भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2019-20/129

DoS.CO/CSITE/BC.4083/31.01.052/2019-20 December 31, 2019

To

The Chairman/Managing Director/Chief Executive Officer

All Primary (Urban) Co-operative Banks

Madam/Dear Sir,

Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach

Please refer to para I (3) of the Statement on Developmental and Regulatory policies of the Fifth Bi-monthly Monetary Policy Statement for 2019-20 dated December 5, 2019 (extract enclosed).

2. Please refer to our Circular DCBS.CO.PCB.Cir.No.1/18.01.000/2018-19 dated October 19, 2018 wherein some basic cyber security controls for Primary (Urban) Cooperative Banks (UCBs) were prescribed. On further examination, a comprehensive Cyber Security Framework for UCBs has been formulated based on a graded approach. The UCBs have been categorised into four levels based on their digital depth and interconnectedness to the payment systems landscape. The levels are defined as below:

Level	Criteria	Regulatory Prescription	Remarks
Level I	All UCBs	Level I controls prescribed in **Annex I**	In addition to the controls prescribed to the UCBs vide circular dated October 19, 2018, bank specific email domain with DMARC controls, two factor authentication for CBS etc., are salient controls prescribed.
Level II	All UCBs, which are sub-members of Centralised Payment Systems[1] (CPS) and satisfying at least one of the criteria given below**:** • offers internet banking facility to its customers (either view or transaction based) • provides Mobile Banking facility through application (Smart phone usage)	Level II controls given in **Annex II**, in addition to Level I controls.	Additional controls include Data Loss Prevention Strategy, Anti-Phishing, VA/PT of critical applications.

[1] Ref: Master Direction DPSS.CO.OD.No.1846/04.04.009/2016-17 dated January 17, 2017 on "Master Directions on Access Criteria for Payment Systems"

पर्यवेक्षण विभाग, केंद्रीय कार्यालय, वर्ल्ड ट्रेड सेंटर, सेंटर- I, कफ परेड, कोलाबा, मुंबई -400005
Department of Supervision, Central Office, World Trade Centre, Cuffe Parade, Colaba, Mumbai 400005
टेलीफ़ोन/ Tele: +91 22 22189131-39; फैक्स / Fax +91 22 22180157; ईमेल /email : cgmicdosco@rbi.org.in

	• is a direct Member of CTS/IMPS/UPI.		
Level III	UCBs having at least one of the criteria given below: • Direct members of CPS • having their own ATM Switch • having SWIFT interface	Level III controls given in **Annex III**, in addition to Level I and II controls.	Additional controls include Advanced Real-time Threat Defence and Management, Risk based transaction monitoring[2]
Level IV	UCBs which are members/ sub-members of CPS and satisfy at least one of the criteria given below: • having their own ATM Switch **and** having SWIFT interface • hosting data centre or providing software support to other banks on their own or through their wholly owned subsidiaries	Level IV controls given in **Annex IV**, in addition to Level I, II and III controls	Additional controls include setting up of a Cyber Security Operation Center (C-SOC) (either on their own or through service providers), IT and IS Governance Framework

3. 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. The major role of top management involves implementing the Board approved cyber security policy, establishing necessary organisational processes for cyber security and providing necessary resources for ensuring adequate cyber security.

4. UCBs shall undertake a self-assessment of the level in which they fit into, based on the criteria given in the table above and report the same to their respective RBI Regional Office, Department of Supervision within 45 days from the date of issuance of this circular.

5. All UCBs shall comply with the control requirements prescribed in **Annex I** within 3 months from the date of issuance of this circular. Similarly, Level II, III and IV UCBs are required to implement additional controls prescribed in **Annex –II**, **III** **and** **IV** respectively.

6. UCBs may adopt higher level of security measures based on their own assessment of risk and capabilities. Further, if a UCB, irrespective of its asset size already has a dedicated CISO and/or governance framework as discussed in **Annex IV**, then as a matter of best practice, it is desirable that it continues with the existing governance structure.

7. A copy of this circular may be placed before the Board of Directors in its ensuing meeting.

8. Please acknowledge receipt.

Yours sincerely,

(R. Ravikumar)
Chief General Manager

Encl: As above.

[2] Risk Based Transaction Monitoring applicable only to those banks as discussed in Annex III of the circular

Extract from the fifth Bi-monthly Monetary Policy Statement, 2019-20 announced on December 05, 2019

3. Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach

The Reserve Bank had prescribed a set of baseline cyber security controls for primary (Urban) cooperative banks (UCBs) in October 2018. On further examination, it has been decided to prescribe a comprehensive cyber security framework for the UCBs, as a graded approach, based on their digital depth and interconnectedness with the payment systems landscape, digital products offered by them and assessment of cyber security risk. The framework would mandate implementation of progressively stronger security measures based on the nature, variety and scale of digital product offerings of banks. Such measures would, among others, include implementation of bank specific email domain; periodic security assessment of public facing websites/applications; strengthening the cybersecurity incident reporting mechanism; strengthening of governance framework; and setting up of Security Operations Center (SOC). This would bolster cyber security preparedness and ensure that the UCBs offering a range of payment services and higher Information Technology penetration are brought at par with commercial banks in addressing cyber security threats. Detailed guidelines in this regard will be issued by December 31, 2019.

Annex I

Baseline Cyber Security and Resilience Requirements - Level I

The basic cyber security controls prescribed vide RBI Circular DCBS.CO.PCB.Cir.No.1/ 18.01.000/2018-19 dated October 19, 2018 remain valid except for the requirement to submit a quarterly 'NIL' report in case of no cyber security incidents. The need for such quarterly submission has been dispensed with. Further, following controls shall be implemented:

(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.
(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)
(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.
(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. [An illustrative but not exhaustive list of practices that should be strictly avoided are: For example, XYZ bank having password as xyz@123; network/server/security solution devices with passwords as device/solution_name123/device_name/solution@123; hard coding of passwords in plain text in thick clients or storage of passwords in plain text in the databases]
(v) Educate employees to strictly avoid clicking any links received via email (to prevent phishing attacks).
(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.

Vendor/Outsourcing Risk Management

In addition to the extant instructions given vide circular UBD.CO.BPD.No.31/09.18.300/2013 -14 dated October 17, 2013, UCBs shall be:

(vii) 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.
(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 recognise 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 authorised 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 reasonable time.
(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.

Annex II

Baseline Cyber Security and Resilience Requirements (in addition to the requirements given in Annex I) - Level II

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 organisation 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. Further, the following controls shall be implemented:

1. **Network Management and Security**
   - 1.1. Maintain an up-to-date/centralised inventory of authorised devices connected to UCB's network (within/outside UCB's premises) and related network devices in the UCB's network.
   - 1.2. Boundary defences 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.
   - 1.3. LAN segments for in-house/onsite ATM and CBS/branch network should be different.
2. **Secure Configuration**
   - 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.
3. **Application Security Life Cycle (ASLC)[3]**
   - 3.1. The development/test and production environments need to be properly segregated. The data used for development and testing should be appropriately masked.
   - 3.2. Software/Application development approach should incorporate secure coding principles, security testing (based on global standards) and secure rollout.
4. **Change Management**
   - 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.
5. **Periodic Testing**
   - 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 atleast once in every 6 months. PT shall be conducted atleast once in a year.

[3] These controls are applicable for the UCBs who are developing the application softwares (ex: core banking solution) themselves or through their subsidiaries. Otherwise, UCBs, apart from securing their production environment, may enforce these requirements with their respective third party vendors developing application softwares.

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.

5.3. Application security testing of web/mobile applications should be conducted before going live and after every major changes in the applications.

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.

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.

6. User Access Control / Management

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.)

7. Authentication Framework for Customers

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/authorised applications and that authentication methodology is robust, secure and centralised.

7.2. Implement authentication framework/mechanism to securely verify and identify the applications of UCB to customers (Example, with digital certificate).

8. Anti-Phishing

8.1. Subscribe to Anti-phishing/anti-rogue application services from external service providers for identifying and taking down phishing websites/rogue applications.

9. Data Leak Prevention Strategy

9.1. Develop and implement a comprehensive data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information.

9.2. Similar arrangements need to be ensured at vendor managed facilities as well.

10. Audit Logs

10.1. Capture the audit logs pertaining to user actions in a system. Such arrangements should facilitate forensic auditing, if need be.

10.2. An alert mechanism should be set to monitor any change in the log settings.

11. Incident Response and Management

11.1. Put in place an effective Incident Response programme. UCBs must have a mechanism/ resources 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.

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.

Annex III

Baseline Cyber Security and Resilience Requirements (in addition to the requirements given in Annex I & II) - Level III

1. **Network Management and Security**
   1.1. Put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.
   1.2. Firewall rules shall be defined to block unidentified outbound connections, reverse TCP shells and other potential backdoor connections.

2. **Secure Configuration**
   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.
   2.2. Enable IP table to restrict access to the clients and servers in SWIFT and ATM Switch environment only to authorised systems.
   2.3. Ensure the software integrity of the ATM Switch/SWIFT related applications.
   2.4. Disable PowerShell in servers where not required and disable PowerShell in Desktop systems.
   2.5. Restrict default shares including IPC$ share (inter-process communication share)

3. **Application Security Life Cycle (ASLC)**
   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.
   3.2. Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data 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.
   3.3. Ensure that software/application development practices adopt principle of defence-in-depth to provide layered security mechanism.
   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.

4. **User Access Control**
   4.1. Implement a centralised authentication and authorisation 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 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.

4.2. Implement centralised policies through Active Directory or Endpoint management systems to whitelist/blacklist/restrict removable media use.

5. Advanced Real-time Threat Defence and Management

5.1. Build a robust defence against the installation, spread, and execution of malicious code at multiple points in the enterprise.

5.2. Implement whitelisting of internet websites/systems.

6. Maintenance, Monitoring, and Analysis of Audit Logs

6.1. Consult all the stakeholders before finalising the scope, frequency and storage of log collection.

6.2. Manage and analyse audit logs in a systematic manner so as to detect, respond, understand or recover from an attack.

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.

7. Incident Response and Management

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.

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 mitigate the risk as well as to meet extant regulatory requirements.

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.

8. User / Employee/ Management Awareness

8.1. Encourage them to report suspicious behaviour incidents to the incident management team.

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.

8.3. Board members may be sensitised on various technological developments and cyber security related developments periodically.

9. Risk based transaction monitoring (*This control shall be applicable to those banks who are direct members of CPS as well as having their own ATM Switch interface or SWIFT interface***)**

9.1. Risk based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system across all -delivery channels.

Annex IV

Baseline Cyber Security and Resilience Requirements (in addition to the requirements given in Annex I, II & III) - Level IV

1. Arrangement for continuous surveillance - Setting up of Cyber Security Operation Centre (C-SOC)

UCBs are mandated that a C-SOC (Cyber Security Operations Centre) be set up at the earliest, if not yet done. It is also essential that this Centre ensures continuous surveillance and keeps itself regularly updated on the latest nature of emerging cyber threats.

1.1. **Expectations from C-SOC**

i. Ability to Protect critical business and customer data/information, demonstrate compliance with relevant internal guidelines, country regulations and laws
ii. Ability to Provide real-time/near-real time information on and insight into the security posture of the UCB
iii. Ability to effectively and efficiently manage security operations by preparing for and responding to cyber risks/threats, facilitate continuity and recovery
iv. Ability to know who did what, when, how and preservation of evidence
v. Integration of various log types and logging options into a Security Information and Event Management (SIEM) system, ticketing/workflow/case management, unstructured data/big data, reporting/dashboard, use cases/rule design (customised based on risk and compliance requirements/drivers, etc.), etc.
vi. C-SOC should be able to monitor the logs of various network activities and should have the capability to escalate any abnormal / undesirable activities.
vii. Key Responsibilities of C-SOC could include:
    - Monitor, analyse and escalate security incidents
    - Develop Response - protect, detect, respond, recover
    - Conduct Incident Management and Forensic Analysis
    - Co-ordination with relevant stakeholders within the UCB/external agencies

1.2. **Steps for setting up C-SOC – Technological Aspects**

i. First step is to arrive at a suitable and cost effective technology framework designed and implemented to ensure proactive monitoring capabilities aligned with the banking technology risk profile and business and regulatory requirements. Clear understanding of the service delivery architecture deployed by the UCB will enable identification of the location for the sensors to collect the logs that are required to carry out the analysis and investigation. SIEM is able to meet this requirement to some extent but a holistic approach to problem identification and solution is required.
ii. Second step is to have a security analytics engine which can process the logs within reasonable time frame and come out with possible recommendations with options for further deep dive investigations
iii. Third step is to look at deep packet inspection approaches
iv. Fourth step is to have tools and technologies for malware detection and analysis as well as imaging solutions for data to address the forensics requirements

v. It is to be noted that the solution architecture deployed for the above has to address performance and scalability requirements in addition to high availability requirements. Some of the aspects to be considered are:
   - Staffing of C-SOC - is it required to be 24x7x365, in shifts, business hours only, etc.
   - Model used - Finding staff with required skills /managed security service provider with required skill set
   - Metrics to measure performance of C-SOC
   - Ensuring scalability and continuity of staff through appropriate capacity planning initiatives

2. Participation in Cyber Drills

2.1. UCBs shall participate in cyber drills conducted under the aegis of Cert-IN, IDRBT etc.

3. Incident Response and Management

3.1. UCBs shall ensure incident response capabilities in all interconnected systems and networks including those of vendors and partners and readiness demonstrated through collaborative and co-ordinated resilience testing that meet the UCB's recovery time objectives.

3.2. Implement a policy & framework for aligning Security Operation Centre, Incident Response and Digital forensics to reduce the business downtime/ to bounce back to normalcy.

4. Forensics and Metrics

4.1. Develop a comprehensive set of metrics that provides for prospective and retrospective measures, like key performance indicators and key risk indicators. Some illustrative metrics include coverage of anti-malware software and their updation percentage, patch latency, extent of user awareness training, vulnerability related metrics, number of open vulnerabilities, IS/security audit observations, etc.

4.2. Have support/ arrangement for network forensics/forensic investigation/distributed denial-of-service (DDOS) mitigation services on stand-by.

5. IT Strategy and Policy

5.1. The UCB shall have a Board approved IT-related strategy and policies covering areas such as:
   - Existing and proposed hardware and networking architecture for the UCB and its rationale
   - Standards for hardware or software prescribed by the proposed architecture
   - Strategy for outsourcing, in-sourcing, procuring off-the-shelf software, and in-house development
   - IT Department's Organisational Structure
   - Desired number and level of IT expertise or competencies in UCB's human resources, plan to bridge the gap (if any) and requirements relating to training and development
   - Strategy for keeping abreast with technology developments and to update systems as and when required
   - Strategy for independent assessment, evaluation and monitoring of IT risks, findings of IT/IS/Cyber security related audits.

6. IT and IS Governance Framework

6.1. Cyber Security Team/Function

UCBs shall form a separate cyber security function/group to focus exclusively on cyber security management. The organisation of the cyber security function should be commensurate with the nature and size of activities of the UCB including factors such as technologies adopted, delivery channels, digital products being offered, internal and external threats, etc. The cyber security function should be adequately resourced in terms of the number of staff, level of skills and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc.

6.2. IT Strategy Committee

UCBs may consider setting up a Board level IT Strategy Committee with a minimum of two directors as members, one of whom should be a professional director. At least two members of the IT Strategy Committee would need to be technically competent[4] while at least one member would need to have substantial expertise[5] in managing/guiding technology initiatives. Some of the roles and responsibilities that the IT Strategy Committee/Board should have are:

i. Approving IT strategy and policy documents
ii. Ensuring that the management has put an effective strategic planning process in place
iii. Ensuring that the IT organizational structure complements the business model and its direction
iv. Ensuring IT investments represent a balance of risks and benefits and that budgets are acceptable
v. Reviewing IT performance measurement and contribution of IT to businesses

6.3. IT Steering Committee

An IT Steering Committee shall be formed with representatives from the IT, HR, legal and business sectors. Its role is to assist the Executive Management in implementing IT strategy that has been approved by the Board. It includes prioritization of IT-enabled investment, reviewing the status of projects (including, resource conflict), monitoring service levels and improvements, IT service delivery and projects. The IT Steering committee/Board should appraise/report to the IT strategy Committee periodically. The committee should focus on implementation. Its functions, *inter-alia,* include:

i. Defining project priorities and assessing strategic fit for IT proposals
ii. Reviewing, approving and funding initiatives, after assessing value-addition to business process
iii. Ensuring that all critical projects have a component for “project risk management”
iv. Sponsoring or assisting in governance, risk and control framework, and also directing and monitoring key IT Governance processes
v. Defining project success measures and following up progress on IT projects

[4] Technically competent herein will mean the ability to understand and evaluate technology systems.

[5] A member will be considered to have “substantial expertise” if he has a minimum of five years of experience in managing IT systems and/or leading/guiding technology initiatives/projects. Such a member should also have an understanding of banking processes at a broader level and of the impact of IT on such processes. If not, then the member should be trained on these aspects.

vi. Provide direction relating to technology standards and practices
vii. Ensure that vulnerability assessments of new technology is performed
viii. Verify compliance with technology standards and guidelines
ix. Ensure compliance to regulatory and statutory requirements
x. Provide direction to IT architecture design and ensure that the IT architecture reflects the need for legal and regulatory compliance, the ethical use of information and business continuity

6.4. **Chief Information Security Officer (CISO)**

A sufficiently senior level official should be designated as Chief Information Security Officer (CISO), responsible for articulating and enforcing the policies that the UCB uses to protect its information assets apart from coordinating the cyber security related issues / implementation within the organisation as well as relevant external agencies. The CISO shall be primarily responsible for ensuring compliance to various instructions issued on information/cyber security by RBI. The following may be noted in this regard:

i. The CISO should report directly to the top executive overseeing the risk management function or in his absence to the CEO directly.
ii. The CISO should have the requisite technical background and expertise.
iii. The CISO should have a reasonable minimum term.
iv. The CISO should place a separate review of cyber security arrangements/ preparedness of the UCB before the Board on a quarterly basis.
v. The UCB's Board should be able to objectively measure steps to assess the effectiveness of the CISO's office.
vi. The CISO will be responsible for bringing to the notice of the Board about the vulnerabilities and cyber security risks that the UCB is exposed to.
vii. The CISO, by virtue of his role as member secretary of information security and/or related committees(s), if any, may ensure, inter alia, current/ emerging cyber threats to banking (including payment systems) sector and the UCB's preparedness in these aspects are invariably discussed in such committee(s).
viii. The CISO's office shall manage and monitor the C-SOC and drive cyber security related projects. It can have a dotted relation with Chief Information Officer (CIO)/ Chief Technology Officer (CTO) for driving such projects.
ix. The CISO shall be an invitee to the IT Strategy committee and IT Steering Committee. The CISO may also be a member of (or invited to) committees on operational risk where IT/ IS risk is also discussed.
x. The CISO's office shall be adequately staffed with technically competent people, if necessary, through recruitment of specialist officers, commensurate with the business volume, extent of technology adoption and complexity.
xi. The CISO shall not have any direct reporting relationship with the CIO/CTO and shall not be given any business targets.
xii. The budget for IT security/ CISO's office may be determined keeping in view the current/ emerging cyber threat landscape.

6.5. **Information Security Committee**

Since IT/ cyber security affects all aspects of an organisation, in order to consider IT/ cyber security from a UCB-wide perspective a steering committee of executives should be formed with formal terms of reference. The CISO would be the member secretary of the Committee. The Information Security Committee may include, among others, the Chief Executive Officer (CEO) or designee and two senior

management officials well versed in the subject. The Committee shall meet atleast on a quarterly basis. Major responsibilities of the Information Security Committee, *inter-alia*, include:

i. Developing and facilitating the implementation of information security policies, standards and procedures to ensure that all identified risks are managed within a UCB's risk appetite.
ii. Approving and monitoring major cyber security projects and the status of cyber security plans and budgets, establishing priorities, approving standards and procedures
iii. Supporting the development and implementation of a UCB-wide information security management programme
iv. Reviewing the position of security incidents and various information security assessments and monitoring activities across the UCB
v. Reviewing the status of security awareness programmes
vi. Assessing new developments or issues relating to information/ cyber security
vii. Reporting to the Board of Directors on cyber security activities
viii. Minutes of the Information Security Committee meetings should be maintained to document the committee's activities and decisions and a review on information/cyber security needs to be escalated to the Board on a quarterly basis.

6.6. **Audit Committee of Board (ACB)**

Vide DCBR.CO.BPD.(PCB).MC.No.3/12.05.001/2015-16 Master circular dated July 1, 2015 all UCBs have been advised to set up an Audit Committee (ACB) at the Board level. In addition to its prescribed role as per extant instructions, the ACB shall also be responsible for the following:

i. Performance of IS Audit and Evaluation of significant IS Audit issues – The ACB should devote appropriate and sufficient time to IS Audit findings identified and members of ACB need to review critical issues highlighted and provide appropriate guidance to the UCB's management.
ii. Monitor the compliance in respect of the information security reviews/VA-PT audits under various scope conducted by internal as well as external auditors/consultants to ensure that open issues are closed on a timely basis and sustenance of the compliance is adhered to.

****