

Control No.	Area	Audit Questionnaire	Regulated Entities / Intermediaries		
			Cat-1	Cat-2	Cat-3
			Gross Insurance Revenue: > = 50 Crs (All Insurance Intermediaries using ISNP and Web Aggregators will fall under this category)	Gross Insurance Revenue: > = 5 Cr and < 50 Cr	Gross Insurance Revenue: < 5 Crs
1	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 by officer(s) preferably at senior levels who are well equipped to understand the business and technical context of the exception(s) ?	Board Approved	MD Approval	MD Approval
2	Security Continuous Monitoring & Detection (DE.CM):	Are the security logs maintained and monitored?	Yes	Yes	Yes
3	Security Continuous Monitoring & Detection (DE.CM):	Are there any procedure to monitor capacity utilization of critical systems and networks ?	Yes	Yes	Yes
4	Security Continuous Monitoring & Detection (DE.CM):	Are there mechanism to periodically incorporate lessons learnt to continually improve the response strategies?	Yes	Yes	Yes
5	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation 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.	Yes	Yes	Yes
6	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Apply host-based firewalls on end systems	Yes	Yes	Yes
7	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 for internally developed software.	Yes	Yes	Yes
8	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Associate active ports, services and protocols to the hardware assets (including cloud resources) in the asset inventory.	Yes	Yes	Yes
9	Security Continuous Monitoring & Detection (DE.CM):	Does the organization disable dormant accounts (preferably automatically) after a set period of inactivity.	Yes	Yes	Yes
10	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Automatically lock workstation sessions after a standard period of inactivity.	Yes	Yes	Yes
11	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Block all e-mail attachments entering the organization's email gateway if the file types are unnecessary for the organization's business.	Yes	Yes	Yes
12	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.	Yes (atleast half yearly)	Annual	Annual
13	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.	Yes	Yes	Yes
14	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Configure devices to not auto-run content from removable media.	Yes	Yes	Yes
15	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Configure monitoring systems to inspect network packets passing through the boundary at each of the organization's network boundaries?	Yes	Yes	Yes
16	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.	Yes	Yes	Optional
17	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.	Yes	Yes	Yes
18	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.	Yes	Yes	Yes
19	Security Continuous Monitoring & Detection (DE.CM):	Does the organization Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks?	Yes	Optional	Optional
20	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Decrypt all encrypted network traffic at the boundary proxy prior to analysing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	Yes	Yes	Optional
21	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Deliver training to address the skills gap identified to positively impact workforce members' security behaviour.	Yes	Yes	Yes
22	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries..	Yes	Yes	Yes
23	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.	Yes	Yes	Limited
24	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Disable 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.	Yes	Yes	Yes
25	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Disable any account that cannot be associated with a business process or business owner.	Yes	Yes	Yes
26	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Disable wireless access on devices that do not have a business purpose for wireless access.	Yes	Yes	Yes
27	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.	Yes	Yes	Yes

28	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Encrypt sensitive information at rest ?	Yes	Yes	Yes
29	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Encrypt all sensitive information in transit?	Yes	Yes	Optional
30	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.	Yes	Yes	Yes
31	Security Continuous Monitoring & Detection (DE.CM):	Does the organization Ensure that micro segmentation shall be implemented in a network to create separate zones for countering lateral movement and assigning appropriate privileged access as defined in the policy?	Yes	Yes	Yes
32	Security Continuous Monitoring & Detection (DE.CM):	Whether group companies' infrastructure, networks, and databases are logically and/or physically segregated, and where a vendor provides services to group companies, whether IT personnel with cross-entity access are segregated, wherever possible?	Yes	Yes	Yes
33	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure that all accounts have an expiration date that is monitored and enforced.	Yes	Yes	Yes
34	Security Continuous Monitoring & Detection (DE.CM):	Does the organization ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities in case of in-house software development. In case of third party software development, SLAs/Agreements contain clauses on adherence to secure coding as per CERT-IN guidelines	Yes	Yes	Yes
35	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	Yes	Yes	Shared
36	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.	Yes	Yes	Yes
37	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 i.e., N-1 and above of the browsers and email clients provided by the vendor.	Yes	Yes	Yes
38	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.	Yes	Yes	Annual
39	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group and whether it educates security researchers about CERT-In's role as a CVE Numbering Authority (CNA), the Responsible Disclosure Framework, and the acknowledgement process administered by CERT-In?.	Yes	Yes	Yes
40	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 (including API) attacks.	Yes	Yes	Limited
41	Security Continuous Monitoring & Detection (DE.CM):	Does the organization establish secure coding practices appropriate to the programming language and development environment being used in case of in-house software development and in case of third party software development adherence to securing coding practices as per CERT-IN guidelines should form part of SLAs/Agreements and vendors to demonstrate adherence through independent secure code review reports	Yes	Yes	Yes
42	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation for applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.	Yes	Yes	Yes
43	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation for all business critical software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.	Yes	Yes	Yes
44	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.	Yes	Yes	Sensitive Data
45	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.	Yes	Yes	Yes
46	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.	Yes	Yes	Yes
47	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.	Yes	Yes	Limited
48	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.	Yes	Yes	Yes
49	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Maintain an inventory of authorized wireless access points connected to the wired network.	Yes	Yes	Yes
50	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Maintain an inventory of each of the organization's authentication systems, including those located on-site or at a remote service provider.	Yes	Yes	Yes
51	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Maintain separate environments for production and non-production systems. Developers should not have unmonitored access to production environments.	Yes	Yes	Yes

52	Security Continuous Monitoring & Detection (DE.CM):	Does the organization manage all critical/core/perimeter network and network security devices using multi- factor authentication and encrypted sessions	Yes	Yes	Limited
53	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices. For troubleshooting purposes if any remote access is granted to network infrastructure the same should be with necessary prior approvals and for limited period of troubleshooting window	Yes	Yes	Seperated VLANs
54	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Monitor attempts to access deactivated accounts through audit logging.	Yes	Yes	Yes
55	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation On a regular basis, review logs to identify anomalies or abnormal events.	Yes	Yes	Yes
56	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.	Yes	Yes	Optional
57	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. The Organisations may over a period of time prepare and retain a Software Bill of Material (SBOM) as per CERT-IN guidelines.	Yes	Yes	Yes
58	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation perform a skills gap analysis to understand the skills and behaviours workforce members are not adhering to, using this information to build a baseline education roadmap.	Yes	Yes	Once in 2 years
59	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.	Yes	Yes	Optional
60	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.	Yes	Yes	Limited
61	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 to them.	Yes	Yes	Annual
62	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Protect web applications by deploying web application 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 the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	Yes	Yes	Limited
63	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Remove sensitive 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.	Yes	Yes	Yes
64	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation ensure all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication (MFA).	Yes	Yes	MFA
65	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation ensure multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider.	Yes	Yes	Yes
66	Security Continuous Monitoring & Detection (DE.CM):	Does the organization segment the network to segregate all sensitive information on separated Virtual Local Area Networks (VLANs) for protecting all sensitive information?	Yes	Yes	Yes
67	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 website category definitions available. Uncategorized sites shall be blocked by default.	Yes	Yes	Optional
68	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.	Yes	Yes	Yes
69	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.	Yes	Yes	Yes
70	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Train workforce members on the importance of enabling and utilizing secure authentication.	Yes	Yes	Yes
71	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.	Yes	Yes	Yes
72	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.	Yes	Yes	Yes
73	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Uninstall or disable any unauthorized browser or email client plugins or add-on applications.	Yes	Yes	Yes
74	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.	Yes	Yes	Limited
75	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Use an automated tool, such as host-based Data Loss Prevention, Email DLP to enforce access controls to data even when data is copied off a system.	Yes	Limited	Optional
76	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Use DNS filtering services to help block access to known malicious domains.	Yes	Yes	Yes
77	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Use only standardized and extensively reviewed encryption algorithms.	Yes	Yes	Yes

78	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Use sandboxing to analyse and block inbound email attachments with malicious behaviour.	Yes	Yes	Optional
79	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.	Yes	Yes	Yes
80	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.	Yes	Optional	Optional
81	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	Yes	Optional	Optional
82	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 the developer or appropriately hardened based on developer security recommendations.	Yes	Yes	Yes
83	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.	Yes	Yes	Optional
84	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?	Yes	Yes	Shared
85	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?	Yes	Yes	Yes
86	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?	Yes	Yes	Yes
87	Security Continuous Monitoring & Detection (DE.CM):	Has the organization implemented mechanism to automatically identify unauthorised device connections to the organization's network and block such connections?	Yes	Yes	Yes
88	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation conduct periodic tests for all the critical application, server, network devices and data bases?	Yes	Yes	Annual
89	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation implement a process to communicate vulnerabilities to vendors?	Yes	Yes	Yes
90	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation maintain tracker for closure and corrective action of VAPT?	Yes	Yes	Yes
91	Security Continuous Monitoring & Detection (DE.CM):	Whether a policy to ensure high availability and timely detection of attacks is defined and implemented ?	Yes	Yes	Yes
92	Security Continuous Monitoring & Detection (DE.CM):	Whether vulnerability assessment and penetration testing procedure and calendar are defined ?	Yes	Yes	Yes
93	Security Continuous Monitoring & Detection (DE.CM):	Is VAPT of internet-facing applications or infrastructure components conducted periodically at least once every 6 months by a CERT-In empaneled Auditor	Yes	Yes	Annual
94	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.	Yes	Yes	Yes
95	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.	Yes	Yes	Major Changes
96	Security Continuous Monitoring & Detection (DE.CM):	Is External Black Grey/White box Penetration Testing (PT) conducted for all internet facing information assets or systems at least once in 6 months by a CERT-In empaneled Auditor.	Yes	Yes	Annual
97	Security Continuous Monitoring & Detection (DE.CM):	Whether, in cases where PT is conducted in a test environment due to unavoidable circumstances, the organization ensures that the test environment's version and configuration resemble the production environment for VAPT, and any deviations are placed before the ISRMC for approval?	Yes	Yes	Yes
98	Security Continuous Monitoring & Detection (DE.CM):	Are High risk gaps, reported from the VAPT closed within the time period prescribed under guidelines (one month) followed by mandatory re-validation test.	Yes	Yes	Yes
99	Security Continuous Monitoring & Detection (DE.CM):	Are audit gaps reported in VAPT closed within the timeframe provided in the guidelines (two months) followed by mandatory re-validation test.	Yes	Yes	Yes
100	Security Continuous Monitoring & Detection (DE.CM):	Whether any exception request exceeding 12 months has undergone reassessment and re-approval, and whether all granted exceptions are formally documented along with the associated risks?	Yes	Yes	Yes
101	Security Continuous Monitoring & Detection (DE.CM):	Is the organizations information assets synchronized with a singular time source? Is there a monitoring process if the devices are not in sync/async with defined time-source ?	Yes	Yes	Yes
102	Detection Processes (DE.DP):	Are roles and responsibilities for detection well defined to ensure accountability?	Yes	Yes	Yes
103	Detection Processes (DE.DP):	Do detection activities comply with all applicable requirements?	Yes	Yes	Yes
104	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?	Yes	Yes	Yes
105	Asset Management (ID.AM)	Does the Organisation use client certificates/server to authenticate hardware assets (including cloud resources) connecting to the organization's trusted network?	Yes	Yes	Yes
106	Asset Management (ID.AM)	Does the organisation Utilize port level access control, following 802.1x standards or cloud native equivalents, to control which devices can authenticate to the network? The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	Yes	Yes	Limited
107	Asset Management (ID.AM)	Does the organization identify critical assets based on their sensitivity?	Yes	Yes	Yes

108	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?	Yes	Yes	Yes
109	Asset Management (ID.AM)	Has organization maintained an up-to-date centralised inventory of authorised software/applications/libraries, etc. ?	Yes	Yes	Yes
110	Asset Management (ID.AM)	Does the organization maintain an up-to-date inventory of its cryptographic assets to ensure preparedness for transition to post-quantum cryptographic environments?	Yes	Yes	Yes
111	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?	Yes	Yes	Yes
112	Asset Management (ID.AM)	Has the organization put in place appropriate environmental controls for securing location of critical assets providing protection from natural threats?	Yes	Yes	Yes
113	Asset Management (ID.AM)	Has the organization put in place mechanism for monitoring any potential compromises or breach to environmental controls?	Yes	Yes	Yes
114	Asset Management (ID.AM)	Is it ensured that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner?	Yes	Yes	Yes
115	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?	Yes	Yes	Yes
116	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)	Yes	Yes	Yes
117	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?	Yes	Yes	Yes
118	Business Environment (ID.BE)	Has the organization maintained up-to-date network architecture diagram at the organization level including wired/wireless networks?	Yes	Yes	Yes
119	Governance (ID.GV)	Is official designated to assume overall responsibility for governance and monitoring of Information Security?	Designated CISO	Designated / Virtual CISO	Designated / Virtual CISO
120	Governance (ID.GV)	Does the organization form an IS RMC which shall be responsible to ensure that the policy remains updated at all times?	IS RMC	IT, Legal, HR, Risk, Business Ops	IT, Legal, HR, Business Ops
121	Governance (ID.GV)	Is the annual audit plan and the reports presented to the Audit Committee of the Board of the organization?	Yes	Yes	MD
122	Governance (ID.GV)	Does Cyber Security Policy include process of recovering from incidents through incident management & other appropriate recovery mechanisms?	Yes	Yes	Yes
123	Governance (ID.GV)	Does Cyber Security Policy include process on detecting incidents, anomalies and attacks via appropriate monitoring tools/process?	Yes	Yes	Yes
124	Governance (ID.GV)	Does Cyber Security Policy include process on protecting assets by deploying suitable controls, tools & measures?	Yes	Yes	Yes
125	Governance (ID.GV)	Does Cyber Security Policy include process on responding after identification of the incident, anomaly or attack?	Yes	Yes	Yes
126	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 the APIs security tested ? Are such practices periodically reviewed?	Yes	Yes	Yes
127	Governance (ID.GV)	Are cybersecurity roles and responsibilities coordinated and aligned with internal roles and external partners?	Yes	Yes	Yes
128	Governance (ID.GV)	Is there a Cyber Crisis Management Plan (CCMP) available? Are Cert-In / NCIIPC guidelines used for preparing Cyber Crisis Management Plan?	Yes	Yes	Yes
129	Governance (ID.GV)	Is there a SOC setup available which ensures continuous surveillance ?	Yes	Yes	Limited/Shared
130	Governance (ID.GV)	Are the reporting procedures being taken to facilitate communication of unusual activities with designated Cyber Security officer ?	Yes	Yes	Yes
131	Governance (ID.GV)	Whether a comprehensive Cyber Security Policy is in place ?	Yes	Yes	Yes
132	Governance (ID.GV)	Whether a cyber risk management policy is available ?	Yes	Yes	Yes
133	Governance (ID.GV)	Whether Business Continuity Plan and Disaster Recovery Plan is in place ?	Yes	Yes	Core Systems
134	Governance (ID.GV)	Whether IT architecture including cloud deployment, Saas etc., has been reviewed by the IT Sub Committee of the board ?	Yes	MD	MD
135	Governance (ID.GV)	Whether the Board of the organization formed an IT Steering Committee (ITSC) and ISRMC ? Does the committee periodically review implementation of the Cyber Security policy and IT Policy?	Yes	MD	MD

136	Governance (ID.GV)	For Cloud and Mobile deployment has the organisation considered the best practices relating to Cloud, Mobile Security and related areas?	Yes	Yes	Yes
137	Governance (ID.GV)	Whether, an Independent External Expert (IEE) with substantial IT and/or cybersecurity expertise in managing or guiding IT/cybersecurity initiatives or projects is included as a member of the RMC?	Yes	Yes	Yes
138	Risk Assessment (ID.RA)	Does the organization identify potential cyber risks (threats and vulnerabilities) along with the likelihood of such threats and impact on the business and deploy controls accordingly to suppress the criticality?	Yes	Yes	Yes
139	Risk Assessment (ID.RA)	Does the organization periodically assess whether all the network devices are configured appropriately to the desired level of network security?	Yes	Yes	Yes
140	Risk Assessment (ID.RA)	Are risk responses identified and prioritized?	Yes	Yes	Yes
141	Risk Assessment (ID.RA)	Are threats from both internal and external parties identified and documented?	Yes	Yes	Yes
142	Risk Management (ID.RM)	Are Risk management processes established, managed, and agreed to by organizational stakeholders?	Yes	Yes	Yes
143	Risk Management (ID.RM)	Is Organizational risk tolerance is determined and clearly expressed?	Yes	Yes	Yes
144	Supply Chain Risk Management (ID.SC)	Does vendors adhere to the applicable guidelines provided in the Cyber Security policy? Does the organization obtains the necessary self-certifications from them to ensure compliance with the policy provisions? Whether periodic assessment of third party vendors is conducted so they remain compliant with the requirements of insurer ?	Yes	Yes	Yes
145	Supply Chain Risk Management (ID.SC)	Has the vendors implemented appropriate information security controls and cybersecurity framework?	Yes	Yes	Yes
146	Supply Chain Risk Management (ID.SC)	Are Vendors agreement documents maintained and updated ?	Yes	Yes	Yes
147	Supply Chain Risk Management (ID.SC)	Are there process for monitoring third - party access to protected or sensitive information?	Yes	Yes	Yes
148	Supply Chain Risk Management (ID.SC)	Whether the Regulated Entity, through SLAs, requires service providers / outsourced entities to obtain prior written permission before any further outsourcing	Yes	Yes	Yes
149	Supply Chain Risk Management (ID.SC)	Is the Cloud Service Provider (CSP) MeitY empaneled CSP and holds a valid STQC (or any other equivalent agency appointed by Government of India) audit status?	Yes	Yes	Yes
150	Supply Chain Risk Management (ID.SC)	Has the organization signed NDA with CSP covering all aspects relating to privacy, confidentiality, security and business continuity?	Yes	Yes	Yes
151	Supply Chain Risk Management (ID.SC)	Does the organization contractually require that the cloud service provider will completely eliminate any trace of data/ information in disks, backups, etc., at the termination of the contract?	Yes	Yes	Yes
152	Identity Management, Authentication and Access Control (PR.AC):	Are ICT infrastructure logs maintained for a rolling period of 180 days as per CERT-In directions?	Yes	Yes	Yes
153	Identity Management, Authentication and Access Control (PR.AC):	Are ICT infrastructure logs, Critical and Business data stored in India?	Yes	Yes	Yes
154	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?	Yes	Yes	Yes
155	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.)?	Yes	Yes	Yes
156	Identity Management, Authentication and Access Control (PR.AC):	Does the access control policy address strong password management control for access to systems, applications, networks and databases?	Yes	Yes	Yes
157	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 access privileges have been withdrawn?	Yes	Yes	Yes
158	Identity Management, Authentication and Access Control (PR.AC):	Has the organization deployed security measures and controls to supervise 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?	Yes	Yes	Yes
159	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?	Yes	Yes	Yes
160	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?	Yes	Yes	Yes
161	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?	Yes	Yes	Yes

162	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 ?	Yes	Yes	Yes
163	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?	Yes	Yes	Yes
164	Identity Management, Authentication and Access Control (PR.AC):	Has the organization implemented controls to minimize invalid login counts, deactivate dormant accounts?	Yes	Yes	Yes
165	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 accompanied all the time by the authorized employee of the organization while third party staff has been given physical access to critical systems ?	Yes	Yes	Yes
166	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?	Yes	Yes	Yes
167	Awareness and Training (PR.AT):	Are the history and versions of training content maintained?	Yes	Yes	Yes
168	Awareness and Training (PR.AT):	Are the targeted awareness/training for key personnel conducted periodically?	Yes	Annual	Annual
169	Awareness and Training (PR.AT):	Are the training programs reviewed and updated periodically?	Yes	Annual	Annual
170	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.	Yes	Yes	Yes
171	Awareness and Training (PR.AT):	Do users indicate that they understand their responsibilities?	Yes	Yes	Yes
172	Awareness and Training (PR.AT):	Is awareness level evaluated periodically?	Yes	Annual	Once in 2 years
173	Awareness and Training (PR.AT):	Is there additional training for leaders to understand their roles in the event of a security incident?	Yes	Yes	Yes
174	Awareness and Training (PR.AT):	Is there a process to handle if a-user does not complete the training?	Yes	Yes	Yes
175	Awareness and Training (PR.AT):	Is someone responsible for creating the security training for the organization?	Yes	Yes	Yes
176	Awareness and Training (PR.AT):	Has the Organization periodically participated in national/ sectoral/ organisational Cyber Security Exercises?	Yes	Yes	Yes
177	Data Security (PR.DS):	Are open ports on network and systems which are not in use blocked ?	Yes	Yes	Yes
178	Data Security (PR.DS):	Does the application be set to automatically log a user off the application after a predefined period of inactivity?	Yes	Yes	Yes
179	Data Security (PR.DS):	Does the application force password expiration and prevent users from reusing a password?	Yes	Yes	Yes
180	Data Security (PR.DS):	Does the system administrator enforce password policy and/or complexity such as minimum length, numbers and alphabet requirements, and upper and lower case constraint, etc.?	Yes	Yes	Yes
181	Data Security (PR.DS):	Does the application force "new" users to change their password upon first login into the application?	Yes	Yes	Yes
182	Data Security (PR.DS):	Does the application prohibit users from logging into the application on more than one workstation at the same time with the same user ID?	Yes	Yes	Yes
183	Data Security (PR.DS):	Does the application support integration with the enterprise identity management system?	Yes	Yes	Yes
184	Data Security (PR.DS):	Does the organization authorize data storage devices within their IT infrastructure through appropriate validation process?	Yes	Yes	Yes

185	Data Security (PR.DS):	Is there a process by which the organization maintains the evidence of media disposal?	Yes	Yes	Yes
186	Data Security (PR.DS):	Has there been a implementation of a data-disposal and data-retention policy?	Yes	Yes	Yes
187	Data Security (PR.DS):	Are there processes for media formatting?	Yes	Yes	Yes
188	Data Security (PR.DS):	Is there measurement a client system's vulnerabilities?	Yes	Optional	Optional
189	Data Security (PR.DS):	Are appropriate and effective security measures in place to share the data with third Parties ?	Yes	Yes	Yes
190	Data Security (PR.DS):	Are appropriate technologies implemented for data mobility security?	Yes	Yes	Yes
191	Information Protection Processes and Procedures (PR.IP):	Does the organisation maintain back-up of source code repository for critical applications developed in-house and for third party softwares considered business critical entered into an escrow arrangement?	Yes	Yes	Yes
192	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.	Yes	Yes	Yes
193	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?	Yes	Yes	Yes
194	Information Protection Processes and Procedures (PR.IP):	Are there methods to prevent unauthorized access by other groups into individual files and department-shared files?	Yes	Yes	Yes
195	Information Protection Processes and Procedures (PR.IP):	Are there procedures for limiting access to LAN and network operating software?	Yes	Yes	Yes
196	Information Protection Processes and Procedures (PR.IP):	Are updates/changes to the Website independently reviewed, approved and tested?	Yes	Yes	Yes
197	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?	Yes	Yes	Yes
198	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?	Yes	Yes	Yes
199	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.	Yes	Yes	Limited
200	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?	Yes	Yes	Yes
201	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.	Yes	Yes	Yes
202	Information Protection Processes and Procedures (PR.IP):	Does the organization's application whitelisting software must ensure that only authorized scripts are allowed to run on a system?	Yes	Yes	Yes
203	Information Protection Processes and Procedures (PR.IP):	Is a periodic inventory taken to verify that the appropriate backup files are being maintained?	Yes	Yes	Yes
204	Information Protection Processes and Procedures (PR.IP):	Is appropriate immutable backup and Failover/Resilient components available for critical hardware?	Yes	Yes	Yes
205	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.	Yes	Yes	Yes
206	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?	Yes	Yes	Yes
207	Information Protection Processes and Procedures (PR.IP):	Is the use of remote access software restricted?	Yes	Yes	Yes



208	Information Protection Processes and Procedures (PR.IP):	Is there documentation describing data, programs, hardware, and system requirements?	Yes	Yes	Yes
209	Information Protection Processes and Procedures (PR.IP):	Are policies and procedures being used to protect critical information at different layers of security?	Yes	Yes	Yes
210	Maintenance (PR.MA):	Is there a process to determine after how many days of identification, patches would be fixed?	Yes	Yes	Yes
211	Maintenance (PR.MA):	Are remote maintenance of organizational assets approved, logged, and performed in a manner that prevents unauthorized access?	Yes	Yes	Yes
212	Maintenance (PR.MA):	Are Defined parameters taken for prioritizing the patches need to be installed?	Yes	Yes	Yes
213	Maintenance (PR.MA):	Are maintenance and repair of organizational assets logged whenever performed, with approved and controlled tools?	Yes	Yes	Yes
214	Maintenance (PR.MA):	Is there a process to deploy critical patches in a test environment?	Yes	Yes	Yes
215	Maintenance (PR.MA):	Are the approved patch management policy have been implemented?	Yes	Yes	Yes
216	Maintenance (PR.MA):	Have parameters been defined for classifying patches?	Yes	Yes	Yes
217	Protective Technology (PR.PT):	Are adequate measures taken to isolate and secure the perimeter and connectivity of the servers running monetary transactions applications/process?	Yes	Yes	Yes
218	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?	Yes	Yes	Yes
219	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?	Yes	Yes	Yes
220	Protective Technology (PR.PT):	Has the organization documented and implemented secure mail and messaging systems that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.?	Yes	Yes	Yes
221	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 devices within their IT environment? Are LAN and wireless networks secured within organizations premises by deploying proper controls?	Yes	Yes	Yes
222	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?	Yes	Yes	Yes
223	Protective Technology (PR.PT):	Has the organization installed network security devices, such as firewalls, 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?	Yes	Yes	Yes
224	Communications (RC.CO):	Are recovery activities communicated to internal and external stakeholders as well as executive and management team?	Yes	Yes	Yes
225	Improvements (RC.IM):	Are recovery strategies updated periodically?	Yes	Yes	Yes
226	Improvements (RC.IM):	Does recovery plans incorporate lessons learned?	Yes	Yes	Yes
227	Recovery Planning (RC.RP):	Is recovery plan executed during or after a cybersecurity incident?	Yes	Yes	Yes
228	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)	Yes	Yes	Yes
229	Analysis (RS.AN)	Does the organisation have a process to ensure that impact of an incident analysed?	Yes	Yes	Yes
230	Analysis (RS.AN)	Does the organisation have a process to ensure that Notifications from detection systems are investigated ?	Yes	Yes	Yes

231	Analysis (RS.AN)	Does the organisation have a process to ensure that forensics are performed?	Yes	Yes	Yes
232	Communications (RS.CO):	Are all the cyber attacks related incidents captured and logged?	Yes	Yes	Yes
233	Communications (RS.CO):	Are the cyber related incident reported to higher authority on periodic basis?	Yes	Yes	Yes
234	Communications (RS.CO):	Are cyber incidents reported to CERT-In within 6 hours of noticing or being brought to notice about such incidents?	Yes	Yes	Yes
235	Communications (RS.CO):	Are third parties contractually required to protect the information that is shared with them as part of an incident?	Yes	Yes	Yes
236	Communications (RS.CO):	Are Contact details of Ministries, stakeholders, vendors and agencies like NCIIPC & CERT-In for incident resolutions up to date and documented?	Yes	Yes	Yes
237	Communications (RS.CO):	Are the timelines prescribed for reporting incidents to external organizations including IRDAI, CERT-In strictly adhered to?	Yes	Yes	Yes
238	Communications (RS.CO):	Is root cause analysis of the incident and Action taken report submitted to the concerned insurer on demand.	Yes	Yes	Yes
239	Improvements (RS.IM):	Are Response strategies updated periodically?	Yes	Yes	Yes
240	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.	Yes	MD	MD
241	Improvements (RS.IM):	Are top management sensitised on various technological developments and cyber security related developments periodically?	Yes	Annual	Annual
242	Improvements (RS.IM):	Are lessons learned captured and shared?	Yes	Yes	Yes
243	Mitigation (RS.MI):	Has the organization defined the incident management response procedure ?	Yes	Yes	Yes
244	Mitigation (RS.MI):	Are newly identified vulnerabilities are mitigated or documented as accepted risks?	Yes	Yes	Yes
245	Mitigation (RS.MI):	Are the corrective action procedure for all the vulnerabilities identified in VAPT?	Yes	Yes	Yes
246	Response Planning (RS.RP):	Are the plans tested quarterly to include management and recovering from backups?	Yes	Annual	Annual
247	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.	Yes	Yes	Yes
248	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 ?	Yes	Yes	Sensitive Data
249	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.	Yes	Yes	Yes
250	Response Planning (RS.RP):	Does the organisation Install the latest stable version of any security-related updates on all network devices.	Yes	Yes	Yes
251	Response Planning (RS.RP):	Does the organisation Maintain standard, documented security configuration standards for all authorized network devices.	Yes	Yes	Yes
252	Response Planning (RS.RP):	Does the organisation Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	Bi-annually	Bi-annually	Annual
253	Response Planning (RS.RP):	Has the business impact analysis conducted?	Yes	Yes	Yes

254	Response Planning (RS.RP):	Has the organization defined the business continuity plan and procedure?	Yes	Yes	Yes
255	Response Planning (RS.RP):	Has the organization ensured that RPO(Recovery point objective) and RTO (Recovery point objective) are inline with the policy?	Yes	Yes	Yes
256	Response Planning (RS.RP):	Are the incidents responded and analysed?	Yes	Yes	Yes
257	Response Planning (RS.RP):	Are the security incidents analysed and corrective actions implemented for continual improvement ?	Yes	Yes	Yes
258	Response Planning (RS.RP):	Is the recovery plan understood and communicated through all security training? Are employee responsibilities and roles explicitly stated in the plan and communicated?	Yes	Yes	Yes
259	Response Planning (RS.RP):	Is there an incident response / crisis team with clearly defined roles and responsibilities?	Yes	Yes	Yes
260	Response Planning (RS.RP):	Is Cyber Crisis plan implemented and exercised or rehearsed periodically	Yes	Yes	Annual
261	Work From Remote Location (WFRL)	Does the Board approved Cyber Security Policy (Policy) of Regulated Entity address risks associated with Work From Remote Location (WFRL) risks?	Yes	MD	MD
262	Work From Remote Location (WFRL)	Does the Policy confirms use of secure network with strong protocols and Wi-Fi passwords at remote location?	Yes	Yes	Yes
263	Work From Remote Location (WFRL)	Does it mandates passwords change periodically?	Yes	Yes	Yes
264	Work From Remote Location (WFRL)	Are users provided with authorized assets of the organization which are hardened as per security policy for strong password authentication?	Yes	Yes	Yes
265	Work From Remote Location (WFRL)	Are servers, applications and networks hardened and secured as per standardized security policy settings?	Yes	Yes	Yes
266	Work From Remote Location (WFRL)	Are device controls implemented on user systems and Information and Communication Technology (ICT) infrastructure systems to block admin level access, unauthorized installation or changes to software, USB and other media, peripherals?	Yes	Yes	Yes
267	Work From Remote Location (WFRL)	Are user systems enabled with Antivirus, Endpoint protection controls, data encryption and Data Loss Prevention mechanisms?	Yes	Yes	Yes
268	Work From Remote Location (WFRL)	Does these controls pervade across all the users from all functions	Yes	Yes	Yes
269	Work From Remote Location (WFRL)	Are user systems and organization ICT infrastructure regularly updated with security patches and fixes. (Auditor to mention the latest update date)	Yes	Yes	Yes
270	Work From Remote Location (WFRL)	Are workflow approvals, deviations or exceptions captured as per Change Management Procedures.	Yes	Yes	Yes
271	Work From Remote Location (WFRL)	Are secure remote access mechanisms of Virtual Private Network (VPN), Internet Proxy or Virtual Device Interface (VDI) provisioned for WFRL users accessing organizational data assets and applications?	Yes	Yes	Yes
272	Work From Remote Location (WFRL)	Is the audit log monitoring and analysis provisioned on organizational ICT infrastructure as a control for unauthorized access risks and cyber threats?	Yes	Yes	Yes
273	Work From Remote Location (WFRL)	Does the policy, spell controls and procedures related to secure access of organizational data assets and applications from user-owned devices like mobile phones, tablets or other Bring Your Own Device (BYOD) of the Insurer?	Yes	Yes	Yes
274	Work From Remote Location (WFRL)	Do data containerization, Multifactor authentication and remote data wipe have been done to prevent data tampering and misuse of lost mobile/tablet devices during the period when WFRL has been permitted by the Insurer?	Yes	Yes	Limited
275	Work From Remote Location (WFRL)	Are users mandated to back-up critical data periodically (Policy shall mandate periodicity) on secure location in organization systems?	Yes	Yes	Yes
276	Work From Remote Location (WFRL)	Are Non-disclosure agreements / Undertaking on data security and confidentiality signed at the time of employee/ consultant/ third-party vendor on boarding before permitting Operations to be commenced at WFRL?	Yes	Yes	Yes

277	Work From Remote Location (WFRL)	Is there an audit of Privileged user identity access authentication taken for administrative purposes?	Yes	Yes	Yes
278	Work From Remote Location (WFRL)	Is there an Audit of security information and events monitoring of audit logs analysis and incident response in place?	Yes	Yes	Limited
279	Work From Remote Location (WFRL)	Are controls in place to identify unauthorized access, malicious code execution, suspicious activities or behaviour, credential theft, presence of advance persistent threats like remote access toolkits and such cyber risks to organizational ICT infrastructure?	Yes	Yes	Yes
280	Work From Remote Location (WFRL)	Are email services secured to prevent spam, spoofed mails and malware filtering?	Yes	Yes	Yes
281	Work From Remote Location (WFRL)	Are users trained to handle spam, phishing scam and fraudulent emails?	Yes	Yes	Yes
282	Work From Remote Location (WFRL)	Are suspicious or malicious domains on the internet detected and blocked on network firewall, web proxy filtering, intrusion prevention systems?	Yes	Yes	Yes
283	Work From Remote Location (WFRL)	Are device controls implemented on user systems and ICT infrastructure systems to block unauthorized internet domains, unauthorized software installation or changes to configuration, USB and any other media, peripherals?	Yes	Yes	Yes
284	Work From Remote Location (WFRL)	Are activities like walkthrough and interviews performed using approved remote access software over secure and hardened systems of auditee and auditor organizations?	Yes	Yes	Yes
285	Work From Remote Location (WFRL)	Are evidences and artefacts classified, securely demonstrated to concerned stakeholders and not shared out of authorized domains?	Yes	Yes	Yes
286	Work From Remote Location (WFRL)	Are project implementation documents, MIS reports classified and shared on Need-to-know basis?	Yes	Yes	Yes
287	Work From Remote Location (WFRL)	Are plans and procedures set in place by the organization for Cybersecurity incident response and Crisis management activities?	Yes	Yes	Yes
288	Work From Remote Location (WFRL)	Is Cyber Security Project management performed remotely?	Yes	Yes	Yes
289	Work From Remote Location (WFRL)	Confirm whether there are hardening procedures to check / scan systems brought back to Office?	Yes	Yes	Yes
290	Work From Remote Location (WFRL)	Confirm whether if all patches, AV, End Point Protection, Data Encryption mechanisms are checked to ensure its appropriate functioning?	Yes	Limited	Limited
291	Work From Remote Location (WFRL)	Are security patch updates reviewed and periodically applied on ICT infrastructure to prevent Distributed Denial of Services(DDoS) attacks?	Yes	Yes	Yes
292	Work From Remote Location (WFRL)	In the case of disruption can IT support be accessed by investment application users through portal, help desk (phone) or email or visit to office?	Yes	Yes	Yes
293	Work From Remote Location (WFRL)	Are backups reviewed periodically and procedures aligned to minimize downtime impact?	Yes	Yes	Yes
294	Work From Remote Location (WFRL)	Is DR Drill performed to ensure adherence to Business Continuity metrics? (DR Drill should have been done on a normal working day)	Yes	Annual	Annual
295	Work From Remote Location (WFRL)	Is data restoration testing performed on periodic basis to ensure integrity of backups?	Bi-annually	Bi-annually	Annual
296	Work From Remote Location (WFRL)	Are alternative site options and resource availability planned as a part of Business Continuity and tested for same?	Yes	Yes	Yes
297	Work From Remote Location (WFRL)	Are Secondary Network Connectivity and IT infrastructure is provisioned and tested for the critical applications and services?	Yes	Yes	Yes
298	Work From Remote Location (WFRL)	Is it possible to <u>access</u> systems without user authentication or by-passing authentication? (Auditor shall specifically confirm that that users cannot bypass security)	Yes	Yes	Yes
299	Work From Remote Location (WFRL)	Are applications accessible ONLY to authorised users through a secured VPN or VDI access?	Yes	Yes	Yes

300	Work From Remote Location (WFRL)	Are users authenticated and authorised by a domain policy server?	Yes	Yes	Yes
301	Work From Remote Location (WFRL)	Are Logs of application IT infrastructure are collected and analysed by 24X7 Security Operation Centre (SOC) team?	Yes	Yes	Shared
302	Work From Remote Location (WFRL)	Is Continuous (Auditor shall specifically comment on the Periodicity interval) monitoring of IT logs to review unauthorized Login/Logout by users, access violations etc. done through Security Information and Event Monitoring (SIEM) and monitored by Security Operations Centre (SOC)?	Yes	Yes	Shared
303	Work From Remote Location (WFRL)	Are Enterprise wide monitoring of Information security incidents done by SOC team on 24X7 basis?	Yes	Yes	Shared
304	Work From Remote Location (WFRL)	Are ICT infrastructure logs maintained as per regulatory guidelines?	Yes	Yes	Yes
305	Work From Remote Location (WFRL)	Are Installation of unapproved software and utilities barred	Yes	Yes	Yes
306	Work From Remote Location (WFRL)	Are users using only Organization approved collaboration software?	Yes	Yes	Yes
307	Work From Remote Location (WFRL)	Is there a preventive control to block Unauthorized Collaboration tools on the firewall/network security devices?	Yes	Yes	Yes
308	Work From Remote Location (WFRL)	Are Cybersecurity awareness circulars and advisories regularly sent to employees, third party vendor and consultants.	Yes	Yes	Yes
309	Work From Remote Location (WFRL)	Does the Organization has a Dealing room policy and Standard operating policy to supervise controls over the dealing activities during WFRL?	Yes	Yes	Yes
310	Work From Remote Location (WFRL)	Are all agreements/documents with third parties digitally signed using a special tool?	Yes	Yes	Optional
311	Work From Remote Location - Investment (WFRL.IN)	Are Recorded lines working and in well-maintained condition?	Yes	Yes	Yes
312	Work From Remote Location - Investment (WFRL.IN)	Does Mid-office check voice recording as per a defined process in Standard Operating Procedure (SOP)?	Yes	Yes	Yes
313	Work From Remote Location - Investment (WFRL.IN)	Are Dealers provided with a dedicated and secured recording line during WFH for placing the calls to the brokers.	Yes	Yes	Yes
314	Work From Remote Location - Investment (WFRL.IN)	Is Voice logger used for recording of calls made from office location?	Yes	Yes	Yes
315	Work From Remote Location - Investment (WFRL.IN)	Is Back up/storage of call recordings enabled as a part of proof of transaction that can be accessed anytime?	Yes	Yes	Yes
316	Work From Remote Location - Investment (WFRL.IN)	Does the SOP define process to handle disruption in communication links between the dealers and brokers?	Yes	Yes	Yes
317	Work From Remote Location - Investment (WFRL.IN)	Are such communications logged /recorded?	Yes	Yes	Yes
318	Work From Remote Location - Investment (WFRL.IN)	Does the Mid-Office independently review these logs / records ?	Yes	Yes	Yes
319	Work From Remote Location - Investment (WFRL.IN)	Are appropriate prior approvals / authorisations taken to process such transactions?	Yes	Yes	Yes
320	Work From Remote Location - Investment (WFRL.IN)	Do Dealers execute ALL transactions only through recorded telephone lines?	Yes	Yes	Yes
321	Work From Remote Location - Investment (WFRL.IN)	Are all authorized Bloomberg terminals / Bloomberg anywhere ID's / NDS terminals/TREPS Terminals/Emails only and are completely disabled for SMS / Chat facilities? If OEM Confirms in writing that disabling chat/SMS is not technically feasible, then the same should be archived for audit purposes.	Yes	Yes	Yes
322	Work From Remote Location - Investment (WFRL.IN)	Confirm that Bloomberg terminals/ Bloomberg anywhere ID's / NDS terminals/TREPS Terminals are accessible through multi factor authentication and are disabled for SMS / Chat facilities	Yes	Yes	Yes

323	Work From Remote Location - Investment (WFRL.IN)	In the event of disruption of communication link, are there defined policies / processes to guide the officials of the Investments Function to process transactions with appropriate approvals?	Yes	Yes	Yes
324	Work From Remote Location - Investment (WFRL.IN)	Confirm specifically that investment transactions are executed with all mandates defined as a part of Dealing room Work flow / SOP with requisite approvals	Yes	Yes	Yes
325	Work From Remote Location - Investment (WFRL.IN)	Do Dealers execute all transactions via recorded telephone lines or authorized Bloomberg terminals / Bloomberg anywhere ID's / NDS terminals/TREPS terminals/Emails only?	Yes	Yes	Yes
326	Work From Remote Location - Investment (WFRL.IN)	Confirm specifically that in addition to the recorded lines the dealers places the orders only through empanelled brokers ONLY through authorized communication modes as per SOP/Dealing room policy?	Yes	Yes	Yes
327	Work From Remote Location - Investment (WFRL.IN)	Are Contingency policy and plans, revised and tested periodically for an effective business continuity?	Yes	Yes	Yes
328	Work From Remote Location - Investment (WFRL.IN)	Are Disaster Recovery (DR) Drills performed to verify the availability of applications, processes and resources at remote backup site. Are issues identified during DR testing addressed?	Bi-annually	Bi-annually	Annual
329	Work From Remote Location - Investment (WFRL.IN)	Is IT support accessed by Investment application users by way of portal, helpdesk or visit to office.	Yes	Yes	Yes
330	Work From Remote Location - Investment (WFRL.IN)	Are Backup/Alternative locations and resources identified within Investment function to ensure business continuity?	Yes	Yes	Yes
331	Work From Remote Location - Investment (WFRL.IN)	Is Email facility enabled with empanelled broker, counter parties, custodian etc.	Yes	Yes	Yes
332	Work From Remote Location - Investment (WFRL.IN)	Are Emails shared ONLY through authorized company email addresses registered with concerned counterparties?	Yes	Yes	Yes
333	Work From Remote Location - Investment (WFRL.IN)	Is Voice recording analysis and rate scan done on a regular basis to supervise trades and transaction price as defined in dealing room policy?	Yes	Yes	Yes
334	Work From Remote Location - Investment (WFRL.IN)	Is there a supervisory monitoring process check list which includes transaction price monitoring and trade monitoring etc.?	Yes	Yes	Yes
335	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary prominently published on its website, mobile based application or both, as the case may be, the rules and regulations, privacy policy and user agreement for access or usage of its computer resource by any person?	Yes	Yes	Yes
336	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the rules and regulations, privacy policy or user agreement of the intermediary informed the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update or share any information that (i) belongs to another person and to which the user does not have any right; (ii) is defamatory, obscene, pornographic, paedophilic, invasive of another privacy including bodily privacy, insulting or harassing on the basis of gender, libellous, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise inconsistent with or contrary to the laws in force; (iii) is harmful to child; (iv) infringes any patent, trademark, copyright or other proprietary rights; (v) violates any law for the time being in force; (vi) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact; (vii) impersonates another person; (viii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting other nation; (ix) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource; (x) is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person;	Yes	Yes	Yes
337	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary periodically informed its users, at least once every year, that in case of non-compliance with rules and regulations, privacy policy or user agreement for access or usage of the computer resource of such intermediary, it has the right to terminate the access or usage rights of the users to the computer resource immediately or remove non-compliant information or both, as the case may be	Yes	Yes	Yes
338	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary, on whose computer resource the information is stored, hosted or published, upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the Act, not host, store or publish any unlawful information, which is prohibited under any law for the time being in force relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force	Yes	Yes	Yes
339	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary periodically, and at least once in a year, informed its users of its rules and regulations, privacy policy or user agreement or any change in the rules and regulations, privacy policy or user agreement, as the case may be	Yes	Yes	Yes
340	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	If the intermediary collected information from a user for registration on the computer resource, has it retained his information for a period of one hundred and eighty days after any cancellation or withdrawal of his registration, as the case may be	Yes	Yes	Yes

341	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary taken all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011	Yes	Yes	Yes
342	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Does the intermediary, as soon as possible, but not later than seventy two hours of the receipt of an order, provide information under its control or possession, or assistance to Government agency which is lawfully authorised for investigative or protective or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents	Yes	Yes	Yes
343	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary reported cyber security incidents and share related information with the Indian Computer Emergency Response Team in accordance with the policies and procedures as mentioned in the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.	Yes	Yes	Yes
344	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Is the intermediary aware that it shall not knowingly deploy or install or modify technical configuration of computer resource or become party to any act that may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force	Yes	Yes	Yes
345	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary prominently published on its website, mobile based application or both, as the case may be, the name of the Grievance Officer and his contact details as well as mechanism by which a user or a victim may make complaint against violation of the provisions of this rule or any other matters pertaining to the computer resources made available by it, and the Grievance Officer shall – (i) acknowledge the complaint within twenty four hours and dispose off such complaint within a period of fifteen days from the date of its receipt; (ii) receive and acknowledge any order, notice or direction issued by the Appropriate Government, any competent authority or a court of competent jurisdiction.	Yes	Yes	Yes
346	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary, within twenty-four hours from the receipt of a complaint made by an individual or any person on his behalf under this sub-rule, in relation to any content which is prima facie in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual, take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it	Yes	Yes	Yes
347	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	Has the intermediary implemented a mechanism for the receipt of complaints under clause (b) of this sub-rule which may enable the individual or person to provide details, as may be necessary, in relation to such content or communication link	Yes	Yes	Yes