GDCC BANK

Guntur District Cooperative Central Bank Limited

Cyber Security Policy

Guntur District Cooperative Central Bank Limited

POLICY MANUAL

Subject: **CYBER SECURITY POLICY**

Approved: Chief Executive Officer **Effective Date:**

1 DEFINITION

The use of the term "Bank" is in reverence to the **Guntur District Cooperative Central Bank Ltd.**

Cyber Security Framework in GDCCB

2 Introduction

a. Use of Information Technology by **Guntur District Cooperative Central Bank Ltd** and their constituents has grown rapidly and is now an integral part of the operational strategies of banks. As per the Reserve Bank guide lines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (G.Gopalakrishna Committee), wherein it was indicated that the measures suggested for implementation cannot be static and our Bank need to pro-actively create/fine-tune/modify their policies, procedures and technologies based on new developments and emerging concerns.

b. Since then, the use of technology by DCCB has gained further momentum. On the other hand, 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 banks, underlining the urgent need to put in place a robust cyber security/resilience framework at banks and to ensure adequate cyber-security preparedness among banks on a continuous basis. In view of the low barriers to entry, evolving nature, growing scale/velocity, motivation and resourcefulness of cyber-threats to the banking system, it is essential to enhance the resilience of the banking system by improving the current defences in addressing cyber risks. These would include, but not limited to, putting in place an adaptive Incident Response, Management and Recovery framework to deal with adverse incidents/disruptions, if and when they occur.

c. The Cyber Security Policy serves several purposes. The main purpose is to inform Bank users: employees, contractors and other authorized users of their obligatory requirements for protecting the technology and information assets of the Bank. The Cyber Security Policy describes the technology and information assets that we must protect and identifies many of the threats to those assets.

d. The Cyber Security Policy also describes the user's responsibilities and privileges. What is considered acceptable use? What are the rules regarding Internet access? The policy

answers these questions, describes user limitations and informs users there will be penalties for violation of the policy. This document also contains procedures for responding to incidents that threaten the security of the Bank computer systems and network.

3 IMPACT OF INFORMATION TECHNOLOGY

The banking industry has felt considerable impact of the paradigm shift that has taken place and is taking place, in technology and in its business usage particularly ours.

3.1 The Information ages

in the banking industry business landscape has experienced dramatic changes in the past decade and the pace of change shows no signs of abatement. Intense competition has necessitated new economics, new organizations and new market dynamics. Banks are targeting like different channels like internet banking and ATM's, increased customer base using technology as an enabler, everywhere banking and a renewed and invigorated emphasis on customer.

These forces have driven banks to constantly improve business processes and to make them effective and efficient. It has also created an intense demand for processing large amount of information within banks to assist faster information availability and better decision making in response to the changing business environment. The ability of technology to meet these needs has transformed information technology from a support function to an integral part of core processes spanning across all business functions and processes.

3.2 Significance of Information technology

The importance of information technology on information processing has been phenomenal. The complex information requirements of top management can be effectively met only through the use of IT. IT is central to ensuring quick, reliable and efficient processing of business transactions and also plays a vital role as an enabler to increase the customer base by adding various new channels to banking.

3.3 Usage of IT in Bank

The contemporary banking processes involve 24/7 uptime, real time data update, ATM's network, internet banking, anytime-anywhere banking, credit and debit cards, payment gateway for ecommerce, etc. further, IT is also used for efficient processing of internal activities and back office operations.

Moreover, IT is using big way of keeping data/ information of internal resources such as man power resources. This information is also be safeguarded.

3.4 Dependency on IT

In view of such extensive usage of IT, the dependency of the bank on IT will be fairly high. The entire business process cycle will be enabled through the use of IT. Moreover, IT will be central to all transaction processing. This dependency on IT is only expected to increase with time as newer technology comes into being and keeps on creating better prospects for banking business.

3.5 Vulnerability

The use of IT has resulted in the need for a completely different set of controls and processes to maintain and monitor security controls. The gap between the traditional security and controls and demand put forth by newer technologies has resulted in business, public service and individuals relying on newer technologies that are not yet sufficient secure.

Any IT usage or implementation is vulnerable to external or internal attack, which may result in failure of underlying information systems. There is risk of data loss due to mollified or accidental unauthorized access, use, misappropriation, modification or destruction of information, information system and IT. While the number of users accessing information, systems is increasing the control exercised by system owners or provider is being dissipated. Increased technology usage and inherent security and controls weaknesses has led the bank to draft a guiding cyber security policy to ensure that that it's information assets are secured and controlled.

4 STATEMENT OF INTENT

The bank's endeavor has been making optimum use of technology in carrying out our business, not sidelining under any circumstances, the important and pivotal aspect of information and data security.

The Bank is committed to ensuring that business conducts its activities in such a way that it makes right use of IT and at the same time its information assets are optimally secured.

4.1 Need for security and controls

Implementation of latest technology will change the way we do our business from branch focus to a bank focus. In wake such changes to our business, certain risks are foreseen in the area of security of bank information security assets.

Embracing new technology exposes the bank to the risk of possible unauthorized access to bank's data. Also, there could be over dependency on IT leading to breakdowns in business due to unavailability of technology support.

Despite highest level of IT usage in business, the bank's users and customers must have confidence that information systems will operate as intended and without unanticipated failures or problems. Though all these cannot be guaranteed, the bank will like to minimize such exposure. This will ensure that technology is optimally utilized and IT enhances future growth.

The bank wants to put in place information security and control environment to minimize the risk of security incidents involving IT usage.

4.2 Legal requirements

The Bank is also bounded by various regulatory requirements requiring implementation of IT security policy. These regulatory requirements are of great importance, as the bank has additional business channels in place over the internet such as internet banking, mobile banking, call center etc.

5 SCOPE

Information technology Cyber security policy covers all information used/ generated by the bank, which is stored, processed, transmitted or printed by a computer system or network and communication lines, and on any storage, medium including printed output. It applies to all the Bank employees and all others who directly or indirectly use or support the bank's computing services or information.

The scope of the cyber security policy can be enhanced to cover any other organization, which may be created to fulfill our legal or operational requirements.

Information technology Cyber Security policy applies to:

- All department and functions.
- All branches and geographical locations
- All information technology assets used; and
- Third parties with whom we have a long-term association for regular operations as well as independent service providers engaged to provide infrequent or on-off services.

6. Baseline Cyber Security and Resilience Requirements

An indicative but not exhaustive list of requirements to be put in place by banks to achieve baseline cyber-security/resilience is given. This may be evaluated periodically to integrate risks that arise due to newer threats, products or processes. Important security controls for effective

cyber security as may be articulated by CERT-In also may be referred. Some of the key points to be kept in mind are:

a. In view of the growing technology adoption and potential threats, the role of IT Sub-committee may be reviewed; Board level involvement and guidance would set the right tone at the top.

b. It is important to endeavour to stay ahead of the adversary.

c. Cyber Security Operations Centre should have the capacity to monitor various logs / incidents in real time / near real time.

d. It is important to keep the vigil and to constantly remain alert.

e. While hardware devices and software applications may provide security, it is important to configure them appropriately.

f. Human resources are the key and ensure that they are provided with appropriate training. Communicate the security policy of the bank periodically.

Baseline Controls

1. Inventory Management of Business IT Assets

1.1. DCCB Maintains an up-to-date inventory of Assets, including business data/information including customer data/information, business applications, supporting IT infrastructure and facilities – hardware/software/network devices, key personnel, services, etc. indicating bank business criticality.

1.2. Classification of data/information based on information classification/sensitivity criteria of the bank.

1.3. Appropriately manage and provide protection within and outside organization borders/network taking into consideration how the data/information are stored, transmitted, processed, accessed and put to use within the bank's network, and level of risk exposed to depending on the sensitivity of the data/information.

2. Preventing execution of unauthorized software

2.1. DCCB maintains an up-to-date and preferably centralised inventory of authorised/unauthorised software(s). Considers in implementing whitelisting of authorised applications / software/libraries, etc.

2.2. DCCB manages centrally installation of software/applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. and has the mechanism to block /prevent and identify installation and running of unauthorised software/applications on such devices/systems.

2.3. Continuously monitor the release of patches by various vendors / OEMs, advisories issued by CERT-in and other similar agencies and expeditiously apply the security patches as per the patch management policy of the bank. If a patch/series of

patches is/are released by the OEM/manufacturer/vendor for protection against well-known/ well publicised/reported attacks exploiting the vulnerability patched, bank has a mechanism to apply emergency patches expeditiously following an emergency patch management process.

2.4. DCCB has defined framework including requirements justifying the exception(s), duration of exception(s), process of granting exceptions, and authority for approving, authority for review of exceptions granted on a periodic basis by officer(s) at senior levels who are well equipped in understanding the business and technical context of the exception(s).

3. Environmental Controls

3.1. Bank has appropriate environmental controls for securing location of critical assets providing protection from natural and man-made threats.

3.2. Bank has pre-defined 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 are taken to protect the critical assets of the bank.

4. Network Management and Security

4.1. Bank has an up-to-date network architecture diagram at the organisation level including wired/wireless networks;

4.2. Bank has up-to-date/centralized inventory of authorised devices connected to bank's network (within/outside bank's premises) and authorised devices enabling the bank's network. The bank has central monitoring system to monitor the devices connected to banks network including branches.

4.3. All the network devices are configured appropriately and periodically assess whether the configurations are appropriate to the desired level of network security;

4.4. Bank has appropriate controls to secure wireless local area networks, wireless access points, wireless client access systems.

4.5. Has amechanism to identify authorized hardware / mobile devices like Laptops, mobile phones, tablets, etc. and ensure that they are provided connectivity only when they meet the security requirements prescribed by the bank.

4.6. Has strong mechanism to automatically identify unauthorised device connections to the bank's network and block such connections.

4.7. Has strong mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.

4.8. Established Standard Operating Procedures (SOP) for all major IT activities including for connecting devices to the network.

4.9. Security Operation Centre to monitor the logs of various network activities and should have the capability to escalate any abnormal / undesirable activities.

4.10. Boundary defenses of the bank is multi-layered with properly configured firewalls, proxies, DMZ perimeter networks, and network---based IPS and IDS. Mechanism to filter both inbound and outbound traffic is in place.

5. Secure Configuration

5.1. Documented and applied 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 and carry out reviews periodically,

5.2. periodically evaluate critical device such as firewall, network switches, security devices, etc. configurations and patch levels for all systems in the bank's network including in Data Centres, in third party hosted sites, shared-infrastructure locations like branches.

6. Application Security Life Cycle (ASLC)

6.1. Incorporated information security across all stages of application life cycle.

6.2. In respect of critical business applications, bank also considers conducting source code audits by professionally by having assurance from application providers/OEMs that the application is free from embedded malicious / fraudulent code.

6.3. Secure coding practices are implemented for internally /collaboratively developed applications.

6.4. 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 clearly specified at the initial and ongoing stages of system development/acquisition/implementation.

6.5. The development, test and production environments are properly segregated.

6.6. Software/Application development approach should be based on threat modelling, incorporate secure coding principles and security testing based on global standards and secure rollout.

6.7. The current process ensures that software/application development practices address the vulnerabilities based on best practices baselines such as Open Web Application Security Project (OWASP) proactively and adopt principle of defence-in-depth to provide layered security mechanism.

6.8. Bank Considers implementing measures such as installing a "containerized" apps on mobile/smart phones for exclusive business use that is encrypted and separated from other smartphone data/applications; measures to initiate a remote wipe on the containerized app, rendering the data unreadable, in case of requirement may also be considered.

6.9. Ensured that adoption of new technologies is adequately evaluated for existing/evolving security threats and IT/security team of the bank reach reasonable level of comfort and maturity with such technologies before introducing for critical systems of the bank.

7. Patch/Vulnerability & Change Management

7.1. DCCB follows documented risk-based strategy for inventorying IT components that need to be patched, identification of patches and applying patches so as to minimize the number of vulnerable systems and the time window of vulnerability/exposure.

7.2. appropriate systems and processes are in place to identify, track, manage and monitor the status of patches to operating system and application software running at end-user devices directly connected to the internet and in respect of Server operating Systems/Databases/Applications/ Middleware, etc.

7.3. Changes to business applications, supporting technology, service components and facilities are managing using robust configuration management processes, configuration baseline that ensure integrity of any changes thereto.

7.4. Periodically conduct VA/PT of internet facing web/mobile applications, servers & network components throughout their lifecycle (pre-implementation, post implementation, after changes etc.)

7.5. Periodically conduct Application security testing of web/mobile applications throughout their lifecycle (pre-implementation, post implementation, after changes) in environment closely resembling or replica of production environment.

7.6. As a threat mitigation strategy, identification of the root cause of incident and apply necessary patches to plug the vulnerabilities.

7.7. Periodically evaluate the access device configurations and patch levels to ensure that all access points, nodes between (i) different VLANs in the Data Centre (ii) LAN/WAN interfaces (iii) bank's network to external network and interconnections with partner, vendor and service provider networks are securely configured.

8. User Access Control / Management

8.1. Bank provides secure VPN access to the bank's assets/services from within/outside bank's network by protecting data/information at rest and in-transit.

8.2. Bank Sensibly protect customer access credentials such as logon user ID, authentication information and tokens, access profiles, etc. against leakage/attacks

8.3. Disallow administrative rights on end-user workstations/PCs/laptops and provide access rights on a need to know basis and for specific duration when it is required following an established process.

8.4. Implemented centralized authentication and authorization system like active directory authentication for accessing and administering applications, operating systems, databases, network and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, also exploring two-factor/multi-factor authentication depending on risk assessment and following the principle of least privileges and separation of duties.

8.5. Implemented centralized systems and controls to allow, manage, log and monitor privileged/super user/administrative access to critical systems (Servers/OS/DB, applications, network devices etc.).

8.6. Implemented policy level controls to minimize invalid logon counts, deactivate dormant accounts.

8.7. Monitor any abnormal change in pattern of logon.

8.8. Implemented measures to control installation of software on PCs/laptops, etc.

8.9. Implemented appropriate controls for remote management/wiping/locking of mobile devices including laptops, etc.

9. Authentication Framework for Customers

9.1. Implemented authentication mechanism to provide positive identify verification of bank to customers.

9.2. Customer identity information should be kept secure.

9.3. Bank acts as the identity provider for identification and authentication of customers for access to partner systems using secure authentication technologies.

10. Secure mail and messaging systems

10.1. Implemented secure mail and messaging systems, including those used by bank's partners & vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.

10.2. Documented and implemented email server specific controls.

11. Vendor Risk Management

11.1. Bank is accountable for ensuring appropriate management and assurance on security risks in outsourced and partner arrangements.

11.2. Bank carefully evaluated the need for outsourcing critical processes like facility management services, desktop management, UPS management etc. And selection of vendor/partner based on comprehensive risk assessment done by the bank.

11.3. Among others, banks shall regularly conduct effective due diligence, oversight and management of third party vendors/service providers & partners.

11.4. Established appropriate framework, policies and procedures supported by baseline system security configuration standards to evaluate, assess, approve, review, control and monitor the risks and materiality of all its vendor/outsourcing activities are in place.

11.5. Banks shall ensure and demonstrate that the service provider (including another bank) adheres to all regulatory and legal requirements of the country. DCCB necessarily enter into agreement with the service provider that amongst others provides for right of audit by the bank and inspection by the regulators of the country.

11.6. Reserve Bank of India shall have access to all information resources (online/in person) that are consumed by banks, to be made accessible to RBI officials by the banks when sought, though the infrastructure/enabling resources may not physically be located in the premises of banks.

11.7. Further, bank adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders.

11.8. Banks thoroughly satisfy about the credentials of vendor/third-party personnel accessing and managing the bank's critical assets.

11.9. Background checks, non-disclosure and security policy compliance agreements are mandated for all third-party service providers

12. Removable Media

12.1. Defined and implemented policy for restriction and secure use of removable media/BYOD on various types/categories of devices including but not limited to workstations/PCs/Laptops/Mobile devices/servers, etc. and secure erasure of data on such media after use.

12.2. Limited media types and information that could be transferred/copied to/from such devices.

12.3. Get the removable media scanned for malware/anti-virus prior to providing read/write access.

12.4. Considered and implemented centralized policies through Active Directory and Endpoint management systems to whitelist/blacklist/restrict removable media use.

12.5. As default rule, use of removable devices and media should not be permitted in the banking environment unless specifically authorised for defined use and duration of use.

13. Advanced Real-time Threat Defense and Management

13.1. Built a robust defense at perimeter level and other required levels against the installation, spread, and execution of malicious code at multiple points in the enterprise.

13.2. Implemented Anti-malware, Antivirus protection including behavioural detection systems for all categories of devices – (Endpoints such as PCs/laptops/ mobile devices etc.), servers (operating systems, databases, applications, etc.), Web/Internet gateways, email-gateways, Wireless networks, SMS servers etc. including tools and processes for centralized management and monitoring.

13.3. Considered and implemented whitelisting of internet websites/systems at firewall level and also at end point security level.

13.4. Considered and implemented secure web gateways with capability to deep scan network packets including secure (HTTPS, etc.) traffic passing through the web/internet gateway

14. Anti-Phishing

14.1. Subscribed at firewall level for Anti-phishing/anti-rouge app services from external service providers for identifying and taking down phishing websites/rouge applications.

15. Data Leak prevention strategy

15.1. Developed and implemented a comprehensive data loss/leakage prevention strategy at firewall level to safeguard sensitive (including confidential) business and customer data/information.

15.2. This includes protecting data processed in end point devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline.

16. Maintenance, Monitoring, and Analysis of Audit Logs

16.1. Log retention is as per the recommendations and best practices by consulting all the stakeholders before finalising the scope, frequency and storage of log collection.

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

16.3. Enough care has been taken to capture audit logs into a syslog server pertaining to user actions in a system.

17. Audit Log settings

17.1. Implemented 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, and various other useful elements of each packet and/or event and/or transaction.

18. Vulnerability assessment and Penetration Test and Red Team Exercises

18.1. Periodically conduct vulnerability assessment and penetration testing exercises for all the critical systems, particularly those facing the internet.

18.2. The vulnerabilities detected are to be remedied promptly in terms of the bank's risk management/treatment framework so as to avoid exploitation of such vulnerabilities.

18.3. Penetration testing of public facing systems as well as other critical applications are to be carried out by professionally qualified teams.

18.4. Findings of VA/PT and the follow up actions necessitated are to be monitored closely by the Information Security and Information Technology Audit team as well as top Management.

18.5. Information Security teams may be used to identify the vulnerabilities and the business risk, assess the efficacy of the defences and check the mitigating controls already in place by simulating the objectives and actions of an attacker.

19. Incident Response & Management Responding to Cyber-Incidents:

19.1. Bank has fully effective Incident Response program and procedures with due approval of the Board Management.

19.2. Have written incident response procedures including the roles of staff / outsourced staff handling such incidents; Response strategies shall consider readiness to meet various incident scenarios based on situational awareness and potential/post impact, consistent communication & co-ordination with stakeholders during response;

19.3. Have a mechanism to dynamically incorporate lessons learnt to continually improve the response strategies. Recovery from Cyber - Incidents:

19.4. Bank's BCP/DR capabilities are adequately and effectively support the Bank's cyber resilience objectives and should be so designed to enable the bank 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.

19.5. Banks shall ensure such capabilities in all interconnected systems and networks including those of vendors and partners and readiness demonstrated through collaborative &coordinated resilience testing that meet the bank's recovery time objectives.

19.6. Such testing shall also include testing of crisis communication to customers and other internal and external stakeholders, reputation management. Adequate capacity shall be planned and maintained, in consideration thereof. The following may be considered:

a. Define incidents, method of detection, methods of reporting incidents by employees, vendors and customers and periodicity of monitoring, collection/sharing of threat information, expected response in each scenario/incident type, allocate and communicate clear roles and responsibilities of personnel manning/handling such incidents, provide specialised training to such personnel, post incident review, periodically test incident response plans.
b. Establish and implement a Security Operations Centre for centralised and coordinated monitoring and management of security related incidents.
c. Establish and implement systems to collect and share threat information from local/national/international sources following legally accepted/defined means/process
d. Document and communicate strategies to respond to advanced attacks containing ransom ware/cyber extortion, data destruction, DDOS, etc.
e. Contain the level of cyber-attack by implementing shielding controls/quarantining the affected devices/systems.
f. Implement a policy & framework for aligning Security Operation Centre, Incident Response and Digital forensics to reduce the business downtime/ to bounce back to normalcy.

20. Risk based transaction monitoring

20.1. Risk based transaction monitoring and surveillance process are implemented as part of fraud risk management system across all -delivery channels.

20.2. The bank should notify the customer, through alternate communication channels, of all payment or fund transfer transactions above a specified value determined by the customer.

21. Metrics

21.1. Developed a comprehensive set of metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators.

21.2. Few illustrative metrics included coverage of anti-malware software and their updating percentage, patch latency, extent of user awareness training, vulnerability related metrics, etc.

22. Forensics

22.1. Have support/ arrangement for network DDOS mitigation services on stand-by.

23. User / Employee/ Management Awareness

23.1. Defined and communicated to users/employees, vendors & partners security policies covering secure and acceptable use of bank's network/assets including customer information/data, educating them about cyber security risks and protection measures at their level.

23.2. Have the procedure to encourage them to report suspicious behaviour incidents to the incident management team.

23.3. Conduct targeted awareness/training for key personnel (at executive, operations, security related administration/operation and management roles, etc.). DCCB made it part of the induction and on going training sessions to all employees.

23.4. Evaluate the awareness level periodically.

23.5. Established a mechanism for adaptive capacity building for effective Cyber security Management. Making cyber security awareness programs mandatory for new recruits as part of induction.

23.6. Board members are sensitised on various technological developments and cyber security related developments periodically which is monthly basis.

23.7. Board members are provided with awareness programmes on IT Risk / Cyber security Risk and evolving best practices in this regard so as to cover all the Board members at least once a year.

24. Customer Education and Awareness

24.1. Improve and maintain customer awareness and education with regard to cyber security risks.

24.2. Encourage customers to report phishing mails/ Phishing sites and on such reporting take effective remedial action.

24.3. Educate the customers on the downside risk of sharing their login credentials /passwords etc. to any third-party vendor and the consequences thereof.

Setting up and Operationalising Cyber Security Operation Centre (C-SOC)

Introduction

1. **Guntur District Cooperative Central Bank Ltd** has evolved technologically over the years and currently delivering innovative services to its customers. These services are delivered nonstop, round the clock and the customers access these services using Internet and Mobile Connectivity. Security of the financial transactions is of paramount importance and therefore the RBI has come out with guidelines from time to time addressing the security and operational aspects for specific applications and services.

2. It is important and pertinent to look at specifically the Internet facing applications and services that are currently delivered and proposed to be delivered in the immediate future in the Banking Industry and come out with Cyber Security guidelines across the applications and services.

3. Constant and Continuous monitoring of the environment using appropriate and cost-effective technology tools, clearly defined policies and procedures based on best practices and monitored by technically competent and capable manpower is the urgent need for the Industry. Compliance to the Government guidelines that are put out periodically covering the cyber security policy, protecting critical information infrastructure and the Information Technology Act are of paramount importance. It is important to address the governance, technology, operational, outsourcing and legal issues while setting up the Cyber Security Operations Centre.

4. Issues that need to be kept in mind while setting up the CSOC is given below. These are indicative but not exhaustive.

Governance Aspects:

- Top Management/Board Briefing on Threat Intelligence
- Dashboards and oversight
- Policy, measurement and enforcement (key metrics, reporting structure, define what is to be reported)
- Informing stakeholders, stakeholder participation

Expectations from SOC:

- Ability to Protect critical business and customer data/information, demonstrate compliance with internal guidelines, country regulations and laws
- Ability to Provide real-time/near-real time information on and insight into the security posture of the bank
- Ability to Effectively and Efficiently manage security operations by preparing for and responding to cyber risks/threats, facilitate continuity and recovery
- Ability to assess threat intelligence and the proactively identify/visualize impact of threats on the bank
- Ability to know who did what, when, how and preservation of evidence
- Integration of various log types and logging options into SIEM, ticketing/workflow/case management, unstructured data/big data, reporting/dashboard, use cases/rule design (customized based on risk and compliance requirements/drivers, etc.), etc.

Key Responsibilities of SOC could include:

- Monitor, analyse and escalate security incidents
- Develop Response - protect, detect, respond, recover
- Conduct Incident Management and Forensic Analysis
- Co-ordination with contact groups within the bank/external agencies

Points to keep in mind while planning for SOC in view of

a. Specialized skill set requirements of operating and managing a SOC,
b. Difficulty in finding experienced staff,
c. Time consuming and expensive trainings,
d. Designing of suitable compensation strategies,
e. Difficulty of retaining staff due to continual need for updated training, lack of adequate career path options, and overstretching,
f. Resource requirements pertaining to other supporting functions such as
    i. System administration of systems facilitating SOC operations such as SIEM/dashboard/reporting/workflow/case management systems, etc.,
    ii. receiving, integrating and using threat intelligence,
    iii. implementing communication strategy,
    iv. Supervision/ management of SOC staff/personnel,
    v. meeting compliance requirements of regulators/laws/regulations

Recommendation

Considering the sensitivity and significant importance of the cyber security operations center, it is to decide that either DCCB has to be established C-SOC to monitor all security event and report to respected stake holders on security incidents or we have to engage with professional C-SOC service provider after detailed evaluation of the requirements of the Bank