APPLICABILITY OF CYBERSECURITY FRAMEWORK

The applicability of different **Sub Chapters** in Cybersecurity Framework as per **National Institute of Standards and Technology (NIST)** in respect of **Framework for Improving Critical Infrastructure Cybersecurity** are as under:

1. Identify (**ID**)
2. Protect (**PR**)
3. Detect (**DE**)
4. Respond (**RS**)
5. Recover (**RC**)

Additionally, there are some controls that are required to be evaluated as part of a work from remote location (**WFRL**) and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (**IGDM**)

The entities which are to be covered are as under:

1. Insurers (Life, Non-Life, Health, Re-insurer and Foreign Re-Insurance Branches)
2. **Brokers**
3. Corporate Agents
4. Web Aggregators
5. Third Party Administrators
6. Insurance Marketing Firms (IMFs)
7. Insurance Repositories
8. Insurance Information Bureau (IIB)
9. Insurance Agents
10. Insurance Self Networking Portal (ISNP)
11. Motor Dealers
12. Common Service Centres (CSC)
13. Point of Sale (POS)

The various Categories of NIST Cyber Security Framework for IRDAI Regulated Entities to whom the Cybersecurity framework is applicable

Category	Applicability
1. Insurers (Life , Non-Life, Health , Re-insurer and Foreign Re-Insurance Branches)	**All** Sub-Chapters (ID, PR, DE, RS, RC and WFRL)
2. Brokers	

Category	Applicability
3. Corporate Agents	See Table Below
4. Web Aggregators	
5. Third Party Administrators	
6. Insurance Marketing Firms (IMFs)	
7. Insurance Repositories	
8. Insurance Information Bureau (IIB)	
9. Agents	
10. Insurance Self Networking Portal	
11. Motor Dealers	
12. Common Service Centres	
13. Point of Sale (POS)	

The above entities, based on **access** to Insurer's Systems are classified as under:

Category	Applicability
a. Entities having access to Insurer's **internal systems** to view data, get proposals, download reports etc. (3rd party must not be able to **upload** or **edit** data, but can only **view** products / proposals / documents / reports	**PR** Sub-Chapter
b. 3rd parties who: 1. **connect** to Insurer systems **through automated interfaces** [Application Programming Interfaces (**APIs**), Electronic Data Interchange (**EDI**) etc.,] 2. do **processing of data** for Insurers **either through 3rd party systems** or insurers **own systems**. 3. **access** Insurers systems either **remotely** or from within **Insurer** controlled environment to **edit** data and systems	**All** Sub-Chapters (**ID, PR, DE, RS, RC and WFRL**). Where, Insurers operate from within their controlled facility, sections that need "**not be made applicable**", shall be approved by the **Board** of the Insurer.
c. Entities connected to Insurer's Systems to **upload data** or **sharing data** in predefined	

Category	Applicability
formats (such as from an **excel** or **text** file, **images, xml** etc.) ***Note:*** *The Insurer must process such uploaded files or maintain in its repository.*	**PR, DE** Sub-Chapters
d. Entities which store Insurer's data (which is not in public domain) as those relating to Policyholders, investment etc. ***Note:*** *They do not have right to access insurer systems to edit or maintain such data*	**PR, DE, RS** Sub-Chapters
e. Entities which retain only insurer data in **physical forms** and do not hold any **electronic database** of the insurers' data or do not access insurer systems	Sub-Chapters **not** applicable
f. Entities which connect insurers systems and applications to access production systems, database etc. such as Application Maintenance, IT Support services etc.,	**All** Sub-Chapters (ID, PR, DE, RS, RC and WFRL).

SECTION 2 - SUMMARY

Part A – Background Information

Nature of Activities Performed by M/s……

Application Sections of the **framework**

For ……..

Chartered Accountants

Part B - Overall Status of Findings

Area Code	Area	No of Controls (A)	NA (B)	AC (c) = A-B	H	M	L	C	Risk Mark (Hx3+Mx2+ Lx1+Cx0)
DE.AE	Anomalies and Events (DE.AE):	1							
DE.CM	Security Continuous Monitoring & Detection (DE.CM):	91							
DE.DP	Detection Processes (DE.DP):	3							
ID.AM	Asset Management (ID.AM)	9							
ID.BE	Business Environment (ID.BE)	4							
ID.GV	Governance (ID.GV)	14							
ID.RA	Risk Assessment (ID.RA)	4							
ID.RM	Risk Management (ID.RM)	2							
ID.SC	Supply Chain Risk Management (ID.SC)	4							
PR.AC	Identity Mgmt, Authentication and Access Control (PR.AC):	14							
PR.AT	Awareness and Training (PR.AT):	9							
PR.DS	Data Security (PR.DS):	16							
PR.IP	Information Protection Processes and Procedures (PR.IP):	19							
PR.MA	Maintenance (PR.MA):	7							
PR.PT	Protective Technology (PR.PT):	7							
RC.CO	Communications (RC.CO):	1							
RC.IM	Improvements (RC.IM):	2							
RC.RP	Recovery Planning (RC.RP):	1							
RS.AN	Analysis (RS.AN)	4							

Area Code	Area	No of Controls (A)	NA (B)	AC (c) = A-B	H	M	L	C	Risk Mark (Hx3+Mx2+ Lx1+Cx0)
RS.CO	Communications (RS.CO):	3							
RS.IM	Improvements (RS.IM):	4							
RS.MI	Mitigation (RS.MI):	3							
RS.RP	Response Planning (RS.RP):	14							
WFRL	Work From Remote Location (WFRL)	58							
WFRL.IN	Work From Remote Location Investment (WFRL.IN)	25							
IGDM	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IGDM)	13							
	Total	**332**							

Note on Controls: **NA** (Not Applicable), **AC** (Applicable Controls), **H** – High, **M** – Medium, **L** – Low, **C** – Complied

Part C - Details of Non-Compliances

Sl. No	Area	Audit Questionnaire	Auditors Observation	Risk Rating

Risk Rating Guidelines

Control is Designed Adequately	Control is Effectively complied with	Risk Rating
Y	Y	NA. This will not be reported
N	N	**High** Control has to be designed and implemented
N	Y	**High/Medium** – A subjective Auditor's call depending on the nature of control. Control must be designed appropriately or reflect the controls in operation
Y	N	**Low /Medium** – A subjective Auditor's call depending on the nature of control. Controls must be implemented as designed

SECTION 3 - AUDIT CHECKLIST

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		Applicable for Investment Function			
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) ?			
2	Security Continuous Monitoring & Detection (DE.CM):	Are the security logs maintained and monitored?			
3	Security Continuous Monitoring & Detection (DE.CM):	Are there any procedure to monitor capacity utilization of critical systems and networks ?			
4	Security Continuous Monitoring & Detection (DE.CM):	Are there mechanism to dynamically incorporate lessons learnt to continually improve the response strategies?			
5	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Alert when users deviate from normal login behaviour, such as time-of-day, workstation location and duration.			
6	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Any user or system accounts used to perform penetration testing should be controlled and monitored			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.			
7	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
8	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.			
9	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Associate active ports, services and protocols to the hardware assets in the asset inventory.			
10	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Automatically disable dormant accounts after a set period of inactivity.			
11	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Automatically lock workstation sessions after a standard period of inactivity.			
12	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.			
13	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.			
14	Security Continuous Monitoring & Detection	Does the organisation Configure access for all accounts through			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
	(DE.CM):	as few centralized points of authentication as possible, including network, security, and cloud systems.			
15	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Configure devices to not auto-run content from removable media.			
16	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.			
17	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.			
18	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.			
19	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.			
20	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Create a test bed that mimics a production environment 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			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		other control systems.			
21	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.			
22	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Deliver training to address the skills gap identified to positively impact workforce members' security behaviour.			
23	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,.			
24	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.			
25	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.			
26	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Disable any account that cannot be associated with a business process or business owner.			
27	Security Continuous Monitoring & Detection	Does the organisation Disable wireless access on devices that do			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
	(DE.CM):	not have a business purpose for wireless access.			
28	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.			
29	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			
30	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Encrypt all sensitive information in transit.			
31	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.			
32	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.			
33	Security Continuous Monitoring & Detection	Does the organisation Ensure that all accounts have an expiration			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
	(DE.CM):	date that is monitored and enforced.			
34	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.			
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.			
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.			
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 of the browsers and email clients provided by the vendor.			
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.			
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.			
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,			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		client-based, and web application attacks.			
41	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Establish secure coding practices appropriate to the programming language and development environment being used.			
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.			
43	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.			
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.			
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.			
46	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.			
47	Security Continuous Monitoring & Detection	Does the organisation Log all URL requests from each of the			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
	(DE.CM):	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.			
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.			
49	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Maintain an inventory of authorized wireless access points connected to the wired network.			
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.			
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.			
52	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Manage all network devices using multi-factor authentication and encrypted sessions.			
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.			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
54	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Monitor attempts to access deactivated accounts through audit logging.			
55	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation On a regular basis, review logs to identify anomalies or abnormal events.			
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.			
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.			
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.			
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.			
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.			
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			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		communication channels, decision making, and incident responders technical capabilities using tools and data available to them.			
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.			
63	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.			
64	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.			
65	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			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		third-party provider.			
66	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).			
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.			
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.			
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.			
70	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Train workforce members on the importance of enabling and utilizing secure authentication.			
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			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		mobile devices or emailing the wrong person due to autocomplete in email.			
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.			
73	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Uninstall or disable any unauthorized browser or email client plugins or add-on applications.			
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.			
75	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 even when data is copied off a system.			
76	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Use DNS filtering services to help block access to known malicious domains.			
77	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Use only standardized and extensively reviewed encryption algorithms.			
78	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation Use sandboxing to analyse and block inbound email attachments with malicious behaviour.			
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			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		focus penetration testing efforts.			
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.			
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.			
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.			
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.			
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?			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
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?			
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?			
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?			
88	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation conduct periodic tests for all the critical application, server, network devices and data bases?			
89	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation implement a process to communicate vulnerabilities to vendors?			
90	Security Continuous Monitoring & Detection (DE.CM):	Does the organisation maintain tracker for closure and corrective action of VAPT?			
91	Security Continuous Monitoring & Detection (DE.CM):	Whether a policy to ensure high availability and timely detection of attacks is defined and implemented ?			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
92	Security Continuous Monitoring & Detection (DE.CM):	Whether vulnerability assessment and penetration testing procedure and calendar are defined ?			
93	Detection Processes (DE.DP):	Are roles and responsibilities for detection well defined to ensure accountability?			
94	Detection Processes (DE.DP):	Do detection activities comply with all applicable requirements?			
95	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?			
96	Asset Management (ID.AM)	Does the Organisation use client certificates to authenticate hardware assets connecting to the organization's trusted network.			
97	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 asset inventory data to ensure only authorized devices can connect to the network.			
98	Asset Management (ID.AM)	Does the organization identify critical assets based on their sensitivity?			
99	Asset Management (ID.AM)	Does the organization maintain an up-to-date inventory of its hardware, software, information assets, details of network			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		resources and also maintain records of those personnel who are issued such assets?			
100	Asset Management (ID.AM)	Has organization maintained an up-to-date centralised inventory of authorised software/applications/libraries, etc. ?			
101	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?			
102	Asset Management (ID.AM)	Has the organization put in place appropriate environmental controls for securing location of critical assets providing protection from natural threats?			
103	Asset Management (ID.AM)	Has the organization put in place mechanism for monitoring any potential compromises or breach to environmental controls?			
104	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?			
105	Business Environment (ID.BE)	Are Priorities for organizational mission, objectives, and activities are established and communicated?			
106	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)			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
107	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?			
108	Business Environment (ID.BE)	Has the organization maintained up-to-date network architecture diagram at the organization level including wired/wireless networks?			
109	Governance (ID.GV)	Does Cyber Security Policy include process of recovering from incidents through incident management & other appropriate recovery mechanisms?			
110	Governance (ID.GV)	Does Cyber Security Policy include process on detecting incidents, anomalies and attacks via appropriate monitoring tools/process?			
111	Governance (ID.GV)	Does Cyber Security Policy include process on protecting assets by deploying suitable controls, tools & measures?			
112	Governance (ID.GV)	Does Cyber Security Policy include process on responding after identification of the incident, anomaly or attack?			
113	Governance (ID.GV)	Does the organization that implements any operation/process/monetary transactions through API follow best practices from international standards like ISO 27001, COBIT 5, etc? Are such practices periodically reviewed?			
114	Governance (ID.GV)	How are cybersecurity roles and responsibilities coordinated and aligned with internal roles and external partners?			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
115	Governance (ID.GV)	Is there a Cyber crisis management plan available ?			
116	Governance (ID.GV)	Is there a SOC setup available which ensures continuous surveillance ?			
117	Governance (ID.GV)	What are the reporting procedures have been taken to facilitate communication of unusual activities with designated Cyber Security officer ?			
118	Governance (ID.GV)	Whether a comprehensive Cyber Security Policy is in place ?			
119	Governance (ID.GV)	Whether a cyber risk management policy is available ?			
120	Governance (ID.GV)	Whether Business Continuity Plan and Disaster Recovery Plan is in place ?			
121	Governance (ID.GV)	Whether IT architecture has been reviewed by the IT Sub Committee of the board ?			
122	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 ?			
123	Governance (ID.GV)	For Cloud and Mobile deployment has the insurer considered the guidelines issued by IRDA relating to Cloud, Mobile Security and related areas. Please refer Annexure for the guidelines			
123	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?			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
124	Risk Assessment (ID.RA)	Does the organization periodically assess whether all the network devices are configured appropriately to the desired level of network security?			
125	Risk Assessment (ID.RA)	How are risk responses identified and prioritized?			
126	Risk Assessment (ID.RA)	How are threats from both internal and external parties identified and documented?			
127	Risk Management (ID.RM)	Are Risk management processes are established and how are they managed, and agreed to by organizational stakeholders?			
128	Risk Management (ID.RM)	Is Organizational risk tolerance is determined and clearly expressed?			
129	Supply Chain Risk Management (ID.SC)	Does vendors adhere to the applicable guidelines in the Cyber Security policy? Does the organization obtains the necessary self-certifications from them to ensure compliance with the policy guidelines?			
130	Supply Chain Risk Management (ID.SC)	Has the vendors implemented information security policies and have appropriate framework?			
131	Supply Chain Risk Management (ID.SC)	Vendors agreement documents are maintained and updated ?			
132	Supply Chain Risk Management (ID.SC)	Are there process for monitoring third - party access to protected or sensitive information?			
133	Identity Management, Authentication and Access Control (PR.AC):	Are logs of users' access to critical systems and activities performed on critical systems stored in a secured location at least for 2 years?			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
134	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?			
135	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.)?			
136	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?			
137	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?			
138	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?			
139	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?			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
140	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?			
141	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?			
142	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 ?			
143	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?			
144	Identity Management, Authentication and Access Control (PR.AC):	Has the organization implemented controls to minimize invalid login counts, deactivate dormant accounts?			
145	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			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		?			
146	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?			
147	Awareness and Training (PR.AT):	Are the history and versions of training content maintained?			
148	Awareness and Training (PR.AT):	Are the targeted awareness/training for key personnel conducted periodically?			
149	Awareness and Training (PR.AT):	Are the training programs reviewed and updated periodically?			
150	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.			
151	Awareness and Training (PR.AT):	How do users indicate that they understand their responsibilities?			
152	Awareness and Training (PR.AT):	Is awareness level evaluated periodically?			
153	Awareness and Training (PR.AT):	Is there additional training for leaders to understand their roles in the event of a security incident?			
154	Awareness and Training (PR.AT):	Is there a process to handle if a users does not complete the training?			
155	Awareness and Training (PR.AT):	Is someone responsible for creating the security training for the organization?			
156	Data Security (PR.DS):	Are open ports on network and systems which are not in use			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		blocked ?			
157	Data Security (PR.DS):	Can the application be set to automatically log a user off the application after a predefined period of inactivity?			
158	Data Security (PR.DS):	Can the application force password expiration and prevent users from reusing a password?			
159	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.?			
160	Data Security (PR.DS):	Does the application force "new" users to change their password upon first login into the application?			
161	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?			
162	Data Security (PR.DS):	Does the application support integration with the enterprise identity management system?			
163	Data Security (PR.DS):	Does the organization authorize data storage devices within their IT infrastructure through appropriate validation process?			
164	Data Security (PR.DS):	Is there a process by which the organization maintains the evidence of media disposal?			
165	Data Security (PR.DS):	has there been a implementation of a data-disposal and data-retention policy?			
166	Data Security (PR.DS):	Are there processes for media formatting?			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
167	Data Security (PR.DS):	Is there measurement a client system's vulnerabilities?			
168	Data Security (PR.DS):	Is user authentication controlled by means other than user account and password or PIN?			
169	Data Security (PR.DS):	Are various security mechanism used to share the data with third parties?			
170	Data Security (PR.DS):	What are the different technologies implemented for the encryption of data?			
171	Data Security (PR.DS):	Are appropriate technologies implemented for data mobility security?			
172	Information Protection Processes and Procedures (PR.IP):	Are duplicate copies of PC software and documentation maintained off-location?			
173	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.			
174	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?			
175	Information Protection Processes and Procedures (PR.IP):	Are there methods to prevent unauthorized access by other groups into individual files and department-shared files?			
176	Information Protection Processes and Procedures (PR.IP):	Are there procedures for limiting access to LAN and network operating software?			
177	Information Protection Processes and Procedures (PR.IP):	Are updates to the Web site independently reviewed, approved and tested?			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
178	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?			
179	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.?			
180	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.			
181	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?			
182	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.			
183	Information Protection Processes and Procedures (PR.IP):	Does the organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.psl, *.py, macros, etc.) are allowed to run on a system.			
184	Information Protection Processes and Procedures (PR.IP):	Is a periodic inventory taken to verify that the appropriate backup files are being maintained?			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
185	Information Protection Processes and Procedures (PR.IP):	Is appropriate hardware backup available?			
186	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.			
187	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?			
188	Information Protection Processes and Procedures (PR.IP):	Is the use of remote access software restricted?			
189	Information Protection Processes and Procedures (PR.IP):	Is there documentation describing data, programs, hardware, and system requirements?			
190	Information Protection Processes and Procedures (PR.IP):	what policies and procedures have been used to protect critical information at different layers of security?			
191	Maintenance (PR.MA):	Is there a process to determine after how many days of identification, patches would be fixed?			
192	Maintenance (PR.MA):	Are remote maintenance of organizational assets approved, logged, and performed in a manner that prevents unauthorized access?			
193	Maintenance (PR.MA):	Are Defined parameters taken for prioritizing the patches need			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		to be installed?			
194	Maintenance (PR.MA):	How are maintenance and repair of organizational assets are logged whenever performed, with approved and controlled tools?			
195	Maintenance (PR.MA):	Is there a process to deploy critical patches in a test environment?			
196	Maintenance (PR.MA):	Are the approved patch management policy have been implemented?			
197	Maintenance (PR.MA):	Have perimeters been defined for classifying patches?			
198	Protective Technology (PR.PT):	Are adequate measures taken to isolate and secure the perimeter and connectivity of the servers running monetary transactions applications/process?			
199	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?			
200	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?			
201	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			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		spoofing, identical mail domains, protection of attachments, malicious links etc.?			
202	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?			
203	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?			
204	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?			
205	Communications (RC.CO):	How are recovery activities are communicated to internal and external stakeholders as well as executive and management team?			
206	Improvements (RC.IM):	Are recovery strategies updated periodically?			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
207	Improvements (RC.IM):	Does recovery plans incorporate lessons learned?			
208	Recovery Planning (RC.RP):	How is recovery plan is executed during or after a cybersecurity incident?			
209	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)			
210	Analysis (RS.AN)	Does the organisation have a process to ensure that impact of an incident analysed?			
211	Analysis (RS.AN)	Does the organisation have a process to ensure that Notifications from detection systems are investigated ?			
212	Analysis (RS.AN)	Does the organisation have a process to ensure that often forensics are performed?			
213	Communications (RS.CO):	Are all the cyber attacks related incidents captured and logged?			
214	Communications (RS.CO):	Are the cyber related incident reported to higher authority on periodic basis?			
215	Communications (RS.CO):	Are third parties contractually required to protect the information that is shared with them as part of an incident?			
216	Improvements (RS.IM):	Are Response strategies are updated periodically?			
217	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.			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
218	Improvements (RS.IM):	Are top management sensitised on various technological developments and cyber security related developments periodically?			
219	Improvements (RS.IM):	How are lessons learned captured and shared?			
220	Mitigation (RS.MI):	Has the organization defined the incident management response procedure ?			
221	Mitigation (RS.MI):	Are newly identified vulnerabilities are mitigated or documented as accepted risks?			
222	Mitigation (RS.MI):	What are the corrective action procedure for all the vulnerabilities identified in VAPT?			
223	Response Planning (RS.RP):	Are the plans tested quarterly to include management and recovering from backups?			
224	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.			
225	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.			
226	Response Planning (RS.RP):	Does the organisation Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		system.			
227	Response Planning (RS.RP):	Does the organisation Install the latest stable version of any security-related updates on all network devices.			
228	Response Planning (RS.RP):	Does the organisation Maintain standard, documented security configuration standards for all authorized network devices.			
229	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.			
230	Response Planning (RS.RP):	Has the business impact analysis conducted?			
231	Response Planning (RS.RP):	Has the organization defined the business continuity plan and procedure?			
232	Response Planning (RS.RP):	Has the organization ensured that RPO(Recovery point objective) and RTO (Recovery point objective) are inline with the policy?			
233	Response Planning (RS.RP):	How are the incidents responded and analysed?			
234	Response Planning (RS.RP):	How are the security incidents analysed and corrective actions implemented for continual improvement ?			
235	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?			
236	Response Planning (RS.RP):	Is there an incident response / crisis team with clearly defined roles and responsibilities?			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
237	Work From Remote Location (WFRL)	Does the Board approved Cyber Security Policy (Policy) of the Insurer address risks associated with Work From Remote Location (WFRL) risks?			
238	Work From Remote Location (WFRL)	Does the Policy confirms use of secure network with strong protocols and Wi-Fi passwords at remote location?			
239	Work From Remote Location (WFRL)	Does it mandates passwords change periodically?			
240	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?			
241	Work From Remote Location (WFRL)	Are servers, applications and networks hardened and secured as per standardized security policy settings?			
242	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?			
243	Work From Remote Location (WFRL)	Are user systems enabled with Antivirus, Endpoint protection controls, data encryption and Data Loss Prevention mechanisms?			
244	Work From Remote Location (WFRL)	Does these controls pervade across all the users from all functions			
245	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)			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
246	Work From Remote Location (WFRL)	Are workflow approvals, deviations or exceptions captured as per Change Management Procedures.			
247	Work From Remote Location (WFRL)	Are secure remote access mechanisms of Virtual Private Netowrk (VPN), Internet Proxy or Virtual Device Interface (VDI) provisioned for WFRL users accessing organizational data assets and applications?			
248	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?			
249	Work From Remote Location (WFRL)	Are user systems enabled with Antivirus, Endpoint protection controls, data encryption and Data Loss Prevention mechanisms?			
250	Work From Remote Location (WFRL)	Are users provided with assets authorized by the Insurer which are hardened as per the Insurers security policy settings for strong password authentication?			
251	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?			
252	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?			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
253	Work From Remote Location (WFRL)	Are users mandated to back-up critical data periodically (Policy shall mandate periodicity) on secure location in organization systems?			
254	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?			
255	Work From Remote Location (WFRL)	Are users provided with assets authorized by the Insurer and are hardened as per security policy settings and strong password authentication?			
256	Work From Remote Location (WFRL)	Is there an audit of Privileged user identity access authentication taken for administrative purposes?			
257	Work From Remote Location (WFRL)	Is there an Audit of security information and events monitoring of audit logs analysis and incident response in place?			
258	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?			
259	Work From Remote Location (WFRL)	Are email services secured to prevent spam, spoofed mails and malware filtering?			
260	Work From Remote Location (WFRL)	Are users trained to handle spam, phishing scam and fraudulent			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		emails?			
261	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?			
262	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?			
263	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)			
264	Work From Remote Location (WFRL)	Are user systems enabled with Antivirus, Endpoint protection controls, data encryption and Data Loss Prevention mechanisms?			
265	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?			
266	Work From Remote Location (WFRL)	Are evidences and artefacts classified, securely demonstrated to concerned stakeholders and not shared out of authorized domains?			
267	Work From Remote Location (WFRL)	Are project implementation documents, MIS reports classified and shared on Need-to-know basis?			
268	Work From Remote Location (WFRL)	Are plans and procedures set in place by the organization for			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		Cybersecurity incident response and Crisis management activities?			
269	Work From Remote Location (WFRL)	Is Cyber Security Project management performed remotely?			
270	Work From Remote Location (WFRL)	Confirm whether there are hardening procedures to check / scan systems brought back to Office?			
271	Work From Remote Location (WFRL)	Confirm whether if all patches, AV, End Point Protection, Data Encryption mechanisms are checked to ensure its appropriate functioning?			
272	Work From Remote Location (WFRL)	Are user systems and organization ICT infrastructure systems regularly updated with security patches and fixes?			
273	Work From Remote Location (WFRL)	Are user systems enabled with Antivirus, Endpoint protection controls, data encryption and Data Loss Prevention mechanisms?			
274	Work From Remote Location (WFRL)	Is the security event audit log monitoring and analysis provisioned on Insurers ICT infrastructure?			
275	Work From Remote Location (WFRL)	Are security patch updates reviewed and periodically applied on ICT infrastructure to prevent Distributed Denial of Services(DDoS) attacks?			
276	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?			
277	Work From Remote Location (WFRL)	Is backups reviewed periodically and procedures aligned to minimize downtime impact?			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
278	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)			
279	Work From Remote Location (WFRL)	Is data restoration testing performed on periodic basis to ensure integrity of backups?			
280	Work From Remote Location (WFRL)	Are alternative site options and resource availability planned as a part of Business Continuity and tested for same?			
281	Work From Remote Location (WFRL)	Are Secondary Network Connectivity and IT infrastructure is provisioned and tested for the critical applications and services?			
282	Work From Remote Location (WFRL)	Is it possible to systems without user authentication or by-passing authentication? (Auditor shall specifically confirm that that users cannot bypass security)			
283	Work From Remote Location (WFRL)	Are applications accessible ONLY to authorised users through a secured VPN access?			
284	Work From Remote Location (WFRL)	Are users authenticated and authorised by a domain policy server?			
285	Work From Remote Location (WFRL)	Are Logs of application IT infrastructure are collected and analysed by 24X7 Security Operation Centre (SOC) team?			
286	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			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		monitored by Security Operations Centre (SOC)?			
287	Work From Remote Location (WFRL)	Are Enterprise wide monitoring of Information security incidents done by SOC team on 24X7 basis?			
288	Work From Remote Location (WFRL)	Are ICT infrastructure logs maintained as per regulatory guidelines?			
289	Work From Remote Location (WFRL)	Are Installation of unapproved software and utilities barred by centrally enforced policy?			
290	Work From Remote Location (WFRL)	Are users using only Organization approved collaboration software?			
291	Work From Remote Location (WFRL)	Is there a preventive control to block Unauthorized Collaboration tools on the firewall/network security devices?			
292	Work From Remote Location (WFRL)	Are Cybersecurity awareness circulars and advisories regularly sent to employees, third party vendor and consultants.			
293	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?			
294	Work From Remote Location (WFRL)	Are all agreements/documents with third parties digitally signed using a special tool?			
295	Work From Remote Location - Investment (WFRL.IN)	Are Recorded lines working and and well-maintained condition?			
296	Work From Remote Location - Investment (WFRL.IN)	Does Mid-office check voice recording as per a defined process in Standard Operating Procedure (SOP)?			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
297	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.			
298	Work From Remote Location - Investment (WFRL.IN)	Is Voice logger used for recording of calls made from office location?			
299	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?			
300	Work From Remote Location - Investment (WFRL.IN)	Does the SOP define process to handle disruption in communication links between the dealers and brokers?			
301	Work From Remote Location - Investment (WFRL.IN)	Are such communications logged /recorded?			
302	Work From Remote Location - Investment (WFRL.IN)	Does the Mid-Office independently review these logs / records ?			
303	Work From Remote Location - Investment (WFRL.IN)	Are appropriate prior approvals / authorisations taken to process such transactions?			
304	Work From Remote Location - Investment (WFRL.IN)	Do Dealers execute ALL transactions only through recorded telephone lines?			
305	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?			
306	Work From Remote Location - Investment (WFRL.IN)	Confirm that Bloomberg terminals are accessible through multi factor authentication and are disabled for SMS / Chat facilities.			
307	Work From Remote Location - Investment	In the event of disruption of communication link, are there			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
	(WFRL.IN)	defined policies / processes to guide the officials of the Investments Function to process transactions with appropriate approvals?			
308	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			
309	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?			
310	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?			
311	Work From Remote Location - Investment (WFRL.IN)	Are Contingency policy and plans, revised and tested periodically for an effective business continuity?			
312	Work From Remote Location - Investment (WFRL.IN)	Is Secondary network connectivity and IT infrastructure provisioned and tested for the critical applications and services? Check for are any SPoFs - Single Point of Failure			
313	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?			
314	Work From Remote Location - Investment	Is IT support accessed by Investment application users by way of			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
	(WFRL.IN)	portal, helpdesk or visit to office.			
315	Work From Remote Location - Investment (WFRL.IN)	Are Backup/Alternative locations and resources are identified within Investment function to ensure business continuity?			
316	Work From Remote Location - Investment (WFRL.IN)	Is Email facility enabled with empanelled broker, counter parties, custodian etc.			
317	Work From Remote Location - Investment (WFRL.IN)	Are Emails shared ONLY through authorized company email addresses registered with concerned counterparties?			
318	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?			
319	Work From Remote Location - Investment (WFRL.IN)	Is there a supervisory monitoring process check list which includes transaction price monitoring and trade monitoring etc.?			
320	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?			
321	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;			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		(ii) is defamatory, obscene, pornographic, paedopholic, 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;			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		(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;			
322	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			
323	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			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		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:			
324	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			
325	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;			
326	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			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		and Sensitive Personal Information) Rules, 2011			
327	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 the 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:			
328	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.			
329	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			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
		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			
330	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 anddispose offsuch 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.			
331	Information Technology (Intermediary Guidelines and Digital Media Ethics	Has the intermediary, within twenty-four hours from the receipt of a complaint made by			

No	Area	Audit Questionnaire	Auditors Observation		
			Y	N	Comments
	Code) Rules, 2021 (IGDM)	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:			
332	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			