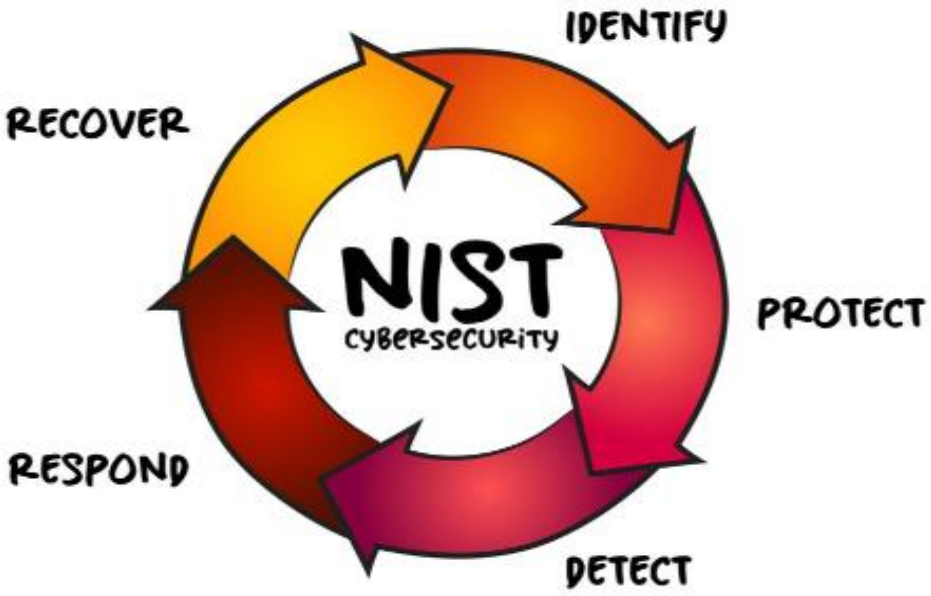
The checklist is prepared as per **National Institute of Standards and Technology (NIST) Framework** for Improving Critical Infrastructure Cybersecurity.

NIST Cybersecurity Framework



This PDF covers only the checkpoints related to Step 1, i.e. IDENTIFY.

The next post will include checkpoints related to Step 2, "PROTECT.

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

Area	Audit Questionnaire	Auditor remarks
Asset Management (ID.AM)	Does the Organisation use client/server certificates to authenticate hardware assets connecting to the organization's trusted network?	
Asset Management (ID.AM)	Does the organisation utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network? The authentication system shall be tied into the hardware assetinventory data to ensure only authorized devices can connect to the network.	
Asset Management (ID.AM)	Does the organization identify critical assets based on their sensitivity?	
Asset Management (ID.AM)	Does the organization maintain an up-to-date inventory of its hardware, software, information assets, details of network resources and also maintain records of those personnel who are issued such assets?	
Asset Management (ID.AM)	Has organization maintained an up-to-date centralised inventory of authorised software / applications / libraries, etc.?	
Asset Management (ID.AM)	Has the organization managed and protected data/information asset considering how the data/information are stored, transmitted, processed, accessed and put to use within / outside the organization's network, and level of risk they are exposed to depending on the sensitivity of the data / information?	
Asset Management (ID.AM)	Has the organization put in place appropriate environmental controls for securing location of critical assets providing protection from natural threats?	
Asset Management (ID.AM)	Has the organization put in place mechanism for monitoring any potential compromises or breach to environmental controls?	
Asset Management (ID.AM)	Is it ensured that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timelymanner?	
Business Environment (ID.BE)	Are Priorities for organizational mission, objectives, and activities w.r.t cybersecurity roles, responsibilities, and risk management decisions, established and communicated?	
Business Environment (ID.BE)	Are Resilience requirements to support delivery of critical services are established for all operating states? (e.g. under duress/attack, during recovery, normal operations)	
Business Environment (ID.BE)	Has the organization established Standard Operating Procedures (SOP) for all major IT activities including for connecting devices to the network environment of the organization?	
Business Environment (ID.BE)	Has the organization maintained up-to-date network architecturediagram at the organization level including wired / wireless networks?	
Governance (ID.GV)	Is official designated to assume overall responsibility for governance and monitoring of Information Security	

Area	Audit Questionnaire	Auditor remarks
Governance (ID.GV)	Does the organization form an IS RMC which shall be responsible to ensure that the policy remains updated at all times?	
Governance (ID.GV)	Is the annual audit plan and the reports presented to the Audit Committee of the Board of the organization?	
Governance (ID.GV)	Does Cyber Security Policy include process of recovering from incidents through incident management & other appropriate recovery mechanisms?	
Governance (ID.GV)	Does Cyber Security Policy include process on detecting incidents, anomalies and attacks via appropriate monitoring tools / process?	
Governance (ID.GV)	Does Cyber Security Policy include process on protecting assets by deploying suitable controls, tools & measures?	
Governance (ID.GV)	Does Cyber Security Policy include process on responding after identification of the incident, anomaly or attack?	
Governance (ID.GV)	Does the organization implement any operation / process / monetary transactions through API follow best practices from international standards like ISO 27001, COBIT 5, etc? Are such practices periodically reviewed?	
Governance (ID.GV)	Are cyber security roles and responsibilities coordinated and alligned with internal roles and external partners?	
Governance (ID.GV)	Is there a Cyber Crisis Management Plan (CCMP) available? Are Cert-In / NCIIPC guidelines used for preparing Cyber Crisis Management Plan?	
Governance (ID.GV)	Is there a SOC setup available which ensures continuous surveillance ?	
Governance (ID.GV)	Are the reporting procedures being taken to facilitate communication of unusual activities with designated Cyber Security officer ?	
Governance (ID.GV)	Whether a comprehensive Cyber Security Policy is in place ?	
Governance (ID.GV)	Whether a cyber risk management policy is available?	
Governance (ID.GV)	Whether Business Continuity Plan and Disaster Recovery Plan is in place ?	
Governance (ID.GV)	Whether IT architecture has been reviewed by the IT Sub Committee of the board ?	
Governance (ID.GV)	Whether the Board of the organization formed an internal technology committee of experts? Does the committee periodically review implementation of the Cyber Security policy?	
Governance (ID.GV)	For Cloud and Mobile deployment has the organisation considered the best practices relating to Cloud, Mobile Security and related areas?	
Governance (ID.GV)	Is the commitment of Senior Management ensured?	
Risk Assessment (ID.RA)	Does the organization identify potential cyber risks (threats andvulnerabilities) along with the likelihood of such threats and impact on the business and deploy controls accordingly to suppress the criticality?	

Area	Audit Questionnaire	Auditor remarks
Risk Assessment (ID.RA)	Does the organization periodically assess whether all the network devices are configured appropriately to the desired level of network security?	
Risk Assessment (ID.RA)	Are risk responses identified and prioritized?	
Risk Assessment (ID.RA)	Are threats from both internal and external parties identified and documented?	
Risk Management (ID.RM)	Are Risk management processes established, managed, and agreed to by organizational stakeholders?	
Risk Management (ID.RM)	Is Organizational risk tolerance is determined and clearly expressed?	
Supply Chain Risk Management (ID.SC)	Do vendors adhere to the applicable guidelines provided in the Cyber Security policy? Does the organization obtain the necessary self-certifications from them to ensure compliance with the policy provisions?	
Supply Chain Risk Management (ID.SC)	Has the vendors implemented appropriate information security controls and cybersecurity framework?	
Supply Chain Risk Management (ID.SC)	Vendors agreement documents are maintained and updated ?	
Supply Chain Risk Management (ID.SC)	Are there process for monitoring third - party access to protected or sensitive information?	

The next post will include checkpoints related to Step 2, "PROTECT.

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