Document Name	Statement of Applicability (SOA)
Document Owner	ISMS Manager
Classification	Internal Use Only

Date of Release	Version	Summary
7th Septemer 202	1.0	First Release

Brief Summary

 - Statement of Applicability is a mandatory document that explains:

- Applicable and Not Applicable controls

- Management system Controls, with reference to risk owner and associated documentation

-Annexure Controls, with reference to applicable and not applicable controls. For those that are applic

Term	Explanation
Risk Owner/s	Risk owners are those that are responsible for the control requirements. When a control requirements relates to a policy - this is generally someone at the PG central level, but when it comes to evidences these names can vary depending upon the kind of control references.

S. No.	ISO 27001	Controls Description	Applicable (Yes or No)	Risk Owner	Documentation Evidences and associated artefacts
1	4.1 Understanding the organization and its context	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system. NOTE: Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009.	Yes	ISMS Manager	HC-ISMS Context
2	4.2 Understanding the needs and expectations of interested parties	The organization shall determine: a) interested parties that are relevant to the information security management system; and b) the requirements of these interested parties relevant to information security. NOTE - The requirements of interested parties may include legal and regulatory requirements and contractual obligations.	Yes	ISMS Manager	HC-ISMS Context
3	4.3 Determining the scope of the information security management system	The organization shall determine the boundaries and applicability of the Information security management system to establish its scope. When determining this scope, the organization shall consider: a) the external and internal issues referred to in 4.1 b) the requirements referred to in 4.2 ;and c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations. The scope shall be available as documented information.	Yes	ISMS Manager	Statement - ISMS Scope

4	4.4 Information security management system	The organization shall establish, implement, maintain and continually Improve an information security management system, In accordance with the requirements of this International Standard.	Yes	Top Management	Policy - ISMS
5	5.1 Leadership and commitment	Top management shall demonstrate leadership and commitment with respect to the information security management system by: a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization; b) ensuring the integration of the information security management system requirements Into the organization's processes; c) ensuring that the resources needed for the information security management system ate available; d) communicating the importance of effective information security management and of conforming to the information security management system requirements; e) ensuring that the information Security management system achieves its intended outcome(s); f) directing and supporting persons to contribute to the effectiveness of the information security management system; g) promoting continual improvement; and h) supporting other relevant management roles to demonstrate their leadership as 'it applies to their areas of responsibility.	Yes	Top Management	Policy - ISMS Roles and responsibilities

6	5.2 Policy	Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; and d) includes a commitment to continual improvement of the information security management system. The information security policy shall: e) be available as documented information; f) be communicated within the organization; and g) be available to interested parties, as appropriate.	Yes	ISMS Manager	Policy - ISMS
7	5.3 Organizational roles, responsibilities and authorities	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated. Top management shall assign the responsibility and authority for: a) ensuring that the information security management system conforms to the requirements of this International Standard; and b) reporting on the performance of the information security management system to top management NOTE: Top management may also assign responsibilities and authorities for reporting performance of the information security management system within the organization.	Yes	ISMS Manager	Policy - ISMS Roles and responsibilities

8	6.1.1 General	When planning for the information security management system, the organization shall consider the; issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the Information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement. The organization shall plan: d) actions to address these risks and opportunities; and e) how to 1) integrate and implement the actions into its information security management system processes; and 2) evaluate the effectiveness of these actions.	Yes	ISMS Manager	Procedure - ISMS Risk Assessment and Risk Management
9	6.1.2 Information security risk assessment	The organization shall define and apply an information security risk assessment process that: a) establishes and maintains information security risk criteria. b) ensures that repeated information security risk assessments produce consistent, valid and comparable results; c) identifies the information security risks: d) analyses the information security risks e) evaluates the information security risks: The organization shall retain documented information about the information security risk assessment process.	Yes	ISMS Manager	Procedure - ISMS Risk Assessment and Risk Management

10	6.1.3 Information security risk treatment	security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results; b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen; NOTE Organizations can design controls as required, or identify them from any source. c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted; NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked. NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed. d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A; e) formulate an information security risk treatment plan; and f) obtain risk owners’ approval of the information security risk treatment plan and acceptance of the residual information security risks. The organization shall retain documented information about the information security risk treatment process.	Yes	ISMS Manager	Procedure - ISMS Risk Assessment and Risk Management

11	6.2 Information security objectives and plans to achieve them	The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall: a) be consistent with the information security policy; b) be measurable (if practicable); c) take into account applicable information security requirements, and results from risk assessment and risk treatment; d) be communicated; and e) be updated as appropriate. The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organization shall determine: f) what will be done; g) what resources will be required; h) who will be responsible: i) when It will be completed: and j) how the results will be evaluated.	Yes	ISMS Manager	Procedure - ISMS Monitoring
12	7.1 Resources	The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual Improvement of the information security management system.	Yes	ISMS Manager	Procedure - ISMS Risk Assessment and Risk Management

13	7.2 Competence	The organization shall: a) determine the necessary competence of person(s) doing work under its control that affects its information security performance: b) ensure that these persons are competent on the basis of appropriate education, training, or experience c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and d) retain appropriate documented information as evidence of competence. NOTE: Applicable actions may include, for example: the provision of training to the mentoring of or the re-assignment of current employees; or the hiring or contracting of competent persons.	Yes	ISMS Manager	Policy – ISMS Education, Training and Awareness
14	7.3 Awareness	Persons doing work under the organization's control shall be aware of: a) the information security policy; b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and c) the implications of not conforming with the information security management system requirements.	Yes	ISMS Manager	Policy – ISMS Education, Training and Awareness
15	7.4 Communication	The organization shall determine the need for internal and external communications relevant to the information security management system including: a) on what to communicate; b) when to communicate; c) with whom to communicate; d) who shall communicate; and e) the processes by which communication shall be effected.	Yes	ISMS Manager	Process - ISMS Program Communication

16	7.5.1 General	The organization's information security management system shall Include: a) documented information required by this International Standard; and b) documented information determined by the organization as being necessary for the effectiveness of the information security management system. NOTE: The extent of documented information for an information security management system can differ from one organization to another due to: 1) the size of organization and its type of activities, processes, products .and services; 2) the complexity of processes and their interactions; and 3) the competence of persons.	Yes	ISMS Manager	Procedure - Document Management
17	7.5.2 Creating and updating	When creating and updating documented information the organization shall ensure appropriate: a) identification and description (e.g. a title, date, author, or reference number); b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and c) review and approval for suitability and adequacy.	Yes	ISMS Manager	Procedure - Document Management

18	7.5.3 Control of documented information	Documented information required by the information security management system and by this International Standard shall be controlled to ensure: a) it is available and suitable for use, where and when it Is needed; and b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity). For the control of documented information, the organization shall address the following activities, as applicable: c) distribution, access, retrieval and use; d) storage and preservation, including the preservation of legibility; e) control of changes (e.g. Version control): and t) retention and disposition. Documented information of external origin. determined by the organization to be necessary for the planning and operation of the information security management system. shall be identified as appropriate, and controlled. NOTE: Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information. etc.	Yes	ISMS Manager	Procedure - Document Management

19	8.1 Operational planning and control	The organization shall plan, implement and control the processes needed to meet information security requirements, and to Implement the actions determined in 6.1. The organization shall also Implement plans to achieve Information security objectives determined in .6.2 The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary. The organization shall ensure that outsourced processes are determined and controlled.	Yes	ISMS Manager	Statement of Applicability
20	8.2 Information security risk assessment	The organization shall perform information security risk assessments at planned Intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a) The organization shall retain documented information of the results of the information security risk assessments.	Yes	ISMS Manager	Procedure - ISMS Risk Assessment and Risk Management
21	8.3 Information security risk treatment	The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.	Yes	ISMS Manager	Procedure - ISMS Risk Assessment and Risk Management

22	9.1 Monitoring, measurement, analysis and evaluation	The organization shall evaluate the information security performance and the effectiveness of the information security management system. The organization shall determine: a) what needs to be monitored and measured, Including information security processes and controls; b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results; NOTE The methods selected should produce comparable and reproducible results to be considered valid. c) when the monitoring and measuring shall be performed; d) who shall monitor and measure; e) when the results from monitoring and measurement shall be analysed and evaluated; and f) who shall analyse and evaluate these results. The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.	Yes	ISMS Manager	Procedure - ISMS Monitoring

23	9.2 Internal audit	The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system: a) conforms to 1) the organization's own requirements for its information security management system; and 2) the requirements of this International Standard; b) is effectively implemented and maintained. The organization shall: c) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits; d) define the audit criteria and scope for each audit; e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process; f) ensure that the results of the audits are reported to relevant management; and g) retain documented information as evidence of the audit programme(s) and the audit results.	Yes	ISMS Manager	Process - Internal Audit

24	9.3 Management Review	Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of: a) the status of actions from previous management reviews; b) changes in external and internal issues that are relevant to the information security management system; c) feedback on the information security performance d) feedback from interested parties; e) results of risk assessment and status of risk treatment plan; and t) opportunities for continual improvement. The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. The organization shall retain documented information as evidence of the results of management reviews.	Yes	ISMS Manager	Procedure-Management Review

25	10.1 Non conformity and corrective action	When a nonconformity occurs, the organization shall: a) react to the nonconformity, and as applicable: 1) take action to control and correct it; and 2) deal with the consequences; b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur; c) implement any action needed; d) review the effectiveness of any corrective action taken: and e) make changes to the information security management system, if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of: f) the nature of the nonconformities and any subsequent actions taken, and g) the results of any corrective action.	Yes	ISMS Manager	Process - Internal Audit
26	10.2 Continual improvement	The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.	Yes	ISMS Manager	Procedure - ISMS Risk Assessment and Risk Management

S. No.	ISO 27001	Controls Description	Applicable (Yes or No)	Risk Owner	Documentation Evidences and associated artefacts
27	A.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	Top Management	Policy - ISMS
28	A.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	Top Management	Policy - ISMS
29	A.6.1.1 - Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	Yes	Top Management	Policy - ISMS Roles and responsibilities
30	A.6.1.2 - Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.	Yes	Top Management	Policy - ISMS Roles and responsibilities
31	A.6.1.3 - Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	Yes	Head - IT Operations	Procedure-Security-Incident-Response
32	A.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	Head - IT Operations	Procedure-Security-Incident-Response
33	A.6.1.5 - Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	Yes	Head - IT Operations	Process - Security-in-Project-management Policy-Secure-Software-Development-Lifecycle

34	A.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	Head - IT Operations	Policy - Acceptable Usage
35	A.6.2.2 - Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Yes	Head - IT Operations	Policy - Acceptable Usage
36	A.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. Employees below Middle Management Reference Check 1) Referees (Prev Employer) 2) Educational and Professional Certification 3) Identity Check 4) Proof of address Optional - Risk based a) Criminal Check b) Prev employer check Middle Management and above a) Criminal Check b) Prev employer check	Yes	Head - Human Resources	Manual - Human Resources
37	A.7.1.2 - Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization’s responsibilities for information security.	Yes	Head - Human Resources	Manual - Human Resources

38	A.7.2.1 - Management responsibilities	Management shall require all employees and contractors to apply information security principles in accordance with the established policies and procedures of the organization.	Yes	Head - Human Resources	Policy - Acceptable Usage
39	A.7.2.2 - Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Yes	Head - Human Resources	Policy – ISMS Education, Training and Awareness
40	A.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	Head - Human Resources	Manual - Human Resources
41	A.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	Head - Human Resources	Manual - Human Resources
42	A.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	Head - IT Operations	Asset Inventory
43	A.8.1.2 - Ownership of assets	Assets maintained in the inventory shall be owned.	Yes	ISMS Manager	Policy - Acceptable Usage
44	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 shall be identified, documented and implemented.	Yes	ISMS Manager	Policy - Acceptable Usage

45	A.8.1.4 - Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement. Commercial Settlement Payroll next cycle	Yes	Head - Human Resources	Manual - Human Resources
46	A.8.2.1 - Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.	Yes	ISMS Manager	Information Classification Procedure
47	A.8.2.2 - Labeling 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 organization.	Yes	Head - IT Operations	Information Labelling Procedure
48	A.8.2.3 - Handling of assets	Procedures for handling information assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	ISMS Manager	Asset Handling Procedure
49	A.8.3.1 - Management of removable media	Procedures shall be implemented for management of removable media in accordance with the classification adopted by the organization.	Yes	Head - IT Operations	Procedure for the Management of Removable Media
50	A.8.3.2 - Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	Yes	Head - IT Operations	Policy - Media Management
51	A.8.3.3 - Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Yes	Head - IT Operations	Policy - Media Management
52	A.9.1.1 - Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Yes	Head - IT Operations	Policy - Access Control
53	A.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 authorized to use.	Yes	Head - IT Operations	Policy - Access Control
54	A.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	Head - IT Operations	Policy - Access Control

55	A.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	Head - IT Operations	Policy - Access Control
56	A.9.2.3 - Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	Yes	Head - IT Operations	Policy - Access Control
57	A.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	Head - IT Operations	Policy - Access Control
58	A.9.2.5 - Review of user access rights	Asset owners shall review users' access rights at regular intervals.	Yes	Head - IT Operations	Policy - Access Control
59	A.9.2.6 - Removal or adjustment of access rights	The access rights of all employees and external users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Yes	Head - IT Operations	Policy - Access Control
60	A.9.3.1 - Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	Yes	Head - IT Operations	Policy - Acceptable Usage
61	A.9.4.1 - Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Yes	Head - IT Operations	Access Control Policy
62	A.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	Head - IT Operations	Policy - Cloud Security
63	A.9.4.3 - Password management system	Password management systems shall be interactive and shall ensure quality passwords.	Yes	Head - IT Operations	Policy - Cloud Security
64	A.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	Head - IT Operations	Change Management Process

65	A.9.4.5 - Access control to program source code	Access to program source code shall be restricted.	Yes	Head - Software Development	Process-Secure-Software-Development
66	A.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	Head - IT Operations	Cryptographic Policy
67	A.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	Head - IT Operations	Policy - Cloud Security
68	A.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	All employees	Policy - Acceptable Use
69	A.11.1.2 - Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Yes	All employees	Policy - Acceptable Use
70	A.11.1.3 - Securing office, room and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	Yes	All employees	Policy - Acceptable Use
71	A.11.1.4 - Protecting against external end environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	Yes	All employees	Policy - Acceptable Use
72	A.11.1.5 - Working in secure areas	Procedures for working in secure areas shall be designed and applied.	Yes	All employees	Policy - Acceptable Use
73	A.11.1.6 - Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Yes	All employees	Policy - Acceptable Use
74	A.11.2.1 - Equipment sitting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Yes	All employees	Policy - Acceptable Use
75	A.11.2.2 - Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	All employees	Policy - Acceptable Use

76	A.11.2.3 - Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Yes	All employees	Policy - Acceptable Use
77	A.11.2.4 - Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Yes	All employees	Policy - Acceptable Use
78	A.11.2.5 - Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	Yes	All employees	Policy - Acceptable Use
79	A.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 organization’s premises.	Yes	Head - IT Operations	Policy - Acceptable Usage
80	A.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	Head - IT Operations	Procedure – Desktop and Notebook Installation (end user device management)
81	A.11.2.8 - Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	Yes	Head - IT Operations	Policy - Acceptable Usage
82	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 shall be adopted.	Yes	All employees	Clear Desk and Clear Screen Policy
83	A.12.1.1 - Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	Yes	Head - IT Operations	Individual Team Specific Documentation
84	A.12.1.2 - Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Yes	Head - IT Operations	Change Management Process
85	A.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	Head - IT Operations	Annual Capacity Plan
86	A.12.1.4 - Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	Yes	Head - IT Operations	Policy - Cloud Security

87	A.12.2.1 - Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Yes	Head - IT Operations	Policy - Cloud Security
88	A.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	Head - IT Operations	Backup Policy
89	A.12.4.1 - Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Yes	Head - IT Operations	Logging and Monitoring Policy
90	A.12.4.2 - Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Yes	Head - IT Operations	Policy - Cloud Security
91	A.12.4.3 - Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Yes	Head - IT Operations	Policy - Cloud Security
92	A.12.4.4 - Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.	Yes	Head - IT Operations	Policy - Cloud Security
93	A.12.5.1 - Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	Yes	Head - IT Operations	Change Management Process
94	A.12.6.1 - Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization’s exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Yes	Head - IT Operations	Policy - Cloud Security
95	A.12.6.2 - Restrictions on software installations	Rules governing the installation of software by users shall be established and implemented.	Yes	Head - IT Operations	Change Management Process

96	A.12.7.1 - Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.	Yes	Head - IT Operations	Process - Internal Audit
97	A.13.1.1 - Network controls	Networks shall be managed and controlled to protect information in systems and applications.	Yes	Head - IT Operations	Policy - Cloud Security
98	A.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	Head - IT Operations	Policy - Cloud Security
99	A.13.1.3 - Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	Yes	Head - IT Operations	Policy - Cloud Security
100	A.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	Head - IT Operations	Information Transfer Policies and Procedure
101	A.13.2.2 - Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	Yes	Head - IT Operations	Policy - Supplier Risk Management
102	A.13.2.3 - Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	Yes	Head - IT Operations	Policy - Cloud Security
103	A.13.2.4 - Confidentiality or non-disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information shall be identified, regularly reviewed and documented.	Yes	Head - Supplier Management	Policy - Supplier Risk Management

104	A.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	Head - IT Operations	Change Management Process
105	A.14.1.2 - Securing applications services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Yes	Head - IT Operations	Policy - Cloud Security
106	A.14.1.3 - Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Yes	Head - IT Operations	Process-Secure-Software-Development
107	A.14.2.1 - Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	Yes	Head - Software Development	Process-Secure-Software-Development
108	A.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	Head - Software Development	Change Management Process
109	A.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 organizational operations or security.	Yes	Head - IT Operations	Change Management Process
110	A.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.	No	Not Applicable	Not Applicable
111	A.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	Head - Software Development	Process-Secure-Software-Development

112	A.14.2.6 - Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Yes	Head - Software Development	Policy - Cloud Security
113	A.14.2.7 - Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	No	Not Applicable	Not Applicable
114	A.14.2.8 - System security testing	Testing of security functionality shall be carried out during development.	Yes	Head - Software Development	Process-Secure-Software-Development
115	A.14.2.9 - System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Yes	Head - Software Development	Process-Secure-Software-Development
116	A.14.3.1 - Protection of test data	Test data shall be selected carefully, protected and controlled.	Yes	Head - Software Development	Process-Secure-Software-Development
117	A.15.1.1 - Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	Yes	Head - Supplier Management	Policy - Supplier Risk Management
118	A.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 organization's information	Yes	Head - Supplier Management	Policy - Supplier Risk Management
119	A.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	Head - Supplier Management	Policy - Supplier Risk Management
120	A.15.2.1 - Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	Yes	Head - Supplier Management	Policy - Supplier Risk Management

121	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, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	Yes	Head - Supplier Management	Policy - Supplier Risk Management
122	A.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	Head - IT Operations	Procedure-Security-Incident-Response Policy - Incident Management
123	A.16.1.2 - Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	Yes	Head - IT Operations	Policy - Acceptable Usage
124	A.16.1.3 - Reporting information security weaknesses	Employees and contractors using the organization’s information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	Yes	Head - IT Operations	Policy - Acceptable Usage
125	A.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	Head - IT Operations	Procedure-Security-Incident-Response
126	A.16.1.5 - Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Yes	Head - IT Operations	Procedure-Security-Incident-Response
127	A.16.1.6 - Learning from information security incidents	Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Yes	ISMS Manager	Procedure-Security-Incident-Response
128	A.16.1.7 - Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Yes	Head - IT Operations	Information Security Incident Response Procedure

129	A.17.1.1 - Planning information security continuity	The organization 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	Head - IT Operations	Business/IT continuity Plan
130	A.17.1.2 - Implementing information security continuity	The organization 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	Head - IT Operations	Business/IT continuity Plan
131	A.17.1.3 - Verify, review and evaluate information security continuity	The organization 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	Head - IT Operations	Business/IT continuity Plan
132	A.17.2.1 - Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes	Head - IT Operations	Availability Management Policy
133	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 shall be explicitly identified, documented and kept up to date for each information system and the organization.	Yes	Head - Legal	Compliance with Legal requirements
134	A.18.1.2 - Intellectual property rights (IPR)	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	Head - Legal	License Register
135	A.18.1.3 - Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements.	Yes	Head - Legal	Policy - Information-Retention and Destruction Methods
136	A.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	Head - Legal	Policy - Privacy

137	A.18.1.5 - Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Yes	Head - IT Operations	Policy - Cloud Security Encryption Policy Website Certificate Encryption Status @ Rest & Transmission
138	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) shall be reviewed independently at planned intervals or when significant changes occur.	Yes	ISMS Manager	Process - Internal Audit
139	A.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	ISMS Manager	Policy - ISMS Roles and responsibilities
140	A.18.2.3 - Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization’s information security policies and standards.	Yes	Head - IT Operations	No VA-PT reports

S. No.	ISO 27001	Applicable (Yes or No)	Where is this control driven from(Control Location/Context)?	Risk Owner	Justification for Inclusion/exclusion
110	A.14.2.4 - Restrictions on changes to software packages	No	Not Applicable	Not Applicable	No package software
113	A.14.2.7 - Outsourced development	No	Not Applicable	Not Applicable	No third party software development