ISO 27001:2022

AUDIT CHECKLIST

PART 4
A.8 TECHNOLOGICAL CONTROLS

MINISTRY OF SECURITY

A.8 Technological Controls				
Control No.	**Control**	**Control Description**	**Assessment Questions**	**Response**
8.1	User end point devices	Information stored on, processed by or accessible via user end point devices shall be protected	1.Whether a mobile device policy exists and is approved? 2. Inventory details of the mobile devices registered 3.Whether policy document address additional risk of using mobile devices (eg.Theft of devices, use of open Wi-Fi hotspots? 4.Whether organisation have access control and malware protection in place for mobile devices? 5. Does organisation take regular backup of mobile devices? 6. Is there a process for registration of user endpoint devices? 7. Is there any restriction of software installation on user endpoint devices? 8. Is there any remote disabling, deletion or lockout controls implemented on user endpoint devices? 9. Are the USB ports disabled on user endpoint devices?	
8.2	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed	1. What are the criteria that your organisation has planned for a user to be assigned access privileges? 2. How your authorise and record access privileges and maintain them? 3. Whether there is an access control policy? 4. How organisation notify their employees about their assigned privileged access? 5. Procedure in place for preventing unauthorised use of generic ID 6.Whether organisation defined the conditions of expiry for privilege access? 7. Is there a process to review the privilege access rights assigned to users? 8. How often are the access review performed?	
8.3	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	1.Do you ensure that sensitive information is kept confidential, and no unauthorised identities have access to that information? 2. Whether organisation has a defined, maintained and controlled what data can be accessed by whom? 3. Does the organisation control which identified will have which access (Read,write,delete,execute) 4.Whetheher the organisation provide physical/logical access control for isolating sensitive systems, application and data?	

8.4	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed	1.Whether the organisation manages the access to program source code and its libraries according to established procedures. 2. Whether granting and revoking of read/ write access is on need basis? 3. Does your organisation assure that the developers have source code access only through developer tools which has proper authorisation? 4. Does you organisation maintain the audit log of all accesses and all changes done to source code?	
8.5	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control	1.Does your organisation test that no confidential information is displayed before log on process has successfully completed? 2. Whether your organisation display generic notices /warnings that systems should be accessed by authorised users only? 3. Whether there is a defined limit on unsuccessful login attempts? 4. Whether a procedure defined for raising a security issue? 5. whether passwords are masked? 6. Whether the passwords are encrypted before transmission? 7. Whether a session time out is in place to logout the inactive sessions? 8. Are the users mandated to change passwords upon first login? 9. Are the default vendor accounts and passwords changed?	
8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirement	1. Is there a process to manage capacity requirements of all systems based on the business process and criticality of the process. 2. Is there a process to identify expected capacity requirements for the future. 3. Are there any detective controls implemented to indicate problems and notify administrators. 4. Whether the organisation follows the retention practises and remove absolute data?	
8.7	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	1.Whether your organisation created a formal policy for managing Malware? 2. Is the Antimalware solution implemented on all systems? 3. Is the antimalware solution configured to perform periodic scans? 4. Is the antimalware solution configured to get signature updates on regular basis? 5. Is the antimalware solution configured to send alerts to system administrators upon identifying malware? 6. Is there a process in place for detecting malicious websites?	

8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be take	1. Are the Roles and responsibilities pertaining to vulnerability monitoring, vulnerability risk assessment, patching defined? 2. Is the scope and frequency of technical vulnerability assessments defined? 3. Is there a process to rate the vulnerabilities as Critical, High, Medium and Low? 4. Are the remediation timelines defined as per the vulnerability ratings? 5. Is there a formal process to install patches for remediating vulnerabilities? 6. Are we testing and evaluating the patches before they are installed?	
8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	1. Whether your organisation has a policy and procedure in place for documenting the configurations of hardware, software and network devices? 2. Is there a proper role and ownership assigned to individuals for managing configuration on device? 3. Whether organisation follows a standardised template for hardening hardware's and softwares? 4. Does organisation have appropriate mechanism in place to review system, hardware updates at regular intervals and any current security threats to ensure optimal performance?	
8.1	Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	1. Does your organisation have policy that covers maintenance activities related to deletion and destruction of data and or IT assets including the utilisation of specialised software and liaison with vendors specialising in data and device deletion? 2. Whether organisation regularly identifies data which is no longer in use and needs to be removed to prevent from unauthorised access or misuse? 3. When employing specialised deletion vendor, whether sufficient evidence is obtained (via documentation) that the deletion has been performed?	
8.11	Data masking	Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration	1.Whether the organisation has a policy and procedure in place to ensure anonymization or pseudonymization of data for protection of data as per legal and regulatory requirements? 2. Process in place to discover how masked data is accessed? 3. Whether data masking policy and procedure includes following requirements? -Implement masking techniques to expose only the lowest possible amount of data those who use it -At the request of the subject, certain data may be hidden and staff access to relevant sections is restricted to only certain members. -Constructing their data masking procedure in accordance with legal and regulatory requirements.	

			-Pseudonymization requires use of an algorithm to unmask data and this must be kept secure	
8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information	1. Has the organisation defined a procedure in place to reduce the risks of data leakage from emails, inward outward file transfer and USB devices? 2. Has the organisation established proper measures to ensure data is organised according to industry standards to assign different levels of risk? 3. Has organisation setup proper authorisation methods? 4. Whether the data in back up and all sensitive data is encrypted? 5. Whether organisation has implemented gateway security and leakage retention measures to protect against external influences? 6. Has the organization identified monitoring channels for identifying data leakage?	
8.13	Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	1. Has organisation got approved policy and procedure for managing backup of data on devices, storage media, cloud, DB and servers? 2. How often the servers and configuration data are getting backed up ? 3.Whether the backed up data are restored and checked at regular intervals. 4. Whether the results of restorations are recorded? 5. Whether backup plan is updated on regular basis? 6. Has the organization defined the backup restoration testing frequency?	
8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements	1.Has the organisation have a policy and procedure in place to ensure data processed through any ICT technology, physical facility, software is duplicated to ensure availability in event of disruption? 2.Has organisation considered geographically disparate locations when outsourcing data services (file storage/data centre amenities) 3.Whether redundancy is in place for all systems to ensure availability of information processing facility	

8.15	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed	1. Do you have a process to review security audit logs in timely and act upon threats ? 2.Are appropriate event logs maintained and regularly reviewed? 3.Whether logging facilities protected against tampering and unauthorised access? 4.Whether system admin /operator activities logged and reviewed regularly? 5.Whether NTP services are deployed and systems are synced with the NTP services 6.Whether log archives are maintained ? 7.How log collection and aggregating from different network ,security , servers , DB, Identity systems and applications is managed?	
8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	1. Whether company has a policy and procedure in place to suspect events which should be reported to relevant personnel in order to maintain the network integrity and improve business continuity 2. Has the organization established a baseline for normal working conditions to identify anomalies in the network?	
8.17	Clock synchronizatio n	The clocks of information processing systems used by the organization shall be synchronized to approved time sources	1. Has the organization identified reputed time source? 2. Whether all devices are in sync with this NTP server hosted in organisation 3. Is there a process to restrict access to time data in the organization? 4. Is there a process to identify and monitor all changes to NTP systems?	
8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding see	1.Whether organisation has defined list of utility programs? 2. Does organisation has procedure in place to identify, authorise and authenticate using utility programs? 3.Whether ad hoc utility programs ae used? If yes, the approval process for the same. 4. Details of logging for utility program	
8.19	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems	1.Policy and procedure in place for software installation and to upgrade existing software's 2.List of whitelisted software approved by management to be used in organisation 3.Audit logs maintained for changes carried out? 4. Change management procedure, policy for installing/upgrading new software's 5.Sample change management tickets raised for such installation and upgradation of software's	

8.20	Networks security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications	1.Does the organisation have a approved copy of the network diagram? 2.Network asset inventory for the organisation? 3.Whether logging and monitoring of network equipment's in place? 4.Details of network configuration files storage and their backup? 5. What is the encryption controls deployed for data in transit? 6.Is there a Procedure in place for authenticating network devices?	
8.21	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored	1. Policy and procedure in place for network security management? 2.Procdeure for updating the OS patches, NW OS? 3.Details of approved individuals who can make changes to network ? 4. Details of SIEM,DLP.SOAR,IDS,IPS implemented? 5. Is there a procedure in place to access network devices?	
8.22	Segregation of networks	Groups of information services, users and information systems shall be segregated in the organization's networks.	1. What security controls are implemented to ensure Segregation of access for production, testing and development environment? 2. How is the network segmented and how is the access monitored to different segments of network?	
8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	1. Are the Web filtering rules implemented to permit access to specific websites only? 2.Whether there is an approved list of high risk website/content category 3. are the controls implemented to block malicious content from being downloaded(Eg.Web proxy, email gateway, ant phishing module, EDR ?	
8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented	1. Has organisation got an cryptography policy in place? 2. How are the cryptographic keys accessed, stored and safeguarded? 3. Is the Inventory of cryptography keys and certificates used maintained? 4. Is there a process defined to decide the encryption key strength and encryption algorithm? 5. Is the crypto period defined for all encryption keys?	
8.25	Secure development life cycle	Rules for the secure development of software and systems shall be established and applied	1. Does the organization have a Secure application development policy? 2. Are security requirements considered in all phases of development? 3. Is there any secure coding guidelines used for development? 4. Does the organization have secure source code repositories?	

			5. Does the organization maintain version controlling on source code?	
8.26	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications	1. Is there a process to ensure identify all information security requirements when developing or acquiring applications? 2. Are the legal, statutory and regulatory requirements considered during application development 3. Are the privacy requirements considered during application development?	
8.27	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities	1.Documented standards, evidence for engineering secure system and system architecture 2. Whether Secure Engineering guidelines include the following -Methods of user authentication -Secure session control guidance -Procedure for sanitising and validating data -Security measures for protecting information assets and systems against known threats -Security measures analysed for their ability to identify, eliminate and respond to security threats -How and where the security measures will be implemented 3. Procedure in place for validating the practises, standards of service provider/third parties so they are in line with secure engineering protocols	
8.28	Secure coding	Secure coding principles shall be applied to software development	1. Details of Secure Development policy and procedures 2. Threat and vulnerability process 3.Tools for secure code development if any 4.Reports on Secure code review, SAST,DAST 5.Whether development team is regularly trained on real world threats 6.Whether secure coding takes into account following points -Details on attack surface - OWASP Top 10 Vulnerabilities	
8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	1.Whether user authentication, access restrictions and use of cryptographic techniques tested? 2.Whether organisation tests the secure configs of OS , firewalls and other components 3.Whether the organisation has a test plan defined, documented and implemented? 4. Whether organization carriers out VA , if yes the frequency and reports of the same 5. Whether organisation conducts PT, if yes the frequency and the reports of the same 6.Whether organisation tests their DB for their security	

8.3	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	1.Whether licensing , code ownership and IPR related to outsourced development in place? 2.Does organisation have contractual requirements for secure design, coding and testing practises 3.Whether provision for threat modelling considered by external developers? 4.Whether UAT is done and approved 5.Details of software ESCROW in place 6. Details of organisation conducting an audit on third party in place?	
8.31	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured	1. Whether organisation has segregated environment for application (Development, test and production) 2.Access control list for each environment and review of the same. 3.Privilege user access management process in place 4.Patch, Backup management process in place 5.VAPT detailed reports 6.Details of web application security	
8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	1. Whether organisation has a change management policy and procedure? 2. Is there a formal change request process? 3. Are the change Impact assessment, testing and roll back plan defined for all changes? 4. Are the changes approved before implementation? 5. Is there a process to manage emergency changes?	
8.33	Test information	Test information shall be appropriately selected, protected and managed	1.Whether organisation applies same access control procedures to test and production environments? 2.Details of approval if prod data is coped to testing environment? 3.Sample of data used in testing, development and production environment? 4.Does organisation have defined the data management process and guidelines in place	
8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management	1.Whether organisation has a system audit and assurance plan? 2.List of all privacy laws and regulations 3. Details of the audit calendar and recent audit reports 4. Procedure in place for protecting the PII data 5. User awareness records of personal involving system operations	

FOLLOW US ON LINKEDIN FOR MORE FREE CHECKLISTS

PLAYBOOK MADE WITH 

MINISTRY OF SECURITY