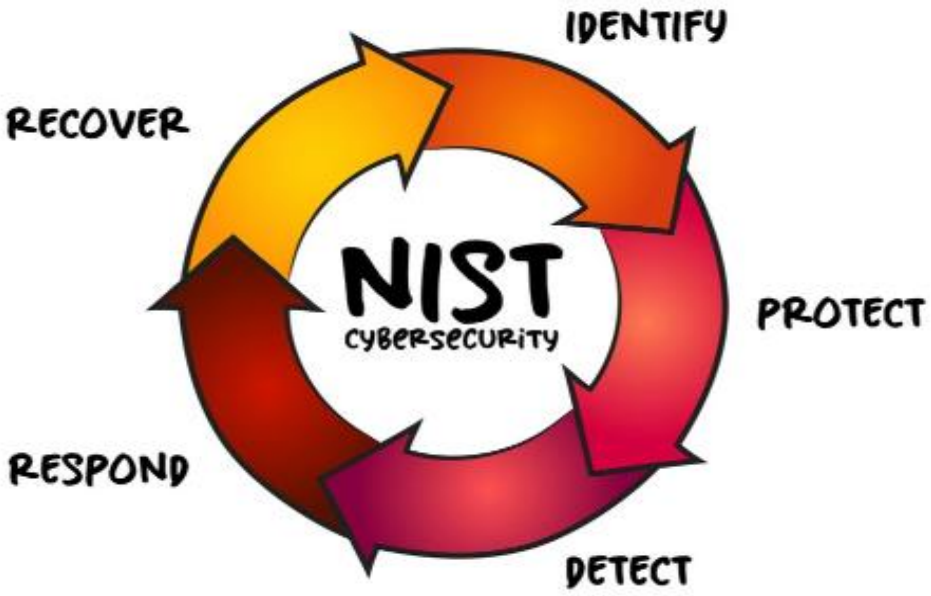
The checklist is prepared as per **National Institute of Standards and Technology (NIST) Framework** for Improving Critical Infrastructure Cybersecurity.

NIST Cybersecurity Framework



This PDF covers only the checkpoints related to Step 4 & 5, i.e. RESPOND (RS) and RECOVER (RC).

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

Area	Audit Questionnaire	Auditor remarks
Analysis (RS.AN)	Are processes established to receive, analyse and respond to vulnerabilities disclosed to the organization from internal and external sources? (e.g. internal testing, security bulletins, or security researchers)	
Analysis (RS.AN)	Does the organisation have a process to ensure that impact of an incident analysed?	
Analysis (RS.AN)	Does the organisation have a process to ensure that notifications from detection systems are investigated?	
Analysis (RS.AN)	Does the organisation have a process to ensure that forensics are performed?	
Communications (RS.CO):	Are all the cyber attacks related incidents captured and logged?	
Communications (RS.CO):	Are the cyber related incident reported to higher authority on periodic basis?	
Communications (RS.CO):	Are cyber incidents reported to CERT- In within 6 hours of noticing or being brought to notice about such incidents?	
Communications (RS.CO):	Are third parties contractually required to protect the information that is shared with them as part of an incident?	
Communications (RS.CO):	Are Contact details of Ministries, stakeholders, vendors and agencies like NCIIPC & CERT- In for incident resolutions up to date and documented?	
Communications (RS.CO):	Are the timelines prescribed for reporting incidents to external organizations including IRDAI, CERT-IN strictly adhered to?	
Communications (RS.CO):	Is root cause analysis of the incident and Action taken report submitted to the concerned insurer on demand?	
Improvements (RS.IM):	Are Response strategies updated periodically?	
Improvements (RS.IM):	Are the Board members provided with training programmes on IT Risk / Cybersecurity Risk and evolving best practices in this regard so as to cover all the Board members at least once a year.	
Improvements (RS.IM):	Are top management sensitised on various technological developments and cyber security related developments periodically?	
Improvements (RS.IM):	Are lessons learned captured and shared?	
Mitigation (RS.MI):	Has the organization defined the incident management response procedure?	
Mitigation (RS.MI):	Are newly identified vulnerabilities are mitigated or documented as accepted risks?	
Mitigation (RS.MI):	Are the corrective action procedure for all the vulnerabilities identified in VAPT?	
Response Planning (RS.RP):	Are the plans tested quarterly to include management and recovering from backups?	
Response Planning (RS.RP):	Does the organisation compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.	
Response Planning (RS.RP):	Does the organisation Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls / offline backup ?	

Area	Audit Questionnaire	Auditor remarks
Response Planning (RS.RP):	Does the organisation Ensure that all of the organization's key / critical systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system?	
Response Planning (RS.RP):	Does the organisation install the latest stable version of any security-related updates on all network devices.	
Response Planning (RS.RP):	Does the organisation Maintain standard, documented security configuration standards for all authorized network devices.	
Response Planning (RS.RP):	Does the organisation Test data integrity on backup media on aregular basis by performing a data restoration process to ensure that the backup is properly working.	
Response Planning (RS.RP):	Has the business impact analysis conducted?	
Response Planning (RS.RP):	Has the organization defined the business continuity plan and procedure?	
Response Planning (RS.RP):	Has the organization ensured that RPO(Recovery point objective) and RTO (Recovery point objective) are inline with the policy?	
Response Planning (RS.RP):	Are the incidents responded and analysed?	
Response Planning (RS.RP):	Are the security incidents analysed and corrective actions implemented for continual improvement ?	
Response Planning (RS.RP):	Is the recovery plan understood and communicated through all securitytraining? Are employee responsibilities and roles explicitly stated in the plan and communicated?	
Response Planning (RS.RP):	Is there an incident response / crisis team with clearly defined roles and responsibilities?	
Response Planning (RS.RP):	Is Cyber Crisis plan implemented and exercised or rehearsed periodically?	
Communications (RC.CO):	Are recovery activities communicated to internal and external stakeholders as well as executive and management team?	
Improvements (RC.IM):	Are recovery strategies updated periodically?	
Improvements (RC.IM):	Does recovery plans incorporate lessons learned?	
Recovery Planning (RC.RP):	Is recovery plan executed during or after a cybersecurity incident?	

Area	Audit Questionnaire	Auditor remarks

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

https://youtube.com/@sachinhissaria6512