



Systems Audit Report: 2025-26



Redacted Ltd.

Head Office: Green Heights Apartment, MG Road, Andheri East,
Mumbai, Maharashtra, 400069.

Systems Audit of Bank's IT infrastructure as per RBI Cybersecurity Framework for UCB's

Date of Report: 2nd May 2026

Audit Conducted By:

Mr. Vivek Gupta

Mr. Krishna J ISO 27001 LA, CCNA, CCSA

Reviewed By

Mr. Lalit Vazirani ISO 27001 LA, ISO 22301

Website: www.darknext.com

M/s DarkNext LLP,

RIIDL, K.J. Somaiya Institute of

Technology Sion East, Mumbai 400022

Table of Contents

1. Revision History.....2

2. Details of Auditor.....3

3. References:.....3

4. Introduction.....4

5. Scope.....5

6. Summary of Findings.....6

7. Detailed Audit findings.....7

Revision History:

Document Control	Revision History	Date
V1.0	Initial Release	2 nd May 2026

Details of Auditor:

Bank	Redacted Ltd
Audit	Systems Audit of Bank's IT infrastructure as per RBI Cybersecurity Framework for UCB's
Auditor	Mr. Vivek Gupta
Audit dates	2 nd Feb 2026 to 25 th April 2026
Report Date	2 nd May 2026

References:

1. Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) - RBI Circular dated 19-10-2018.
2. Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) - A Graded Approach - RBI Circular dated 31-12-2019.
3. Compliance of Cyber Security Framework - Restriction on outward RTGS/NEFT/IMPS transactions - RBI Circular dated 09-01-2023.
4. Bank Policies: -
Cyber Security Policy v1.5 dated 20th May 2023

Introduction:

Redacted Ltd DarkNext to conduct an IS Audit of their Bank's IT infrastructure as per the RBI Cybersecurity Framework for UCB's. Redacted Ltd is a Level 3 Cooperative Bank in terms of their size and complexity, outlining mandatory cybersecurity measures. The Bank currently has 13 branches. It offers facilities like Lockers, Savings and Current Accounts, Fixed Deposits, Loans, Insurance, E-Banking, RTGS/NEFT. It is a member of the Centralized Payment Systems (CPS), but does not have any ATMs. The bank also does not offer SWIFT services or has a SWIFT interface implemented as of the date of the audit.

The Audit team has used the checklist, based on RBI guidelines for Cyber Security Framework, with the amendments to Regulations and Rules, Guidelines till date, general IS Audit practices and the Policies, Guidelines & Procedures prescribed the Bank for its operations.

The audit encompasses the checklist prepared, interviews with personnel, observations, and simulations of certain scenarios. The objective of the audit is to verify compliance and to safeguard the interests of the Bank in connection with implementation of various technologies and related guidelines.

Our observations are based on the situation prevailing at the time of Audit. The projection of any conclusions, based on our findings, to future periods is subject to the risk that:

- Changes may have been made to the system or controls.
- Changes may have been made in processing requirements.
- Changes may have been made as required due to the passage of time, or
- Degree of compliance with the policies or procedures.
- May have altered the validity of such conclusions.

Scope:

The Reserve Bank of India's (RBI) Level 3 cyber security framework for urban cooperative banks (UCBs) includes requirements for network management & security, secure configuration, application security life cycle, user access controls, advanced real time threat defense and management, maintenance, monitoring and analysis of audit logs to protect customer data and systems from cyber threats.

Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) broad scope includes:

Level III Requirements (Annexure III)

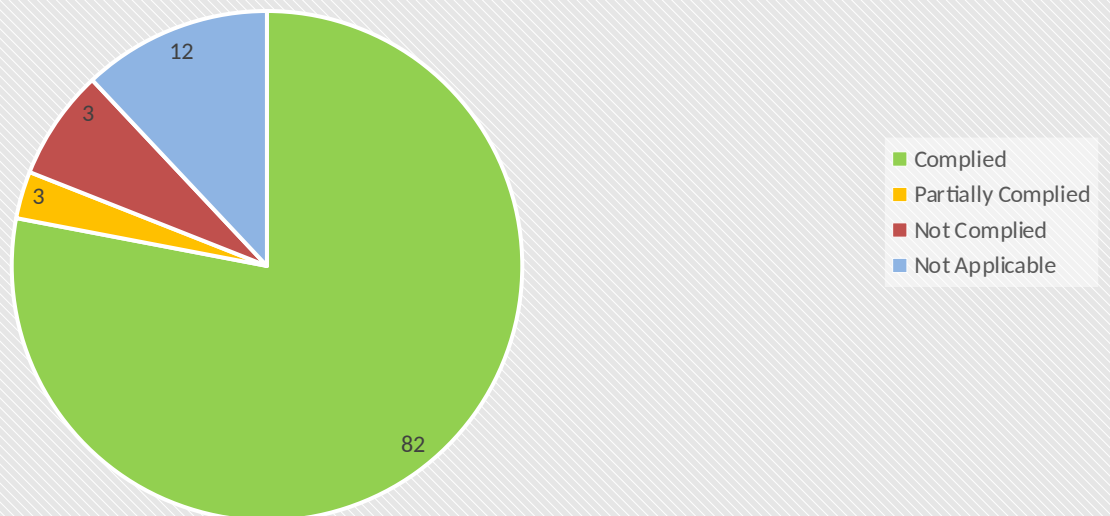
- Network Management & security
- Secure Configuration
- Application Security Life cycle
- User Access controls
- Advanced Real Time Threat Defense & Management
- Maintenance, Monitoring & Analysis of audit logs
- Incident Response & Management
- User/Employee/Management Awareness
- Risk Based Transaction Monitoring

Summary of Findings:

Control Compliance Status:

Sr.	Risk Category Description	No. of Observations
01	Complied	82
02	Partially Complied	03
03	Not Complied	03
04	Not Applicable	12
	Total	100

No. of Observations





Comprehensive Assessment of Compliance with Graded Cyber Security Framework



Detailed Audit findings:

SL. No	Control Point	Observations	Complied Yes / No	Suggestion
Compliance with circular no. RBI/2018-19/63 DCBS.CO.PCB. Cir.Not Complied. 1/18.01.000/2018-19 dated October 19, 2018 - Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs)				
1.	4.0 All UCBs should immediately put in place a Cyber Security policy, duly approved by them Board/Administrator, giving a framework and the strategy containing a suitable approach to check cyber threats depending on the level of complexity of business and acceptable levels of risk. On completion of the process of policy formulation by the Board, a confirmation shall be sent to Department of Cooperative Bank Supervision, Central Office, C-9, 1st Floor, BKC, Mumbai – 400051 by email within three months from the date of circular.	A board approved Cyber Security policy version 1.5 dated 1 st June 2023 was in place as required and found adequate.	Complied	
2.	4.1 The Cyber Security Policy should be distinct from the IT/IS policy of the UCB so that it highlights the risks from cyber threats and the measures to address/reduce these risks. While identifying and assessing the inherent risks, UCBs should keep in view the technologies adopted, delivery channels, digital products being offered, internal and external threats etc., and rate each of these risks as Low, Medium, High and Very High.	The Cybersecurity policy is distinct from the IS policies and highlights the risks from cyberthreats and measures to address/reduce these threats. A documented Risk Assessment Sheet highlighting the threats, vulnerabilities and risks is maintained, however it was not reviewed in the FY 25 – 26. (This Observation was rectified During Audit)	Complied	.



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



3.	4.2. IT Architecture/Framework should be security compliant. The IT architecture/ framework which includes network, server, database and application, end user systems, etc., should take care of security measures at all times and this should be reviewed by the Board or IT Sub-committee of the Board periodically. For this purpose, UCBs may carry out the following steps: -Identify weak/vulnerable areas in IT systems and processes, -Allow restricted access to networks, databases and applications wherever permitted, through well-defined processes and approvals including rationale for permitting such access, -Assess the cost of impact in case of breaches/failures in these areas and, -Put in place suitable Cyber Security System to address them, -Specify and document clearly the responsibility for each of above steps. -A proper record should be kept of the entire process to enable supervisory assessment.	There is no documented IT architecture/ framework. However, there is a documented Network diagram, and contractual agreements and SLAs with 3rd parties who manage the Core Banking System, SOC, Data Centers etc. The bank has a flat network, with each branch having its own segment, and a firewall providing network isolation. The Primary and Secondary Data Centers are hosted with a 3rd party, namely ESDS in Airoli (Navi Mumbai) and Nashik respectively (This Observation was rectified During Audit)	Complied	.
----	--	---	-----------------	---



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



4.	5. Organizational Arrangements: - UCBs should review the organizational arrangements so that the security concerns are brought to the notice of suitable/concerned officials to enable quick action.	Periodic employee IS Awareness through classroom sessions, emails and banners ensures security concerns or incidents are brought to the notice of suitable/concerned officials	Complied	
5.	6. Cyber Security awareness among Top Management/Board/other concerned parties: Managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This will require a high level of awareness/familiarization among staff at all levels including Board and Top Management. UCBs should actively promote among their customers, vendors, service providers and other concerned parties an understanding of its cyber security objectives. Security awareness among customers, employees, vendors, service providers, etc. about the potential impact of cyber-attacks helps in cyber security preparedness of UCBs.	Cyber Security awareness has been conducted by the Bank among employees, management, Vendors, Service Providers and customers. We have evidenced the last classroom awareness session training certificate which was conducted on 18 th March 2024 by Pheonix Techno Cyber. Phishing Awareness Campaign was last conducted by the Bank in April 2025 to all 179 email ids of the bank. Prior campaign was run on 8 th May 2024	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



6.	7. Ensuring protection of customer information UCBs, as owners of customer sensitive data, should take appropriate steps in preserving the Confidentiality, Integrity and Availability of the same, irrespective of whether the data is stored/in transit within themselves or with the third-party vendors; the confidentiality of such custodial information should not be compromised in any situation. To achieve this, suitable systems and processes across the data/information lifecycle need to be put in place by UCBs. As regards customers, UCBs may educate and create awareness among them with regard to cyber security risks.	Sufficient safeguards as stipulated by RBI's basic Cybersecurity framework is in place to protect customer information. The bank has displayed awareness posters in the branch as well as on the website to help create customer awareness.	Complied	
----	---	---	-----------------	--



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



SL. No.	Control Point	Observations	Complied Yes / No	Suggestion
7.	8. Supervisory reporting framework: UCBs should report immediately all unusual cyber security incidents (whether they were successful or mere attempts) to Department of Co-operative Bank Supervision, Central Office, C-9, 1st Floor, BKC, Mumbai – 400051 by email, giving full details of the incident. A 'NIL' report shall be submitted on quarterly basis in case of no cyber security incidents.	As mentioned earlier, internet access is not available in Bank network, and hence there have been no incidents so far. Bank has not sent "NIL" report on quarterly basis so far. However, the stipulation of sending "NIL" returns is withdrawn vide RBI Circular DoS.CO/CSITE/ BC 4083/ 31.01.052/2019-20 DATED 31/12/2019.	Complied	
Compliance with Level I controls, Additional level I controls and Level II controls				
	1. Inventory management			
8..	1.1 UCBs should maintain an up-to-date business IT Asset Inventory Register containing the following fields, as a minimum: a. Details of the IT Asset (viz., hardware/software/network devices, key personnel, services, etc.) b. Details of systems where customer data are stored c. Associated business applications, if any d. Criticality of the IT asset (For example, High/Medium/Low)	An IT Asset Inventory Register was in place. However, the register was not up to date with latest OS and some end of support operating systems were still installed as per this inventory. (This Observation was rectified During Audit)	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



SL. No.	Control Point	Observations	Complied Yes / No	Suggestion
9..	1.2 Classify data/information based on sensitivity criteria of the information.	Bank has classified information in the Cyber Security Polic v 1.5 dated 1 st June 2024. The data classification is based on the sensitivity criteria into 4 categories. The data is classified based on the severity.	Complied	
10.	1.3 Appropriately manage and provide protection within and outside UCB/network, keeping in mind how the data/information is stored, transmitted, processed, accessed and put to use within/outside the UCB's network, and level of risk they are exposed to depending on the sensitivity of the data/information.	The Bank has outsourced the CBS, SOC and Data Center functions to 3 rd parties, and has implemented adequate protection for bank data, considering the risks they are exposed to. Internet and USB access is blocked down for all users.	Complied	
	2. Preventing access of unauthorized software			
11.	2.1 Maintain an up-to-date and preferably centralized inventory of authorized software(s) / approved applications / software / libraries etc.,	A list of Software is maintained in the IT Authorized Software.pdf file, which was approved by the Board of Directors as on 30 st May 2025	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



SL. No.	Control Point	Observations	Complied Yes / No	Suggestion
12.	2.2 Put in place a mechanism to control installation of software/applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. Also, put in place a mechanism to block/prevent and identify installation and running of unauthorized software/applications on such devices/systems.	Active Directory was in place at the Bank as on the day of audit. Local admin rights were revoked on all the endpoints as on the day of the audit.	Complied	
13.	2.3 The web browser settings should be set to auto update and consider disabling scripts like JavaScript, Java and ActiveX controls when they are not in use.	Web browsers are set to auto update. JavaScript, Java and ActiveX are not disabled, as they are required for some integrations with various applications. However, the exception was not mentioned in the Risk Register. (This Observation was rectified During Audit)	Complied	
	3. Environmental Controls			
14.	3.1 Place appropriate controls for securing physical location of critical assets (as identified by the UCB under its inventory of IT assets), providing protection from natural and man-made threats	Appropriate controls are in place to secure the physical location where critical assets are located. Each branch has security guards and CCTV controls. Data Center is hosted with a leading hosting service provider ESDS which has appropriate physical controls to restrict access to critical IT assets.	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



15.	3.2 Put in place mechanisms for monitoring of breaches/compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access logs, etc. Appropriate physical security measures shall be taken to protect the critical assets of the UCB	Data Center is hosted with a leading hosting service provider, ESDS which has appropriate physical and environmental controls to restrict access to critical IT assets. ESDS monitors the temp, humidity, access logs, etc. to ensure only authorized personnel are able to access the critical assets. However the reports are not shared with the Bank. (This Observation was rectified During Audit)	Complied	1.
	4. Network Management and Security			
16.	4.1 Ensure that all the network devices are configured appropriately and periodically assessed to ensure that such configurations are securely maintained.	Firewall configuration review is performed periodically and was last performed in April 2025 for the Sophos and FortiGate firewalls, however there are open issues identified in the report. As of our audit, these findings have not been remediated. (This Observation was rectified During Audit)	Complied	
17.	4.2 The default passwords of all the network devices/systems should be changed after installation	Default passwords have been changed after installation. However, the Secure configuration document does not mention this check. (This Observation was rectified During Audit)	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



SL. No.	Control Point	Observations	Complied Yes / No	Suggestion
18.	4.3 Put in appropriate controls to secure wireless local area networks, wireless access points, wireless client access systems.	There was no Wi-Fi facility at the bank as on the day of audit. So, this control is not applicable.	Not Applicable	
19.	4.4 Critical infrastructure of UCB (viz., NEFT, RTGS, SWIFT, CBS, ATM infrastructure) should be designed with adequate network separation controls	Adequate network separation is ensured for Critical infrastructure through VLAN's	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



Additional controls as per RBI Circular DoS.CO/CSITE/BC4083/31.01.052/2019-20 DATED 31/12/2019				
20.	1.1. Maintain an up-to-date/centralized inventory of authorized devices connected to UCB's network (within/outside UCB's premises) and related network devices in the UCB's network.	A list of Network devices is maintained and found adequate.	Complied	
21.	1.2. Boundary defenses should be multi-layered with properly configured firewalls, proxies, De-Militarized Zone (DMZ) perimeter networks, and network-based Intrusion Prevention System (IPS)/Intrusion Detection System (IDS). Mechanism to filter both inbound and outbound traffic shall be put in place	Defense in depth is in place. Perimeter Firewall, Internal Firewall, and End Point Protection are in place to give adequate protection against cyber threats. However, DMZ is not in place. (This Observation was rectified During Audit)	Complied	
22.	1.3. LAN segments for in-house/onsite ATM and CBS/branch network should be different.	As mentioned earlier, there is no ATM network, and hence Branch network is the only network. CBS is hosted by a 3 rd party, and is not hosted in house.	Not applicable	
5. Secure Configuration				
23.	5.1 The firewall configurations should be set to the highest security level and evaluation of critical device (such as firewall, network switches, security devices, etc.) configurations should be done periodically.	Firewall configuration review is performed periodically and was last performed in April 2025 for the Sophos and FortiGate firewalls, however there are open issues identified in the Report. As of our audit, these findings have not been remediated (This Observation was rectified During Audit).	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



SL. No.	Control Point	Observations	Complied Yes / No	Suggestion
24.	5.2 Systems such as Network, application, database and servers should be used dedicatedly for the purpose for which they have been set up.	Application Servers, Database Servers and Network systems are used dedicatedly for the purpose for which they have been deployed.	Complied	
Additional controls as per RBI Circular DoS.CO/CSITE/ BC 4083/ 31.01.052/2019-20 DATED 31/12/2019				
25.	2.1 Document and apply baseline security requirements/configurations to all categories of devices (end-points/workstations, mobile devices, operating systems, databases, applications, network devices, security devices, security systems, etc.), throughout the lifecycle (from conception to deployment) and carry out reviews periodically	Baseline security configurations have not been documented. Endpoints are using outdated Win 7, with no security patches. Similarly, there was no baseline defined for the firewalls, email server etc. (This Observation was rectified During Audit)	Complied	
	6. Anti-virus and Patch Management			
26.	6.1 Put in place systems and processes to identify, track, manage and monitor the status of patches to servers, operating system and application software running at the systems used by the UCB officials (end-users).	Patching is done through ESDS patch solution and email is sent after the patching. Periodic VAPT scans check for missing patches. (This Observation was rectified During Audit)	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



27.	6.2 Implement and update antivirus protection for all servers and applicable end points preferably through a centralized system.	Seqrite centralized Anti-Virus is place for all endpoints	Complied	
.	7. User Access Control / Management			
28..	7.1 Disallow administrative rights on end-user workstations/PCs/laptops and provide access rights on a 'need to know' and 'need to do' basis.	Users are given access rights on "need to do" basis through Microsoft Active Directory.	Complied	
29.	7.2 Passwords should be set as complex and lengthy and users should not use same passwords for all the applications/systems/devices.	Complex and lengthy Passwords are in use. This is controlled on all the endpoints and servers by the way of active directory. CBS application has 2 FA enabled via means of OTP on mobile phones.	Complied	
30.	7.3 Remote Desktop Protocol (RDP) which allows others to access the computer remotely over a network or over the internet should be always disabled and should be enabled only with the approval of the authorized officer of the UCB. Logs for such remote access shall be enabled and monitored for suspicious activities	RDP is disabled through Active directory for endpoints. RDP protocol was found to be enabled on the domain controller as per the Network VAPT report dated 25 th April 2025. (This Observation was rectified During Audit)	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



31.	7.3 Implement appropriate (e.g. centralized) systems and controls to allow, manage, log and monitor privileged/super user/administrative access to critical systems (servers/databases, applications, network devices etc.)	Privileged/super user/administrative access Logs are enabled and continuously monitoring for critical systems SOC is also outsourced to Tech OWL.	Complied	
Additional controls as per RBI Circular DoS.CO/CSITE/ BC 4083/ 31.01.052/2019-20 DATED 31/12/2019				
32.	6.1 Provide secure access to the UCB's assets/services from within/outside UCB's network by protecting data/information at rest (e.g. using encryption, if supported by the device) and in-transit (e.g. using technologies such as VPN or other standard secure protocols, etc.)	CBS connectivity from branches to Data Centre is through SD-WAN.	Complied	
8. Secure mail and messaging systems				

SL. No.	Control Point	Observations	Complied Yes / No	Suggestion
33.	8.1 Implement secure mail and messaging systems, including those used by UCB's partners & vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.	Emails spoofing controls are implemented with DMARC set to Reject. All emails are scanned for malware, including password protected files and compressed files.	Complied	
34..	8.2 Document and implement email server specific controls.	Emails are encrypted with TLS and adequate email controls were in place as seen on the day of assessment.	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



	9. Removable Media			
35.	9.1 As a default rule, use of removable devices and media should not be permitted in the banking environment unless specifically authorized for defined use and duration of use.	Removable media are totally blocked through the E-Scan AV solution as verified on the day of assessment.	Complied	
36.	9.2 Secure the usage of removable media on workstations/PCs/Laptops, etc. and secure erasure/ deletion of data on such media after use	Use of removable media is not permitted on PCs in Bank network. This is controlled by the way of the E-Scan Securit AV solution. Only 10 PCs for senior personnel is allowed to use USB drives.	Complied	
37.	9.3 Get the removable media scanned for malware/anti-virus prior to providing read/write access	Removable media are blocked. If and when exemption is given, they are scanned for malware.	Complied	
	10. User/Employee/Management Awareness			
38.	10.1 Communicate to users/employees, vendors & partners security policies covering secure and acceptable use of UCB's network/assets including customer information/data, educating them about cyber security risks and protection measures at their level.	As mentioned earlier, Cyber security awareness programs are held periodically for employees, vendors and customers.	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



SL. No.	Control Point	Observations	Complied Yes / No	Suggestion
39.	10.2 Conduct awareness/training for staff on basic information security controls (Do's and Don'ts), incident reporting, etc.	As mentioned earlier, Awareness/training for staff on basics of information security is carried out.	Complied	
40..	10.3 Board members may be kept updated on basic tenets/principles of IT risk/cyber security risk at least once a year.	Board members are updated on Cyber Security regularly.	Complied	
41.	10.4 The end-users should be made aware to never open or download an email attachment from unknown sources	End users are aware that it is dangerous to open email attachments from unknown sources. Phishing awareness campaign was run in April 2025 to ensure user awareness. Prior campaign was run in May 2024.	Complied	
	11. Customer Education and Awareness			
42.	11.1 Improve and maintain customer awareness and education with regard to cyber security risks	Bank educates customers through SMS, Mobile Banking and other literature such as displays at the branches.	Complied	
43.	11.2 Educate the customers on keeping their card, PIN etc. secure and not to share with any third party	Bank regularly sends SMS and notifications to customers cautioning them to keep their Cards and PINs securely and not to share with others.	Complied	

SL. No.	Control Point	Observations	Complied Yes / No	Suggestion
	12. Backup and Restoration			
44.	12.1 Take periodic back up of the important data and store this data 'off line' (i.e., transferring important files to a storage device that can be detached from a computer/system after copying all the files).	Backup & restoration Policy dated 12 th April 2024, defines the backup frequency as daily incremental and weekly full. backup is taken every day in the primary Data Centre on external HDD and kept in DR as on the day of assessment. Two HDDs are in use for every end of the day.	Complied	
	13. Vendor / Outsourcing Risk Management			
45.	13.1 All the outsourcing service level agreements (SLAs) signed with the vendors must clearly mention the responsibility of the UCB and vendor in case of any failure of services.	Responsibilities of each party to the agreement are clearly mentioned.	Complied	
46.	13.2 The agreements must clearly mention the grievance redressal mechanism to resolve customer complaints	The agreements contain the grievance redressal mechanism to help resolve any disputes. There are also SLA's defined.	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



47.	13.3 Vendors' service level agreements shall be periodically reviewed for performance in security controls	Vendor's service level agreements are reviewed on quarterly periodically as a part of cyber security posture review. (This Observation was rectified During Audit)	Complied	
SL. No.	Control Point	Observations	Complied Yes / No	Suggestion
Additional controls as per RBI Circular DoS.CO/CSITE/ BC 4083/ 31.01.052/2019-20 DATED 31/12/2019				
48.	(vii) UCBs shall be: Accountable for ensuring appropriate management and assurance on security risks in outsourced vendor arrangements. UCBs shall carefully evaluate the need for outsourcing critical processes and selection of vendor/partner based on comprehensive risk assessment. UCBs shall regularly conduct effective due diligence, oversight and management of third-party vendors/service providers and partners.	The Vendors are carefully evaluated before outsourcing to them. Although there is regular interaction with the vendors on a daily basis, there is no evidence of a documented Risk Assessment prior to outsourcing or post award of contract. (This Observation was rectified During Audit)	Complied	
49.	(viii) Required to necessarily enter into agreement with the service provider that, among other things, provides for right to audit by the UCB. The outsourcing agreements should include clauses to recognize the right of the Reserve Bank to cause an inspection to be made of a service provider of the UCB and allow the Reserve Bank of India or persons authorized by it to access the bank's documents, records of transactions, logs and other necessary information given to, stored or processed by the service provider within a	Right to audit clause is documented in the Vendor Agreements and has been agreed by the vendors.	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



reasonable time.



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



SL. No.	Control Point	Observations	Complied Yes / No	Suggestion
50.	(ix) Required to thoroughly satisfy about the credentials of vendor/third-party personnel accessing and managing the UCB's critical assets. Background checks, non-disclosure and security policy compliance agreements shall be mandated for all third-party service providers.	Background checks, non-disclosure and security policy compliance mandated for all service providers. We have evidenced the BGV certification issued by the SOC vendor, Tech OWL. Credentials of Vendor personnel are verified before giving them access.	Complied	
RBI Circular DoS.CO/CSITE/ BC 4083/ 31.01.052/2019-20 DATED 31/12/2019 - Annex II – Baseline Cyber Security and Resilience Requirements (in addition to the requirements given in Annex I) - Level II				
51.	UCBs shall identify an official (not necessarily designated as CISO), responsible for articulating and enforcing the policies that UCBs use to protect their information assets, apart from coordinating the cyber security related issues / implementation within the organization as well as relevant external agencies. The official shall be primarily responsible for ensuring compliance to various instructions issued on information/cyber security by RBI	Manager- IT has been designated as CISO for information systems protection and compliance. However, there is no documented appointment letter or Org chart showing him as the CISO.	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



	Other Controls			
	Additional controls as per RBI Circular DoS.CO/CSITE/ BC 4083/ 31.01.052/2019-20 DATED 31/12/2019			
52.	(i) Implement bank specific email domains (example, XYZ bank with mail domain xyz.in) with anti-phishing and anti-malware, DMARC controls enforced at the email solution.	As mentioned earlier, bank specific email domain is implemented. DMARC is set to REJECT	Complied	
53.	(ii) UCBs shall put in place two factor authentication for accessing their CBS and applications connecting to the CBS with the 2nd factor being dynamic in nature. (Eg: 2nd factor should not be a static password and must not be associated with the PC/terminal used for putting through payment transactions)	Two Factor Authentication was implemented at the Bank for CBS application by the way of mobile OTP. All the users are required to log in into the CBS application through their user ID, PW and then an OTP sent over their mobile phone.	Complied	
54.	(iii) Conduct security review of PCs/terminals used for accessing corporate Internet Banking applications of Scheduled Commercial Banks (SCBs), CBS servers and network perimeter through a qualified information security auditor.	Information Systems Audit and VAPT audit are conducted annually, which covers security review of computers, CBS servers and network perimeter.	Complied	
55.	(iv) There should be a robust password management policy in place, with specific emphasis for sensitive activities like accessing critical systems, putting through financial transactions. Usage of trivial passwords shall be avoided.	Password complexity is implemented. Following PW complexity was in place: PW Length: 8 Characters 1 – Upper Case 1 – Lower Case 1 – Special Character 1 - Number	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



56.	(v) Educate employees to strictly avoid clicking any links received via email (to prevent phishing attacks).	As mentioned earlier, employees are appropriately educated. Phishing awareness campaign was also conducted in April 2025. Prior to that, the previous phishing awareness campaign was run on 8 th May 2024	Complied	
57.	(vi) Put in place an effective mechanism to report the cyber security incidents in a timely manner and take appropriate action to mitigate the incident. UCBs shall also report all unusual cyber security incidents to CERT-In and IB-CART.	A mechanism is in place to report cyber security incidents as per RBI circulars. All vendors/3 rd parties have been informed via email of the need to ensure cyber security incidents are reported to the bank in a timely manner. However, no cyber incident has taken place in the Bank till date.	Complied	
	Application Security Life Cycle (ASLC)			
	Additional controls as per RBI Circular DoS.CO/CSITE/ BC 4083/ 31.01.052/2019-20 DATED 31/12/2019			
58.	3.1 The development/ test and production environments need to be properly segregated. The data used for development and testing should be appropriately masked.	Bank does not develop applications. Hence, Development environment and Test environment is not in place. No masking done since no dev and test environment.	Not Applicable	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



59.	3.2 Software/Application development approach should incorporate secure coding principles, security testing (based on global standards) and secure rollout.	This control is not applicable as Software development activities are not done in the Bank. Software applications are procured from vendors on subscription basis.	Not Applicable	
	Change Management			
	Additional controls as per RBI Circular DoS.CO/CSITE/ BC 4083/ 31.01.052/2019-20 DATED 31/12/2019			
60.	4.1 UCBs should have a robust change management process in place to record/ monitor all the changes that are moved/ pushed into production environment. Changes to business applications, supporting technology, service components and facilities should be managed using robust configuration management processes that ensure integrity of any changes thereto.	Board approved Change Management policy version 1.0 dated 14 April 2024 was in place at the Bank. Any changes in the IT environment are done in line with this policy as per the auditee. There were no changes documented at the Bank as on the day of assessment.	Complied	
	Periodic Testing			
	Additional controls as per RBI Circular DoS.CO/CSITE/ BC 4083/ 31.01.052/2019-20 DATED 31/12/2019			
61.	5.1 Periodically conduct Vulnerability Assessment/ Penetration Testing (VA/PT) of internet facing web/mobile applications, servers and network components throughout their lifecycle (pre-implementation, post implementation, after changes etc.). VA of critical applications and those on DMZ shall be conducted at least once in every 6 months.	VAPT for Network, Applications etc. was conducted in April 2025. Prior to that, the VAPT was done on 15 th March 2024. Hence the VA is not being done every 6 months. The findings therein were not yet remediated as of the date of our audit. No DMZ implemented as of now.	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



SL. No.	Control Point	Observations	Complied Yes / No	Suggestion
62.	5.2 UCBs having their CBS on a shared infrastructure of an Application Service Provider (CBS-ASP) shall get their CBS application including the infrastructure hosting it subjected to VA/PT through the CBS-ASP.	No evidence of the VAPT being done through the CBS-ASP Infrasoft Technologies.	Not Complied	Bank should get the CBS application VAPT through the CBS-ASP
63.	5.3 Application security testing of web/mobile applications should be conducted before going live and after every major change in the applications.	Application Security testing of web application has been conducted in April 2025. Mobile application is still in development.	Complied	
64.	5.4 The vulnerabilities detected are to be remedied promptly in terms of the UCB's risk management/treatment framework so as to avoid exploitation of such vulnerabilities.	The vulnerabilities brought out in the reports dated April 2025 were not yet mitigated	Not Complied	Vulnerabilities detected should be remediated at the earliest and retest should be conducted to verify that they are closed.



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



65.	5.5 Penetration testing of public facing systems as well as other critical applications are to be carried out by professionally qualified teams. Findings of VA/PT and the follow up actions necessitated are to be monitored closely by the Information Security/Information Technology Audit team as well as Top Management.	Penetration testing report was conducted by professionally qualified teams. Findings are to be monitored to closure	Partially Complied	Bank should close the findings.
Authentication Framework for Customers				
Additional controls as per RBI Circular DoS.CO/CSITE/ BC 4083/ 31.01.052/2019-20 DATED 31/12/2019				
66.	7.1 UCBs should have adequate checks and balance to ensure (including security of customer access credentials held with them) that transactions are put only through the genuine/authorized applications and that authentication methodology is robust, secure and centralized.	Bank has provided for secure customer access through centralized authentication and encrypted communication.	Complied	
67.	7.2 Implement authentication framework/mechanism to securely verify and identify the applications of UCB to customers (Example, with digital certificate).	Bank has implemented authentication mechanisms to verify customers before logging to bank application.	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



Anti-Phishing				
Additional controls as per RBI Circular DoS.CO/CSITE/ BC 4083/ 31.01.052/2019-20 DATED 31/12/2019				
68.	8.1 Subscribe to Anti-phishing/anti-rogue application services from external service providers for identifying and taking down phishing websites/rogue applications.	Bank has E-Scan AV security solution which provides for Phishing Protection.	Complied	
Data Leak Prevention Strategy				
Additional controls as per RBI Circular DoS.CO/CSITE/ BC 4083/ 31.01.052/2019-20 DATED 31/12/2019				
SL. No.	Control Point	Observations	Complied Yes / No	Suggestion
69.	9.1 Develop and implement a comprehensive data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information.	Bank has implemented the following measures, which helps in Data loss prevention. 1. Internet connection is not available on Bank network. 2. All USB and removable devices are blocked and cannot be used in the Banking environment. 3. E-Scan endpoint protection to block the USB.	Complied	
70.	9.2 Similar arrangements need to be ensured at vendor managed facilities as well.	Vendors have confirmed that they have implemented Data loss prevention measures. However, there was no documented evidence made available on the same during the assessment.	Not Complied	The Bank shall ensure that vendor conducts the respective audits and get the reports of the same available. The same shall be presented during the audit.
Audit Logs				



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



Additional controls as per RBI Circular DoS.CO/CSITE/ BC 4083/ 31.01.052/2019-20 DATED 31/12/2019				
71.	10.1 Capture the audit logs pertaining to user actions in a system. Such arrangements should facilitate forensic auditing, if need be.	Audit logs are enabled and capturing for critical systems regularly.	Complied	
72.	10.2 An alert mechanism should be set to monitor any change in the log settings.	The Servers are configured to log various system and user events. Any changes in the log settings can be made only by the admin and the admin credentials are only with the IT head manager of the bank. Additionally, the logs are shipped to the SOC managed by Tech OWLS, and they respond and alert to any incidents	Complied	
Incident Response and Management				
Additional controls as per RBI Circular DoS.CO/CSITE/ BC 4083/ 31.01.052/2019-20 DATED 31/12/2019				
73.	11.1 Put in place an effective Incident Response program. UCBs must have a mechanism/ resource to take appropriate action in case of any cyber security incident. They must have written incident response procedures including the roles of staff / outsourced staff handling such incidents.	Board approved Incident Response Plan version 1.0 dated 27-04-2024 was in place and found adequate. As per auditee, any incidents in the Bank's IT environment are handled in line with this policy.	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



74.	11.2 UCBs are responsible for meeting the requirements prescribed for incident management and BCP/DR even if their IT infrastructure, systems, applications, etc., are managed by third party vendors/service providers.	Bank is responsible for meeting the requirements prescribed for incident management and BCP/DR as the IT infrastructure is hosted in house. Last DR Drill was conducted on 29th March 2024. RTO of 15 mins and RPO of 10 mins was defined to switch from the DC to DR and vice versa. Both RTO and RPO were met during the drill. The Business Analysis document dated 27th April 2024 defines the following RTO's (pg4): 1) Customer Service -4 hrs. 2) Loans & Credit – 8hrs 3) ATM services-12hrs 4) Online Banking -24hrs	Complied	
Compliance of Cyber Security Framework- Restriction on Outward RTGS/NEFT/IMPS transactions				
Additional Controls as per CO.DOS.RSD.Not Complied.S6481/31.01.097/2022-23 dated 09/01/23				
75.	3 UCBs shall apply value-based limits (per customer per day limits) on outward RTGS / NEFT / IMPS transactions during business and non-business hours including on bank holidays based on a policy to be approved by the Board. These limits may be put in place within month of receipt of this letter, under intimation to us.	Bank has informed us that limits of 50 lacs for RTGS, 1 lac for NEFT and 5 lacs for IMPS are enforced at the counter, since they do not have Internet banking, however we did not see any documented evidence of Value based limits on outward RTGS/NEFT/IMPS transactions being applied. (This Observation was rectified During Audit)	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



SL. No.	Control Point	Observations	Complied Yes / No	Suggestion
Baseline Cyber Security and Resilience Requirements (in addition to the requirements given in Annex I & II) - Level III				
1. Network Management & Security				
76.	1.1 Put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.	Bank has engaged a 3 rd party SOC provider Tech OWLS to monitor, detect and alert them to any unusual activity on their systems, servers, network devices and endpoints.	Complied	
77.	1.2 Firewall rules shall be defined to block unidentified outbound connections, reverse TCP shells and other potential backdoor connections.	The Firewall configuration Audit report dated 17 th April 2025 identifies a Critical finding of "Inadequate Firewall Rule Restrictions"	Partially Complied	1) Firewall rules shall be defined to block unidentified outbound connections, reverse TCP shells and other potential backdoor connections. 2) All open issues in the Firewall configuration audit should be remediated.
2. Secure Configuration				
78.	2.1 Disable remote connections from outside machines to the network hosting critical payment infrastructure (Ex: RTGS/NEFT, ATM Switch, SWIFT Interface). Disable Remote Desktop Protocol (RDP) on all critical systems.	The bank does not have any ATM switch or SWIFT interface. It has NEFT/RTGS/IMPS, which is done through the CBS application. However, RDP is enabled on endpoints. (This Observation was rectified During Audit)	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



SL. No.	Control Point	Observations	Complied Yes / No	Suggestion
79.	2.2 Enable IP table to restrict access to the clients and servers in SWIFT and ATM Switch environment only to authorized systems.	No SWIFT & ATM SWITCH environment	Not Applicable	
80.	2.3 Ensure the software integrity of the ATM Switch/SWIFT related applications.	No SWIFT & ATM SWITCH environment	Not Applicable	
81.	2.4 Disable PowerShell in servers where not required and disable PowerShell in Desktop systems.	PowerShell is disabled in servers where not required. Desktops have PowerShell disabled	Complied	
82.	2.5 Restrict default shares including IPC\$ share (inter-process communication share)	Default shares are restricted.	Complied	
	3. Application Security Life Cycle (ASLC)			
83.	3.1. In respect of critical business applications, UCBs may conduct source code audits by professionally competent personnel/service providers or have assurance from application providers/OEMs that the application is free from embedded malicious / fraudulent code.	The bank is subscribing to 3 rd party applications and does not do any in house Application development. It also does not do any customized software, hence the ASLC controls are not applicable	Not Applicable	
84.	3.2. Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data	Not applicable	Not Applicable	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



	integrity, system activity logging, audit trail, session management, security event tracking and exception handling are required to be clearly specified at the initial and ongoing stages of system development/acquisition/implementation.			
85.	3.3. Ensure that software/application development practices adopt principle of defense-in-depth to provide layered security mechanism.	Not Applicable	Not Applicable	
86.	3.4 Ensure that adoption of new technologies is adequately evaluated for existing/evolving security threats and that the IT/security team of the UCB achieve reasonable level of comfort and maturity with such technologies before introducing them for critical systems of the UCB.	All applications adopted are thoroughly tested by the banks 3 rd parties who are providing the same services to other banks. Hence these are tried and proven technologies.	Not Applicable	
	4. User Access Control			
87,	4.1. Implement a centralized authentication and authorization system through an Identity and Access Management solution for accessing and administering critical applications, operating systems, databases, network and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, two-factor/multi-factor authentication, securing privileged accesses following the principle of least privileges and separation of duties. This shall be implemented by	Bank has implemented Active Directory with centralized authentication and authorization functionality. Strong password policies are enforced through the AD, and through applications which have 2FA enabled to help ensure only authorized individuals are able to access the applications.	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



	the bank either with the in-house team managing the infrastructure or through the service provider if their infrastructure is hosted at a shared location at the service provider's end.			
88.	4.2. Implement centralized policies through Active Directory or Endpoint management systems to whitelist/blacklist/restrict removable media use.	Active Directory and Endpoint management system using E-Scan is implemented	Complied	
	5. Advanced Real-time Threat Defense and Management			
89.	5.1. Build a robust defense against the installation, spread, and execution of malicious code at multiple points in the enterprise.	USB drives are blocked via E-Scan, Anti-virus is enabled on all PCs. Internet access is not allowed on PCs. Firewalls restrict traffic to only authorized users. SOC monitors alerts in real time. SOC also subscribes to threat intel to ensure the systems are protected from any outbreak.	Complied	
90	5.2 Implement whitelisting of internet websites/systems.	No Internet access from endpoints, hence not applicable	Not Applicable	
	6. Maintenance, Monitoring, and Analysis of Audit Logs			
91.	6.1. Consult all the stakeholders before finalizing the scope, frequency and storage of log collection.	SIEM is implemented and logs are being collected and analyzed as per the agreement with the vendor Tech OWLS.	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



92.	6.2. Manage and analyze audit logs in a systematic manner so as to detect, respond, understand or recover from an attack.	This is being done by SOC provider Tech OWLS	Complied	
93.	6.3. Implement and periodically validate settings for capturing of appropriate logs/audit trails of each device, system software and application software, ensuring that logs include minimum information to uniquely identify the log for example by including a date, timestamp, source addresses, destination addresses.	This has been implemented and as per the auditee is reviewed by the bank as part of the periodical review of the SOC services	Complied	
	7. Incident Response and Management			
94.	7.1. UCB's BCP/DR capabilities shall adequately and effectively support the UCB's cyber resilience objectives and should be so designed to enable the UCB to recover rapidly from cyber-attacks/other incidents and safely resume critical operations aligned with recovery time objectives while ensuring security of processes and data is protected.	Capabilities to recover from the DR are tested annually and the results of the last test have been in line with the defined RTO and RPO	Complied	
95.	7.2. UCBs shall have necessary arrangements, including a documented procedure, with such third-party vendors/service providers for such purpose. This shall include, among other things, to get informed about any cyber security incident occurring in respect of the bank on timely basis to early	Bank has communicated the incident management requirements to the 3 rd parties and the SOC is informing the bank in a timely manner of any outages or any abnormal activity.	Complied	



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



	mitigate the risk as well as to meet extant regulatory requirements.			
96.	7.3. Have a mechanism to dynamically incorporate lessons learnt to continually improve the response strategies. Response strategies shall consider readiness to meet various incident scenarios based on situational awareness and potential/post impact, consistent communication and co-ordination with stakeholders during response.	No incidents as of now however the bank has documented policies to perform RCA and incorporate lessons learnt from any future incident	Complied	
	8. User / Employee/ Management Awareness			
97.	8.1. Encourage them to report suspicious behavior incidents to the incident management team.	Cyber Security awareness has been conducted by the Bank among employees, management, Vendors, Service Providers and customers. We have evidenced the last classroom awareness session training certificate which was conducted on 18 th March 2024 by Pheonix Techno Cyber. Phishing Awareness Campaign was last conducted by the Bank in April 2025 to all 179 email ids of the bank. Prior campaign was run on 8 th May 2024	Complied	
98.	8.2. Make cyber security awareness programs mandatory for new recruits and web-based quiz and training for lower, middle and upper management every year.	Awareness program is mandatory, however there is no web-based quiz as of now.	Partially Complied	Bank to implement web-based quiz



Comprehensive Assessment of Compliance with Graded Cyber Security Framework



99.	8.3. Board members may be sensitized on various technological developments and cyber security related developments periodically.	Being done already	Complied	
	9. Risk based transaction monitoring			
100.	9.1. Risk based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system across all -delivery channels.	The bank does not have SWIFT and ATM Switch; hence this is not applicable	Not Applicable	

Place: Mumbai

Krishna J

Date: 2nd May 2026

IS Auditor



Comprehensive Assessment of Compliance with Graded Cyber Security Framework

