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 -

## 3. Management of IT

## 4. Maintain IT

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

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| C | **Management of IT** | | |
| | **Service delivery** | | |
| C.1 | Whether measures are taken to ensure that the security controls, service definitions and delivery levels, included in the third party service delivery agreement, are implemented, operated and maintained by a third party. | Low | |
| | **Manage third party services** | | |
| | **MONITORING AND REVIEW OF THIRD PARTY SERVICES** | | |
| C.2 | • Whether the services, reports and records provided by third party are regularly monitored and reviewed.<br>• Whether audits are conducted on the above third party services, reports and records, on regular interval. | Medium | |
| | **MANAGING CHANGES TO THIRD PARTY SERVICES** | | |
| C.3 | • Whether changes to provision of services, including maintaining and improving existing information security policies, procedures and controls, are managed.<br>• Does this take into account criticality of business systems, processes involved and re-assessment of risks? | Medium | |
| | **Manage Performance and capacity** | | |
| | **PATCH MANAGEMENT** | | |
| C.4 | Are steps taken to ensure that information about the latest patches is always available? How is the patch level status of systems verified? | Medium | |
| | **CAPACITY PLANNING** | | |
| C.5 | Whether the capacity demands are monitored and projections of future capacity requirements are made. This is to ensure that adequate processing power and storage are available. Example: Monitoring Hard disk space, RAM, CPU on critical servers. | Medium | |
| | **Ensure continuous service** | | |
| | **BUSINESS CONTINUITY PLANNING FRAMEWORK** | | |
| C.6 | Whether there is a single framework of Business continuity plan. | High | |
| C.7 | Whether this framework is maintained to ensure that all plans are consistent and identify priorities for testing and maintenance. | High | |
| C.8 | Whether this identifies conditions for activation and individuals responsible for executing each component of the plan. | High | |
| | **WRITING AND IMPLEMENTING CONTINUITY PLAN** | | |
| C.9 | Whether plans were developed to restore business operations within the required time frame following an interruption in or failure of business process. | High | |
| C.10 | Whether the plan is regularly tested and updated. | High | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| C.11 | Review the written BCP / DRP (s) and verify whether the BCP / DRP(s):<br>• Address(es) the recovery of each business unit/department/ function,<br>• According to its priority ranking in the Risk Assessment; and<br>• Considering interdependencies among systems. | High | |
| C.12 | Whether it take(s) into account:<br>• Personnel;<br>• Facilities;<br>• Technology (hardware, software, operational equipment);<br>• Telecommunications/networks;<br>• Vendors;<br>• Utilities;<br>• Documentation (data and records);<br>• Law enforcement;<br>• Security;<br>• Media; and<br>• Shareholders | High | |
| C.13 | Whether it include(s) emergency preparedness and crisis management aspects:<br>• Has an accurate employee/ manager contact tree;<br>• Clearly defines responsibilities and decision- making authorities for designated teams and/or staff members, including those who have authority to declare a disaster;<br>• Explains actions to be taken in specific emergency situations;<br>• Defines the conditions under which the back-up site would be used;<br>• Has procedures in place for notifying the back-up site;<br>• Designates a public relations spokesperson; and<br>• Identifies sources of needed office space and equipment and list of key vendors (hardware/ software/ communications, etc.) | High | |
| C.14 | Whether the BCP/ DRP establishes processing priorities to be followed in the event not all applications can be processed. | High | |
| C.15 | Whether adequate procedures are in place to ensure the BCP / DRP (s) is (are) maintained in a current fashion and updated regularly. | High | |
| C.16 | Whether a senior manager has been assigned responsibility to oversee the development, implementation, testing, and maintenance of the BCP/ DRP. | High | |
| C.17 | Whether the board reviews and approves the written BCP / DRP(s) and testing results at least annually and documents these reviews in the board minutes. | High | |
| C.18 | Whether senior management periodically reviews and prioritizes each business unit, business process, department, and subsidiary for its critical importance and recovery prioritization. If so, determine how often reviews are conducted. | High | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| C.19 | If applicable, determine whether the senior management has evaluated the adequacy of the BCP/DRPs for its service providers, and ensured the organization's BCP/DRP is compatible with those service provider plans, commensurate with adequate recovery priorities. | High | |
| | **BUSINESS IMPACT ANALYSIS** | | |
| C.20 | Are all functions and departments included in the BIA? | High | |
| C.21 | Review the BIA to determine whether the identification and prioritization of business functions are adequate. | High | |
| C.22 | Does the BIA identifies maximum allowable downtime for critical business functions, acceptable levels of data loss and backlogged transactions, and the cost and recovery time objectives associated with downtime? | High | |
| C.23 | Review the risk assessment and determine if it includes scenarios and probability of occurrence of disruptions of information services, technology, personnel, facilities, and service providers from internal and external sources, including:<br>• Natural events such as fires, floods, and severe weather;<br>• Technical events such as communication failure, power outages, and equipment and software failure; and<br>• Malicious activity including network security attacks, fraud, and terrorism. | High | |
| C.24 | Whether the risk assessment and BIA have been reviewed and approved by senior management and the board. | High | |
| C.25 | Are reputation, operational, compliance, and other risks considered in plan(s). | High | |
| | **RISK MITIGATION STRATEGIES** | | |
| C.26 | Whether adequate risk mitigation strategies have been considered for:<br>• Alternate locations and capacity for:<br>• Data centers and computer operations;<br>• Back-room operations;<br>• Work locations for business functions; and<br>• Telecommunications. | Low | |
| C.27 | Is there a policy for Back-up of:<br>• Data;<br>• Operating systems;<br>• Applications;<br>• Utility programs; and<br>• Telecommunications | Low | |
| C.28 | Is there a policy for Off-site storage of:<br>• Back-up media;<br>• Supplies; and<br>• Documentation, e.g., BCP(s), DRP, operating and other procedures, inventory listings, etc? | Low | |
| C.29 | Is there a provision for Alternate power supplies such as Uninterruptible power supplies (UPS); and Back-up generators. | Low | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| C.30 | Whether there are procedures for,<br>• Duplicates of the operating systems are available both on- and off-site.<br>• Duplicates of the production programs are available both on- and off-site, including both source (if applicable) and object versions.<br>• All programming and system software changes are included in the back up.<br>• Back-up media is stored off- site in a place from which it can be retrieved quickly at any time.<br>• Frequency and number of back-up generations is adequate in view of the volume of transactions being processed and the frequency of system updates.<br>• Duplicates of transaction files are maintained on- and off-site.<br>• Data file back-ups are taken off-site in a timely manner and not brought back until a more current | Low | |
| C.31 | Review the written IT continuity plan(s) and determine whether the plan(s) addresses the back- up of the systems and programming function (if applicable), including,<br>Back-up of programming tools and software; and<br>Off-site copies of program and system documentation. | Low | |
| C.32 | Does the plan deal with how backlogged transactions and other activity will be brought current. | Low | |
| C.33 | Whether adequate physical security and access controls exist over data back-ups and program libraries throughout their life cycle, including when they are created, transmitted/delivered to storage, stored, retrieved and loaded, and destroyed. | Low | |
| C.34 | Do appropriate policies, standards, and processes address business continuity planning issues including:<br>• Systems Development Life Cycle, including project management;<br>• The change control process;<br>• Data synchronization, back up, and recovery;<br>• Employee training and communication planning;<br>• Insurance; and<br>• Government and community coordination? | Low | |
| C.35 | Whether personnel are adequately trained as to their specific responsibilities under the plan(s) and whether emergency procedures are **posted in prominent locations** throughout the facility. | Low | |
| C.36 | Does the continuity strategy include alternatives for interdependent components and stakeholders, including:<br>• Utilities;<br>• Telecommunications;<br>• Third-party technology providers;<br>• Key suppliers/business partners; and<br>• Customers/members. | Low | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| C.37 | • Are there adequate processes in place to ensure the plan(s) are maintained to remain accurate and current?<br>• Designated personnel are responsible for maintaining changes in processes, personnel, and environment(s)?<br>• The board of directors reviews and approves the plan(s) annually and after significant changes and updates?<br>• Process includes notification and distribution of revised plans to personnel and recovery locations? | Low | |
| | **DISASTER RECOVERY SITE / ALTERNATE PROCESSING SITE** | | |
| C.38 | Does the Insurer have a clear Off-site Back-up of Data in a City falling under a different Seismic Zone, either on its own or through a Service Provider? | High | |
| C.39 | Does the Insurer have, in addition to above, the necessary infrastructure for Mission Critical Systems to address at least the following:<br>• Calculation of daily NAV (Fund wise) Redemption processing? | High | |
| C.40 | • Whether satisfactory consideration has been given to geographic diversity for:<br>• Alternate processing locations;<br>• Alternate locations for business processes and functions; and<br>• Off-site storage. | High | |
| C.41 | Are there arrangements for alternative processing capability in the event any specific hardware, the data center, or any portion of the network becomes disabled or inaccessible, and determine if those arrangements are in writing? | High | |
| C.42 | If the organization is relying on in-house systems at separate physical locations for recovery, whether the equipment is capable of independently processing all critical applications. | High | |
| C.43 | • If the organization is relying on outside facilities for recovery, whether the recovery site,<br>• Has the ability to process the required volume;<br>• Provides sufficient processing time for the anticipated workload based on emergency priorities; and,<br>• Allows the organization to use the facility until it achieves a full recovery from the disaster and resumes activity at the organization’s own facilities. | High | |
| C.44 | Review the contract between applicable parties, such as recovery vendors if any. Determine if the terms and conditions of the contract relate to the BCP/DRP | High | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| C.45 | Whether the organization ensures that when any changes (e.g. hardware or software upgrades or modifications) in the production environment occur that a process is in place to make or verify a similar change in each alternate recovery location. | High | |
| C.46 | Whether the organization is kept informed of any changes at the recovery site that might require adjustments to the organization’s software or its recovery plan(s). | High | |
| C.47 | Whether there are plans in place that address the return to normal operations and original business locations once the situation has been resolved and permanent facilities are again available. | High | |
| C.48 | Whether adequate documentation is housed at the alternate recovery location including:<br>• Copies of each BCP/ DRP;<br>• Copies of necessary system documentation | High | |
| C.49 | Whether appropriate physical and logical access controls have been considered and planned for the inactive production system when processing is temporarily transferred to an alternate facility. | High | |
| C.50 | • Whether the methods by which personnel are granted temporary access (physical and logical) during continuity planning implementation periods are reasonable.<br>• Evaluate the extent to which back-up personnel have been reassigned different responsibilities and tasks when business continuity planning scenarios are in effect and if these changes require a revision to the levels of systems, operational, data, and facilities access.<br>• Review the assignment of authentication and authorization credentials to determine if they are based upon primary job responsibilities and if they also include business continuity planning responsibilities. | High | |
| C.51 | Whether the intrusion detection and incident response plan considers resource availability, and facility and systems changes that may exist when alternate facilities are placed in use. | High | |
| | **TESTING** | | |
| C.52 | Whether the BCP / DRP(s) is tested periodically | High | |
| C.53 | Whether all critical business units/departments/ functions are included in the testing. | High | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| C. 54 | Whether the tests include:<br>• Setting goals and objectives in advance;<br>• Realistic conditions and activity volumes;<br>• Use of actual back-up system and data files while maintaining off-site back-up copies for use in case of an event concurrent with the testing;<br>• Participation and review by internal audit;<br>• A post-test analysis report and review process that includes a comparison of test results to the original goals;<br>• Development of a corrective action plan(s) for all problems encountered; and<br>• Board of Directors' review. | High | |
| C.55 | Whether interdependent departments, vendors, and key market providers have been involved in testing at the same time to uncover potential conflicts and/or inconsistencies. | High | |
| C.56 | Whether the level of testing is adequate for the size and complexity of the organization. Determine if the testing includes:<br>• Testing the operating systems and utilities (infrastructure);<br>• Testing of all critical applications (application level);<br>• Data transfer between applications (integrated testing); and<br>• Testing the complete environment and workload (stress test). | High | |
| C.57 | Whether testing at an alternative location includes:<br>• Network connectivity;<br>• Items processing and backroom operations connectivity and information; and<br>• Other critical data feed connections/interfaces. | High | |
| C.58 | Whether testing of the information technology infrastructure includes:<br>• Rotation of personnel involved; and<br>• Business unit personnel involvement. | High | |
| C.59 | Whether management considered testing with:<br>• Critical service providers;<br>• Customers;<br>• Affiliates;<br>• Correspondent institutions;<br>and<br>• Payment systems and major financial market participants. | High | |
| C.60 | When testing with the critical service providers, determine whether management considered testing,<br>• From the institution's primary location to the TSPs' alternative location;<br>• From the institution's alternative location to the TSPs' primary location; and<br>• From the institution's alternative location to the TSPs' alternative location. | High | |
| | **INFORMATION BACK-UP** | | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| C.61 | Whether Back-up of essential business information such as production server, critical network components, configuration backup etc., were taken regularly. | High | |
| C.62 | Whether the backup media along with the procedure to restore the backup are stored securely and well away from the actual site. | High | |
| C.63 | Can data restoration be performed with the help of the documentation even by a person other than the one who backed up the data? | High | |
| C.64 | Are the persons responsible for data backup and restoration sufficiently trained? | High | |
| C.65 | Are data restoration exercises carried out periodically? | High | |
| C.66 | Whether the backup media are regularly tested to ensure that they could be restored within the time frame allotted in the operational procedure for recovery. | High | |
| | **Ensure systems security** | | |
| | **MANAGEMENT INFORMATION SECURITY FORUM** | | |
| C.67 | Whether there is a management forum to ensure there is a clear direction and visible management support for security initiatives within the organisation. | High | |
| | **IT SECURITY GUIDELINES AND PROCEDURES** | | |
| C.68 | Does the organization have a detailed IT Security Guidelines and procedures manual? | High | |
| C.69 | Is there a process of reviewing and updating these manuals at periodic intervals? | High | |
| | **ENDPOINT USAGE GUIDELINES** | | |
| C.70 | Have Endpoint Use Guidelines been established? | High | |
| C.71 | How is compliance with the Endpoint Use Guidelines monitored? | High | |
| C.72 | Does every user have a copy of these Endpoint Use Guidelines? | High | |
| | **SECURITY OF ELECTRONIC OFFICE SYSTEMS** | | |
| C.73 | Whether there is an acceptable use policy to address the use of Electronic office systems. | High | |
| C.74 | Whether there are any guidelines in place to effectively control the business and security risks associated with the electronic office systems. | High | |
| | **DISABLING REMOVABLE DRIVES** | | |
| C.75 | Has it been ensured that floppy disk / USB drives will generally be locked and can be accessed only through authorized use? | High | |
| | **POWER SUPPLIES / UPS** | | |
| C.76 | Is the equipment protected from power failures by multiple feeds, through uninterruptible power supply (UPS), backup generator etc.? | High | |
| C.77 | Are the required intervals for UPS maintenance being observed? | High | |
| C.78 | Is the effectiveness of the UPS system being tested on a regular basis? | High | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| C.79 | If any failures due to the location occurred in the past, had remedial action been taken for the same? | High | |
| C.80 | Are generators available to protect against prolonged power loss and are they in working condition? | High | |
| | **GRANTING OF (SYSTEM/NETWORK) ACCESS RIGHTS** | | |
| C.81 | Are the issue and the retrieval of access authorizations and access-granting means documented? | High | |
| C.82 | Is separation of functions being observed in the granting of access rights? | High | |
| C.83 | Are users being trained in the correct handling of access- granting means? | High | |
| C.84 | If use of access-granting means is logged, are such logs also analysed? | High | |
| | **USER PASSWORD MANAGEMENT** | | |
| C.85 | Is the allocation and reallocation of passwords controlled through a formal management process? | High | |
| C.86 | Are the users asked to sign a statement to keep the password confidential? | High | |
| C.87 | Have users been informed on how to handle passwords correctly? | High | |
| C.88 | Is the password quality controlled? | High | |
| C.89 | Are password changes mandatory? | High | |
| C.90 | Has every user been provided with a password? | High | |
| C.91 | Are there any fixed procedures relating to the escrow of passwords? | High | |
| C.92 | If Yes, are the escrowed passwords complete and up-to- date? | High | |
| C.93 | Have provisions been made to ensure proper handling of escrowed passwords? | High | |
| C.94 | Is the system of password changes controlled on the basis of updating entries for escrowed passwords? | High | |
| | **PASSWORD USE** | | |
| C.95 | Are there any guidelines in place to guide users in selecting and maintaining secure passwords? | High | |
| | **POLICY ON USE OF NETWORK SERVICES** | | |
| C.96 | Does a policy exist that does address concerns relating to networks and network services such as: Parts of network to be accessed, Authorisation services to determine who is allowed to do what, Procedures to protect the access to network connections and network services? | High | |
| C.97 | Are users provided with standard configuration of work stations? If not, are deviations authorized and documented? | High | |
| | **TERMINAL LOGON PROCEDURES** | | |
| C.98 | Has it been ensured that access to information system is attainable only via a secure log- on process? | High | |
| C.99 | Are machines configured to boot from hard drives? | High | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| C.100 | Is there a BIOS password set for PC to disable users from booting through CD drives? | High | |
| C.101 | Is the number of unsuccessful log-in attempts restricted? | High | |
| C.102 | Whether After each unsuccessful log-in attempt, the waiting time until the next log-in prompt increases. | High | |
| C.103 | Are unsuccessful log-in attempts reported to the user? | High | |
| C.104 | Is access to the console protected by passwords or other means? | High | |
| | **USER IDENTIFICATION AND AUTHORISATION** | | |
| C.105 | Whether unique identifier is provided to every user such as operators, system administrators and all other staff including technical. | High | |
| C.106 | Whether the generic user accounts are supplied under exceptional circumstances only where there is a clear business benefit. Additional controls may be necessary to maintain accountability. | High | |
| C.107 | Whether the authentication method used does substantiate the claimed identity of the user. Commonly used method: Password that only the user knows. | High | |
| | **PASSWORD MANAGEMENT SYSTEM** | | |
| C.108 | Whether there exists a password management system that enforces various password controls such as individual password for accountability, enforcing password changes, storing passwords in encrypted form, not displaying passwords on screen etc. | High | |
| | **TERMINAL TIMEOUT** | | |
| C.109 | Whether Inactive terminal in public areas are configured to clear the screen or shut down automatically after a defined period of inactivity. | High | |
| | **LIMITATION OF CONNECTION TIME** | | |
| C.110 | Whether there exists any restriction on connection time for high-risk applications. This type of set up should be considered for sensitive applications for which the terminals are installed in high-risk locations. | High | |
| | **USER REGISTRATION** | | |
| C.111 | Whether there is any formal user registration and deregistration procedure for granting access to multi-user information systems and services.<br>The creation of a user account must be approved by the business owner of the application in question or their nominee. | High | |
| C.112 | Are there standard rights profiles for different functions or tasks? | High | |
| | **PRIVILEGE MANAGEMENT** | | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| C.113 | Whether the allocation and use of any privileges in multi-user information system environment is restricted and controlled i.e., privileges are allocated on need- to-use basis; privileges are allocated only after formal authorisation process. | High | |
| C.114 | Are there any organisational procedures governing the designation of users or user groups? | High | |
| C.115 | Is there any program for the configuration of users or user groups? | High | |
| C.116 | Are there records of the authorized users and groups and their authorisation profiles? | High | |
| | **REVIEW OF USER ACCESS RIGHTS** | | |
| C.117 | Whether there exists a process to review user access rights at regular intervals. Example: Special privilege review every 3 months, normal privileges every 6 months. | High | |
| | **INFORMATION ACCESS RESTRICTION** | | |
| C.118 | Whether access to application by various groups/ personnel within the organisation has been defined in the access control policy as per the individual business application requirement and whether it is consistent with the organisation's Information access policy. | High | |
| | **MONITORING SYSTEM USE** | | |
| C.119 | Whether procedures are set up for monitoring the use of information processing facility. The procedure should ensure that the users are performing only the activities that are explicitly authorized. | High | |
| C.120 | Whether the results of the monitoring activities are reviewed regularly. | High | |
| | **UNAUTHORISED SOFTWARE** | | |
| C.121 | Has a procedure for the authorisation and registration of software been laid down? | High | |
| C.122 | Has the ban on use of non- approved software been put in writing? | High | |
| C.123 | Have all staff members been informed of the ban? | High | |
| C.124 | What possibilities happen to be there for installation or use of unauthorised software? | High | |
| C.125 | Are checks carried out periodically on the software inventory? | High | |
| | **ADMINISTRATOR FUNCTIONS** | | |
| C.126 | To which persons is the supervisor password known? | High | |
| C.127 | Have administrator roles been divided up? | High | |
| C.128 | Are the authorisations assigned by the administrator randomly checked? | High | |
| C.129 | How frequently are logins and logouts using administrator ID checked? | High | |
| | **EVENT LOGGING** | | |
| C.130 | Whether audit logs recording exceptions and other security relevant events are produced and kept for an agreed period to assist in future investigations and access control monitoring. | High | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| | **REPORTING SECURITY WEAKNESSES** | | |
| C.131 | Whether a formal reporting procedure or guideline exists for users, to report security weakness in, or threats to, systems or services. | High | |
| C.132 | Are staff members informed in a suitable form of IT security incidents which have occurred either within the organisation or which have become public knowledge, and are they told how to avoid them? | High | |
| | **DISCIPLINARY PROCESS** | | |
| C.133 | Whether there is a formal disciplinary process in place for employees who have violated organisational security policies and procedures. Such a process can act as a deterrent to employees who might otherwise be inclined to disregard security procedures. | High | |
| | **EQUIPMENT SITING PROTECTION** | | |
| C.134 | Whether critical equipment is located in appropriate place to minimize unnecessary access into work areas. | High | |
| C.135 | Whether the items requiring special protection were isolated to reduce the general level of protection required. | High | |
| C.136 | Whether controls were adopted to minimize risk from potential threats such as theft, fire, explosives, smoke, water, dust, vibration, chemical effects, electrical supply interfaces, electromagnetic radiation, flood. | High | |
| C.137 | Whether there is a policy towards eating, drinking and smoking in proximity to information processing services. | High | |
| C.138 | Whether environmental conditions, which would adversely affect the information processing facilities, are monitored. | High | |
| C.139 | Verify that heating, ventilation and air-conditioning systems maintain constant temperatures within the data center. | High | |
| C.140 | Verify that ground earthing exists to protect the computer systems. Ensure that power is conditioned to prevent data loss. | High | |
| C.141 | Is the Server Room designed as a closed secure area? | High | |
| | **CABLING SECURITY** | | |
| C.142 | Whether the power and telecommunications cable carrying data or supporting information services are protected from interception or damage. | Low | |
| C.143 | Whether there are any additional security controls in place for sensitive or critical information. | Low | |
| | **SECURITY OF NETWORK SERVICES** | | |
| C.144 | Whether the organisation, using public or private network service does ensure that a clear description of security attributes of all services used is provided. | High | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| C.145 | Are all Internet connections routed through a Firewall? Does a dedicated team manage the Firewall? Are the ports opened only on a "need to have" basis? | High | |
| C.146 | Is there an Intruder Detection System (IDS) implemented? | High | |
| C.147 | Are the application and database servers kept separated from the web server in the de-militarized zone? | High | |
| C.148 | Is the de-militarized zone separated from the Internet cloud by means of a Firewall? | High | |
| C.149 | If the de-militarized zone is connected to the Intranet, is it separated by a Firewall? | High | |
| C.150 | Is the Firewall rule base treated as a sensitive information and is knowledge of the same restricted to only authorized officials in the IT / Computer operations department? | High | |
| C.151 | Is the decision to open specific firewall ports/rule base approved in accordance with IT Security Policy (IT Security Policy should list out such ports) e.g. firewalls should block unwanted ports running services such as ftp, telnet, SMTP, etc. into the de-militarized zone? | High | |
| | **CLOCK SYNCHRONISATION** | | |
| C.152 | Whether the computer or communication device has the capability of operating a real time clock. If yes, has it been set to an agreed standard such as Universal Coordinated Time or local standard time? The correct setting of the computer clock is important to ensure the accuracy of the audit logs. | Low | |
| | **UNATTENDED USER EQUIPMENT** | | |
| C.153 | 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 | |
| | **SENSITIVE SYSTEM ISOLATION** | | |
| C.154 | 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 | |
| | **SECURITY OF ELECTRONIC EMAIL** | | |
| C.155 | Whether there is a policy in place for the acceptable use of electronic mail or does security policy address the issues with regards to use of electronic mail. | Low | |
| C.156 | Whether there are adequate procedures, which require that all the incoming e-mail messages be scanned for virus to prevent virus infection to the network | Low | |
| C.157 | Have regulations governing file transfer and exchange of messages with external parties been established? | Low | |
| C.158 | Are there formal rules based on which e-mail addresses are assigned? | Low | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| C.159 | Are security measures such as filtering and text search in emails implemented? | Low | |
| C.160 | Is the criterion for e-mail filtering adequate? What are the procedures for changes in filtering parameters? | Low | |
| C.161 | Have controls such as anti-virus checking, isolating potentially unsafe attachments, spam control, anti relaying etc., been put in place to reduce the risks created by electronic mail? | Low | |
| | **CONTROL AGAINST MALICIOUS SOFTWARE** | | |
| C.162 | Whether there exists any control against malicious software usage. | Medium | |
| C.163 | Whether the security policy does address software licensing issues such as prohibiting usage of unauthorized software. | Medium | |
| C.164 | Whether there exists any Procedure to verify that all warning bulletins are accurate and informative with regards to the malicious software usage. | Medium | |
| C.165 | Whether Antivirus software is installed on the computers to check and isolate or remove any viruses from computer and media. | Medium | |
| C.166 | Whether this software signature is updated on a regular basis to check any latest viruses. | Medium | |
| C.167 | Whether all the traffic originating from un-trusted network into the organisation is checked for viruses. Example: Checking for viruses on email, email attachments and on the web, FTP traffic. | Medium | |
| C.168 | Are periodic runs of a virus detection program configured? | Medium | |
| C.169 | Are there occasional checks as to whether updates have been performed? Have the results been documented? | Medium | |
| C.170 | Use of a virus scanning program when exchanging of data media and data transmission – Is Anti Virus auto enabled to check CDs and floppies? | Medium | |
| C.171 | Are received files and data media checked for virus infection before being imported? | Medium | |
| | **REMOTE DIAGNOSTIC PORT PROTECTION** | | |
| C.172 | Whether accesses to diagnostic ports are securely controlled i.e., protected by a security mechanism. | Low | |
| | **SEGREGATION IN NETWORKS** | | |
| C.173 | Whether the network (where business partner’s and/ or third parties need access to information system) is segregated using perimeter security mechanisms such as firewalls. | High | |
| | **NETWORK CONNECTION PROTOCOLS** | | |
| C.174 | Whether there exists any network connection control for shared networks that extend beyond the organisational boundaries. Example: electronic mail, web access, file transfers, etc., | High | |
| | **NETWORK ROUTING CONTROL** | | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| C.175 | Are changes to network configuration documented? | Low | |
| C.176 | Is the system administrator the only person who is able to change the configuration? | Low | |
| C.177 | Is the system administrator the only person who is able to read the network log files | Low | |
| | **SECURITY OF MEDIA IN TRANSIT** | | |
| C.178 | Whether security of media while in transit has been taken into account. | Low | |
| C.179 | Whether the media is well protected from unauthorised access, misuse or corruption. | Low | |
| | **ELECTRONIC COMMERCE SECURITY** | | |
| C.180 | Whether Electronic commerce is well protected and controls implemented to protect against fraudulent activity, contract dispute and disclosure or modification of information. | Low | |
| C.181 | Whether Security controls such as Authentication, Authorisation are considered in the E- Commerce environment. | Low | |
| C.182 | Whether electronic commerce arrangements between trading partners include a documented agreement, which commits both parties to the agreed terms of trading, including details of security issues. | Low | |
| | **USER AUTHENTICATION FOR EXTERNAL CONNECTIONS** | | |
| C.183 | Whether there exists any authentication mechanism for challenging external connections. Examples: Cryptography based technique, hardware tokens, software tokens, challenge/ response protocol etc., | Low | |
| | **FIRE DETECTION AND PREVENTION CONTROLS** | | |
| C.184 | Are Fire detection measures adequate such as fire alarms available? | Medium | |
| C.185 | Has staff been informed of the location of hand-held fire extinguishers? | Medium | |
| C.186 | Can the hand-held fire extinguishers actually be accessed in case of a fire? | Medium | |
| C.187 | Is training provided for the use of hand-held fire extinguishers? | Medium | |
| C.188 | Are hand-held fire extinguishers regularly inspected and maintained? | Medium | |
| C.189 | Is the fire alarm system checked periodically to ensure that it is working properly? | Medium | |
| C.190 | Has all the staff been informed of the steps to be taken in the event that an alarm goes off? | Medium | |
| C.191 | Is there an adequate number of fire extinguishers (generally one for every 50 sqft of area)? | Medium | |
| C.192 | • Is a fire suppression system in place consisting of Fire extinguishers and Sprinklers?<br>• Are they in working order and being monitored? | Medium | |
| | **Manage the configuration** | | |
| | **CONTROL OF TECHNICAL VULNERABILITIES** | | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| C.193 | • Whether timely information about technical vulnerabilities of information systems being used is obtained.<br>• Whether the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to mitigate the associated risk. | Medium | |
| | **SAFEGUARDING OF ORGANISATIONAL RECORDS** | | |
| C.194 | Whether important records of the organisation are protected from loss destruction and falsification. | High | |
| | **DISPOSAL OF MEDIA** | | |
| C.195 | Whether the media that are no longer required are disposed off securely and safely. | High | |
| C.196 | Whether disposal of sensitive items is logged where necessary in order to maintain an audit trail. | High | |
| | **SECURE DISPOSAL OR RE- USE OF EQUIPMENT** | | |
| C.197 | Whether storage device containing sensitive information is physically destroyed or securely over-written. | High | |
| | **INFORMATION HANDLING PROCEDURES** | | |
| C.198 | Whether there exists a procedure for handling the storage of information. Does this procedure address issues such as information protection from unauthorised disclosure or misuse? | Low | |
| | **DATA MANAGEMENT** | | |
| C.199 | Are the persons responsible for the exchange of data media familiar with the process of physical erasure? | Low | |
| | **MANAGEMENT OF REMOVABLE MEDIA** | | |
| C.200 | • Whether procedures exist for management of removable media, such as tapes, disks, cassettes, memory cards, and reports.<br>• Whether all procedures and authorization levels are clearly defined and documented. | Low | |
| | **BUSINESS INFORMATION SYSTEMS** | | |
| C.201 | Whether policies and procedures have been developed and enforced to protect information associated with the interconnection of business information systems. | Low | |
| | **Manage the physical environment** | | |
| | **PHYSICAL SECURITY PERIMETER** | | |
| C.202 | • Are physical border security facilities implemented adequate to protect the Information processing service? Some examples of such security facilities are: card control for entry gate, walls, manned reception etc.?<br>• Are visitors required to record their entry inside the premises in a separate register?<br>• Are details of their possessions recorded and verified at the time of their exit from the premises<br>• Are cameras disallowed inside the premises? | Medium | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| C.203 | • Does Data Center exterior Lighting, building orientation provide a secure environment?<br>• Data Centers should be anonymous. Ensure that there is no signage or listings in directories? | Medium | |
| | **SECURING OFFICES, ROOMS AND FACILITIES** | | |
| C.204 | Whether the rooms, which have the Information processing service, are:<br>• locked<br>• have lockable cabinets<br>• safes. | Medium | |
| C.205 | Whether the Information processing service is protected from natural and man-made disaster such as raised floors, good exterior walls /or other suitable acceptable infrastructure | Medium | |
| C.206 | Whether there is any potential threat from neighboring premises. | Medium | |
| C.207 | Ensure that water alarm system is configured to detect water in high risk areas of the data center | Medium | |
| C.208 | Ensure that burglar alarm is protecting the data center from physical intrusion. | Medium | |
| C.209 | Are there adequate controls over modems and other dial up devices for employees and visitors (data cards, etc)? | Medium | |
| C.210 | Ensure that surveillance systems (CCTV) are designed and operating properly? | Medium | |
| | **PHYSICAL ENTRY CONTROLS** | | |
| C.211 | Are entry controls in place to allow only authorised personnel into various areas within organisation? | Medium | |
| C.212 | Is there a practice of Supervising or escorting outside staff/visitors? | Medium | |
| | **REMOVAL OF PROPERTY** | | |
| C.213 | Whether equipment, information or software can be taken off-site without appropriate authorisation. | Medium | |
| | **PROTECTING AGAINST EXTERNAL AND ENVIRONMENTAL THREATS** | | |
| C.214 | Whether physical protection against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster has been designed and applied. | Medium | |
| D | **Maintain IT** | | |
| | **Monitoring and Compliance** | | |
| | **COMPLIANCE WITH SECURITY POLICIES AND STANDARDS** | | |
| D.1 | • Whether managers ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.<br>• Do managers regularly review the compliance of information processing facility within their area of responsibility for compliance with appropriate security policy and procedure? | Medium | |
| | **ADMINISTRATOR AND OPERATOR LOGS** | | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| D.2 | • Whether system administrator and system operator activities are logged.<br>• Whether the logged activities are reviewed on regular basis. | Medium | |
| | **TECHNICAL COMPLIANCE CHECKING** | | |
| D.3 | • Whether information systems are regularly checked for compliance with security implementation standards.<br>• Whether the technical compliance check is carried out by, or under the supervision of, competent, authorized personnel. | Medium | |
| | **INFORMATION SYSTEMS AUDIT CONTROLS** | | |
| D.4 | • Whether audit requirements and activities involving checks on operational systems have been carefully planned and agreed to minimise the risk of disruptions to business process.<br>• Whether the audit requirements, scope are agreed with appropriate management. | Medium | |
| | **Application and logical access controls** | | |
| | Name of the application used for investment operations: | | |
| D.5 | Obtain a list of valid user IDs at the location and,<br>• Reconcile Active users to those present in the location as per attendance roles<br>• Validate User Work Class with the designation of the users at the location<br>• Verify if concurrent auditors have been provided with only view access<br>• Check for user with maximum inactive time greater than 10 minutes<br>• Check for user with password expiry date greater than 40 days from the current day.<br>• For user ID disabled, check whether these have been done immediately after their names have been removed from the attendance register. In case any delays are noticed from the time of removal from attendance register to the actual date of disabling the user Id report the same. | High | |
| D.6 | Are Access privileges defined for each user as per the designation? | High | |
| D.7 | Whether the User Ids of employees who have been transferred, or have retired/ resigned are deleted from application. | High | |
| D.8 | • Whether the application logs out the user after 5 minutes of inactivity.<br>• Whether the system forces the user to change the initial password given by system manager.<br>• Users acknowledge receipt of the password on the register maintained for the purpose | High | |
| D.9 | Whether the user log-off the application whenever they leave the work place for break. | High | |
| D.10 | • Check that all user accounts are identifiable to a user and generic user- ids, which cannot be attributed to any individual, are not allowed.<br>• Check that all default vendor accounts shipped with the application have been disabled. | High | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| D.11 | Is the user ID temporarily suspended when the staff members are out on training/outstation assignment and the user ID will remain inactive for certain days? | High | |
| D.12 | Whether an undertaking for maintaining secrecy and confidentiality of password has been obtained from every user and preserved. | High | |
| D.13 | Whether super user passwords are changed immediately after those are used by support persons for rectification of problems and this usage is documented. | High | |
| D.14 | Whether every user has only one identifiable user ID and not more than one user id has been given to any user. | High | |
| D.15 | Whether Super user passwords (for applications hosted at the location) are confined to systems manager only and the same are kept with the location in charge in a sealed cover. | High | |
| D.16 | Password Security:-<br>• Whether the users change their password periodically.<br>• Does the application force the user to set an alpha numeric password/<br>• Is the minimum length of the password set to 8 characters?<br>• Whether password entry is disabled after three unsuccessful log-on attempts?<br>• Whether the system forces the users to change their password after 40 days from the date of last creation / modification.<br>• Whether password history is maintained by the application. From Transaction records, day end reports or audit trails, perform a sample check to verify if user ID has been used on any day when the user is on leave | High | |
| | **ENFORCED PATH** | | |
| D.17 | Whether there is any control that restricts the route between the user terminal and the designated computer services the user is authorised to access, for example, enforced path to reduce the risk. | Low | |
| | **NODE AUTHENTICATION** | | |
| D.18 | Whether connections to remote computer systems that are outside organisations security management are authenticated. Node authentication can serve as an alternate means of authenticating groups of remote users where they are connected to a secure, shared computer facility. | Low | |
| | **NETWORK TESTS** | | |
| D.19 | Is it ensured that products/services that use the Internet for connectivity or communications have undergone a successful penetration test prior to production implementation? | Medium | |

| Ref # | Audit objective | Risk Category | Auditors Remark |
|---|---|---|---|
| D.20 | Is there a penetration test process that ensures that modifications to the product/service that uses the Internet for connectivity or communication have been reviewed to determine whether a subsequent penetration test is warranted? | Medium | |
| D.21 | Is there an intrusion detection system in place for all the external IP connections? | Medium | |
| | **ON-LINE TRANSACTIONS** | | |
| D.22 | Whether information involved in online transactions is protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. | Medium | |

**IF YOU FIND THIS USEFUL , SHARE WITH YOUR NETWORK.**

**FOLLOW FOR MORE SUCH CHECKLIST | TEMPLATE | IT AUDIT RELATED STUFF**

https://www.linkedin.com/in/sachin-hissaria/

https://youtube.com/@sachinhissaria