Company	[Company Name]
Document	Statement of Applicability
Classification	Confidential

Version Control

Version	Document Changes	Last Modified By	Date
0.1			

[Company] : Statement of Applicability | ISO 27001:2022 Annex A / ISO 27002:2022 Controls

Classification: Confidential

ISO 27002 Clause	Title	Control Objective	Driver why control is required				Is this Applicable?	Date Last Assessed	Why is this not applicable?
			Business	Risk	Legal	Contract			
5	**Organisational Controls**								
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.	Yes	Yes	Yes	No	Applicable		
5.2	Information security roles and responsibilities	[redacted]	Yes	Yes	No	No	Applicable		
5.3	Segregation of duties	[redacted]	Yes	Yes	Yes	No	Applicable		
5.4	Management Responsibilities	[redacted]	Yes	Yes	Yes	No	Applicable		
5.5	Contact with Authorities	[redacted]	Yes	Yes	Yes	No	Applicable		
5.6	Contact with special interest groups	[redacted]	Yes	Yes	Yes	No	Applicable		
5.7	Threat intelligence	[redacted]	Yes	Yes	Yes	No	Applicable		
5.8	Information security in project management	[redacted]	Yes	Yes	Yes	No	Applicable		
5.9	Inventory of information and other associated assets	[redacted]	Yes	Yes	Yes	No	Applicable		
5.10	Acceptable use of information and other associated assets	[redacted]	Yes	Yes	Yes	No	Applicable		

5.11	Return of Assets	[redacted]	Yes	Yes	Yes	No	Applicable		
5.12	Classification Of Information	[redacted]	Yes	Yes	Yes	No	Applicable		
5.13	Labelling of Information	[redacted]	Yes	Yes	Yes	No	Applicable		
5.14	Information Transfer	[redacted]	Yes	Yes	Yes	No	Applicable		
5.15	Access Control	[redacted]	Yes	Yes	Yes	No	Applicable		
5.16	Identity Management	[redacted]	Yes	Yes	Yes	No	Applicable		
5.17	Authentication information	[redacted]	Yes	Yes	Yes	No	Applicable		
5.18	Access rights	[redacted]	Yes	Yes	Yes	No	Applicable		
5.19	Information security in supplier relationships	[redacted]	Yes	Yes	Yes	No	Applicable		
5.20	Addressing information security within supplier agreements	[redacted]	Yes	Yes	Yes	No	Applicable		
5.21	Managing information security in the ICT supply chain	[redacted]	Yes	Yes	Yes	No	Applicable		
5.22	Monitoring, review and change management of supplier services	[redacted]	Yes	Yes	Yes	No	Applicable		
5.23	Information security for use of cloud services	[redacted]	Yes	Yes	Yes	No	Applicable		
5.24	Information security incident management planning and preparation	[redacted]	Yes	Yes	Yes	No	Applicable		

5.25	**Assessment and decision on information security events**	[redacted]	Yes	Yes	Yes	No	Applicable		
5.26	**Response to information security incidents**	[redacted]	Yes	Yes	Yes	No	Applicable		
5.27	**Learning from information security incidents**	[redacted]	Yes	Yes	Yes	No	Applicable		
5.28	**Collection of evidence**	[redacted]	Yes	Yes	Yes	No	Applicable		
5.29	**Information security during disruption**	[redacted]	Yes	Yes	Yes	No	Applicable		
5.30	**ICT readiness for business continuity**	[redacted]	Yes	Yes	Yes	No	Applicable		
5.31	**Legal, statutory, regulatory and contractual requirements**	[redacted]	Yes	Yes	Yes	No	Applicable		
5.32	**Intellectual property rights**	[redacted]	Yes	Yes	Yes	No	Applicable		
5.33	**Protection of records**	[redacted]	Yes	Yes	Yes	No	Applicable		
5.34	**Privacy and protection of PII**	[redacted]	Yes	Yes	Yes	No	Applicable		
5.35	**Independent review of information security**	[redacted]	Yes	Yes	Yes	No	Applicable		
5.36	**Compliance with policies, rules and standards for information security**	[redacted]	Yes	Yes	Yes	No	Applicable		
5.37	**Documented operating procedures**	[redacted]	Yes	Yes	Yes	No	Applicable		
6	**People Controls**								

6.1	Screening	[redacted]	Yes	Yes	Yes	No	Applicable		
6.2	Terms and conditions of employment	[redacted]	Yes	Yes	Yes	No	Applicable		
6.3	Information security awareness, education and training	[redacted]	Yes	Yes	Yes	No	Applicable		
6.4	Disciplinary process	[redacted]	Yes	Yes	Yes	No	Applicable		
6.5	Responsibilities after termination or change of employment	[redacted]	Yes	Yes	Yes	No	Applicable		
6.6	Confidentiality or non-disclosure agreements	[redacted]	Yes	Yes	Yes	No	Applicable		
6.7	Remote working	[redacted]	Yes	Yes	Yes	No	Applicable		
6.8	Information security event reporting	[redacted]	Yes	Yes	Yes	No	Applicable		
7	**Physical Controls**								
7.1	Physical security perimeters	[redacted]	Yes	Yes	Yes	No	Applicable		
7.2	Physical entry	[redacted]	Yes	Yes	Yes	No	Applicable		
7.3	Securing offices, rooms and facilities	[redacted]	Yes	Yes	Yes	No	Applicable		
7.4	Physical security monitoring	[redacted]	Yes	Yes	Yes	No	Applicable		
7.5	Protecting against physical and environmental threats	[redacted]	Yes	Yes	Yes	No	Applicable		

7.6	Working in secure areas	[redacted]	Yes	Yes	Yes	No	Applicable		
7.7	Clear desk and clear screen	[redacted]	Yes	Yes	Yes	No	Applicable		
7.8	Equipment siting and protection	[redacted]	Yes	Yes	Yes	No	Applicable		
7.9	Security of assets off-premises	[redacted]	Yes	Yes	Yes	No	Applicable		
7.10	Storage media	[redacted]	Yes	Yes	Yes	No	Applicable		
7.11	Supporting utilities	[redacted]	Yes	Yes	Yes	No	Applicable		
7.12	Cabling security	[redacted]	Yes	Yes	Yes	No	Applicable		
7.13	Equipment maintenance	[redacted]	Yes	Yes	Yes	No	Applicable		
7.14	Secure disposal or re-use of equipment	[redacted]	Yes	Yes	Yes	No	Applicable		
8	**Technological Controls**								
8.1	User endpoint devices	[redacted]	Yes	Yes	Yes	No	Applicable		
8.2	Privileged access rights	[redacted]	Yes	Yes	Yes	No	Applicable		
8.3	Information access restriction	[redacted]	Yes	Yes	Yes	No	Applicable		
8.4	Access to source code	[redacted]	Yes	Yes	Yes	No	Applicable		

8.5	Secure authentication	[redacted]	Yes	Yes	Yes	No	Applicable		
8.6	Capacity management	[redacted]	Yes	Yes	Yes	No	Applicable		
8.7	Protection against malware	[redacted]	Yes	Yes	Yes	No	Applicable		
8.8	Management of technical vulnerabilities	[redacted]	Yes	Yes	Yes	No	Applicable		
8.9	Configuration management	[redacted]	Yes	Yes	Yes	No	Applicable		
8.10	Information deletion	[redacted]	Yes	Yes	Yes	No	Applicable		
8.11	Data masking	[redacted]	Yes	Yes	Yes	No	Applicable		
8.12	Data leakage prevention	[redacted]	Yes	Yes	Yes	No	Applicable		
8.13	Information backup	[redacted]	Yes	Yes	Yes	No	Applicable		
8.14	Redundancy of information processing facilities	[redacted]	Yes	Yes	Yes	No	Applicable		
8.15	Logging	[redacted]	Yes	Yes	Yes	No	Applicable		
8.16	Monitoring activities	[redacted]	Yes	Yes	Yes	No	Applicable		
8.17	Clock synchronization	[redacted]	Yes	Yes	Yes	No	Applicable		
8.18	Use of privileged utility programs	[redacted]	Yes	Yes	Yes	No	Applicable		

8.19	Installation of software on operational systems	[redacted]	Yes	Yes	Yes	No	Applicable		
8.20	Networks security	[redacted]	Yes	Yes	Yes	No	Applicable		
8.21	Security of network services	[redacted]	Yes	Yes	Yes	No	Applicable		
8.22	Segregation of networks	[redacted]	Yes	Yes	Yes	No	Applicable		
8.23	Web filtering	[redacted]	Yes	Yes	Yes	No	Applicable		
8.24	Use of cryptography	[redacted]	Yes	Yes	Yes	No	Applicable		
8.25	Secure development life cycle	[redacted]	Yes	Yes	Yes	No	Applicable		
8.26	Application security requirements	[redacted]	Yes	Yes	Yes	No	Applicable		
8.27	Secure system architecture and engineering principles	[redacted]	Yes	Yes	Yes	No	Applicable		
8.28	Secure coding	[redacted]	Yes	Yes	Yes	No	Applicable		
8.29	Security testing in development and acceptance	[redacted]	Yes	Yes	Yes	No	Applicable		
8.30	Outsourced development	[redacted]	Yes	Yes	Yes	No	Applicable		
8.31	Separation of development, test and production environments	[redacted]	Yes	Yes	Yes	No	Applicable		
8.32	Change management	[redacted]	Yes	Yes	Yes	No	Applicable		

8.33	**Test information**	[redacted]	Yes	Yes	Yes	No	Applicable		
8.34	**Protection of information systems during audit testing**	[redacted]	Yes	Yes	Yes	No	Applicable		

[Company] : Statement of Applicability | ISO27001:2013 Annex A / ISO27002:2013 Controls

Classification: Confidential

ISO 27002 Clause	Title	Control Objective	Driver why control is required				Is this Applicable?	Date Last Assessed	Why is this not applicable?
			Business	Risk	Legal	Contract			
5	**Information security policies**								
5.1	**Management direction for information security**	**To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.**							
5.1.1	**Policies for information security**	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Yes	Yes	Yes	No	Applicable		
5.1.2	**Review of the policies for information security**	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Yes	Yes	No	No	Applicable		
6	**Organisation of information security**								
6.1	**Internal organisation**	**Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation.**							
6.1.1	**Information security roles and responsibilities**	All information security responsibilities shall be defined and allocated.	Yes	Yes	No	No	Applicable		
6.1.2	**Segregation of duties**	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.	Yes	Yes	No	No	Applicable		
6.1.3	**Contact with authorities**	Appropriate contacts with relevant authorities shall be maintained	Yes	Yes	No	No	Applicable		
6.1.4	**Contact with special interest groups**	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Yes	Yes	No	No	Applicable		
6.1.5	**Information security in project management**	Information security shall be addressed in project management, regardless of the type of the project.	Yes	Yes	No	No	Applicable		

6.2	**Mobile devices and teleworking**	**Objective: To ensure the security of teleworking and use of mobile devices.**							
6.2.1	**Mobile device policy**	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Yes	Yes	No	No	Applicable		
6.2.2	**Teleworking**	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Yes	Yes	No	No	Applicable		
7	**Human resource security**								
7.1	**Prior to Employment**	**Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.**							
7.1.1	**Screening**	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Yes	Yes	No	No	Applicable		
7.1.2	**Terms and conditions of employment**	The contractual agreements with employees and contractors shall state their and the organisation's responsibilities for information security.	Yes	Yes	No	No	Applicable		
7.2	**During employment**	**Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.**							
7.2.1	**Management responsibilities**	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.	Yes	Yes	No	No	Applicable		
7.2.2	**Information security awareness, education and training**	All employees of the organisation and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function.	Yes	Yes	No	No	Applicable		
7.2.3	**Disciplinary process**	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Yes	Yes	No	No	Applicable		
7.3	**Termination or change of employment**	**Objective: Does the organisation ensure that employees, contractors and third party users exit the organisation or change employment in an orderly manner?**							
7.3.1	**Termination or change of employment responsibilities**	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Yes	Yes	No	No	Applicable		
8	**Asset management**								

8.1	**Responsibility for assets**	**Objective: To identify organisational assets and define appropriate protection responsibilities.**							
8.1.1	**Inventory of assets**	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Yes	Yes	No	No	Applicable		
8.1.2	**Ownership of assets**	Assets maintained in the inventory shall be owned.	Yes	Yes	No	No	Applicable		
8.1.3	**Acceptable use of assets**	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Yes	Yes	No	No	Applicable		
8.1.4	**Return of assets**	All employees and external party users shall return all of the organisational assets in their possession upon termination of their employment, contract or agreement.	Yes	Yes	No	No	Applicable		
8.2	**Information classification**	**Objective: Does the organisation ensure that information receives an appropriate level of protection?**							
8.2.1	**Classification of information**	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Yes	Yes	No	No	Applicable		
8.2.2	**Labelling of information**	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.	Yes	Yes	No	No	Applicable		
8.2.3	**Handling of assets**	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.	Yes	Yes	No	No	Applicable		
8.3	**Media handling**	**Objective: Management of removable media**							
8.3.1	**Management of removable media**	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.	Yes	Yes	No	No	Applicable		
8.3.2	**Disposal of media**	Media shall be disposed of securely when no longer required, using formal procedures.	Yes	Yes	No	No	Applicable		
8.3.3	**Physical media transfer**	Media containing information shall be protected against unauthorised access, misuse or corruption during transportation.	Yes	Yes	No	No	Applicable		
9	**Access control**								

9.1	**Business requirements for access control**	**Objective: To limit access to information and information processing facilities.**							
9.1.1	**Access control policy**	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Yes	Yes	No	No	Applicable		
9.1.2	**Access to networks and network services**	Users shall only be provided with access to the network and network services that they have been specifically authorised to use	Yes	Yes	No	No	Applicable		
9.2	**User access management**	**Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.**							
9.2.1	**User registration and de-registration**	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Yes	Yes	No	No	Applicable		
9.2.2	**User access provisioning**	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Yes	Yes	No	No	Applicable		
9.2.3	**Management of privileged access rights**	The allocation and use of privileged access rights shall be restricted and controlled.	Yes	Yes	No	No	Applicable		
9.2.4	**Management of secret authentication information of users**	The allocation of secret authentication information shall be controlled through a formal management process.	Yes	Yes	No	No	Applicable		
9.2.5	**Review of user access rights**	Asset owners shall review users' access rights at regular intervals	Yes	Yes	No	No	Applicable		
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 shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Yes	Yes	No	No	Applicable		
9.3	**User responsibilities**	**Objective: To make users accountable for safeguarding their authentication information.**							
9.3.1	**Use of secret authentication information**	Users shall be required to follow the organisation's practices in the use of secret authentication information.	Yes	Yes	No	No	Applicable		
9.4	**System and application access control**	**Objective: To prevent unauthorised access to systems and applications.**							
9.4.1	**Information access restriction**	Access to information and application system functions shall be restricted in accordance with the access control policy.	Yes	Yes	No	No	Applicable		

9.4.2	**Secure log-on procedures**	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Yes	Yes	No	No	Applicable		
9.4.3	**Password management system**	Password management systems shall be interactive and shall ensure quality passwords.	Yes	Yes	No	No	Applicable		
9.4.4	**Use of privileged utility programs**	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Yes	Yes	No	No	Applicable		
9.4.5	**Access control to program source code**	Access to program source code shall be restricted.	Yes	Yes	No	No	Applicable		
10	**Cryptography**								
10.1	**Cryptographic controls**	**Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.**							
10.1.1	**Policy on the use of cryptographic controls**	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Yes	Yes	No	No	Applicable		
10.1.2	**Key management**	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Yes	Yes	No	No	Applicable		
11	**Physical and environmental security**								
11.1	**Secure areas**	**Objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.**							
11.1.1	**Physical security perimeter**	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Yes	Yes	No	No	Applicable		
11.1.2	**Physical entry controls**	Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.	Yes	Yes	No	No	Applicable		
11.1.3	**Securing offices, rooms and facilities**	Physical security for offices, rooms and facilities shall be designed and applied.	Yes	Yes	No	No	Applicable		
11.1.4	**Protecting against external and environmental threats**	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	Yes	Yes	No	No	Applicable		

11.1.5	**Working in secure areas**	Procedures for working in secure areas shall be designed and applied.	Yes	Yes	No	No	Applicable		
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 shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.	Yes	Yes	No	No	Applicable		
11.2	**Equipment**	**Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.**							
11.2.1	**Equipment siting and protection**	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.	Yes	Yes	No	No	Applicable		
11.2.2	**Supporting utilities**	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	Yes	No	No	Applicable		
11.2.3	**Cabling security**	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Yes	Yes	No	No	Applicable		
11.2.4	**Equipment maintenance**	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Yes	Yes	No	No	Applicable		
11.2.5	**Removal of assets**	Equipment, information or software shall not be taken off-site without prior authorisation.	Yes	Yes	No	No	Applicable		
11.2.6	**Security of equipment and assets off premises**	Security shall be applied to off-site assets taking into account the different risks of working outside the organisation's premises.	Yes	Yes	No	No	Applicable		
11.2.7	**Secure disposal or reuse of equipment**	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Yes	Yes	No	No	Applicable		
11.2.8	**Unattended user equipment**	Users shall ensure that unattended equipment has appropriate protection.	Yes	Yes	No	No	Applicable		
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 shall be adopted.	Yes	Yes	No	No	Applicable		
12	**Operations security**								
12.1	**Operational procedures and responsibilities**	**Objective: To ensure correct and secure operations of information processing facilities.**							

12.1.1	**Documented operating procedures**	Operating procedures shall be documented and made available to all users who need them.	Yes	Yes	No	No	Applicable		
12.1.2	**Change management**	Changes to the organisation, business processes, information processing facilities and systems that affect information security shall be controlled.	Yes	Yes	No	No	Applicable		
12.1.3	**Capacity management**	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Yes	Yes	No	No	Applicable		
12.1.4	**Separation of development, testing and operational environments**	Development, testing, and operational environments shall be separated to reduce the risks of unauthorised access or changes to the operational environment.	Yes	Yes	No	No	Applicable		
12.2	**Protection from malware**	**Objective: To ensure that information and information processing facilities are protected against malware.**							
12.2.1	**Controls against malware**	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Yes	Yes	No	No	Applicable		
12.3	**Backup**	**Objective: To protect against loss of data.**							
12.3.1	**Information backup**	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Yes	Yes	No	No	Applicable		
12.4	**Logging and monitoring**	**Objective: To record events and generate evidence.**							
12.4.1	**Event logging**	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Yes	Yes	No	No	Applicable		
12.4.2	**Protection of log information**	Logging facilities and log information shall be protected against tampering and unauthorised access.	Yes	Yes	No	No	Applicable		
12.4.3	**Administrator and operator logs**	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Yes	Yes	No	No	Applicable		
12.4.4	**Clock synchronisation**	The clocks of all relevant information processing systems within an organisation or security domain shall be synchronised to a single reference time source.	Yes	Yes	No	No	Applicable		
12.5	**Control of operational software**	**Objective: To ensure the integrity of operational systems.**							

12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	Yes	Yes	No	No	Applicable		
12.6	Technical vulnerability management	Objective: To prevent exploitation of technical vulnerabilities.							
12.6.1	Management of technical vulnerabilities	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Yes	Yes	No	No	Applicable		
12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	Yes	Yes	No	No	Applicable		
12.7	Information systems audit considerations	Objective: To minimise the impact of audit activities on operational systems.							
12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	Yes	Yes	No	No	Applicable		
13	Communications security								
13.1	Network security management	Objective: To ensure the protection of information in networks and its supporting information processing facilities.							
13.1.1	Network controls	Networks shall be managed and controlled to protect information in systems and applications.	Yes	Yes	No	No	Applicable		
13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Yes	Yes	No	No	Applicable		
13.1.3	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	Yes	Yes	No	No	Applicable		
13.2	Information transfer	Objective: To ensure the protection of information in networks and its supporting information processing facilities.							
13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Yes	Yes	No	No	Applicable		
13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organisation and external parties.	Yes	Yes	No	No	Applicable		

13.2.3	**Electronic messaging**	Information involved in electronic messaging shall be appropriately protected.	Yes	Yes	No	No	Applicable		
13.2.4	**Confidentiality or non-disclosure agreements**	Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, regularly reviewed and documented.	Yes	Yes	No	No	Applicable		
14	**System acquisition, development and maintenance**								
14.1	**Security requirements of information systems**	**Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.**							
14.1.1	**Information security requirements analysis and specification**	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Yes	Yes	No	No	Applicable		
14.1.2	**Securing application services on public networks**	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.	Yes	Yes	No	No	Applicable		
14.1.3	**Protecting application services transactions**	Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.	Yes	Yes	No	No	Applicable		
14.2	**Security in development and support processes**	**Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.**							
14.2.1	**Secure development policy**	Rules for the development of software and systems shall be established and applied to developments within the organisation.	Yes	Yes	No	No	Applicable		
14.2.2	**System change control procedures**	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Yes	Yes	No	No	Applicable		
14.2.3	**Technical review of applications after operating platform changes**	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organisational operations or security.	Yes	Yes	No	No	Applicable		
14.2.4	**Restrictions on changes to software packages**	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Yes	Yes	No	No	Applicable		
14.2.5	**Secure system engineering principles**	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	Yes	Yes	No	No	Applicable		
14.2.6	**Secure development environment**	organisations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Yes	Yes	No	No	Applicable		

14.2.7	**Outsourced development**	The organisation shall supervise and monitor the activity of outsourced system development.	Yes	Yes	No	No	Applicable		
14.2.8	**System security testing**	Testing of security functionality shall be carried out during development.	Yes	Yes	No	No	Applicable		
14.2.9	**System acceptance testing**	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions	Yes	Yes	No	No	Applicable		
14.3	**Test data**	**Objective: To ensure the protection of data used for testing.**							
14.3.1	**Protection of test data**	Test data shall be selected carefully, protected and controlled.	Yes	Yes	No	No	Applicable		
15	**Supplier Relationships**								
15.1	**Information security in supplier relationships**	**Objective: To ensure protection of the organisation's assets that is accessible by suppliers.**							
15.1.1	**Information security policy for supplier relationships**	Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets shall be agreed with the supplier and documented.	Yes	Yes	No	No	Applicable		
15.1.2	**Addressing security within supplier agreements**	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation's information.	Yes	Yes	No	No	Applicable		
15.1.3	**Information and communication technology supply chain**	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Yes	Yes	No	No	Applicable		
15.2	**Supplier service delivery management**	**Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.**							
15.2.1	**Monitoring and review of supplier services**	Organisations shall regularly monitor, review and audit supplier service delivery.	Yes	Yes	No	No	Applicable		
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, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	Yes	Yes	No	No	Applicable		
16	**Information security incident management**								

16.1	**Management of information security incidents and improvements**	**Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.**							
16.1.1	**Responsibilities and procedures**	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Yes	Yes	No	No	Applicable		
16.1.2	**Reporting information security events**	Information security events shall be reported through appropriate management channels as quickly as possible.	Yes	Yes	No	No	Applicable		
16.1.3	**Reporting information security weaknesses**	Employees and contractors using the organisation's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	Yes	Yes	No	No	Applicable		
16.1.4	**Assessment of and decision on information security events**	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Yes	Yes	No	No	Applicable		
16.1.5	**Response to information security incidents**	Information security incidents shall be responded to in accordance with the documented procedures.	Yes	Yes	No	No	Applicable		
16.1.6	**Learning from information security incidents**	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Yes	Yes	No	No	Applicable		
16.1.7	**Collection of evidence**	The organisation shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Yes	Yes	No	No	Applicable		
17	**Information security aspects of business continuity management**								
17.1	**Information security continuity**	**Objective: Information security continuity should be embedded in the organisation's business continuity management systems.**							
17.1.1	**Planning information security continuity**	The organisation shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Yes	Yes	No	No	Applicable		
17.1.2	**Implementing information security continuity**	The organisation shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Yes	Yes	No	No	Applicable		
17.1.3	**Verify, review and evaluate information security continuity**	The organisation shall 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.	Yes	Yes	No	No	Applicable		
17.2	**Redundancies**	**Objective: To ensure availability of information processing facilities.**							

17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes	Yes	No	No	Applicable		
18	**Compliance**								
18.1	**Compliance with legal and contractual requirements**	**Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements**							
18.1.1	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organisation's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organisation.	Yes	Yes	No	No	Applicable		
18.1.2	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Yes	Yes	No	No	Applicable		
18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislatory, regulatory, contractual and business requirements.	Yes	Yes	No	No	Applicable		
18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Yes	Yes	No	No	Applicable		
18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Yes	Yes	No	No	Applicable		
18.2	**Information security reviews**	**Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements**							
18.2.1	Independent review of information security	The organisation's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	Yes	Yes	No	No	Applicable		
18.2.2	Compliance with security policies and standards	Managers shall 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.	Yes	Yes	No	No	Applicable		
18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organisation's information security policies and standards.	Yes	Yes	No	No	Applicable		