ISO 27001 Compliance for Services			
SL No:	**Services**	**ISO 27001 Control number**	**Description**
1	24x7 Security Operation Center – Implementation and Finetuning	A.16.1.1	Control: Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents
		A.16.1.2	Control: Information security events shall be reported through appropriate management channels as quickly as possible.
		A.17.1.2	Control: 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.
2	24x7 Security Operation Center – Active Monitoring	A.8.2.1	Control: Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.
		A.8.2.2	Control: An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
		A.8.2.3	Control: Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
		A.8.3.1	Control: Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
		A.9.1.1	Control: An access control policy shall be established, documented and reviewed based on business and information security requirements.
		A.9.4.1	Control: Access to information and application system functions shall be restricted in accordance with the access control policy
		A.12.4.1	Control: Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed
		A.12.4.3	Control: System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
		A.12.5.1	Control: Procedures shall be implemented to control the installation of software on operational systems.
3	Security Advisory services	A.5.1.1	Control: A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
		A.5.1.2	Control: The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
		A.6.1.1	Control: All information security responsibilities shall be defined and allocated.

		A.6.1.2	Control: Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
		A.6.1.3	Control: Appropriate contacts with relevant authorities shall be maintained
		A.6.1.4	Control: Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
		A.6.1.5	Control: Information security shall be addressed in project management, regardless of the type of the project.
		A.8.3.3	Control: Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.
4	Threat Hunting Services	A.16.1.1	Control: Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents
		A.16.1.2	Control: Information security events shall be reported through appropriate management channels as quickly as possible
5	Cyber Emergency Response	A.16.1.4	Control: Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
		A.16.1.5	Control: Information security incidents shall be responded to in accordance with the documented procedures.
6	Active Vulnerability Management – External Network	A.6.2.1	Control: A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices
		A.6.2.2	Control: A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.
7	Active Vulnerability Management – Internal Network	A.9.4.2	Control: Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.
		A.9.4.3	Control: Password management systems shall be interactive and shall ensure quality passwords.
		A.9.4.5	Control: Access to program source code shall be restricted.
		A.12.6.1	Control: 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.
		A.12.6.2	Control: Rules governing the installation of software by users shall be established and implemented.
		A.18.1.3	Control: Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.
8	Active Penetration testing – Full Blackbox/Greybox	A.9.4.2	Control: Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

		A.9.4.3	Control: Password management systems shall be interactive and shall ensure quality passwords.
		A.10.1.1	Control: A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
		A.10.1.2	Control: A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.
9	Active Penetration testing – Periodic Scans	A.18.2.3	Control: Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.
		A.17.1.3	Control: 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.
10	Threat intelligence service	A.16.1.6	Control: Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents
11	Red & Purple team activities	A.14.2.8	Control: Testing of security functionality shall be carried out during development.
		A.13.1.3	Control: Groups of information services, users and information systems shall be segregated on networks.
12	OSINT Threat Exposure Assessment	A.18.1.4	Control: Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.
13	Threat Modeling	A.9.2.2	Control: A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.
		A.9.2.6	Control: 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.
		A.17.1.2	Control: 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.
14	Wireless Penetration Testing	A.13.1.1	Control: Networks shall be managed and controlled to protect information in systems and applications.
		A.13.1.2	Control: 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.
15	Security Configuration Assessment	A.6.2.1	Control: A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices
		A.6.2.2	Control: A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

		A.8.1.1	Control: Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
		A.8.1.2	Control: Assets maintained in the inventory shall be owned
		A.8.1.3	Control: Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.
		A.9.1.1	Control: An access control policy shall be established, documented and reviewed based on business and information security requirements.
		A.9.1.2	Control: Users shall only be provided with access to the network and network services that they have been specifically authorized to use.
		A.9.2.5	Control: Asset owners shall review users' access rights at regular intervals.
16	Active Attack Surface Monitoring	A.6.2.1	Control: A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.
		A.6.2.2	Control: A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.
		A.8.2.1	Control: Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.
		A.8.2.2	Control: An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization
		A.8.2.3	Control: Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
		A.9.1.1	Control: An access control policy shall be established, documented and reviewed based on business and information security requirements.
		A.9.1.2	Control: Users shall only be provided with access to the network and network services that they have been specifically authorized to use.
17	Malware Analysis	A.12.2.1	Control: Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness
18	Cyber Forensics	A.16.1.4	Control: Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
		A.16.1.5	Control: Information security incidents shall be responded to in accordance with the documented procedures.

		A.16.1.6	Control: Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
		A.16.1.7	Control: The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.
19	Response Readiness Assessment	A.12.7.1	Control: Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.
		A.16.1.1	Control: Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
		A.18.2.1	Control: 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.