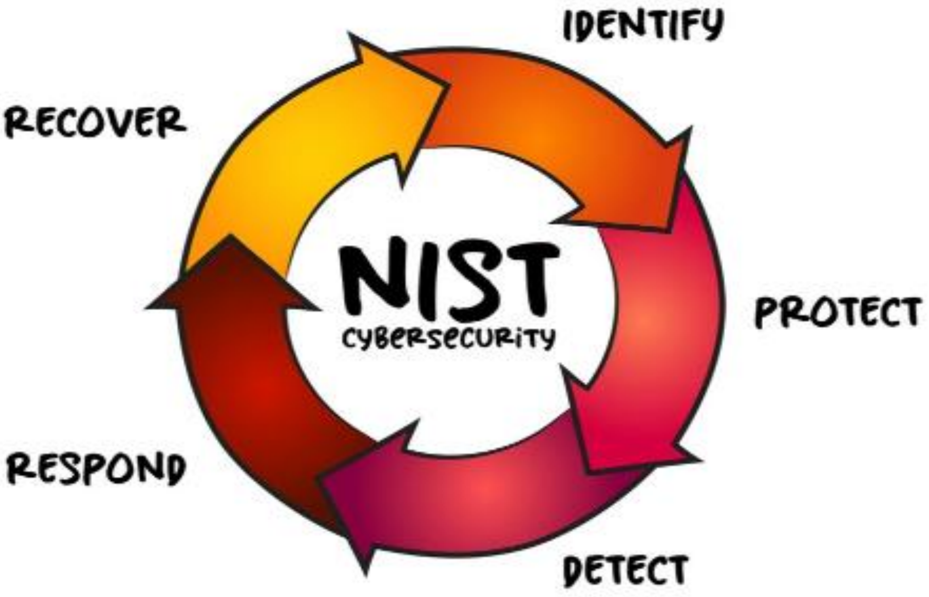
The checklist is prepared as per **National Institute of Standards and Technology (NIST) Framework** for Improving Critical Infrastructure Cybersecurity.

NIST Cybersecurity Framework



This PDF covers only the checkpoints related to Step 2 & 3, i.e. PROTECT (PR) and DETECT (DE).

The next post will include checkpoints related to Step 4 and 5

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

Area	Audit Questionnaire	Auditor remarks
Identity Management, Authentication and Access Control (PR.AC):	Are ICT infrastructure logs maintained for a rolling period of180 days as per CERT-In directions?	
Identity Management, Authentication and Access Control (PR.AC):	Are ICT infrastructure, Critical and Business data stored in India?	
Identity Management, Authentication and Access Control (PR.AC):	Are third-party staff who are given access to the organization's critical systems, networks, and other computer resources subjected to strict supervision, monitoring, and access restrictions?	
Identity Management, Authentication and Access Control (PR.AC):	Do all critical systems of the organization that is accessible over the internet have two-factor security (Such as VPNs, Firewall Controls, etc.)?	
Identity Management, Authentication and Access Control (PR.AC):	Does the access control policy addressstrong password management control for access to systems, applications, networks and databases?	
Identity Management, Authentication and Access Control (PR.AC):	Does the organization proactively deactivate access of privileges of users who are leaving the organization or whose accessprivileges have been withdrawn?	
Identity Management, Authentication and Access Control (PR.AC):	Has the organization deployed security measures and controls tosupervise staff with elevated access entitlements (Such as privileged users) to organization's critical systems? Has the organization also restricted the no. of privileged user to the least number and deployed periodic review mechanism / process against privileged users' activities? Are such privileged users restricted of access to system logs where their activities are being captured?	
Identity Management, Authentication and Access Control (PR.AC):	Has the organization ensured that no personnel in the company have natural rights to access confidential data, applications,system resources or facilities by virtue of rank or position?	
Identity Management, Authentication and Access Control (PR.AC):	Has the organization ensured that the perimeter of the critical equipment’s room / area are physically secured and continuously monitored by employing physical, human, and procedural controls such as security guards, CCTVs, Card access systems, mantrap, bollards, etc?	

Area	Audit Questionnaire	Auditor remarks
Identity Management, Authentication and Access Control (PR.AC):	Has the organization formulated an internet access policy to monitor and regulate the use of internet & internet based services such as social media sites, cloud-based storage sites, etc. within the organization's critical IT infrastructure?	
Identity Management, Authentication and Access Control (PR.AC):	Has the organization implemented access to IT systems, applications, databases and networks on a need-to-use basis and the principle of least privilege? Is the access granted using strong authentication mechanisms and only when it is required ?	
Identity Management, Authentication and Access Control (PR.AC):	Has the organization implemented controls for providing identification and authentication of customers for access to partner systems using secure authentication technologies?	
Identity Management, Authentication and Access Control (PR.AC):	Has the organization implemented controls to minimize invalid login counts, deactivate dormant accounts?	
Identity Management, Authentication and Access Control (PR.AC):	Is physical access to the critical systems of the organization restricted to the minimum number of authorized officials? Are third party staffs strictly monitored and physically accompaniedall the time by the authorized employee of the organization while third party staff has been given physical access to critical systems?	
Identity Management, Authentication and Access Control (PR.AC):	Is physical access to the critical systems of the organization revoked immediately if the same is no longer required?	
Awareness and Training (PR.AT):	Are the history and versions of training content maintained?	
Awareness and Training (PR.AT):	Are the targeted awareness / training for key personnel conducted periodically?	
Awareness and Training (PR.AT):	Are the training programs reviewed and updated periodically?	
Awareness and Training (PR.AT):	Are security policy/ies covering secure and acceptable use of network/assets including customer information/data defined and communicated to users/ employees, vendors & partners, and also educating them about cybersecurity risks and protection measures at their level.	
Awareness and Training (PR.AT):	Do users indicate that they understand their responsibilities?	
Awareness and Training (PR.AT):	Is awareness level evaluated periodically?	

Area	Audit Questionnaire	Auditor remarks
Awareness and Training (PR.AT):	Is there additional training for leaders to understand their roles in the event of a security incident?	
Awareness and Training (PR.AT):	Is there a process to handle if a user does not complete the training?	
Awareness and Training (PR.AT):	Is someone responsible for creating the security training for the organization?	
Awareness and Training (PR.AT):	Has the Organization periodically participated in national/ sectoral/ organisational Cyber Security Exercises?	
Data Security (PR.DS):	Are open ports on network and systems which are not in use blocked ?	
Data Security (PR.DS):	Can the application be set to automatically log a user off the application after a predefined period of inactivity?	
Data Security (PR.DS):	Can the application force password expiration and prevent users from reusing a password?	
Data Security (PR.DS):	Can the system administrator enforce password policy and / or complexity such as minimum length, numbers and alphabet requirements, and upper and lower case constraint, etc.?	
Data Security (PR.DS):	Does the application force “new” users to change their password upon first login into the application?	
Data Security (PR.DS):	Does the application prohibit users from logging into the application on more than one workstation at the same time withthe same user ID?	
Data Security (PR.DS):	Does the application support integration with the enterprise identity management system?	
Data Security (PR.DS):	Does the organization authorize data storage devices within their IT infrastructure through appropriate validation process?	
Data Security (PR.DS):	Is there a process by which the organization maintains the evidence of media disposal?	
Data Security (PR.DS):	Has there been a implementation of a data-disposal and data-retention policy?	
Data Security (PR.DS):	Are there processes for media formatting?	
Data Security (PR.DS):	Is there a measurement of client system's vulnerabilities?	
Data Security (PR.DS):	Is user authentication controlled by means other than user account and password or PIN?	
Data Security (PR.DS):	Are various security mechanism used to share the data with third parties?	
Data Security (PR.DS):	Are different technologies implemented for the encryption of data?	
Data Security (PR.DS):	Are appropriate technologies implemented for data mobility security?	
Information Protection Processes and Procedures (PR.IP):	Are duplicate copies of PC software and documentation maintained off-location?	

Area	Audit Questionnaire	Auditor remarks
Information Protection Processes and Procedures (PR.IP):	Are Physically or logically segregated systems used to isolate and run software that is required for business operations but incur higher risk for the organization.	
Information Protection Processes and Procedures (PR.IP):	Are the contents of the Web site backed-up to ensure an orderly recovery if the site is corrupted?	
Information Protection Processes and Procedures (PR.IP):	Are there methods to prevent unauthorized access by other groups into individual files and department - shared files?	
Information Protection Processes and Procedures (PR.IP):	Are there procedures for limiting access to LAN and network operating software?	
Information Protection Processes and Procedures (PR.IP):	Are updates to the Web site independently reviewed, approved and tested?	
Information Protection Processes and Procedures (PR.IP):	Does information security policy cover use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data?	
Information Protection Processes and Procedures (PR.IP):	Does the organisation utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.?	
Information Protection Processes and Procedures (PR.IP):	Does the organisation utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.	
Information Protection Processes and Procedures (PR.IP):	Does the organization have a documented disaster recovery plan for processing critical jobs in the event of a major hardware or software failure?	
Information Protection Processes and Procedures (PR.IP):	Does the organization's application whitelisting software ensure that only authorized software libraries (such as *.dll, *.ocx,*.so,etc.) are allowed to load into a system process.	
Information Protection Processes and Procedures (PR.IP):	Does the organization's application whitelisting software mustensure that only authorized, digitally signed scripts (such as *.ps1,*.py, macros, etc.) are allowed to run on a system.	

Area	Audit Questionnaire	Auditor remarks
Information Protection Processes and Procedures (PR.IP):	Is a periodic inventory taken to verify that the appropriate backup files are being maintained?	
Information Protection Processes and Procedures (PR.IP):	Is appropriate hardware backup available?	
Information Protection Processes and Procedures (PR.IP):	Is it ensured that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory? Unsupported software should be tagged as unsupported in the inventory system.	
Information Protection Processes and Procedures (PR.IP):	Is it ensured that the software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location?	
Information Protection Processes and Procedures (PR.IP):	Is the use of remote access software restricted?	
Information Protection Processes and Procedures (PR.IP):	Is there documentation describing data, programs, hardware, and system requirements?	
Information Protection Processes and Procedures (PR.IP):	Are policies and procedures being used to protect critical information at different layers of security?	
Maintenance (PR.MA):	Is there a process to determine after how many days of identification, patches would be fixed?	
Maintenance (PR.MA):	Are remote maintenance of organizational assets approved, logged, and performed in a manner that prevents unauthorized access?	
Maintenance (PR.MA):	Are defined parameters taken for prioritizing the patches need to be installed	
Maintenance (PR.MA):	Are maintenance and repair of organizational assets logged whenever performed, with approved and controlled tools?	
Maintenance (PR.MA):	Is there a process to deploy critical patches in a test environment?	
Maintenance (PR.MA):	Are the approved patch management policy implemented?	
Maintenance (PR.MA):	Have perimeters been defined for classifying patches?	
Protective Technology (PR.PT):	Are adequate measures taken to isolate and secure the perimeter and connectivity of the servers running monetary transactions applications/process?	

Area	Audit Questionnaire	Auditor remarks
Protective Technology (PR.PT):	Does the organization Continuously monitor the release of patches by various vendors / OEMs, advisories issued by CERT- in and other similar agencies and expeditiously apply the security patches as per the patch management policy?	
Protective Technology (PR.PT):	Has the organization deployed controls like host / network / application based IDS systems, customized kernels for Linux, anti- virus and anti-malware software etc., to prevent from virus / malware / ransomware attacks?	
Protective Technology (PR.PT):	Has the organization documented and implemented secure mail and messaging systems, including those used by organization's partners & vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.?	
Protective Technology (PR.PT):	Has the organization established baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile deviceswithin their IT environment? Are LAN and wireless networks secured within organizations premises by deploying proper controls?	
Protective Technology (PR.PT):	Has the organization implemented mechanism to control installation of software/applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. and mechanism to block /prevent and identify installation and running of unauthorised software / applications on such devices/ systems?	
Protective Technology (PR.PT):	Has the organization installed network security devices, such asfirewalls, proxy servers, intrusion detection and prevention systems (IDS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources?	
Anomalies and Events (DE.AE):	Does the organization have a clearly defined policy including requirements justifying the exceptions, duration of exceptions, process of granting exceptions, and authority for approving, authority for review of exceptions granted on a periodic basis byofficer(s) preferably at senior levels who are well equipped to understand the business and technical context of the exception(s)?	
Security Continuous Monitoring & Detection (DE.CM):	Are the security logs maintained and monitored?	
Security Continuous Monitoring & Detection (DE.CM):	Are there any procedure to monitor capacity utilization of critical systems and networks ?	
Security Continuous Monitoring & Detection (DE.CM):	Are there mechanism to dynamically incorporate lessons learnt to continually improve the response strategies?	

Area	Audit Questionnaire	Auditor remarks
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Alert when users deviate from normal login behaviour, such as time-of-day, workstation location andduration.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Apply host-based firewalls or port filteringtools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to forinternally developed software.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Associate active ports, services and protocols to the hardware assets in the asset inventory.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Automatically disable dormant accounts after a set period of inactivity.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Automatically lock workstation sessions after a standard period of inactivity.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Block all e-mail attachments entering theorganization's email gateway if the file types are unnecessary for the organization's business.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectorsthat can be used to exploit enterprise systems successfully.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Configure devices to not auto-run content from removable media.	

Area	Audit Questionnaire	Auditor remarks
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Configure monitoring systems to record network packets passing through the boundary at each of theorganization's network boundaries.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Configure network vulnerability scanningtools to detect and alert on unauthorized wireless access points connected to the wired network.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Create a test bed that mimics a productionenvironment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Decrypt all encrypted network traffic at the boundary proxy prior to analysing the content. However, theorganization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Deliver training to address the skills gap identified to positively impact workforce members' security behaviour.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Deny communications with known malicious or unused Internet IP addresses and limit access only totrusted and necessary IP address ranges at each of the organization's network boundaries,.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation andanalysis.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighbouring systems, through technologies such as Private VLANs or micro segmentation.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Disable any account that cannot be associated with a business process or business owner.	

Area	Audit Questionnaire	Auditor remarks
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Disable wireless access on devices that do not have a business purpose for wireless access.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Disable wireless peripheral access ofdevices (such as Bluetooth and NFC), unless such access is required for a business purpose.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanismnot integrated into the operating system, in order to access the information.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Encrypt all sensitive information in transit.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure that all accounts have an expiration date that is monitored and enforced.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure that all software developmentpersonnel receive training in writing secure code for their specific development environment and responsibilities.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure that appropriate logs are being aggregated to a central log management system for analysis andreview.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure that only authorized scripting languages are able to run in all web browsers and email clients.	

Area	Audit Questionnaire	Auditor remarks
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Establish a process to accept and addressreports of software vulnerabilities, including providing a means for external entities to contact your security group.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Establish secure coding practicesappropriate to the programming language and development environment being used.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation For applications that rely on a database, use standard hardening configuration templates. All systems thatare part of critical business processes should also be tested.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation For in-house developed software, ensure that explicit error checking is performed and documented for allinput, including for size, data type, and acceptable ranges or formats.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation If USB storage devices are required, ensure all data stored on such devices must be encrypted while at rest.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	

Area	Audit Questionnaire	Auditor remarks
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Maintain an inventory of all sensitive information stored, processed, or transmitted by theorganization's technology systems, including those located on-site or at a remote service provider.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Maintain an inventory of authorized wireless access points connected to the wired network.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Maintain an inventory of each of theorganization's authentication systems, including those located on-site or at a remote service provider.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Maintain separate environments for production and non-production systems. Developers should nothave unmonitored access to production environments.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Manage all network devices using multi-factor authentication and encrypted sessions.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Manage the network infrastructure across network connections that are separated from the business use ofthat network, relying on separate VLANs or, preferably,on entirely different physical connectivity for management sessions for network devices.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Monitor attempts to access deactivated accounts through audit logging.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation On a regular basis, review logs to identify anomalies or abnormal events.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation On a regular basis, tune SIEM system to better identify actionable events and decrease event noise.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Only use up-to-date and trusted third-party components for the software developed by the organization.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Perform a skills gap analysis to understandthe skills and behaviours workforce members are not adhering to, using this information to build a baseline education roadmap.	

Area	Audit Questionnaire	Auditor remarks
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or torespond quickly and effectively.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Place application firewalls in front of anycritical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Plan and conduct routine incident, response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats.Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available tothem?	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation protect web applications by deploying webapplication firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting thetraffic prior to analysis. If neither option is appropriate, a host- based web application firewall should be deployed.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation require all remote login access to theorganization's network to encrypt data in transit and use multi-factor authentication.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation require multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs)?	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation subscribe to URL categorization services to ensure that they are up-to-date with the most recent websitecategory definitions available? Uncategorized sites shall be blocked by default.	

Area	Audit Questionnaire	Auditor remarks
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation to lower the chance of spoofed or modified emails from valid domains, implement Domain- based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the Domain Keys Identified Mail(DKIM) standards?	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation train the workforce on how to identifydifferent forms of social engineering attacks, such as phishing, phone scams and impersonation calls.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisationtrain workforce memberson the importance of enabling and utilizing secure authentication.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation train workforce on how to identify and properly store, transfer, archive and destroy sensitiveinformation?	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation uninstall or disable any unauthorized browser or email client plugins or add-on applications?	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation use a wireless intrusion detection system(WIDS) to detect and alert on unauthorized wireless access points connected to the network?	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation use an automated tool, such as host- based Data Loss Prevention, to enforce access controls to data evenwhen data is copied off a system?	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation use DNS filtering services to help block access to known malicious domains?	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation use only standardized and extensively reviewed encryption algorithms?	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation use sandboxing to analyse and block inbound email attachments with malicious behaviour?	

Area	Audit Questionnaire	Auditor remarks
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation use vulnerability scanning and penetration testing tools in concert.The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts?	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider, and update the organization's sensitive information inventory.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation verify that the version of all software acquired from outside your organization is still supported by thedeveloper or appropriately hardened based on developer security recommendations.	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation wherever possible, ensure that Red Team results are documented using open, machine-readable standards (e.g.,SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.	
Security Continuous Monitoring & Detection (DE.CM):	Has the organization defined and set a procedure to implement a Security Operations Centre for centralised and coordinated monitoring and management of security related incident?	
Security Continuous Monitoring & Detection (DE.CM):	Has the organization defined incidents, method of detection, methods of reporting incidents by employees, vendors and customers and periodicity of monitoring, collection/sharing of threat information, expected response in each scenario/incident type, allocate and communicate clear roles and responsibilities of personnel manning/handling such incidents, provide specialised training to such personnel, post incident review, periodically test incident response plans?	
Security Continuous Monitoring & Detection (DE.CM):	Has the organization implemented measures to control use of VBA/macros in MS office documents, control permissible attachment types in email systems?	
Security Continuous Monitoring & Detection (DE.CM):	Has the organization implemented mechanism to automatically identify unauthorised device connections to the organization'snetwork and block such connections?	

Area	Audit Questionnaire	Auditor remarks
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation conduct periodic tests for all the critical application, server, network devices and data bases?	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation implement a process to communicate vulnerabilities to vendors?	
Security Continuous Monitoring & Detection (DE.CM):	Does the organisation maintain tracker for closure and corrective action of VAPT?	
Security Continuous Monitoring & Detection (DE.CM):	Whether a policy to ensure high availability and timely detection of attacks is defined and implemented ?	
Security Continuous Monitoring & Detection (DE.CM):	Whether vulnerability assessment and penetration testing procedure and calendar are defined ?	
Security Continuous Monitoring & Detection (DE.CM):	Is VAPT of internet-facing applications or infrastructure components conducted periodically	
Security Continuous Monitoring & Detection (DE.CM):	Does Business applications including APIs or Web Services etc. undergo VAPT Testing including secure code review periodically & before go live.	
Security Continuous Monitoring & Detection (DE.CM):	Is mandatory security testing conducted for all changes to internet facing information assets or systems and reported gaps closed before moving into production.	
Security Continuous Monitoring & Detection (DE.CM):	Is External Black box Penetration Testing (PT) conducted for all internet facing information assets or systems once in a 6 months.	
Security Continuous Monitoring & Detection (DE.CM):	Are High risk gaps, reported from the VAPT closed within the time period prescribed under guidelines followed by validation test.	
Security Continuous Monitoring & Detection (DE.CM):	Are audit gaps reported in VAPT closed within the timeframe provided in the guidelines.	

Area	Audit Questionnaire	Auditor remarks
Security Continuous Monitoring & Detection (DE.CM):	Is the organizations information assets synchronized with a singular time source?	
Detection Processes (DE.DP):	Are roles and responsibilities for detection well defined to ensure accountability?	
Detection Processes (DE.DP):	Do detection activities comply with all applicable requirements?	
Detection Processes (DE.DP):	Has the organization put in place processes / mechanism to identify authorised hardware / mobile devices like Laptops, mobile phones, tablets, etc. and ensure that they are provided connectivity only when they meet the security requirements prescribed by the organization?	

The next post will include checkpoints related to Step 4 and 5, i.e. RESPOND and RECOVER

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/@sachinhissaria6512