‘Technology Vision for Cyber Security’ for Urban Co-operative Banks – 2020-2023

1. FOREWORD

1.1 Use of Information Technology by banks has grown rapidly and is now an important part of the operational strategy of banks. The number, frequency and impact of cyber incidents/attacks have increased manifold in the recent past, more so in the case of financial sector including Urban Co-operative Banks (UCBs). It has, therefore, become essential to enhance the security posture of UCBs so as to prevent, detect, respond to and recover from cyber-attacks. In view of the same, a circular DCBS.CO.PCB.Cir.No.1/18.01.000/2018-19 dated October 19, 2018 prescribing basic cyber security controls was issued to all the UCBs.

1.2 Considering the heterogeneity of the UCB sector in terms of size, regions, financial health and digital depth, it was recognised that a ‘one size fits all’ approach may not be suitable while prescribing cyber security guidelines for UCBs. In view of the same, formulation of cyber security controls for UCBs came to be guided by the following principles:

- A differentiated tier-wise approach will be followed while prescribing cyber security controls for UCBs. The tiers would be decided based on risk exposure in terms of the digital services offered by the UCBs.
- The approach will ensure that the UCBs with high IT penetration/ and offering all payment services are brought at par with other banks having mature cyber security infrastructure and practices.
- The Board of the UCBs shall be assigned the primary responsibility for implementing the cyber security controls.
- Considering that implementation of cyber security framework would be a cost intensive process, the responsibility for implementation, monitoring, compliance and response would have to be assigned from the Board level and percolate down till the end user. The IT/IS Governance Framework would include appointing a Chief Information Security Officer (CISO), setting up of various committees such as IT Strategy Committee, IT Steering Committee, etc for UCBs with higher digital depth.

Accordingly, circular DoS.CO/CSITE/BC.4083/31.01.052/2019-20 dated December 31, 2019 on “Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach” was issued to all UCBs and circular DoS.CO/CSITE/BC.4084/31.01.015/2019-20 dated December 31, 2019 on “Cyber Security controls for Third party ATM Switch Application Service Providers” was issued to all regulated Entities including Primary UCBs.

'Vision for Cyber Security' for UCBs – 2023

Enhancing the cyber security posture of the Urban Co-operative banking sector against evolving IT and cyber threat environment through a five-pillared strategic approach GUARD., viz., - Governance Oversight, Utile Technology Investment, Appropriate Regulation and Supervision, Robust Collaboration and Developing necessary IT, cyber security skills set.

To accomplish the Vision, the Mission is established with following action points

Mission – Specific Action Points

Governance Oversight

i. Focus on Board Oversight over Cyber security
ii. IT Vision document

Utile Technology Investment

iii. Creation of reserve/ fund for implementation of IT/ cyber security projects
iv. Management of Business IT Assets
v. Banking Services Availability

Appropriate Regulation and Supervision

vi. Supervisory reporting framework
vii. Appropriate guidance in implementing secure practices

Robust Collaboration

viii. Forum to share best Practices and discuss practical issues and challenges
ix. CISO Forum for UCBs
x. Adoption of Cloud Services – Phase I

Developing necessary IT, cyber security skills set

xi. Imparting technical Skills to manage IT and Cyber Security
xii. Providing awareness/ training for all UCBs on cyber security

The details of the action points enumerated in the Mission statement is given below.

Governance Oversight

2.1 Focus on Board Oversight over Cyber security

As is advised in the Comprehensive Cyber Security Framework for UCBs, the Board of Directors is ultimately responsible for the information security of the UCB and shall play a proactive role in ensuring an effective IT (Information Technology) and IS (Information

Security) governance. Therefore, matters related to cyber security needs to be part of discussion in the Board meetings. In this regard, instructions will be issued to banks to include the review on cyber security posture along with specific indicators, as part of the calendar of reviews to be submitted to the Board of Directors during its meetings. (**Action**: RBI: 2020)

2.2 IT Vision document

Today, almost every UCB is at some stage of technology adoption including expanding their footprint on digital delivery channels: Core banking solution (CBS), or digital delivery channels such as internet banking, mobile banking and ATMs. UCBs could play a crucial role in furthering financial inclusion. Technology is increasingly becoming the key business driver for the banking sector including UCBs to deliver their services to its customers. Therefore, UCBs need to develop their own technology vision document outlining their plans to incorporate IT solutions into their business in a secure manner. This vision document shall provide guidelines that can be used by the banks to design, develop, and implement IT operations not only as an organisational capability but as a strategic asset. The vision document should compulsorily have timelines for achieving the desired results. The banks should put in place a mechanism to review the vision document on periodic basis to reflect the changes as mandated by the regulator from time to time. (**Action**: For UCBs in Level 2 to 4 : 2021; For UCBs in Level 1: 2022)

Utile Technology Investment

2.3 Creation of reserve/ fund for implementation of IT/ cyber security projects

Considering that implementation of cyber security controls will be capital intensive, UCBs may consider creating a reserve/ fund earmarked for implementing IT/ cyber security projects. This reserve may be created out of its annual net profits over a period of time. To start with, an approach paper may be brought out by NAFCUB and Federations of UCB in Phase I and creation of fund may be carried out in Phase II.

(**Action**: Phase I - NAFCUB and Federations of UCB: All UCBs: 2022)

2.4 Management of Business IT Assets

The UCBs should have proper monitoring of lifecycle of its IT assets, both hardware and software, so as not to run the risk of operating obsolete hardware/ software. Therefore, UCBs

shall endeavour to invest and upgrade their IT inventory with supporting IT infrastructure and facilities to ensure that IT infrastructure is not exposed to risk due to obsolete hardware/software. Furthermore, a comprehensive process for Software License Management (SLM) shall be implemented by the UCBs. Review and appraisal of IT assets (criticality, privilege access, password policy, etc.) may be conducted by UCBs atleast on a yearly basis. (**Action**: For UCBs in Level 2 to 4 : 2021; For UCBs in Level 1: 2022)

2.5 Banking Services Availability

Unforeseen circumstances at times create major operational disruptions posing substantial risk to the continued operation and functioning of UCBs. To effectively address the risk, UCBs shall have a Business Continuity Plan (BCP) for all processes covering the aspects not just limited to the availability of backup systems and ensure that it is well-communicated, well-rehearsed and reviewed periodically. Based on the requirement, this shall also discuss adopting to establish a secure elastic digital workplace, on need basis, as BCP encompasses inter-alia business, technological and human aspects in compliance with extant regulatory instructions. The focus may be on prioritizing systems and processes in terms of their importance for keeping business operating smoothly and safely. (**Action**: For UCBs in Level 2 to 4 : 2021; For UCBs in Level 1: 2022)

Appropriate Regulation and Supervision

2.6 Supervisory reporting framework

As per extant instructions, UCBs have been advised to report immediately all unusual cyber security incidents (whether they were successful or mere attempts) to RBI, apart from other concerned authorities. Further, considering the large number of UCBs, an effective offsite supervision of UCBs will be setup to monitor compliance of UCBs with respect to cyber security guidelines as well as to have an overall and up-to-date understanding of the cyber security posture of the UCB sector. (**Action**: RBI: 2021)

Digital regulatory reporting shall be explored for automation based on a predetermined interpretation of the relevant regulations and straight through reporting to the regulator in a standard format. (**Action**: RBI: 2022)

2.7 Appropriate guidance in implementing secure practices

A uniform 'Cyber Security Hygiene' document for all the cooperative banks shall be issued. This document shall essentially cover various best practices seen across the supervised entities in different areas including Privilege access management, network segmentation, secure configuration, Security incident and event management which could be used by UCBs as a reference document for implementing applicable controls. Further, it shall be reviewed at periodic intervals to counter effectively the ever-changing threat landscape and continuously increase the 'Cyber Security Hygiene' to improve the overall UCBs cyber resiliency.

(**Action**: RBI: 2021)

Robust Collaboration

2.8 Forum to share best Practices and discuss practical issues and challenges

UCBs may explore the possibility of setting up a forum at State/regional level in which key personnel and/or management from various banks and other relevant stakeholders (e.g. third-party providers) may interact and coordinate on cyber security aspects on a periodic basis. The forum can also act as a platform for UCBs in benchmarking their practices with peers, sharing of threat intelligence, exploring their strengths and weaknesses in combating cyber threats. The forum can meet at least on a half yearly basis, to start with, to share best practices and discuss practical issues and challenges in the adoption and implementation of controls.

(**Action**: All Federations of UCB: 2021)

2.9 CISO Forum for UCBs

It is necessary to keep track of technology changes and to develop cyber security response processes. New technologies and concepts are required to be explored to ascertain if they add substantial business benefits. To this effect, as in the case for commercial banks, IDRBT may set up a separate CISO forum for UCBs to engage with them more closely. Considering the number of UCBs, initially, this could be set up for Level 3 and 4 UCBs (graded as per Comprehensive Cyber Security Framework) and engage with them at least on a quarterly basis. (**Action**: IDRBT: 2021)

2.10 Adoption of Cloud Services – Phase I[1]

The cost for implementing cyber security controls could be an impediment considering the limited capital of the UCBs. Cost effective technologies such as cloud (preferably community) based services may be used for implementing IT solutions and cyber security controls after

[1] On its completion, Phase 2 would discuss about implementation under the 2nd pillar – Utile technology investment

taking appropriate risk assessment and complying with extant regulatory instructions. Adoption of cloud services may be spearheaded by Federations of UCBs and/or any other equivalent that could emerge in the future. In Phase I, through collaborative approach, a blue-print may be prepared in the adoption of cloud services for the UCBs. ReBIT/IDRBT/IFTAS could be consulted for guidance.

(**Action**: Federations of UCBs. Timeline: 2022)

Developing necessary IT, cyber security skills set

2.11 Imparting technical Skills to manage IT and Cyber Security

The level of IT maturity at the UCBs[2] in managing the IT systems is minimal. Therefore, it requires substantial hand holding to implement the cyber security controls prescribed to them and to manage and monitor them on an ongoing basis. Targeted skill-oriented training and certification programmes would be designed to bring UCBs of different categories not only up to speed with the new framework in a time bound manner but also to manage the IT and security measures in the changing and challenging scenario. Measures would be taken to tap expertise available in various institutes/ universities of repute, across the country to provide such training in regional languages. (**Action**: RBI: 2021)

2.12 Providing awareness/ training for all UCBs on cyber security

Certification for Directors of the Board, Senior Management and employees of UCBs: Awareness/ certification programmes would be developed and customised to functions/ responsibilities of the stakeholders (Board to employee) in the UCBs. These programmes would be imparted with assistance of various training institutes of the RBI and other institutes of repute as approved by RBI. The objective of this initiative, is to, among other things, create awareness and predominantly communicate the IT/cyber security challenges and regulatory expectations to the UCBs in local language for better understanding of the cyber security and general controls so as to ensure a safe and secure IT environment in their day to day operations. (**Action**: RBI: 2021)

****

[2] Majorly in the UCBs at Level 1 and Level 2 (Grade as per December 31, 2019 circular)