The checklist is prepared based on the **best practices followed in the industry** to Improve the IT related process.

This PDF covers only the checkpoints related to below mentioned area -

1. Planning the IT Function
2. Implement IT Plan

The next post will include checkpoints related to Step 3 and Step 4

SACHIN HISSARIA
CA | CISA | DISA | CEH | COBIT-19 | ISO27001:2022 | RPA | Trainer

Ref #	Audit objective	Risk Category	Auditors Remark
A	**Planning the IT Function**		
	IT Plan and Strategy		
A.1.	Does the Organization have an IT strategy / IT plan approved by Management	High	
A.2.	Is there a process of minimum of annual review of the IT strategy /Plan	High	
A.3.	Is there a periodic review (minimum annual) of IT performance - covering key parameters in IT strategy such as Data Sizing, Network Performance?	High	
	Information Architecture – Policy and Procedure Review		
	INFORMATION SECURITY POLICY DOCUMENT		
A.4.	Is there an Information security policy, approved by the management and adopted by the Board?	High	
A.5	Does it state the management commitment and set out the organisational approach in managing information security?	High	
A.6	Does the Information Security Policy cover the following key areas of IT Security • Detailed IT Security Policy and Procedures • Organisation and security • Asset Classification and Control • Personnel Security • Physical and Environmental Security • Communications and Operations Management • Access Control • Systems Development and Maintenance • Information Security Incident Management • Business Continuity Management • Compliance requirements to Policies and Procedures IT Risk Management Process?	High	
A.7.	Has the Security Policy been published and communicated as appropriate to all employees and vendors?	High	
A.8.	Are new members of staff and vendors made aware of Information Security Policy?	High	
A.9.	Are continuous awareness programmes conducted for security awareness?	High	
A.10.	Has the role of Information Security Officer with responsibilities for implementation of the Security Policy been assigned?	High	
A.11.	Whether detailed procedures for each policy statement developed?	High	
A.12	Is the Information Security Officer made responsible for: • Reporting non- compliance with the approved policy • Incidents of security breaches to the Top Management, • Initiating and effecting corrective action?	High	
	INCIDENT MANAGEMENT PROCEDURES		
A.13.	Whether an Incident Management procedure exists to handle security incidents.	High	

Ref #	Audit objective	Risk Category	Auditors Remark
A.14	Whether there are clearly defined procedures and rules covering the different types of security incidents.	High	
A.15	Whether the procedure addresses the incident management responsibilities, orderly and quick response to security incidents	High	
A.16	Whether the procedure addresses different types of incidents ranging from denial of service to breach of confidentiality etc., and ways to handle them.	High	
	INVENTORY OF ASSETS		
A.17.	Whether an inventory or register is maintained with the important assets associated with each information system.	High	
A.18	Whether each asset identified has an owner, the security classification defined and agreed and the location identified.	High	
A.19.	Is there an *up-to-date* network diagram?	High	
A.20.	Is the inventory schedule and networking plan reviewed at regular intervals to ensure that they are complete and up- dated?	High	
A.21.	Are all the system configurations properly documented?	High	
A.22	Is the configuration document regularly updated as per a fixed schedule?	High	
	INFORMATION LABELING AND HANDLING		
A.23.	Whether an appropriate set of procedures are defined for information labeling and handling in accordance with the classification scheme adopted by the organization.	High	
	CORRECT DISPOSAL OF RESOURCES REQUIRING PROTECTION		
A.24.	Is there a policy of identifying resources and media based on their level of sensitivity	High	
A.25.	Is there a disposal process commensurate with each level of sensitivity	High	
A.26.	Are the specified disposal provisions complied with	High	
A.27	Is the disposal procedure reliable	High	
	ACCESS CONTROL POLICY		
A.28.	Whether the business requirements for access control have been defined and documented.	High	
A.29.	Whether the Access control policy does address the rules and rights for each user or a group of user.	High	
A.30.	Whether the users and service providers were given a clear statement of the business requirement to be met by access controls.	High	
	CLASSIFICATION GUIDELINES		
A.31.	Whether there is an Information classification scheme or guideline in place; which will assist in determining how the information is to be handled and protected.	High	
	MANAGEMENT OF REMOVABLE COMPUTER MEDIA		
A.32.	Whether there exists a procedure for management of removable computer media such as tapes, disks, cassettes, memory cards and reports.	High	

Ref #	Audit objective	Risk Category	Auditors Remark
	OTHER FORMS OF INFORMATION EXCHANGE		
A.33.	Whether there are any policies, procedures or controls in place to protect the exchange of information through the use of voice, facsimile and video communication facilities.	High	
A.34.	Whether staffs are reminded to maintain the confidentiality of sensitive information while using such forms of information exchange facility.	High	
	INFORMATION AND SOFTWARE EXCHANGE AGREEMENT		
A.35.	Whether there exists any formal or informal agreement between the organizations for exchange of information and software.	High	
A.36.	Whether the agreement does address the security issues based on the sensitivity of the business information involved.	High	
	Determine technological direction.		
	INDEPENDENT REVIEW OF INFORMATION SECURITY		
A.37.	Whether the implementation of security policy is reviewed independently on regular basis. This is to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective.	High	
	TESTING, MAINTAINING AND RE-ASSESSING BUSINESS CONTINUITY PLAN		
A.38.	Whether Business continuity plans are tested regularly to ensure that they are up to date and effective.	High	
A.39.	Whether Business continuity plans were maintained by regular reviews and updates to ensure their continuing effectiveness.	High	
A.40.	Whether procedures were included within the organizations change management programme to ensure that Business continuity matters are appropriately addressed.	High	
	MOBILE COMPUTING		
A.41.	Whether a formal policy is adopted that takes into account the risks of working with computing facilities such as notebooks, palmtops etc., especially in unprotected environments.	Medium	
	WORKING FROM OFFSITE		
A.42.	• Whether policy, operational plan and procedures are developed and implemented for working from offsite. This should cover both employees and partners. • Whether such activity is authorized and controlled by management and does it ensure that suitable arrangements are in place for this way of working.	High	
	Define the IT Processes, Organization and Relationships		
	AUTHORISATION PROCESS FOR INFORMATION PROCESSING FACILITIES		

Ref #	Audit objective	Risk Category	Auditors Remark
A.43.	Whether there is a management authorization process in place for any new facilities such as • Hardware • Software incl. applications • information processing facility like data centers, offices etc. • changes to configurations in existing Assets.	High	
A.44.	Are log-books kept of system changes	High	
A.45.	Are there any guidelines for implementing changes to IT components, software or configuration data?	High	
A.46.	Are all changes documented?	High	
	INFORMATION SECURITY COORDINATION		
A.47.	Whether there is a cross- functional forum of management representatives from relevant parts of the organization to coordinate the implementation of information security controls.	Low	
	ALLOCATION OF INFORMATION SECURITY RESPONSIBILITIES		
A.48.	Has an IT Security Officer been appointed?	High	
A.49.	Whether responsibilities for the protection of individual assets and for carrying out specific security processes are clearly defined.	High	
A.50.	Is there an establishment of a suitable organizational structure for IT security	High	
	CONFIDENTIALITY AGREEMENTS		
A.51.	Whether employees are asked to sign confidentiality or non- disclosure agreement as a part of their initial terms and conditions of the employment.	High	
A.52.	Whether this agreement covers the security of the information processing facility and organization assets.	High	
	INCLUDING SECURITY IN JOB RESPONSIBILITIES		
A.53.	Whether security roles and responsibilities as laid down in Organization's information security policy documented were appropriate.	Low	
A.54.	Does it include general responsibilities for: implementing or maintaining security policy, specific responsibilities for protection of particular assets, extension of particular security processes or activities.	Low	
	PERSONNEL SCREENING AND POLICY		
A.55.	Whether verification checks on permanent staff were carried out at the time of job applications. This should include: • character reference, • confirmation of claimed academic • professional qualifications • independent identity checks.	High	
	TERMS AND CONDITIONS OF EMPLOYMENT		

Ref #	Audit objective	Risk Category	Auditors Remark
A.56.	Whether terms and conditions of the employment covers the employee's responsibility for information security. Where appropriate: • At the joining date • At time of internal transfers • On termination/end of the employment.	Low	
	INFORMATION SECURITY EDUCATION AND TRAINING		
A.57.	Whether all employees of the organization and third party users (where relevant) receive appropriate Information Security training and regular updates in organizational policies and procedures.	Low	
A.58.	Is the IT Security Management Team involved in the planning and delivery of IT training?	Low	
	DATA PROTECTION AND PRIVACY OF PERSONAL INFORMATION		
A.59.	Whether there is a management structure and control in place to protect data and privacy of personal information.	Medium	
	IDENTIFICATION OF APPLICABLE LEGISLATION		
A.60.	Whether all relevant statutory, regulatory and contractual requirements were explicitly defined and documented for each information system.	Medium	
	INTELLECTUAL PROPERTY RIGHTS		
A.61.	Whether there exist any procedures to ensure compliance with legal restrictions on use of material in respect of which there may be intellectual property (IPR) rights such as copyright, design rights, trade marks.	High	
A.62.	Whether the procedures are well implemented.	High	
A.63.	Whether proprietary software products are supplied under a license agreement that limits the use of the products to specified machines. The only exception might be for making own back- up copies of the software.	High	
	SAFEGUARDING OF ORGANISATIONAL RECORDS		
A.64.	Whether important records of the organization are protected from loss destruction and falsification.	High	
	SECURING OF EQUIPMENT OFF-PREMISES		
A.65.	Whether any equipment usage outside an organization's premises for information processing has to be authorized by the management..	High	
A.66.	Whether the security provided for these equipments while outside the premises is at par with or more than the security provided inside the premises.	High	
	SEGREGATION OF DUTIES		

Ref #	Audit objective	Risk Category	Auditors Remark
A.67.	Whether duties and areas of responsibility are separated in order to reduce opportunities for unauthorized modification or misuse of information or services. This should include. Distinction between IT and Business Development and Production.	High	
	SEPARATION OF DEVELOPMENT AND OPERATIONAL FACILITIES		
A.68.	Whether the development and testing facilities are isolated from operational facilities. For example, development software should run on a computer different from the computer with production software. Where necessary development and production network should be separated from each other.	High	
	NETWORK CONTROLS		
A.69.	Whether effective operational controls such as separate network and system administration facilities were established where necessary.	High	
A.70	Whether responsibilities and procedures for management of remote equipment, including equipment in user areas are established.	High	
A.71	Whether there exist any special controls to safeguard confidentiality and integrity of data processing over the public network and to protect the connected systems.	High	
A.72.	Whether access attempts via *telnet*, *ftp* are logged and reviewed.	High	
	IDENTIFICATION OF RISKS FROM THIRD PARTY		
A.73.	Whether risks from third party access are identified and appropriate security controls implemented.	High	
A.74.	Whether security risks with third party contractors working onsite are identified and appropriate controls are implemented.	High	
	SECURITY REQUIREMENTS IN THIRD PARTY CONTRACTS		
A.75.	Whether there is a formal contract containing, or referring to, all the security requirements to ensure compliance with the organization's security policies and standards.	High	
	WORKING IN SECURE AREAS		
A.76.	Whether there exists any security control for third parties or for personnel working in secure area.	High	
	PREVENTION OF MISUSE OF INFORMATION PROCESSING		
A.77.	Whether use of information processing facilities for any non- business or unauthorized purpose, without management approval is treated as improper use of the facility.	High	
A.78.	Whether at the log-on a warning message is presented on the computer screen indicating that the system facility being entered is private and that unauthorized access is not permitted.	High	
	REGULATION OF CRYPTOGRAPHIC CONTROLS		

Ref #	Audit objective	Risk Category	Auditors Remark
A.79.	Whether the cryptographic controls are used in compliance with all relevant agreements, laws, and regulations.	Low	
	ACCEPTABLE USE OF ASSETS		
A.80.	Whether regulations for acceptable use of information and assets associated with an information processing facility were identified, documented and implemented. The auditor is required to understand the policies with respect to use of Information Assets and controls available to prevent their misuse.	High	
	MANAGEMENT RESPONSIBILITIES		
A.81.	Whether the management requires employees, contractors and third party users to apply security in accordance with the established policies and procedures of the organization.	Low	
	Manage the IT investment		
	REVIEW AND EVALUATION		
A.82.	Whether the IT Security process ensures that a review takes place in response to any changes affecting the basis of the original assessment, for example: significant security incidents, new vulnerabilities or changes to organizational or technical infrastructure.	Low	
	LEARNING FROM INCIDENTS		
A.83.	Whether there are mechanisms in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored.	Low	
	REPORTING SECURITY INCIDENTS		
A.84.	Are steps taken to ensure that anything unusual in the log files gets reported?	Low	
A.85.	Are the users regularly advised of the requirement to inform the administrator at once in case of irregularities?	Low	
	Communicate management aims and direction		
	PUBLICLY AVAILABLE SYSTEMS		
A.86.	Whether there is any formal authorization process in place for the information to be made publicly available. Such as approval from Change Control which includes Business, Application owner etc., Auditor may also evaluate the control to disclose NAV on the website.	Low	
A.87.	Whether there are any controls in place to protect the integrity of such information publicly available from any unauthorized access. The auditor may obtain VA and PT reports of the website and other web applications where investment related data is hosted.	Low	
	SECURITY REQUIREMENTS IN OUTSOURCING CONTRACTS		

Ref #	Audit objective	Risk Category	Auditors Remark
A.88.	• Whether security requirements are addressed in the contract with the third party, when the organization has outsourced the management and control of all or some of its information systems, networks and/ or desktop environments.	Medium	
	• The contract should address how the legal requirements are to be met, how the security of the organization's assets are maintained and tested, and the right of audit, physical security issues and how the availability of the services is to be maintained in the event of disaster.	Medium	
	INFORMATION ACCESS RESTRICTION		
A.89.	Whether access to application by various groups/personnel within the organization has been defined in the access control policy as per the individual business application requirement and whether it is consistent with the organization's Information access policy.	Medium	
	PASSWORD USE		
A.90.	Whether there are any guidelines in place to guide users in selecting and maintaining secure passwords.	High	
	UNATTENDED USER EQUIPMENT		
A.91.	Whether the users and contractors are made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibility to implement such protection.	Low	
	CLEAR DESK AND CLEAR SCREEN POLICY		
A.92.	Whether automatic computer screen locking facility is enabled. This would lock the screen when the computer is left unattended for a period.	Low	
A.93.	Whether employees are advised not to leave any confidential material in the form of paper documents, media, etc., in a locked place while unattended.	Low	
	RETURN OF ASSETS		
A.94.	Whether there is a process in place that ensures all employees, contractors and third party users surrender all of the organization's assets in their possession upon termination of their employment, contract or agreement.	High	
	MANAGEMENT COMMITMENT TO INFORMATION SECURITY		
A.95.	Whether management demonstrates active support for security measures within the organization. This can be done via clear direction, demonstrated commitment, explicit assignment and acknowledgement of information security responsibilities.	Medium	
	ROLES AND RESPONSIBILITIES		

Ref #	Audit objective	Risk Category	Auditors Remark
A.96.	• Whether employee security roles and responsibilities, contractors and third party users were defined and documented in accordance with the organization's information security policy.	Low	
	• Were the roles and responsibilities defined and clearly communicated to job candidates during the pre- employment process	Low	
	Manage IT human resources		
	USER DELETION		
A.97.	Is there a well defined process for revoking user rights on termination of employment?	High	
A.98.	Is the IS Team promptly informed of the termination of service by a staff member?	High	
A.99.	Are there any former staff members who still hold previously issued passes or user ID?	High	
A.100.	Is it ensured that all entry and access rights of a staff member whose services have been terminated are revoked and deleted, and is the process adequate?	High	
A.101.	When the contractual relationship with outside staff is terminated, are all access authorizations revoked or deleted?	High	
	TERMINATION RESPONSIBILITIES		
A.102.	Whether responsibilities for performing employment termination, or change of employment, are clearly defined and assigned.	High	
	Manage quality		
	EXTERNAL FACILITIES MANAGEMENT		
A.103.	Whether any of the Information processing facility is managed by external company or contractor (third party).	Medium	
A.104.	Whether the risks associated with such management were identified in advance, discussed with the third party, and appropriate controls were incorporated into the contract.	Medium	
	OUTSOURCED SOFTWARE DEVELOPMENT		
A.105.	• Whether the outsourced software development is supervised and monitored by the organization.	Medium	
	• Whether points such as: Licensing arrangements, escrow arrangements, contractual requirement for quality assurance, testing before installation to detect Trojan code etc., are considered.	Medium	
	Manage Projects		
	EMERGENCY PROCEDURES		
A.106.	Is there an authorized person to determine the existence of an emergency?	Medium	
A.107.	Is there an Emergency Procedure Manual?	Medium	
A.108.	Is a description of the emergency organization available?	Medium	
A.109.	Is consideration given to all possible emergencies?	Medium	
A.110.	Are all persons and organizational units stated in the Manual aware of the emergency organization?	Medium	

Ref #	Audit objective	Risk Category	Auditors Remark
A.111.	Has configuration back-up been produced for every employed computer type and/or every employed operating system and easily accessible in case of emergency?	Medium	
A.112.	Is a startup disk available for each configuration PC which can be used to boot the system in the event of a boot failure?	Medium	
	NETWORK PERFORMANCE MEASUREMENT		
A.113.	Are performance measurements and traffic-flow	Low	
A.114.	Has a security analysis of the network environment been conducted?	Low	
	SENSITIVE SYSTEM ISOLATION		
A.115.	Whether sensitive systems are provided with isolated computing environment such as running on a dedicated computer, sharing resources only with trusted application systems, etc.	Low	
	ALTERNATE PROCESSING		
A.116.	Is there a specification of internal and external alternatives?	Low	
A.117.	Are these available and effective?	Low	
A.118.	Are the configuration, capacity and compatibility of internal and external alternatives being adapted to the current status of procedures?	Low	
A.119.	Are the integrity and confidentiality of IT application and data moved to external resources ensured in the case of recourse to external alternatives?	Low	
A.120.	Are there any contingency plans for failure of individual assets?	Low	
A.121.	Are there contingency plans in case of breakdown of data transmission?	Low	
A.122.	Has the data transmission capacity required for the use of alternative resources been adequately assessed?	Low	
A.123.	Are there any alternative solutions for important communication links?	Low	
A.124.	Is there a provision of redundant communication lines?	Low	
A.125.	Is there a sufficient redundant arrangement for network components?	Low	
A.126.	Is there any point of failure in the current infrastructure?	Low	
B	**Implement IT Plan**		
	Acquire and maintain application software		
	OPERATIONAL CHANGE CONTROL		
B.1	Whether all programs running on production systems are subject to strict change control i.e., whether any change to be made to those production programs needs to go through the change control authorization.	High	
B.2	Whether audit logs are maintained for any change made to the production programs.	High	
	AUDIT LOGGING		

Ref #	Audit objective	Risk Category	Auditors Remark
B.3	• Whether audit logs recording user activities, exceptions, and information security events are produced and kept for an agreed period to assist in future investigations and access control monitoring. • Whether appropriate Privacy protection measures are considered in Audit log maintenance	Low	
	FAULT LOGGING		
B.4	• Whether faults are logged analyzed and appropriate action taken.	Low	
	• Whether level of logging required for individual system are determined by a risk assessment, taking performance degradation into account.	Low	
	APPLICATION ACCEPTANCE CRITERIA AND TESTS		
	INPUT DATA VALIDATION		
B.5	• Whether data input to application system is validated to ensure that it is correct and appropriate.	Low	
	• Whether the controls such as: Different types of inputs to check for error messages, Procedures for responding to validation errors, defining responsibilities of all personnel involved in data input process etc., are considered.	Low	
	CONTROL OF INTERNAL PROCESSING		
B.6	• Whether validation checks are incorporated into applications to detect any corruption of information through processing errors or deliberate acts.	Low	
	• Whether the design and implementation of applications ensure that the risks of processing failures leading to a loss of integrity are minimized.	Low	
	• Auditor needs to review the tests performed on the application at the time of acquisition and during any change		
	MESSAGE INTEGRITY		
B.7	• Whether requirements for ensuring and protecting message integrity in applications are identified, and appropriate controls identified and implemented.	Low	
	• Whether a security risk assessment was carried out to determine if message integrity is requires, and to identify the most appropriate method of implementation	Low	
	OUTPUT DATA VALIDATION		
B.8	Whether the data output of application system is validated to ensure that the processing of stored information is correct and appropriate to circumstances.	Low	
	ACCESS CONTROL TO PROGRAM SOURCE CODE		
B.9	Whether strict controls are in place to restrict access to program source libraries.	Low	
	(This is to avoid the potential for unauthorized, unintentional changes.)	Low	

Ref #	Audit objective	Risk Category	Auditors Remark
	RESTRICTION ON CHANGES TO SOFTWARE PACKAGES		
B.10	Whether modifications to software package is discouraged and/ or limited to necessary changes. Whether all changes are strictly controlled	Low	
	Acquire and maintain technology infrastructure		
	EQUIPMENT MAINTENANCE		
B.11	Whether the equipment is maintained as per the supplier's recommended service intervals and specifications.	Low	
B.12	Whether the maintenance is carried out only by authorized personnel.	Low	
B.13	Whether appropriate controls are implemented while sending equipment off premises.	Low	
B.14	If the equipment is covered by insurance, whether the insurance requirements are satisfied.	Low	
	LAPTOPS		
B.15	Are laptop users instructed as regards safe keeping of their computers during mobile use?	Low	
B.16	Is there use of an encryption product for laptop PCs?	Low	
	AUTOMATIC TERMINAL IDENTIFICATION		
B.17	Whether automatic terminal identification mechanism is used to authenticate connections.	Low	
	PLANNING OF A WINDOWS 'OS' NETWORK		
B.18	Is there any documentation indicating which directories on which computers have been shared for network access?	Low	
	CONFIGURATION OF 'OS' SERVERS		
B.19	Is there a document detailing the settings of various parameters in the OS Server?	Low	
B.20	Are these settings adhered to?	Low	
B.21	Is protection of the registry under Windows in place?	Low	
B.22	Have the default passwords for local access been replaced by secure ones?	Low	
	PROTECTION OF SYSTEM TEST		
B.23	Whether system test data is protected and controlled. Whether use of personal information or any sensitive information for testing operational database is shunned.	Low	
	Enable operation and use		
	DOCUMENTED OPERATING PROCEDURES		
B.24	Whether the Security Policy has identified any Operating procedures such as Back-up, Equipment maintenance etc.	High	
B.25	Whether such procedures are documented and used.	High	
	SECURITY OF SYSTEM DOCUMENTATION		
B.26	Whether the system documentation is protected from unauthorized access.	High	

Ref #	Audit objective	Risk Category	Auditors Remark
B. 27	Whether the access list for the system documentation is kept to the minimum and authorized by the application owner (for use by a limited number of users.)	High	
	Manage Changes		
	USE OF SYSTEM UTILITIES		
B.28	Whether system utilities that come with computer installations, but may override system and application control are tightly controlled.	High	
	CHANGE MANAGEMENT		
B.29	Whether all changes to information processing facilities and systems are controlled.	High	
B.30	Is there a written SOP covering the change control program that has been approved?	High	
	TECHNICAL REVIEW OF APPLICATIONS AFTER OPERATING SYSTEM CHANGES		
B.31	Whether there is process or procedure in place to review and test business critical applications for adverse impact on organizational operations or security after the change to Operating Systems. Periodically it is necessary to upgrade operating system i.e., to install service packs, patches, hot fixes etc.	High	