The checklist is prepared as per Best practice followed in IT Audit.

The PDF covers checkpoints related to Working From a Remote Location (WFRL).

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

Area	Audit Questionnaire	Auditor remarks
Work From Remote Location (WFRL)	Does the Board approved Cyber Security Policy (Policy) of Regulated entity address risks associated with Work From RemoteLocation (WFRL) risks?	
Work From Remote Location (WFRL)	Does the Policy confirms use of secure network with strong protocols and Wi-Fi passwords at remote location?	
Work From Remote Location (WFRL)	Does it mandates passwords change periodically?	
Work From Remote Location (WFRL)	Are users provided with authorized assets of the organization which are hardened as per security policy for strong passwordauthentication?	
Work From Remote Location (WFRL)	Are servers, applications and networks hardened and secured as per standardized security policy settings?	
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?	
Work From Remote Location (WFRL)	Are user systems enabled with Antivirus, Endpoint protection controls, data encryption and Data Loss Prevention mechanisms?	
Work From Remote Location (WFRL)	Does these controls pervade across all the users from all functions	
Work From Remote Location (WFRL)	Are user systems and organization ICT infrastructure regularly updated with security patches and fixes. (Auditor to mention thelatest update date)	
Work From Remote Location (WFRL)	Are workflow approvals, deviations or exceptions captured as per Change Management Procedures.	

Area	Audit Questionnaire	Auditor remarks
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?	
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?	
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?	
Work From Remote Location (WFRL)	Does the policy, spell controls and procedures related to secureaccess of organizational data assets and applications from user-owned devices like mobile phones, tablets or other Bring Your Own Device (BYOD) of the Insurer?	
Work From Remote Location (WFRL)	Do data containerization, Multifactor authentication and remote data wipe have been done to prevent data tampering and misuseof lost mobile/tablet devices during the period when WFRL has been permitted by the Insurer?	
Work From Remote Location (WFRL)	Are users mandated to back-up critical data periodically (Policy shall mandate periodicity) on secure location in organization systems?	
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?	

Area	Audit Questionnaire	Auditor remarks
Work From Remote Location (WFRL)	Are users provided with assets authorized by the Insurer and arehardened as per security policy settings and strong password authentication?	
Work From Remote Location (WFRL)	Is there an audit of privileged user identity access authentication taken for administrative purposes?	
Work From Remote Location (WFRL)	Is there an audit of security information and events monitoring of audit logs analysis and incident response in place?	
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 tool kits and such cyber risks to organizational ICT infrastructure?	
Work From Remote Location (WFRL)	Are email services secured to prevent spam, spoofed mails and malware filtering?	
Work From Remote Location (WFRL)	Are users trained to handle spam, phishing scam and fraudulent emails?	
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?	
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?	
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)	

Area	Audit Questionnaire	Auditor remarks
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?	
Work From Remote Location (WFRL)	Are evidences and artefacts classified, securely demonstrated to concerned stakeholders and not shared out of authorized domains?	
Work From Remote Location (WFRL)	Are project implementation documents, MIS reports classified and shared on need-to-know basis?	
Work From Remote Location (WFRL)	Are plans and procedures set in place by the organization for cybersecurity incident response and crisis management activities?	
Work From Remote Location (WFRL)	Is Cyber Security Project management performed remotely?	
Work From Remote Location (WFRL)	Confirm whether there are hardening procedures to check / scan systems brought back to Office?	
Work From Remote Location (WFRL)	Confirm whether if all patches, AV, End Point Protection, Data Encryption mechanisms are checked to ensure its appropriate functioning?	
Work From Remote Location (WFRL)	Are user systems and organization ICT infrastructure systems regularly updated with security patches and fixes?	
Work From Remote Location (WFRL)	Is the security event audit log monitoring and analysis provisioned on Insurers ICT infrastructure?	
Work From Remote Location (WFRL)	Are security patch updates reviewed and periodically applied on ICT infrastructure to prevent Distributed Denial of Services(DDoS) attacks?	

Area	Audit Questionnaire	Auditor remarks
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?	
Work From Remote Location (WFRL)	Are backups reviewed periodically and procedures aligned to minimize downtime impact?	
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)	
Work From Remote Location (WFRL)	Is data restoration testing performed on periodic basis to ensure integrity of backups?	
Work From Remote Location (WFRL)	Are alternative site options and resource availability planned as a part of Business Continuity and tested for same?	
Work From Remote Location (WFRL)	Are Secondary Network Connectivity and IT infrastructure is provisioned and tested for the critical applications and services?	
Work From Remote Location (WFRL)	Is it possible to access systems without user authentication or by-passing authentication? (Auditor shall specifically confirm that users cannot bypass security)	
Work From Remote Location (WFRL)	Are applications accessible ONLY to authorised users through a secured VPN or VDI access?	
Work From Remote Location (WFRL)	Are users authenticated and authorized by a domain policy server?	
Work From Remote Location (WFRL)	Are Logs of application IT infrastructure are collected and analysed by 24X7 Security Operation Centre (SOC) team?	

Area	Audit Questionnaire	Auditor remarks
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)?	
Work From Remote Location (WFRL)	Are Enterprise wide monitoring of Information security incidents done by SOC team on 24X7 basis?	
Work From Remote Location (WFRL)	Are ICT infrastructure logs maintained as per regulatory guidelines?	
Work From Remote Location (WFRL)	Are Installation of unapproved software and utilities barred by centrally enforced policy?	
Work From Remote Location (WFRL)	Are users using only organization approved collaboration software?	
Work From Remote Location (WFRL)	Is there a preventive control to block unauthorized collaboration tools on the firewall / network security devices?	
Work From Remote Location (WFRL)	Are cybersecurity awareness circulars and advisories regularly sent to employees, third party vendor and consultants.	
Work From Remote Location (WFRL)	Does the organization has a dealing room policy and Standard operating policy to supervise controls over the dealing activitiesduring WFRL?	
Work From Remote Location (WFRL)	Are all agreements / documents with third parties digitally signed using a special tool?	
Work From Remote Location (WFRL)	Is voice logger used for recording of calls made from office location?	

Area	Audit Questionnaire	Auditor remarks
Work From Remote Location (WFRL)	Is Back up / storage of call recordings enabled as a part of proof of transaction that can be accessed anytime?	
Work From Remote Location (WFRL)	Are such communications logged / recorded?	
Work From Remote Location (WFRL)	Are appropriate prior approvals / authorisations taken to process such transactions?	
Work From Remote Location (WFRL)	Do Dealers execute ALL transactions only through recorded telephone lines?	
Work From Remote Location (WFRL)	Are Contingency policy and plans, revised and tested periodically for an effective business continuity?	
Work From Remote Location (WFRL)	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	
Work From Remote Location (WFRL)	Are Disaster Recovery (DR) Drills performed to verify the availability of applications, processes and resources at remotebackup site. Are issues identified during DR testing addressed?	
Work From Remote Location (WFRL)	Is IT support accessed by Investment application users by way of portal, helpdesk or visit to office.	
Work From Remote Location (WFRL)	Are Backup / Alternative locations and resources identified within Investment function to ensure business continuity?	
Work From Remote Location (WFRL)	Is Email facility enabled with empanelled counter parties.	

Area	Audit Questionnaire	Auditor remarks
Work From Remote Location (WFRL)	Are Emails shared ONLY through authorized company email addresses registered with concerned counterparties?	

IF YOU FIND THIS USEFUL , SHARE WITH YOUR NETWORK.

FOLLOW FOR MORE SUCH CHECKLIST | TEMPLATE | IT AUDIT RELATED STUFF

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

https://youtube.com/@sachinhissaria6512