



VISTA INFOSEC®

TRUSTED ADVISORS, ASSURED COMPLIANCE™

ISO27001 CHECKLIST AND SECURITY CONTROLS EXPLAINED

📞 US Tel: +1-415-513-5261 | UK Tel: +442081333131 | SG Tel: +65-3129-0397
| IN Tel: +91 73045 57744 | Dubai Tel: +971507323723

✉ info@vistainfosec.com | 🌐 www.vistainfosec.com

An ISO27001 Certified Company, CERT-IN Empanelled, PCI QSA, PCI QPA and PCI SSFA
USA. SINGAPORE. INDIA. UK. MIDDLE EAST. CANADA.

Introduction

Information Security Management System is an international standard designed to manage the security of sensitive information. At the core, ISMS is about managing the people, processes, and

technology through a risk management program. While there are many standards under the ISO27000 family, the ISO27001 Standard is the most popular and widely accepted standard in the industry.

The ISO 27001 standard provides a framework for implementing ISMS and securing information assets. The Information Security Standard and Framework help organizations implement security controls that ensure Confidentiality, Integrity, and Availability of sensitive data. Elaborating on the standard in detail, we have in the article also share a comprehensive compliance checklist with a list of security controls that must be implemented for those looking to achieve ISO27001 Certification. But before getting into the details of the security control list, let's understand in brief the ISO27001 Standard and framework.

What is ISO27001 Standard?

ISO/IEC 27001 is an international standard for managing data security through an information security management system (ISMS). The standard which was first published in 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) had last been updated the standard in 2013. The Standard comprises 10 management system clauses and Annex A which lists 114 Information Security Controls that are designed to support the implementation and maintenance of ISMS.

While there is no mandate that all 114 Annex A controls be implemented by the organization, it is however recommended that risk assessment should be conducted to determine which controls are required and provide details explaining why other controls are excluded from the ISMS. So, for the understanding of our reader, we have today shared an ISO 27001 checklist to help an organization approach its implementation plan efficiently and prepare for certification. But this again would depend on the controls applicable to the organization based on the risk assessment findings and outcomes.

ISO27001 Checklist and Security Controls

Achieving ISO 27001 certification helps organization prove their implementation and adoption of industry best security practices to potential customers in the industry. So, achieving the ISO27001 Certification will provide the organization with a competitive edge in the industry. That said, ISO 27001 Annex A comprises 14 controls that are grouped into 14 security control categories. Each of the 14 categories has been explained in the article. Referring to this checklist will help organizations successfully implement an Information Security Management System (ISMS) according to the standard, and prepare the organization for the audit of ISMS to obtain ISO 27001 certification.

ISO27001 Annex A contains 14 Main categories of Security Controls

Annex A.5	Information Security Policies
Annex A.6	Organization of Information Security
Annex A.7	Human Resource Security
Annex A.8	Asset Management
Annex A.9	Access Control
Annex A.10	Cryptography
Annex A.11	Physical and Environmental Security
Annex A.12	Operations Security
Annex A.13	Communications Security
Annex A.14	System Acquisition, Development, and Maintenance
Annex A.15	Supplier Relationships
Annex A.16	Information Security Incident Management
Annex A.17	Information Security Aspects of Business Continuity Management
Annex A.18	Compliance

Control Category A.5 – Information Security Policies

This section guides the management in implementing information security measures in alignment with the industry standards, regulations, and the organization's security requirements. Organizations can achieve this by establishing and documenting Information Security Policies and by regularly reviewing them from time to time.

Control Category A.6 – Organisation of Information Security

This section guides the management to set an Information Security Framework that facilitates the implementation of Information Security within the organization, across verticals and operations. This requires organizations to define information security roles and responsibilities, segregation duties maintain appropriate contact details with ICO and ISACA, and ensure information security in project management,

irrespective of the project type. Organizations are also required to ensure security in remote working including the security of mobile devices and teleworking. For this organizations are required to establish and maintain a stringent security policy supporting the security measures to manage risk associated with remote working including protection of information accessed, processed, stored remotely, and use of mobile devices.

Control Category A.7 – Human Resource Security

This category is about setting security measures and prerequisites for employment to ensure that the employees are aware of their responsibilities and they are suitable for the role they are hired for. This requires organizations to conduct appropriate background checks on candidates. It further requires organizations to have in place information security policies, procedures, and contracts that define the employee's information security roles and responsibility and documented signature of acknowledgment for the same from the candidate. The organization must also ensure the employees receive adequate training and are regularly updated on the policy changes if any concerning information security. There must also be a well-defined, formal disciplinary process in place to ensure necessary actions are taken against any individual who does not adhere to the information security breach. In addition to this, the organization needs to even have an Employee Termination Policy that defines the process for terminating or changing employee duties that are defined and enforced.



Control Category A.8 – Asset Management

This section is about asset security and management. Organizations are expected to maintain an inventory of all assets associated with information and information processing facilities. The asset must be classified and the inventory must include information about the assets and their designated asset owners. The organization must document the policies, procedures, and rules for the acceptable use and handling of assets. There shall also be policies and procedures in place to manage and prevent unauthorized disclosure, modification, removal, or destruction of information stored on media. The policies and procedures must include details on how the media should be handled, rules for disposal of media or systems containing information, and protection of data in transit.

Control Category A.9 – Access control

The organization must have in place Access Control Policies and Procedures to support the implementation of restricted access to information and information processing facilities. Further, the policy must define roles and responsibilities to ensure only authorized individuals are granted access based on their roles. Organizations are expected to make the policies accessible to their employees to know their roles and

responsibilities concerning their access to sensitive data or systems. Further, organizations must define and establish user access management for formal user access provisioning, management of privilege access rights, and removal of access rights for users who leave the organization. Necessary measures should be implemented to ensure users are accountable for securing their passwords and preventing unauthorized access to systems and applications.

Control Category A.10 – Cryptography

Organizations are expected to use the Cryptography technique to ensure confidentiality, integrity, and authenticity of the information. For this, the organization needs to establish and enforce a cryptography policy which should include details such as the use of cryptography controls, and cryptography key management.

Control Category A.11 – Physical and Environmental Security

This category is about ensuring the prevention of unauthorized physical access, damage, and interference to information and systems and facilities comprising information. So security measures must be implemented to secure systems and information and prevent data compromise and interruption to operations. For this, organizations need to implement physical security, for securing offices, rooms, and facilities with necessary access controls in place. They are further required to establish security policies and procedures that support the implementation of these physical security measures. This is to ensure protection against the external environmental threat

Control Category A.12 – Operations Security

This category is about ensuring operational security within the organization. The organization needs to ensure that information processing facilities are operated appropriately and securely. So, to ensure safe and secure operations, the organization needs to establish operational procedures and make them available to all. The procedure must include change management to control changes to business processes, information processing systems, and operations. It should also include capacity management to highlight the capacity requirements. Organizations must also ensure enforcement of segregation of development, test, and and operational environment. This is to reduce risks of unauthorized access or changes to operational environments.



Further, to ensure security, necessary controls against malware should be established to detect, alert and prevent malware attacks. So, organizations are expected to implement anti-malware software for effective detection and prevention of attacks. Organizations are also expected to maintain a backup of information to protect against loss of data.

Control Category A.13 – Communications Security

This category focuses on maintaining the security of Information when transferred internally or externally. The organization must for these reasons have a Network Management process in place which includes risk management, and

ensuring network segmentation where applicable to prevent unauthorized access to sensitive networks and data. This can be achieved by organizations by having in place agreements, and contracts with security-related SLAs mandated. For securing the data transition, the organization must have data transfer policies and procedures including details such as how the data should be



transferred and made available to employees and the implementation of technical controls to prevent unauthorized data transfer. This requires organizations to implement security controls to protect information transferred through emails, social media, and other communication platforms. the organization is also expected to maintain an agreement contract between third parties involved, specifying their responsibility in ensuring the security of data when transferred. There should also be in place Confidentiality or Nondisclosure Agreements that should be subject to regular review and maintenance of such records.


Control Category A.14 – System Acquisition, Development, and Maintenance

The category focuses on ensuring the systems and operations within the environment are secured and the security implementations are an integral part of the systems and operations lifecycle. The organization must ensure information security requirements are specified when new systems are introduced or when systems are being enhanced or upgraded.

The organizations are expected to secure applications sending information over public networks against fraudulent activities, unauthorized access, and modification of data. The organizations must have in place technical security measures to prevent instances of incomplete transmission, unauthorized modification, disclosure of data, misrouting, or duplication of data. The organization must also have in place a secure development policy, system change control procedures, and processes for secure software development, system engineering, secure development environment. The organization must also ensure system security testing is performed on outsourced developments.

Control Category A.15 – Supplier Relationships

This category focuses on ensuring the security of information accessed by suppliers. For this organizations should have in place documented policies and procedures concerning supplier management with details of all suppliers and information they have access to. The organization must also develop an agreement or contract with suppliers mentioning their responsibilities and security requirements, addressing the information security risks associated with information and communications technology services and the supply chain. This should be in line with the security management policy. The Agreement or Contract must also include and mention the agreed level of information security and delivery of service in line with the Supplier Agreement.



Control Category A.16 – Information Security Incident Management

This category focuses on ensuring consistent and effective enforcement of Information Security Incident Management. This includes communication security incidents and weaknesses in systems and processes. For this, organizations must define roles responsibilities, and a clear process for reporting incidents, information security weaknesses, assessment, and response to information security incidents.

Control Category A.17 – Information Security Aspects of Business Continuity Management

This category focuses on ensuring Information Security and Business Continuity Management. The organizations are expected to have in place policies, procedures, and processes in place to facilitate Information Security and Business Continuity in case of an incident. This further needs to be documented for future use, reference, and audit purpose. Organizations are expected to evaluate review and verify the effectiveness of Information Security and Business Continuity Management. The organization must also maintain information on whether the information processing facilities have sufficient redundancy to meet the organization's availability requirements.

Control Category A.18 - Compliance

This category focuses on ensuring compliance with the legal, statutory, regulatory, or contractual obligations related to information security and security requirements. Organizations are expected to identify and document applicable legislation and contractual requirements for compliance. Further, it is a mandate to maintain records of all intellectual property rights and the use of proprietary software products. All records and documents should be secured against unauthorized access, destruction, and modification as per the legislative, regulatory, contractual, and business requirements.

Organizations must maintain the security and privacy of personally identifiable information (PII) and use cryptography controls in line with relevant agreements, legislation, and regulations. Organizations must also regularly conduct audit reviews and implementation of security controls. Further compliance with security policies and standards should be regularly reviewed and verified.



Note - (The checklist broadly includes various requirements but may not be limited to just the listed mentioned below. Also, the applicability of the checklist varies from organization to organization and is based on the security requirements specific to the business)

Standard	Section		Generic Checklist
A.5	Information Security		
A.5.1	Management Direction for Information Security		
A.5.1.1	Policies for Information Security		Access Control Policies, Remote Access Policies Acceptable User Policies Acceptable Encryption & Key Management Policies, Data Breach Response Policy, Disaster Recovery Policy.
A.5.1.2	Review of the policies for information security		Annual, Semi-annual Review of Policies or as and when significant changes are introduced in the environment to be conducted by competent authority and approved by the Senior Management.
A.6	Information Security Organization		
A.6.1	Internal Organization		
A.6.1.1	Information security Roles and Responsibilities		<p>Define roles and responsibilities specific to Supervision of the Information Security Management System (ISMS) with due representation from each department.</p> <p>Appointment of an ISMS Head / Co-ordinator. Evidence required for</p> <ul style="list-style-type: none"> ■ Coordination of all activities related to the ISMS ■ Communication of Information relating to ISMS in the Organization ■ Contacting Authorities and Groups of Interest. ■ Supervision and Co-ordination of the ISMS activities (rollout, monitoring and continual compliance)

Standard	Section	Generic Checklist	
A.6.1.2	Segregation of Duties		Segregation of duties (documented in HR documentation and signoff) based on activities and functions including authorization function, documentation function, custody of assets, reconciliations, and audits.
A.6.1.3	Contact with Authorities		Procedures to identify Information Security Incidents and clarification on when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and reported in a timely manner
A.6.1.4	Contact with Special Interest Groups		Membership in Special Interest Groups or Forums and/or Professional Association with other Specialist Security Forums such as OEM, SANS, NIST, CIS or CERT (local and international).
A.6.1.5	Information Security Organization		Define Information Security Objectives, Definition and Allocation of Roles and Responsibilities in the Project Management, Policy and Procedure for Information Security Risk Assessment, Process for Implementing Information Security in all phases of the applied Project Methodology.
A.6.2	Mobile Device & Teleworking		
A.6.2.1	Mobile Device Policy		Mobile Device Policy including Restriction of Software Installation, Restriction of Connection to Information Services, Access Controls, Remote Access, Usage Policy for Web Services and Web Apps, Application for Firewalls, Malware Protection, Encryption Techniques, and Measures for Physical Protection, Software Updates and Patches, Backups, Disabling, Deletion or Lockout Policy.
A.6.2.2	Teleworking		Access Controls, Malware & Firewalls Installations, Physical Security of the Teleworking Site, Securing Remote Access, Hardware & Software Support and Maintenance, Backup, Business Continuity, Procedures for Regular Audit and Security Monitoring, Teleworking Policies must include Information Restriction, Work Hours Policy Identification/Authentication/Authorisation, Remote Access, User Access, User Guidelines, Software Installation, Data Protection, and Security.

Standard	Section		Generic Checklist
A.7	Human Resource Security		
A.7.1	Prior to Employment		
A.7.1.1	Screening	Adequate Job Descriptions, Pre-Employment Screening including Background Verification, Verification of any Information Concealed or Falsified Information, Qualifications, and Job History, have in place Policies, Processes, and Procedures for Screening, Documenting the Screening Process to be carried out.	
A.7.1.2	Terms and Conditions of Employment	Develop Terms and Conditions of Employment, Signed Agreements, Define Security Roles and Responsibilities, Compliance Obligations.	
A.7.2	During Employment		
A.7.2.2	Information Security Awareness, Education, and training	Information Security Training Program, Regulatory and Compliance Training & Awareness Program, Educating About Roles & Responsibilities, Documenting All Training & Awareness Programs, Have in place Process and Procedures to ensure Regular Interval Employee Training.	
A.7.2.3	Disciplinary Process	Disciplinary Process of Employment Violation, Employee Contracts, Action related to Information Security Breaches, Framework for Information Security Breaches, Disciplinary Action Policies for other violations	
A.7.3	Termination & Change of Employment		
A.7.3.1	Termination or Change of Employment Responsibilities	Policies & Procedures concerning Change of Employment (left voluntarily, been fired or changed role), Process and Procedures of Responsibility an-dover, Policies and Procedures relating to shifting to a different department within the organization. Policy & Process of Deleting Access Right to Information Assets.	
A.8	Asset Management		
A.8.1	Responsibility for Asset		

Standard	Section	Generic Checklist	
A.8.1.1	Inventory of Assets		Documenting Inventory of Assets including Information, IPs, Employees, Temporary Staff, Contractors, Physical Assets such as IT Servers, Network Equipment, Workstations, Mobile Devices, Software Applications, Database Systems, E-mail, Sites, Buildings, Offices, etc. Data Classification in terms of Public, Internal or Confidential Data, Type of Data including whether Personal, Sensitive, Commercial data.
A.8.1.2	Ownership of Assets		Document details such as the name of Asset Owners, the Type of Assets held, Policy and Process concerning the Assigning of the Ownership of Assets, Policy, and Procedures for Asset Management Lifecycle.
A.8.1.3	Acceptable Use of Assets		Policies and Procedures for Acceptable Use of Assets, Documented Asset Use Rules for Employees, Temporary Staff, Contractors, and Other Third Parties, Third-Party Access and Use Policy. The Acceptable Use of Asset Policy must include the Purpose, Scope, Individual Responsibility, Working Offsite, Monitoring and Filtering, Compliance Measures.
A.8.1.4	Return of Assets		Policies, Procedures & Process relating to returning of company assets. Documented rules and Procedures for Return of Assets, Documented listed of Assets and Ownership, Policy for Deletion of Data, Revoking Access rights, Change of Password Policy.
A.8.2	Information Classification		
A.8.2.1	Classification of Information		Policy, Procedure, and Process of Information Classification, Information Classification Policy covering Purpose, Scope, Type of Data, Privacy and Security of Data, Defining and Assigning Responsibility, Confidentiality and Disclosure Policies, Access Policies.
A.8.2.2	Labelling of Information		Procedure and Process for Labelling of Information, Defined Classification Scheme, Protocols for Labelling Information, Employee and Contractor Awareness of the Procedures for Labelling.

Standard	Section	Generic Checklist	
A.8.2.3	Handling of Assets		Handling of Assets Procedures, Access Restrictions, Maintaining of Records, Security Procedures for Handling Assets, Procedure for Storage of Assets, Policies, and Procedures for Transmitting the Assets, Policies for Internal and External Use and Handling of Assets.
A.8.3	Media Handling		
A.8.3.1	Management of Removable Media		Removable Media Policy, Usage Policy of Removable Media, Access Policy of Removable Media, Risk Management Policy and Procedure for Removable Media, User Training Policy, Procedure and Process for Disposal of Removable Media.
A.8.3.2	Disposal of Media		Media Disposal Policy including Protocols for Secure Disposal of Media, Secure Deletion of Data, Third-Party Access Control and Documented Procedures and Record for Disposal of Media, Information Classification for Disposal of Media, Equipment Reuse or Disposal, Non-retrievable Methods of Disposal.
A.8.3.3	Physical Media Transfer		Physical Media Transfer Policy including Physical and Environmental Security Procedures, Process of Secure Media Transfer, Access Control, Cryptography Procedure for Monitoring and Tracking of Media Transfer, Procedure and List of Approved Carriers, Logs, and Identification of Media Transfers.
A.9	Access Controls		
A.9.1	Business Requirement for Access Controls		
A.9.1.1	Access Control Policy		Access Control Policy including User Access Management, System and Application Access Control, Restricted Access Rules, Define and Assign Access Control Responsibility, Provisions for Security, Password Change Policy, Access Rights, Privileged Access Rights, Revocation of Access, and Rules for Authorization of Access, Review of Access Control Policies.

Standard	Section	Generic Checklist	
A.9.1.2	Access to Networks and Network Services	List out Networks and Network Services in Scope for Access, Authorisation Procedures, Assign Access to Networks and Network Services Responsibility, Management of Access Controls and Procedures to Monitor and Log Access.	
A.9.2	User Access Management		
A.9.2.1	User Registration and Deregistration	Policy and Process to Record and Maintain User Registration and Deregistration, Policy and Process to Assign Unique User IDs, User ID Management, Process and Procedure for Regular Review of IDs, Least Privileges, Segregation of Duties, Administrative Policy for Multi-User Systems.	
A.9.2.2	User Access Provisioning	Access Control Policy, User Access Management Policy, Process for Authorization of Access, Process for Verifying Authorization, Level of Access and Access Grants, Process and Procedure for Removal Access Rights, Central Records of User Access Rights, Regular Review & Updating of Access Rights.	
A.9.2.3	Management of Privileged Access Rights	Record of Privilege Access Rights, Process for Granting Privileged Access Rights, Verifying the Grants for Privilege Access, Process for ensuring Role Based Privilege Access Rights, Regular Review & Updating of Access Rights, Expiry of Privileged Access Rights, Process for Verifying Authorization, and Access Grants, Procedures for generic administration of user IDs, Confidentiality of Secret Authentication, Revocation of Privilege Access, Change of Passwords.	
A.9.2.4	Management of Secret Authentication Information of Users	Procedure and Process to maintain Secret Authentication Information of Users, Procedures to Change the Default Secret Authentication Information, Procedures to Verify User prior to providing a New, Replacement or Temporary Secret Authentication Information, Process for providing Unique Temporary Secret Authentication Information, Policy, and Procedure for gaining Acknowledge Receipt of Secret Authentication Information.	

Standard	Section	Generic Checklist	
A.9.2.5	Review of User Access Rights		Process to Regularly Review and Re-allocate User Access Rights, Review Authorizations for Privileged Access Rights, Review Privilege Allocation, Review Changes to Privilege Allocation, Review Maintain Logs of Privilege User Access
A.9.2.6	Removal or Adjustment of Access Rights		User Access Management Policy, Human Resource Policy, Policy and Process to Revoke Access Rights, Process to Report Significant Changes, and Revocation of Access Rights.
A.9.3	User Responsibilities		
A.9.3.1	Use of Secret Authentication Information		Password Policy including Change of Passwords, Encryption of Passwords, Revocation of Access to Secret Authentication Information, Process to Prevent Retrieval of Unauthorized Use of stored Passwords, Policy for non-revealing and sharing of Passwords, Process for accountability of Use of Secret Authentication Information.
A.9.4	Systems and Application Access Controls		
A.9.4.1	Information Access Restriction		Access Control to Application System Functions, Restricted Access Control to Sensitive Data, Restriction of Access Rights, Limiting Information Output, Measures for Physical or Logical Access Controls.
A.9.4.2	Secure Log-on Procedures		Access Control Policy, Process for Secure Log On and Log Off, Process to Track and Monitor Log On, and Log Off activity, Access logs, Password Policies.
A.9.4.3	Password Management System		Password Management Policy, Password Change and Re-set Policy, Process to Review Password Policy, Process to Assign Unique ID and Password, Process to Change Default Passwords, Encryption of Password Policy, Maintain Records of Passwords.
A.9.4.4	Use of Privileged Utility Programs		Procedures for authentication, and authorization of utility programs, Process for Segregation of Utility Program, Policy for Restricted Availability of Utility Program, and Documenting Levels of Authorisation for Utility

Standard	Section	Generic Checklist	
			Programs, Policy, and Process for Deletion or Disabling of Unused Utilities.
A.9.4.5	Access Control to Program Source Code		Procedure for Administering the Source code and Source Library of the Program, Policy and Procedure for Restricted Access to Program Source Libraries, Policy and Process to update Source Library Program and Related Objects, Process to Document Program Listings Securely, Process to Maintain Audit Log of all Accesses to Program Source Libraries.
A.10	Cryptography		
A.10.1	Cryptography Controls		
A.10.1.1	Policy on the Use of Cryptographic Controls		Cryptography Usage Policy, Data Handling Procedure Implementation Policy for Encryption, Process for Training Relating to the Use of Cryptographic Controls, Policy and Process Concerning the Use of Cryptographic Techniques, Remote Access Policy, Email Encryption Policy.
A.10.1.2	Key Management		Cryptography Key Management Policy including Process for Generating Keys for various Cryptographic Schemes and Applications, Process for Storing of Keys, Activation of Keys, Upgrade Keys, Address Missing Keys, Revoke Keys, Backup Keys, Destroy Keys, Logging and Auditing of Key Management Activities, Policy and Procedure in case of Loss and Theft, Encryption Procedures.
A.11	Physical & Environmental Security		
A.11.1	Secure Areas		
A.11.1.1	Physical Security Perimeter		Policy and Process for Physical Access Controls, Process for Monitoring and Tracking Physical Access, Process for Documenting Physical Security Controls, Process for Assigning Responsibility, Process for Authorization and Verification of Authorization, Procedure and Process for Critical Backups of Media.

Standard	Section	Generic Checklist	
A.11.1.2	Physical Entry Controls		Physical Entry Controls include Access to Server Room, Limiting Access to Designated Systems and Operations, Restricted User Account, Remote Access, Verification of Access Authorization, Regular Monitoring of Physical Access, Process to Respond to Physical Security Incidents.
A.11.1.3	Securing Offices, Rooms, and Facilities		Policy and Procedure for Physical Access Control Measures, Process for Maintaining Records of the Visitor, Regularly Reviewing of Access, Process for Appointing Security Officials on-premise, Process for Revoking Access to Old Staff, Process for Regularly Inspecting the Security Controls for Offices, Rooms, and Facilities, Review Risk-based Control Implementation, and Operation.
A.11.1.4	Protecting against External and Environmental Threats		Develop Measures and Processes for Physical Protection against Damage from Fire, Flood, Earthquake, Explosion, Civil Unrest, and other forms of Natural, Man-made Disasters.
A.11.1.5	Working in Secure Areas		Policy for Working in Secure Areas including Process for Implementing Automated Mechanisms for Alerts, Policy, and Process for Restricted Awareness of Location and Function of Secure Areas, Policy for Restrictions on the Use of Policy Restricting Recording Equipment within Secure Areas, Restriction on Unsupervised Working in Secure Areas, Record, and Document In and out Monitoring and Logging.
A.11.1.6	Delivery and Loading Areas		Process for Security Implementation in all Access Points, Physical & Environmental Security Policy, Procedures to Prevent Unauthorized External and Internal Access, Process to Inspect all Material Delivered, Documentation and Registration of all Materials Delivered, Process for Implementing Controls relating to Incoming Materials and Outgoing Materials.
A.11.2	Equipment		
A.11.2.1	Equipment Siting and Protection		Process for Securing the Equipment in Safe Location, Process for Maintaining Working Conditions, Access Control Policy, and Process, Physical Access Control Policy, Process for Protecting of Physical

Standard	Section	Generic Checklist	
			Equipment, Records of Equipment Replacement.
A.11.2.2	Supporting Utilities		Policy for Utility Program, Business Continuity Policy and Procedure, Disaster Recovery Management Policy and Process, Process to Protect Equipment against Power Failure, Backup Policy, and Procedure, Process for Regularly Testing Power Provision and Management, Process to ensure Continued Support and, Availability of Equipment and Information for Business Continuity.
A.11.2.3	Cabling Security		Process to Secure Power and Telecommunication Cables, Provision for Regularly Testing the Cabling Security, Procedure for Segregation of Power Cables, Provision for Regular Inspection of Termination Points against Unauthorised Devices, Provision for Visual Inspection of Cables.
A.11.2.4	Equipment Maintenance		Equipment Maintenance Policy, Process for Annual Review of Equipment, Maintain Reports of Annual Review and Maintenance of Equipment, Process to ensure Continued Security, Availability and Integrity of Equipment, Provision, and Process for Regular Review and Testing of Equipment.
A.11.2.5	Removal of Assets		Asset Management Policy, Records of Asset Allocation, Process for Authorized Asset Allocation & Authorized Asset Access, Records of Asset Removal, Process for Asset Removal, and Process to Check Return of Assets, Policy, and Procedure for Limiting Length of Time Assets are Allowed to be Removed.
A.11.2.6	Security of Equipment and Assets Off-Premises		Security Policy & Procedure for Protecting Equipment and Assets Off Premises, Asset Usage Policy Off Premises, Work From Home Policy and Process, Process for Regular Risk Assessment of Assets and Security Controls, Access Control Policies, Password Management Policy and Process, Encryption Policy, Physical Security Control Policy, and Process, Process for Reviewing Off-Site Security Incident, Policy For Documenting Records of Risk Assessment.
A.11.2.7	Secure Disposal or Reuse of Equipment		Policy and Process to Securely Dispose or Reuse of Equipment, Process to Verify the Disposal & Reuse of Equipment, Third-Party Policy.

Standard	Section	Generic Checklist	
			and Procedure concerning Secure Disposal or Reuse of Equipment, Policy for Maintaining Evidence of Destruction or Secure Erasure of Data.
A.11.2.8	Unattended User Equipment		Secure Policy for Unattended User Equipment, Process for Implementing Security for Unattended User Equipment, Password and Screen Lock Policy, Policies, and Process for Security Awareness Programmes, Documented Records of Security Implementation for Unattended Equipment.
A.11.2.9	Clear Desk and Clear Screen Policy		Operating Procedures for Papers and Removable Storage Media, Clear Screen Policy for Information Processing, Process for Risk Assessment, Process to Review Clear Desk and Clear Screen Policy, Process of Documenting Tested, and Reports of Security Implementation and Management.
A.12	Operational Security		
A.12.1	Operational Procedures & Responsibility		
A.12.1.1	Documented Operating Procedures		Operating Procedure, Policy and Process for Documenting Operating Procedure, Change Management, Operational System Policies, Process for Automated and Manual Processing and Management of Information, Systems Installation and Settings, Backup Process, System Reboot, and Recovery Procedure, Audit-trail Management, and System Log Information, Procedure for Monitoring.
A.12.1.2	Change Management		Policy and Process for Change Management, Process for Authorizing Change, Process for Communicating Changes, Procedure for Emergency Changes, Process to Identify and Record Significant Changes, Process to Test and Verify Modification, Process to Assess the Impact of Change.
A.12.1.3	Capacity Management		Procedure to Check System Performances, Process of System Tuning and Control, Procedure for Removal of Obsolete Data, Process for Optimizing Logic of Program or Database Queries, Process, and Procedure for Refusal or Limitation of Bandwidth for Resource Hungry Applications, Process

Standard	Section	Generic Checklist	
		for Monitoring Use of Resources, Procedure to Measure Future Capacity Requirement, Process to Meet System Performance to Meet the Business Objectives.	
A.12.1.4	Separation of Development, Testing, and Operational Environments		Policy and Procedure for Separating Development, Process for Testing Operational Environment, Process for Verifying Segregation of Test and Live Environments, Formal Procedure for Appropriate Levels of Authorisation for Movement, Changes, and Developments from One Environment to Another, Process for Verifying Authorization, Process to Test Changes and New Developments, Process to Address Accidental Change or Unauthorized Access to Operational Software and Business Data, Process to Avoid Inclusion of Sensitive Data in Test Systems and Environment.
A.12.2	Protection from Malware		
A.12.2.1	Controls Against Malware		Malware Protection Policy, Process to Detect, Prevent, and Recovery Controls to Protect against Malware, Policy and Process for User Awareness, Policy for Use of Removable Media, Process to Restrict or limit the Installation of Software by Users, Process to ensure Unauthorized Use of Software, Patch Management Policy, Software Updating Policy.
A.12.3	Backups		
A.12.3.1	Information Backup		Information Backup Policy and Process, Regular Testing of the Backup Process and Policies, Process for Security of Information Backups, Process for Testing of Backup and Procedure for Restoration of Backups, Monitoring and Recording of Backups, Process for Reporting reports Failed Backup, Encryption Policy for Sensitive Data Backups, Process for Removal Storage Backups, Accurate and Complete Documented Records of Back-ups, Policy Defining the Extent and Frequency of Backups.
A.12.4	Logging and Monitoring		
A.12.4.1	Event Logging		Event Logging Policy, Process for Recording Event Log including ID's of User, User Activities, Date, Times and Key Events, Log-in & Log-Off,

Standard	Section	Generic Checklist	
			System ID, Location, Device Recognition, Records of Successful Access Attempts and Failed Access Attempts, Successful and Unsuccessful Attempts to Access Resource, System Configuration Alterations, Records of System Configuration and Alterations, Records of Utilizing Privilege, Application and Use of Systems Utilities, Network Address and Protocols, Process for Maintaining Logs of Faults and Information Security Events, Process to Regularly Review & Monitor Logs, Process for Management Event Logs, Incident Management Log Policy, Policy and Process for Audit Logs, Capacity Management.
A.12.4.2	Protection of Log Information		Information Security Monitoring Policy for Log Information, Process for Privacy Protection of Log Information, Process for Security of System Log, Process to Monitor Unauthorized Alteration, Deletion of Log Information, Process to Alert in Case of Alteration, Deletion of Information, Process for Copying of Logs to System Outside the Control of System Manager on Real-Time Basis.
A.12.4.3	Administrator and Operator Logs		Policy and Process for Administrative and Operation Logs, Process to Review Access Privileges, Process to Secure Logs, Process to Monitor Activity of System Manager and System Operator, Policy for System and Network Management.
A.12.4.4	Clock Synchronization		Policy and Procedure to Integrate Clock Time to Single Source, Document External, and Internal Time Representation Requirements, Synchronization, and Precision, Process to Maintain a Standard Reference Time, Process to Maintain all Servers in Sync with Master Clock.
A.12.5	Control of Operational Software		
A.12.4.4	Clock Synchronization		Policy and Procedure to Integrate Clock Time to Single Source, Document External, and Internal Time Representation Requirements, Synchronization, and Precision, Process to Maintain a Standard Reference Time, Process to Maintain all Servers in Sync with Master Clock.

Standard	Section		Generic Checklist
A.12.5	Control of Operational Software		
A.12.5.1	Installation of Software on Operational Systems	Procedures to Control Installation of Software on Operational System, Process to Address Inappropriate Installation or Change of Software on Operational Systems, Process for Testing Installation of Software Against Malware, Policy and Process for restricting and Limiting the Installation of Software on Operational Systems, Process for Authorization of Software Installation, Process for Verifying the Authorization of Software Installation, Process to Monitor the Legitimate Installation, Change Management Policy and Procedure, Process to Revoke or Rollback Installation of Software, Process Document Records of Software Changes and Installation.	
A.12.6	Technical Vulnerability Management		
A.12.6.1	Management of Technical Vulnerabilities	Process to Assess, Determine and Address Technical Vulnerabilities, Process for Conducting Regular Vulnerability Assessment and Penetration Test, Process to Determine Risk Levels & Exposure, Policy and Process for Patch Management, Process for Testing of Patches, Process to ensure continued Availability and Integrity of Systems, Process for Conducting Awareness Program.	
A.12.6.2	Restrictions on Software Installation	Policy on Restriction of Software Installation, Define and Enforce a Policy on Types of Software that may be Installed, Rules Governing the Installation of Software by Users, Process for Risk Assessment on Software Installed, Policy for Privileged Grants for Software Installation, Process for Software Updates and Security Patches, Process for Defining Roles for Authorization of Software Installation.	
A.12.7.1	Information Systems Audit Controls	Policy for Information System Audit Management, Process for Information Systems Audit Controls, Process that Defines Audit Standards for Access to Systems and Data, Process to Define Scope on the Technical Audit Tests, Formal and Authorised Process for Auditing and Test of Operational Systems.	

Standard	Section		Generic Checklist
A.13	Communication Security		
A.13.1	Network Security Management		
A.13.1.1	Network Controls		Network Management Policy, Networking Equipment Management, Process for Monitoring Network Information Security, Access Policy, Policy for Access Authorization and Verification, Procedure for Defining Network Operational Roles and Responsibility, Process for Appropriate Logging and Monitoring, Process to Authentication of Network System, Policy and Process for Restricted Network Connection to Device.
A.13.1.2	Security of Network Services		Procedure for Security of Network Service, Security Protocols, Quality of Service, and Management criteria for all Network Services, Procedure for Defining Network Services Agreements, Process to Regularly Supervise Capability of the Network Service, Authentication and Encryption Policy, Procedure for Network Connection Controls, Risk Assessment Process for Network Service.
A.13.1.3	Segregation in Networks		Policy and Procedure for Network Segregation, Process of Segregation Physical Networks or via various Logical Networks, Process for Segregating Duties of Network Operations, Policy of Information Classification and Segregation Requirements, Process for Defining Network Perimeter, Policy for Network Control and Access.
A.13.2	Information Transfer		
A.13.2.1	Information Transfer Policies and Procedures		Formal Information Transfer Policies, Procedures, and Controls, Procedures to Prevent Interception, Copying, Altering, Misrouting or Destruction of Transmitted Information, Procedures to Detect and Protect Malware from Electronic Communications, Procedures for Protection of Communicated Electronically Sensitive Information in An Attachment, Guidelines or Rules Specifying an Appropriate Usage of Communication Facilities, Policy, and Procedure for Use of Encryption Technique, Controls and Constraints Relating to Use of Communication Facilities, Process for Awareness.

Standard	Section	Generic Checklist	
A.13.2.2	Agreements on Information Transfer		Process for Secure Transfer of Business Information, Agreement on Information Transfer must include Management of Transmission, Dispatch, and Receipt, Procedures for ensuring Traceability and Non-Repudiation, Minimum Packaging and Transmission Technical Standards, Escrow Agreement standard of Courier Identification, Special controls to Protect Sensitive Information, Access Control Measures, Chain of Custody, Cryptography.
A.13.2.3	Electronic Messaging		Policy and Procedure for Securing Electronic Messaging, Process for Access Control Measures, Policy Concerning the use of Type of Electronic Messaging used for a Specific Types of Information, Policy for Voice & Fax Communications Transfer, and Physical Transfer, Secure Authentication Policies and Log-On Procedures.
A.13.2.4	Confidentiality or Non-Disclosure Agreements		Policy Defining General Non-Disclosure and Mutual Non-Disclosure Agreements, Privacy Policy, Customer Agreements Defining Standard Terms and Conditions – Expressing Confidentiality, Process for Termination of an Agreement, Process to ensure Unauthorized Disclosure of Information, Expected Duration of an Agreement, Process Assign Responsibility to Protect the Use of and Disclosure of Information. Process to Periodically Review Confidentiality or Non-Disclosure Agreements.
A.14	System Acquisition Development & Maintenance		
A.14.1.1	Information Security Requirements Analysis and Specification		Processes for Access and Authorization of all business Users and Privileged or Skilled Users, Process for Communicating to Users and Managers of their Roles and Responsibilities, Process for Meeting the Security needs of Availability, Confidentiality Integrity of Assets, Process for Transaction Recording and Monitoring, Non-Repudiation Specifications, Process for Logging and Monitoring Interfaces or Data Leak Detection Systems, Process to Perform Threat Analysis, Incident Assessment, Incident Assessments.

Standard	Section	Generic Checklist
A.14.1.2	Securing Application Services on Public Networks	Policy and Process for Securing Application on Public Network, Encryption Policies, Process for using Multi-Factor Authentication, Use of Passwords, Process for ensuring Unauthorized and Fraudulent Access, Process for Limiting Privileges, Process to ensure Communication of Service Provision and Usage Authorization, Process to ensure Protection of any Confidential Information Requirements, Process to ensure Secure Payment Settlement for Fraud Protection, Process to Prevent Information Loss or Duplication.
A.14.1.3	Protecting Application Services Transactions	Information Security Policy for Secure Application Service Transaction, Process to Protect Application Services Transactions, Process to Prevent Incomplete Transmission, Mis-routing, Unauthorised Message Alteration, Unauthorised Disclosure, Unauthorised Message Duplication or Replay, Process to Verify the Secret Authentication, Privacy Policy, Encryption Policy, Policy to Use of Electronic Signature, Policy and Process to Use Secure Protocols, Process to Monitor Transactions near to Real-Time Basis.
A.14.2	Security in Development & Support Process	
A.14.2.1	Secure Development Policy	Policy and Process for Secure Development of Software and Systems, Process for Developing and Implementing System Changes, Security Guidelines for Life Cycle of Software Development, Process concerning Methodology for Software Development, Policy and Process for Use of Secure Code, Process for Hiring and Training Resources on Secure Coding and Development Practices, Process for Secure Code Reviews and Testing.
A.14.2.2	System Change Control Procedures	Change Control Policies, Formal Protocols for Monitoring of Transition, Procedure that Controls the Development Lifecycle, Process to Assign Responsibility for Protecting Information and Asset. Process for Monitoring System Change Control, Process for Authorizing System Change Control, Process for evaluating System Changes and Identifying any Modification Software, Information, Database Entities, and Hardware, Process for Identifying Testing Secure Code, Process for System Documentation Update, Policy and Process for Removal of Old Documents Upon Completion of Amendments, Process to ensure Operational Documentation, and User Procedures are Updated, Process to ensure Business Processes are Updated after Changes.

Standard	Section	Generic Checklist	
A.14.2.3	Technical Review of Applications after Operating Platform Changes		Policy for Change Management and Controls, Process for Reviewing and Testing of Applications after Operating Platform Changes, Process to Evaluate the Impact on Organisational Operations and Security, Procedure to Test Operating System Changes in a Development or Test Environment, Process to Check Compatibility with Changed OS, Procedures for Control and Testing of Operating System Changes, Process ensuring Operating Platform Changes are Communicated Business Continuity Plans.
A.14.2.4	Restrictions on Changes to Software Packages		Policy for Software Package Modification, Process to Prevent or Limit Changes, Process for Controlled Changes to Software Packages, Process to Test Impact on Internal Integrity or Security of Software, Process to Maintain Internal Integrity or Security of Software, Process to Obtain Vendor Consent.
A.14.2.5	Secure System Engineering Principles		Policy and Process for Secure System Engineering, Policy for Secure Development Life Cycle, Process to Evaluate for Security Threats on New Technology, Policy to Use System Engineering Principles, Process for User Authentication, Secure Control of Session, and Validation of Data, Sanitation, and Removal of Debugging Codes.
A.14.2.6	Secure Development Environment		Policy for Secure System Development Lifecycle, Process to Prevent Malicious or Accidental Development, Process for Updating Code, Process for Risk Assessment, Process to Evaluate Reliability of Personnel Working in the Environment, Process for Maintaining Records of Outsourcing Associated with the Production of System, Policy, and Process for Segregation of Environments for Development, Access Control Process, Process for Monitoring Environmental Changes, Process to Secure Offsite Location of Backups Stored, Process for Controlled Data Transfer.

Standard	Section	Generic Checklist	
A.14.2.7	Outsourced Development	Process to	Monitor Outsourced Development of Systems, Process for Secure Design, Coding and Testing Outsourced Development, Vendor Management Policy, Vendor Contract and Agreement Policy, Non-Disclosure and Confidentiality Policy, Security Awareness Training Process.
A.14.2.8	System Security Testing	Process for	Testing of Security Functionality, Process for Testing and Verification during Developing Processes in New and Updated Systems, Process for Documenting Security Testing.
A.14.2.9	System Acceptance Testing	Process for	System Acceptance Test, Process for Verification tools for Code Analysis, Vulnerability Scanners and Security Related Defects, Provisions for Security Acceptance Test. Process to Perform Test in the Real Test Environment.
A.14.3	Test Data		
A.14.3.1	Protection of Test Data	Process for	Defining Testing Purpose and Guidelines, Process for Protecting Operational Data, Access Management Protocol, Process for Authorization of Testing, Policy and Process for Deletion of Operational Information, Process For Maintaining Audit Trails, Process for Maintaining Logs for Audit Trails, Process of Pre-Authorization for Use of Live Data, Process for Log and Monitoring.
A.15	Supplier Relationship		
A.15.1	Information Security in Supplier's Relationship		
A.15.1.1	Information Security Policy for Supplier Relationships	Information Security Policy for	Supplier Relationships, Policy and Process for Supplier Selection and Management, Process for Segmentation of Supply Chain, Vendor Management Policy, Access Management Policy, Process for Controlling Information Assets Around Suppliers, Process for Security of Asset Accessible to Suppliers, Risk Management Process,

Standard	Section	Generic Checklist	
		Process for Documented Information Security, Non-disclosure Agreement, Vendor Contract and Agreement Policy, Security Awareness Training Process.	
A.15.1.2	Addressing Security within Supplier Agreements		Process for Communicating any changes with Suppliers, Process for Addressing Information Security Concerns with Suppliers, Supplier Agreement Contract, Process of Reviewing Agreements and Contracts, Process for Defining and Documenting Supplier Agreements, Process for Defining Roles and Responsibilities of Supplier, Process for Supply and Access to Information Provided or Accessed by Suppliers, Process for Classification of Information for Suppliers, Process to Define Obligation to Enforce Agreed Control Plan, Process for Access Management, Process for Performance Analysis, Monitoring, Reporting and Auditing for each Contracting Party, Process for Acceptable Use of Information, Process for Supplier to Submit Independent Report on Efficiency of Controls, Process for Timely Correction Agreement for the Relevant Issues, Process to Verify Supplier Meets Security Requirements of Organization.
A.15.1.3	Information and Communication Technology Supply Chain		Supplier Agreements and Contracts, Process to Mitigate Information Security Risks Associated with IT Services and Product Supply Chain, Process to Define Security Specifications Across Supply Chain for Information and Communication Technology Services, Monitoring Framework and Appropriate Validation Methods for Information and Communication Technology Products and Services, Process to Track Products Across Supply Chain, Process to Verify IT Products Supplied Function as Expected, Process and Policy Concerning Information Sharing, Process to Conduct Risk Assessment concerning Information and Communication Technology Supply Chain.
A.15.2	Supplier Service Delivery Management		
A.15.2.1	Monitoring and Review of Supplier Services	Process to Regularly Monitor, Review, and Audit Supplier Service Delivery, Process for Information Risk Assessment concerning Supplier Service,	

Standard	Section	Generic Checklist
		Process to Review Proposed Segmentation of Suppliers, Process to ensure Communication upon Formal Change Control Process.
A.15.2.2	Managing Changes to Supplier Services	Policy and Process for Supplier Service Change Management, Process for Changes to the Provision of Services by Suppliers, Process for Maintaining and Improving Existing Information Security Policies and Procedures, Process to Control the Changes to Suppliers Services, Process to Perform Re-Assessment of Risks, Process for Improvements of Existing Offered Services, Process for Development of all New Systems and Applications.
A.16	Information Security Incident Management	
A.16.1	Management of Information Security Incident and Improvements	Policy and Process for Information Security Incident Management, Process to Define Roles and Responsibilities concerning Information Security, Process to communicate Security Incidents and Vulnerabilities.
A.16.1.1	Responsibilities and Procedures	Process to Define Information Security Incident Management Roles and Responsibilities, Management Roles and Procedures for Management of Incident Information Security, Process and Procedure for Incident Response, Process for Monitoring, Identifying, Analysing and Reporting Procedures for Events and Incident-related to Information Security, Process for Logging Procedures for Incident Management, Forensic Evidence Management Procedures, Procedures for Regular Information Security Evaluation, Procedure for Decision Making and Information Security Vulnerability Assessment, Incident Response Protocol including Escalation measures, Managed Recovery from Incidents and Contact to Internal and External Individuals or Organizations, Process and Procedure for Hiring Competent Staff Handling Information Security Issues, Procedure for Contacting for Identification and Reporting of Safety Incidents, Procedure for Maintaining Adequate Contacts with Authorities, Groups of External Interest or Forums that deal with Information Security Issues, Feedback Processes to ensure that Authority is Reported of the Information Security Events and Notified of the results following Resolution and Closure of the Issue.

Standard	Section	Generic Checklist
A.16.1.2	Reporting Information Security Events	Policy and Process for Reporting of Information Security Events, Process of Reporting through Appropriate Management Channels, Process for Conducting Awareness Training of their Responsibility for Reporting Security Incidents, Protocol for Reporting the Incident including the Information to be Reported. Procedure for Incident Reporting Procedures and Responsibilities.
A.16.1.3	Reporting Information Security Weaknesses	Process for Recording and Documenting Information Security Vulnerabilities, Process for Training Staff to ensure System for Reporting is Easy, Open, and Usable, Process for Conducting Test of Systems to determine Deficiency and possible Violation.
A.16.1.4	Assessment of and Decision on Information Security Events	Process of Evaluating and Analyzing Information Security Events and considering it as Incident of Information Security, Process for Classifying Information Security Incidents, and Events of Weaknesses, Procedure to Assess and Determine the Best Course of Action, Procedure for Reporting which includes listing who should be Reported and what Information should be Reported, Process to ensure the Reporting of Incidents meets the Applicable Regulatory Requirements.
A.16.1.5	Response to Information Security Incidents	Process to Assign Responsibilities to Respond to Information Security Incidents, Process to Define Actions, Timescales and Audit Process, Process for Restoring a Normal Level of Security, Process for Conducting Forensic Investigation, Process for Gathering Evidence, Process for Escalation of Measures, Process for Adequate Documentation for Subsequent Analysis of all Responses Activities, Process to Address Addressing the Vulnerabilities Identified for Information Security, Procedure for Formal Closure and Recording of the Incident until Effectively Concluded.
A.16.1.6	Learning from Information Security Incidents	Process to Document the Reports and Findings of the Incident, Process to Analyse the Findings in the Report, Process or Mechanism to Measure and Track the Forms, Quantities, and Costs of Events Affecting Information Security, Process to Classify Recurring or High Impact Events, Process to Review Security Policy Assessment of Information Security Accidents and Process to ensure Improved or Additional Control Requirement.

Standard	Section	Generic Checklist	
A.16.1.7	Collection of Evidence	Process for Forensic Investigation,	Procedure to Collect Evidence, Procedure to Procure and Retain Information as Documentation and Implement Procedures, External Protocols for Treating Evidence for Administrative and Legal Action, Process for Documenting Forensic Findings, Process for Disciplinary Procedures, Information Security Incident Management.
A.17	Information Security Aspects of Business Continuity Management		
A.17.1	Information Security Continuity		
A.17.1.1	Planning Information Security Continuity	Policy and Procedure for Information Security,	Process for Business Continuity Management, Process defining the Information Security Standards and Consistency of Information Security Management, Process to Perform Regular Assessments for Continuity of security in the Management Process of Business Continuity or Disaster Recovery Process, Process for Information Security Standards for Security Criteria related to Adverse Circumstances and Information Security Management.
A.17.1.2	Implementing Information Security Continuity	Process to Mitigate and Respond to Disruptive Events,	Process to hire an Incident Response Personnel for Incident Management and Information Security, Process that defines Roles, Responsibilities, and Authority Incident Response Personnel, Process to Document Plans, Response and Recovery Procedures, Procedure ensuring Information Security Continuity Objectives are Approved through Management.
A.17.1.3	Verify, Review and Evaluate Information Security Continuity	Process to Verify, Review and Evaluate Information Security Continuity,	Process to Review On-going Controls on Safety Information at Regular Intervals, Process to ensure Change in the Environment also Includes Change in the Continuity of Information Security Processes, Procedures and Controls, Process to Exercise and Test Reliability of Systems, Procedures, and Controls, Process to Exercise and Test Expertise and Routine in the Systems, Procedures and Controls for Information Security Continuity, Process to Test Information Security Mechanisms, Policies,

Standard	Section	Generic Checklist	
		and Controls, and Business Continuity Management/Disaster Recovery methods and Strategies to Test Quality and Efficacy of Information Security Initiatives, Tests Verifying Continuity Controls in Information Security.	
A.17.2	Redundancies		
A.17.2.1	Availability of Information Processing Facilities	Process to ensure Availability of Information Processing Systems, Process for Testing of Redundant Components and Systems Periodically, Process to ensure Redundant Components & Systems are in place.	
A.18	Compliance		
A.18.1	Compliance with Legal and Contractual Requirements		
A.18.1.1	Identification of Applicable Legislation and Contractual Requirements	Process to Identify, Document, and Update all Relevant Statutory, Regula-tory, Contractual Requirements, Process for Classifying the Nature of Infor-mation being Handled, Process to Consult Legal Experts, Regulatory bodies, and Contract Managers to Relevant Legislation, Regulation, and Contractual Requirements, Process to Record, Document Legal Contractu-al Obligations.	
A.18.1.2	Intellectual Property Rights	Intellectual Property Rights Policy, Procedures that ensure Compliance with Legislative, Regulatory, and Contractual Requirements related to In-tellectual Property Rights and Use of Proprietary Software Products, Pro-cess for Intellectual Property Rights Management, Process for Protection of IPR and ensure Prevention of Misuse or Breach of IPR, Process for Asset Registers and Acceptable Use Policies concerning the IPR, Guidelines and Controls to Ensure only Authorised and Licensed Software are in Use, Process for Regular Inspection and Audit concerning Authorised and Li-censed Software Use. Process to Maintain to take Disciplinary Steps against Personnel Violating Intellectual Property Rights Policy.	

Standard	Section	Generic Checklist
A.18.1.3	Protection of Records	Provision to Protect Records in accordance with the legislative, regulatory, contractual, and business requirements, Process to Protect Records from Loss, Destruction, Falsification, and Unauthorized Access and Unauthorized Release, Process to Secure relevant Organizational Documents, Encryption Policy, Digital Signature Usage Policy, Guidelines and Process concerning Documents and Information Processing, Storage, Handling and Disposal, Retention Policy for all Recorded Documents, Inventory Policy for all Information Sources, Protocols to Protect against Loss due to Potential Technical Changes.
A.18.1.4	Privacy and Protection of Personally Identifiable Information	Privacy Policy, Data Protection Policy, Process to ensure Confidentiality and Integrity of Personally, Identifiable Information, Security Controls for Data Protection and Management, Process for Training and Awareness of Information Security Principles, Process for Monitoring the Collection, Processing, and Transmission of Personal Information.
A.18.1.5	Regulation of Cryptographic Controls	Policy and Process for Use of Cryptographic Controls, Process to Implement Controls and Awareness Programmes concerning cryptography that ensures Compliance, Process to Restrict Import or Export of Computer Hardware and Software for Cryptographic functions, Policy and Process to Restrict the Use of Encryption, Process of Access to Information Encrypted by Hardware or Software, Access Control Policy, Process for Authorization of Access.
A.18.2	Information Security Reviews	
A.18.2.1	Independent Review of Information Security	Policy for Information Security Management, Policy, and Process for Review of Information Security, Process to ensure Independent Review of Information Security is Consistent, Appropriate, and Efficient, Process to ensure Independent Review Results are Recorded and Reported to the Management Responsible for Initiating the Review, Process for Managing Information Security and its Implementation, Independent Review of Security Risks and Controls, Process to ensure Performing Reviews at Regular Intervals or as and when Significant, Security relevant Changes occur.

Standard	Section	Generic Checklist	
A.18.2.2	Compliance with Security Policies and Standards		Regulatory and Compliance Policy, Process to Regularly Review Compliance of Information Processing, Process to ensure Staff Comply with Organizational Policy and Control, Process Log and Manage Non-compliance identified, Process for Awareness, Education or Training of User, Provision for Proactive Preventative Policies, Controls, and Awareness Programs, Process for Compliance Monitoring, Review, and Audit.
A.18.2.3	Technical Compliance Review		Policy and Process for Technical Compliance Reviews, Policy and Process to ensure Information Systems are Regularly Reviewed for Compliance, Information Security Policies and Standards, Provision to check Systems and Networks for Technical Compliance, Process for Adequate Levels of Compliance Testing based on Risk Levels, Process for Risk Assessments including Penetration Test, Vulnerability Test.



VISTA INFOSEC®

TRUSTED ADVISORS, ASSURED COMPLIANCE™

Contact Us



info@vistainfosec.com

US Tel: +1-415-513-5261

UK Tel: +442081333131

SG Tel: +65-3129-0397

IN Tel: +91 73045 57744

Dubai Tel: +971507323723



www.vistainfosec.com

