Maintaining Reputation and Trust, Operational Continuity and Employee Awareness and Training.
A.5.2	**Information security roles and responsibilities.** Information security roles and responsibilities should be defined and allocated according to the organization needs.	True	Clear roles and responsibilities across the organization are crucial for the success of the ISMS. Formally identifying roles and responsibilities ensures an effective ISMS implementation, maintenance and maturity, guides compliance and Conformity, identifies and manages risks, provides communication and coordination, focuses on training and awareness, and ensures the continual monitoring and improvement of our ISMS.
A.5.3	**Segregation of duties.** Conflicting duties and conflicting areas of responsibility should be segregated.	True	Segregation of duties is integral to maintaining our robust ISMS. It ensures that critical tasks such as access control, change management, risk assessment, and other security-related functions are appropriately distributed among different roles or individuals. This distribution helps us establish a system of checks and balances, reducing our overall risk exposure and enhancing the integrity and reliability of our ISMS.
A.5.4	**Management responsibilities.** Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	True	Management responsibilities are pivotal for the successful implementation and maintenance of our ISMS. Our Management Teams commitment, involvement, and active support ensures our ISMS is part of our culture and ensures the effectiveness of the security measures in place. Our Management team provides leadership and direction, supports resource allocation, role models effective risk management, ensures compliance and conformance, champions continuous improvement, oversees communication and training and prioritises incident response and preparedness.
A.5.5	**Contact with authorities.** The organization should establish and maintain contact with relevant authorities.	True	Maintaining a channel of contact with relevant authorities is crucial for our organisation's ISMS, ensuring compliance, staying informed about legal requirements, accessing resources and guidance, and establishing a cooperative approach towards securing sensitive data and systems.
A.5.6	**Contact with special interest groups.** The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	True	Special interest groups keep our organisation up to date in industry insights and best practices, facilitate networking and collaboration, provide education and training, provide opportunities for advocacy and influence, give us access to information sharing and threat intelligence, provide professional development and sometimes give validation and recognition.

Clause	Clause Description	Is Applicable?	Justification
A.5.7	**Threat intelligence.** Information relating to information security threats should be collected and analysed to produce threat intelligence.	True	We leverage threat intelligence to fortify our information security practices and align with the ISO 27001 standard. Threat Intelligence provides the necessary insights we need to be proactive in addressing potential threats and vulnerabilities, ensuring a more robust and adaptive security posture.
A.5.8	**Information security in project management.** Information security should be integrated into project management.	True	We incorporate information security in project management to help create a more secure project environment, reducing vulnerabilities, and ensure that security is not an afterthought but an integral part of the project's success.
A.5.9	**Inventory of information and other associated assets.** An inventory of information and other associated assets, including owners, should be developed and maintained.	True	We maintain an accurate and up-to-date inventory of information and associated assets for effective information security management. Our software and data asset register provides the foundation for our risk assessment, resource allocation, incident response, and compliance, contributing to our robust security posture.
A.5.10	**Acceptable use of information and other associated assets.** Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.	True	By establishing and consistently enforcing our acceptable use of technology and workspace policy, we significantly reduce the risks associated with information and asset misuse, ensuring a more secure and compliant environment. Our policy fosters a culture of responsible information handling and contributes to our robust security posture.
A.5.11	**Return of assets.** Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	True	Asset return is an essential component of information security and asset management within our organisation. When employees leave the company or when assets are no longer needed, a structured and secure asset return process is critical to protect sensitive information, comply with regulations, control cost, and ensure efficient resource utilisation, all contributing to our secure and well-managed organisational environment.
A.5.12	**Classification of information.** Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	True	We classify information by categorising data according to its sensitivity, importance, and the level of protection required, to ensure data protection, access control, risk management, compliance, and resource allocation, contributing significantly to our overall security posture.
A.5.13	**Labelling 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 organization.	True	We label our data to reflect the classification, sensitivity, and handling requirements of that information. This is so that the sensitivity of that data is communicated, access control is guided, compliance is facilitated, and our culture of information security is promoted.
A.5.14	**Information transfer.** Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	True	We ensure secure information transfer so that we maintain the CIA (Confidentiality, Integrity and Availability) of data. By implementing encryption, secure protocols, access controls, and user education, we effectively manage information transfer securely and mitigate potential risks associated with data movement.
A.5.15	**Access control.** Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.	True	Access control is one of the primary focus areas of our ISMS. Our securely designed access controls protect our information and associated devices and infrastructure against unauthorised access and information access. A defined access control policy is in place to set the direction and principles for access control.
A.5.16	**Identity management.** The full life cycle of identities should be managed.	True	Identity management plays an important role in ensuring that the right people have the appropriate access to information and systems. Our identity management practices allow us to strengthen our access control measures, enhance information security, manage the lifecycle of our user identities, ensure appropriate access, and reduce the risk of unauthorised access or security breaches.

Clause	Clause Description	Is Applicable?	Justification
A.5.17	**Authentication information.** Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.	True	Authentication information are the credentials and mechanisms we use to verify the identity of individuals or entities seeking access to our systems, networks, or applications. These help us enhance the security of authentication information, reduce the risk of unauthorised access, and improve our security and resilience.
A.5.18	**Access rights.** Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	True	Access rights, refer to the level of privileges or permissions granted to individuals or entities within our organisation, to access specific resources, systems, or information. By effectively managing access rights, we reduce the risk of unauthorised access and enhance the confidentiality and integrity of our information.
A.5.19	**Information security in supplier relationships.** Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	True	Due to the amount of service providers/external parties used by the organisation (including cloud providers) and the risks identified these controls are vital for the success of the ISMS. Suppliers may have access to the organisation's information and controls need to be applied to them.
A.5.20	**Addressing information security within supplier agreements.** Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	True	Due to the amount of service providers/external parties used by us (including cloud providers), and the risks identified, these controls are vital for the success of the ISMS. Suppliers may have access to our information, so controls need to be applied. By addressing information security in supplier relationships through a comprehensive and proactive approach, we minimise risks, protect sensitive information, and foster a secure and collaborative environment with external partners, contributing to the overall resilience of our ISMS.
A.5.21	**Managing information security in the ICT supply chain.** Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	True	Managing information security in our supply chain is crucial for us to ensure the protection of our sensitive information throughout the procurement and sourcing processes. Our robust approach to information security in the supply chain helps us to mitigate risks, enhance resilience and information security, and foster a secure and resilient supply chain ecosystem.
A.5.22	**Monitoring, review and change management of supplier services.** The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	True	Monitoring, reviewing, and managing changes in supplier services are integral components of our proactive and resilient information security strategy. The outcomes of the reviews, and details of the changes inform our risk assessments and treatment, help us stay vigilant, allow us to respond effectively to changes, and promote a secure and reliable supply chain environment.
A.5.23	**Information security for use of cloud services.** Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.	True	Information security in the use of cloud services is essential for us to safeguard data, ensure compliance, manage risks, and maintain the trust of our customers and stakeholders.
A.5.24	**Information security incident management planning and preparation.** The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	True	Information security incident management planning helps us respond effectively to security incidents, reduce their impact, and continuously improve our information security practices. Our proactive and systematic approach safeguards information assets and maintains the integrity and resilience of our ISMS.
A.5.25	**Assessment and decision on information security events.** The organization should assess information security events and decide if they are to be categorized as information security incidents	True	Assessing information security events and determining whether they should be categorised as information security incidents is a crucial step in our incident management process. It helps us detect security incidents early, differentiate incidents from non-incident events, allocate resource to manage the incident, mitigate false positives, manage risks, remain compliant, categorise the severity, manage the incident, including communication and reporting (incident response), learn from the incident and take action to reduce the risk of the incident reoccurring and maintain our trust and reputation.
A.5.26	**Response to information security incidents.** Information security incidents should be responded to in accordance with the documented procedures.	True	Responding to information security incidents in accordance with our documented procedures is a fundamental aspect of effective incident management. It ensures consistency, efficiency, legal compliance, and the ability to learn and improve from each incident, ultimately contributing to a more resilient and secure information environment.

Clause	Clause Description	Is Applicable?	Justification
A.5.27	**Learning from information security incidents.** Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	True	Learning from security incidents is crucial for us because it contributes to our continuous improvement culture, gives us enhanced resilience, and a more robust information security posture. Reviewing major incidents enables us to identifying vulnerabilities, strengthening security controls, improve incident response, enhance threat intelligence, focus awareness, training and education, implement corrective actions, build a proactive security culture, meet compliance requirements, prevent recurrence, and maintain trust and reputation. Learning from security incidents is an integral part of our proactive and maturing ISMS. It allows us to continuously improve our security posture, mitigate risks, and respond effectively to threats.
A.5.28	**Collection of evidence.** The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	True	Procedures for the identification, collection, acquisition, and preservation of evidence are in place to support effective incident response, legal compliance, and maintain the integrity of information security investigations. Our formal evidence procedures ensure that security incidents are detected and give us data to prosecute the attackers. Our defined evidence procedures improve the investigation process by ensuring that evidence preservation is a focus.
A.5.29	**Information security during disruption.** The organization should plan how to maintain information security at an appropriate level during disruption.	True	Planning how to maintain information security at an appropriate level during disruptions is crucial to ensure the resilience and continuity of business operations in the face of various challenges. Planning for information security during disruptions is a proactive and strategic approach that helps us navigate challenges, protect critical assets, and ensure the continuity of business operations. It is an integral component of our business resilience and risk management.
A.5.30	**ICT readiness for business continuity.** ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	True	Aligning ICT readiness with business continuity objectives is integral to our resilience. It ensures that our ICT systems are prepared to withstand disruptions, respond effectively to incidents, and contribute to overall business continuity goals. Regular testing and continuous improvement are essential elements of our process.
A.5.31	**Legal, statutory, regulatory and contractual requirements.** Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date.	True	Staying informed about and adhering to legal, statutory, regulatory, and contractual requirements is essential for ensuring the security of information, managing risks, maintaining compliance, and safeguarding our organisation's reputation.
A.5.32	**Intellectual property rights.** The organization should implement appropriate procedures to protect intellectual property rights.	True	Compliance to intellectual property rights is required to prevent fines and penalties related to illegal software usage. Implementing procedures to protect intellectual property rights is not only a legal necessity but is also a strategic imperative for our organisation to help us thrive in a competitive and innovation-driven business environment. It safeguards the our investments, fosters innovation, and contributes to our long-term success.
A.5.33	**Protection of records.** Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	True	Protecting records from loss, destruction, falsification, unauthorised access, and unauthorised release is integral to legal compliance, operational continuity, maintaining trust, and safeguarding sensitive information. It is a fundamental aspect of effective information governance and risk management within our organisation.
A.5.34	**Privacy and protection of PII.** The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	True	Compliance to privacy controls is a critical focus area as there are international laws governing how Personally identifiable information (PII) is managed. Not complying with these laws could result in fines and other penalties. Identifying and meeting requirements related to the preservation of privacy and protection of PII is not only a legal obligation but also a strategic and ethical imperative. It helps build trust, mitigate risks, and position our organisation as a responsible steward of sensitive personal information.
A.5.35	**Independent review of information security.** The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.	True	Reviewing our organisation's approach to managing information security is essential for maintaining the effectiveness of security measures, staying compliant with regulations, and adapting to the evolving threat landscape. It is a proactive and strategic approach to safeguarding information assets and maintaining our overall security posture.

Clause	Clause Description	Is Applicable?	Justification
A.5.36	**Compliance with policies, rules and standards for information security.** Compliance with the organization’s information security policy, topic-specific policies, rules and standards should be regularly reviewed.	True	Regular reviews of compliance with information security policies, topic-specific policies, rules, and standards are essential for maintaining the effectiveness of our security measures, staying current with regulatory requirements, adapting to business changes, and continuously improving our organisation's overall security posture. Internal compliance checks are a vital aspect of our organisations risk profile and controls are implemented to ensure that the controls, documentation and overall ISMS status are reviewed regularly by managers within their area of responsibility.
A.5.37	**Documented operating procedures.** Operating procedures for information processing facilities should be documented and made available to personnel who need them.	True	Documenting operating procedures for information processing facilities and making them available to personnel is fundamental for promoting consistency, efficiency, compliance, risk management, and overall effectiveness in the operation of information systems within our organisation. It supports our commitment to best practices, quality, and the ongoing improvement of our information processing capabilities.
A.6	**People Controls.** ...		
A.6.1	**Screening.** Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	True	Conducting background verification checks on candidates before joining our organisation is a comprehensive risk management strategy that protects us, our employees, and our stakeholders. It helps ensure legal compliance, maintain a safe and trusted work environment, and prevent potential issues that could adversely impact our organisation's reputation and success.
A.6.2	**Terms and conditions of employment.** The employment contractual agreements should state the personnel’s and the organization’s responsibilities for information security.	True	Including information security responsibilities in employment contractual agreements is our proactive approach to establishing a strong security culture, ensuring legal compliance, and mitigating the risk of security incidents. It helps create a shared understanding of the critical role that our employees play in safeguarding our organisation's information assets.
A.6.3	**Information security awareness, education and training.** Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	True	Investing in information security awareness, education, and training for our team is our proactive strategy that enhances the our organisation's overall security posture, reduces risks, and fosters a culture of security consciousness and responsibility.
A.6.4	**Disciplinary process.** A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	True	Formalising and communicating our disciplinary process for information security policy violations is our strategic approach that ensures consistency, deterrence, legal compliance, and overall effectiveness in maintaining a secure information environment within our organisation.
A.6.5	**Responsibilities after termination or change of employment.** Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.	True	Defining, enforcing, and communicating ongoing information security responsibilities after termination or change of employment is essential for protecting sensitive information, preventing insider threats, ensuring legal compliance, and upholding our organisation's overall security posture.
A.6.6	**Confidentiality or non-disclosure agreements.** Confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	True	Identifying, documenting, regularly reviewing, and having the right people sign confidentiality or non-disclosure agreements are essential practices for protecting our organisation's sensitive information, maintaining trust, and ensuring legal compliance. These agreements are a fundamental component of our comprehensive information security strategy.
A.6.7	**Remote working.** Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization’s premises.	True	Security measures for remote work are essential to address the challenges and risks associated with accessing, processing, and storing information outside our organisation's premises. These measures are integral to maintaining a secure and resilient information environment in the context of evolving work practices.

Clause	Clause Description	Is Applicable?	Justification
A.6.8	**Information security event reporting.** The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	True	Providing a mechanism for employees to report observed or suspected information security events in a timely manner is our proactive strategy for early detection, rapid response, and overall resilience in the face of evolving cybersecurity threats. It is an integral component of our comprehensive information security program.
A.7	**Physical controls.** ...		
A.7.1	**Physical security perimeters.** Security perimeters should be defined and used to protect areas that contain information and other associated assets.	True	Defining and protecting our physical security perimeters is critical to protect our information and associated assets by preventing unauthorised access, deterring threats, and facilitating a more controlled and secure office environment.
A.7.2	**Physical entry.** Secure areas should be protected by appropriate entry controls and access points.	True	Protecting our secure areas with appropriate entry controls and access points helps safeguard information, assets, and personnel, contributing to the overall resilience and integrity of our operations.
A.7.3	**Securing offices, rooms and facilities.** Physical security for offices, rooms and facilities should be designed and implemented.	True	Designing and implementing physical security for offices, rooms, and facilities helps mitigate potential threats and vulnerabilities, contributing to the overall resilience and security of our organisation.
A.7.4	**Physical security monitoring.** Premises should be continuously monitored for unauthorized physical access.	True	Continuous monitoring of our premises for unauthorised physical access is vital to our security strategy, helping us protect our assets, ensure compliance, and respond effectively to potential threats.
A.7.5	**Protecting against physical and environmental threats.** Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.	True	The design and implementation of protection measures against physical and environmental threats are essential for ensuring safety, preserving assets, maintaining business continuity, and meeting regulatory requirements. It is a critical aspect of our responsible infrastructure management and contributes to the overall resilience of our systems in the face of various challenges.
A.7.6	**Working in secure areas.** Security measures for working in secure areas should be designed and implemented.	True	Security measures for working in secure areas are designed and implemented with the aim of safeguarding our people, information, assets, and the overall integrity of the secure environment. The measures are crucial for safeguarding sensitive information, preventing unauthorised access, ensuring employee and visitor safety, and maintaining the overall integrity of our critical environments.
A.7.7	**Clear desk and clear screen.** Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	True	Defining and appropriately enforcing clear desk rules for papers and removable storage media, as well as clear screen rules for information processing facilities, help protect sensitive information, prevent data breaches, and promote a culture of security within our organisation.
A.7.8	**Equipment siting and protection.** Equipment should be sited securely and protected.	True	Securing and protecting our equipment safeguards against physical damage, theft, environmental factors, and cybersecurity threats.
A.7.9	**Security of assets off-premises.** Off-site assets should be protected.	True	Protecting our off-site assets safeguards our data, ensures business continuity, complies with regulations, and mitigates risks that could impact operations, reputation, and financial stability.

Clause	Clause Description	Is Applicable?	Justification
A.7.10	**Storage media.** Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	True	Managing storage media through its life cycle in alignment with our classification scheme and handling requirements is integral to maintaining our data security, ensuring regulatory compliance, minimising environmental impact, and overall effective risk management. Our holistic approach considers the entire life span of storage media from acquisition to disposal
A.7.11	**Supporting utilities.** Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	True	Protecting information processing facilities from power failures and disruptions caused by failures in supporting utilities ensured operational resilience, data integrity, and overall business continuity. It involves implementing a combination of backup power systems, redundancy, and contingency planning to mitigate the impact of unexpected power-related events.
A.7.12	**Cabling security.** Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	True	Protecting cables carrying power, data, or supporting information services is essential for maintaining the security, integrity, and reliability of our critical systems and infrastructure. It involves implementing physical safeguards, encryption measures, and best practices to minimise the risks associated with interception, interference, or damage.
A.7.13	**Equipment maintenance.** Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	True	Maintaining equipment correctly ensures the reliable operation of critical systems, protects against security threats, and supports compliance with regulatory requirements, ultimately safeguarding the availability, integrity, and confidentiality of information.
A.7.14	**Secure disposal or re-use of equipment.** Items of equipment containing 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.	True	Disposal of equipment containing storage media is critical to ensure that sensitive data and licensed software is removed so that they cannot be accessed, stolen or used by unauthorised parties.
A.8	**Technological controls.** ...		
A.8.1	**User endpoint devices.** Information stored on, processed by or accessible via user endpoint devices should be protected.	True	Protecting information on user endpoint devices is integral to our information security strategy. It involves implementing a combination of technical controls, security policies, and user awareness training to mitigate risks and safeguard sensitive data throughout its lifecycle.
A.8.2	**Privileged access rights.** The allocation and use of privileged access rights should be restricted and managed.	True	A defined access control policy with supporting processes for privileged access is vital to set a direction and principles for access control. Privileged access is a major risk area because of what these accounts are able to access and the services they are able to perform. Malicious parties will target these accounts and use them to access information and perform Malicious attacks.
A.8.3	**Information access restriction.** Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	True	Access control (least privileged access methodology) protects data, ensures compliance, and mitigates risks associated with unauthorised access by preventing unauthorised users from accessing information and application systems.
A.8.4	**Access to source code.** Read and write access to source code, development tools and software libraries should be appropriately managed.	True	Appropriate management of development tools and software libraries is essential for maintaining our stable, secure, and efficient development environment. It supports the entire software development lifecycle, from initial coding to testing, deployment, and maintenance, contributing to the long-term success of software projects. Program source code one of the organizations most valuable assets and needs to be protected from unauthorized access to ensure its confidentiality, integrity and availability.
A.8.5	**Secure authentication.** Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	True	Preventative controls maintain risk by implementing technology and establishing topic-specific secure authentication procedures that ensure human and non-human users and identities undergo a robust and secure authentication procedure when attempting to access ICT resources.

Clause	Clause Description	Is Applicable?	Justification
A.8.6	**Capacity management.** The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	True	Capacity Management supports the network security controls by designing capacity requirements and monitoring the network devices (including servers) for capacity issues which could affect the availability of the devices. This includes security related threats and general operational issues.
A.8.7	**Protection against malware.** Protection against malware should be implemented and supported by appropriate user awareness.	True	Malware Controls are a vital defence against malicious attacks which could come from outside or inside the organization's network. The malware controls we have in place reduce the impacts of Malicious attacks and ensures that the information security team has visibility.
A.8.8	**Management of technical vulnerabilities.** Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.	True	Our vulnerability and penetration testing policy ensures we are regularly conducting testing for vulnerabilities across our network, and aims to help us to identify and resolve vulnerabilities across the organization's infrastructure and reduces the risks related to Malicious attacks.
A.8.9	**Configuration management.** Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	True	We have established documents that govern how we implement, monitor and review the use of configurations across our network.
A.8.10	**Information deletion.** Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	True	Our data retention policy ensures we retain information for the appropriate amount of time, considering any prevailing laws and regulatory guidelines. Alongside this our IT Asset Management Policy defines how assets should be managed and destructed.
A.8.11	**Data masking.** Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	True	Our cryptography controls policy defines where we need to apply data masking techniques and the controls we need to put in place to help the business remain compliant with what's asked of it by legal authorities and regulatory agencies.
A.8.12	**Data leakage prevention.** Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.	True	Our Data Loss Prevention Procedures help to control and reduce the risk of data leakage, with technical controls implemented to prevent the disclosure and/or extraction of information, either by internal and/or external personnel, or logical systems.
A.8.13	**Information backup.** Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	True	Our operating procedures defined the controls we have in place for critical systems and the backup and recovery of information in these systems. Having these controls in place protects us against risks related to the loss or corruption of information.
A.8.14	**Redundancy of information processing facilities.** Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	True	Our BCP focuses on our information security continuity risks and ensures that the business will react effectively and respond to disasters or major incidents.
A.8.15	**Logging.** Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	True	Logging and monitoring controls gives us the ability to identify and respond to malicious attacks and other security incidents. Our logging and monitoring policy guides us on what we need to maintain and monitor.
A.8.16	**Monitoring activities.** Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	True	Logging and monitoring controls gives us the ability to identify and respond to malicious attacks and other security incidents. Our logging and monitoring policy guides us on what we need to maintain and monitor.

Clause	Clause Description	Is Applicable?	Justification
A.8.17	**Clock synchronization.** The clocks of information processing systems used by the organization should be synchronized to approved time sources.	True	Logging and monitoring controls give the organization the ability to identify and respond to malicious attacks and other security incidents. Without a process defining how logs are recorded and kept with rules related to clock synchronisation it is not possible to have an effective incident detection and response process.
A.8.18	**Use of privileged utility programs.** The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	True	Some utility programs allow users to override system and application controls and can be used to access information or perform system tasks so need to be protected.
A.8.19	**Installation of software on operational systems.** Procedures and measures should be implemented to securely manage software installation on operational systems.	True	We have procedures to control the installation of software on operational systems, preventing unauthorised software being installed on operational systems and the related risks of malware and unsupported software leading to operational issues.
A.8.20	**Networks security.** Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	True	Our Network Security Policy gives guidance on the controls we need to have in place to guard against unauthorised access to networks, mitigating risks of information security.
A.8.21	**Security of network services.** Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	True	Our Network Security Policy gives guidance on the controls we need to have in place to guard against unauthorised access to networks, mitigating risks of information security.
A.8.22	**Segregation of networks.** Groups of information services, users and information systems should be segregated in the organization's networks.	True	Our Network Security Policy defines how networks should be segregated to guard against unauthorized access to networks, mitigating risks of information security.
A.8.23	**Web filtering.** Access to external websites should be managed to reduce exposure to malicious content.	True	Filtering the websites accessible enables us to eliminate security risks such as malware infection that may arise as a result of access to external websites with malicious content.
A.8.24	**Use of cryptography.** Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	True	The cryptographic (encryption) controls are an integral part of the ISMS and are required to manage the risks of unauthorized access to information. Encryption is an additional layer of security which allows for information to be encrypted both when transmitted or stored and is required for legal/regulatory requirements.
A.8.25	**Secure development life cycle.** Rules for the secure development of software and systems should be established and applied.	True	Security controls being implemented for the development function ensures that systems are developed and maintained with security controls designed and implemented throughout the life cycle. These controls aim to ensure that risks related to security weaknesses are managed to protect systems.
A.8.26	**Application security requirements.** Information security requirements should be identified, specified and approved when developing or acquiring applications.	True	This enables us to protect information assets stored on or processed through applications by identifying and applying appropriate information security requirements.
A.8.27	**Secure system architecture and engineering principles.** Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.	True	Security controls being implemented for the development function ensures that systems are developed and maintained with security controls designed and implemented throughout the life cycle. Secure engineering principles govern these processes by ensuring that security is integrated into the overall process.

Clause	Clause Description	Is Applicable?	Justification
A.8.28	**Secure coding.** Secure coding principles should be applied to software development.	True	We prevent security risks and vulnerabilities that may arise as a result of poor software coding practices by designing, implementing, and reviewing appropriate secure software coding principles.
A.8.29	**Security testing in development and acceptance.** Security testing processes should be defined and implemented in the development life cycle	True	Security controls being implemented for the development function ensures that systems are developed and maintained with security controls designed and implemented throughout the life cycle. These controls aim to ensure that risks related to security weaknesses are managed to protect systems.
A.8.30	**Outsourced development.** The organization should direct, monitor and review the activities related to outsourced system development.	True	This enables us to ensure that the established information security requirements are adhered to when the system and software development is outsourced to external suppliers.
A.8.31	**Separation of development, test and production environments.** Development, testing and production environments should be separated and secured.	True	Separating the development, testing and operational environments is a fundamental ISMS control to ensure that developers cannot make unauthorized changes between environments which could result in security and operational issues to the environment.
A.8.32	**Change management.** Changes to information processing facilities and information systems should be subject to change management procedures.	True	Change Management is a fundamental ISMS control and ensures that there is a framework to manage how changes are documented, analysed and managed across their life cycle to positively enhance information security requirements. Unmanaged changes can result in major operational and information security risks.
A.8.33	**Test information.** Test information should be appropriately selected, protected and managed.	True	Ensuring that Test data is not a copy of Production data is a vital control as it prevents live data being used in less secure environments reducing risks related to unauthorized access and breaches.
A.8.34	**Protection of information systems during audit testing.** Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.	True	This control is required to manage the risks related to how audits impact on operations and how information provided to auditors is securely managed.