Deloitte.

RBI Guidelines for Cyber Security Framework

July 2016

Cyber

Setting the context

In a race to adopt technology innovations, Banks have increased their exposure to cyber incidents/ attacks thereby underlining the urgent need to put in place a robust cyber security and resilience framework.

The Reserve Bank of India has provided guidelines on Cyber Security Framework vide circular DBS. CO/CSITE/BC.11/33.01.001/2015-16 dated June 2, 2016, where it has highlighted the urgent need to put in place a robust cyber security/resilience framework to ensure adequate cyber-security preparedness among banks on a continuous basis.

The RBI Guidelines related to Cyber Security framework will enable banks to formalize and adopt cyber security policy and cyber crisis management plan. The requirement to share information on cyber security incidents with RBI will also help structure proactive threat identification and mitigation.

Did you know?

Financial services companies are most vulnerable to cyber attacks

- The financial services industry topped the list of 26 different industries that cyber criminals most targeted.[8]
- Financial services remains the industry most susceptible to malicious email traffickers, as consumers are seven times more likely to be the victim of an attack originating from a spoofed email with a bank brand versus one from any other industry.[9]

Difference between Cyber Security and Information Security

While Information Security focuses on protecting confidentiality, integrity, and availability of information, Cyber Security is the ability to protect or defend the use of cyberspace from cyber-attacks. Cyberspace is nothing but interconnected network of information systems or infrastructures such as Internet, telecommunications networks, computer systems, embedded processors and controllers and many others systems.

Traditional information security has limited coverage of risks emanating from cyberspace such as Cyber warfare, negative social impacts of interaction of people (trolling, defamatory viral messages, etc.), software and services on the Internet and threats from Internet of Things (IoT). These and other threats are not classic information security issues and thus need to be covered under a separate Cyber Security Framework. The emerging technologies and tools within the cyberspace is rapidly increasing organizations exposure to new vulnerabilities thereby increasing the risk to the organization. Given the benefits of the cyberspace, it is imperative that organizations manage their risk effectively through a robust Cyber Security Framework.

Structure of RBI

Guidelines on Cyber Security Framework

RBI Guidelines on Cyber Security framework focus on the following three areas:

01. Cyber Security and Resilience
02. Cyber Security Operations Centre (C-SOC)
03. Cyber Security Incident Reporting (CSIR)

The Cyber Security Framework for bank widely covers the follows domains:

Cyber Security Framework			
Cyber Security Policy	Cyber Security Strategy	Continuous Surveillance	**Annex 2 – Cyber Security Operation Centre (C-SOC)**
Risk / Gap Assessment	IT Architecture		
Network and Database Security	Cyber Security Policy	Reporting Cyber Incidents	**Annex 3 – Cyber Security Incident Reporting (CSIR)**
Cyber Crisis Management Plan	Cyber Security Preparedness Indicators		
Organization Structure	Cyber Security Awareness		

Annex 1 – Baseline Cyber Security and Resilience Requirements

Detailed Requirements of Cyber Security Framework

The detailed requirements for each of the Annexures of Cyber Security Framework are as follows:

Annex 1 – Baseline Cyber Security and Resilience Requirements				
Inventory Management of Business IT Assets	Preventing execution of unauthorized software	Environmental Controls	Network Management and Security	Secure Configuration
Application Security Life Cycle (ASLC)	Patch/Vulnerability & Change Management	User Access Control / Management	Authentication Framework for Customers	Secure mail and messaging systems
Vendor Risk Management	Removable Media	Advanced Real-time Threat Defense and Management	Anti-Phishing	Data Leak prevention strategy
Maintenance, Monitoring, and Analysis of Audit Logs	Audit Log settings	Vulnerability assessment and Penetration Test and Red Team Exercises	Incident Response & Management	Risk based transaction monitoring
Metrics	Forensics	User / Employee/ Management Awareness	Customer Education and Awareness	

Annex 2 – Cyber Security Operation Centre (C-SOC)		
C-SOC Functional Requirements	Governance Requirements	Integration Requirements
People Requirements	Process Requirements	Technology Requirements

Annex 3 – Cyber Security Incident Reporting (CSIR)	
Template for reporting Cyber Incidents	Cyber Security Incident Reporting (CSIR) Form

Impact on Banks

Banks need to assess their Cyber Security preparedness under the active guidance and oversight of the IT Sub Committee of the Board or the Bank's Board directly. Also the Banks need to report to Cyber Security and Information Technology Examination (CSITE) Cell of Department of Banking Supervision, Reserve Bank of India the following:

- identified gaps w.r.t. Cyber Security/Resilience Framework
- proposed measures/controls and their expected effectiveness
- milestones with timelines for implementing the proposed controls/measures and
- measurement criteria for assessing their effectiveness including the risk assessment and risk management methodology followed/proposed by the bank

Cyber Security assessment should cover the requirements and implications listed below:
Implications of RBI Requirements

01 **Cyber Security Policy**	• Define and adopt a comprehensive Cyber Security Framework that includes: – Cyber Security Strategy – Cyber Security Policy & Procedures – Assessment of cyber threats and risks • Implement controls defined in Annex 1 of guidelines for Cyber Security framework.
02 **Continuous surveillance**	• Establish cyber security testing/assessment program to identify vulnerabilities/ security flaws in Bank's infrastructure/applications on a periodic basis. • Establish Cyber Security Operations Centre (C-SOC) for proactive monitoring using sophisticated tools for detection, quick response and backed by tools for data analytics. • Ensure that C-SOC covers requirements defined in Annex 2.
03 **IT architecture**	• Establish cyber security testing/assessment program to identify vulnerabilities/ security flaws in Bank's infrastructure/applications on a periodic basis. • Establish Cyber Security Operations Centre (C-SOC) for proactive monitoring using sophisticated tools for detection, quick response and backed by tools for data analytics. • Ensure that C-SOC covers requirements defined in Annex 2.
04 **Network and Database Security**	• Perform comprehensive review of network (firewall rules, opening/closure of ports, etc.) and database (direct database access, back-end updates, etc.) security. • Define and document processes for access to networks and databases for valid business or operational requirement.
05 **Customer Information**	• Bank is the owner of customer's personal and sensitive information collected by the Bank. • Bank is responsible for securing customer information even when it is with the customer or with third party vendor.
06 **Cyber Crisis Management Plan**	• Develop Cyber Crisis Management Plan (CCMP) based on: – National Cyber Crisis Management Plan (CERT-IN) – Cyber Security Assessment Framework (CERT-IN) – CERT-In/NCIIPC/RBI/IDRBT guidance • Review BCP/DR program and align BCP/DR with Cyber Crisis Management Plan (CCMP). • Implement preventive, detective, and corrective controls to protect Bank against cyber-threats, and to promptly detect, respond, contain, and recover from any cyber-intrusions.
07 **Cyber Security preparedness indicators**	• Define indicators to assess and measure adequacy of and adherence to cyber security/resilience framework. • Use indicators for comprehensive testing through independent compliance checks and audits carried out by qualified and competent professionals.
08 **Reporting Cyber Incidents**	• Strengthen information security incident monitoring and management processes to include cyber security incidents and attempts. • Report all unusual cyber security incidents (whether they were successful or were attempts which did not fructify) to the Reserve Bank of India as per format given in Annex 3. • Update incident management policy and procedures to sanitize and share cyber security related incidents on forum's such as CISO forum, and IB-CART.
09 **Organization Structure**	• Review information security organization structure, CISO's roles and responsibilities to ensure that cyber security concerns are adequately highlighted within the Bank.
10 **Cyber Security Awareness**	• Conduct Cyber Security Awareness and Training sessions for all relevant stakeholders of the Bank including Board of Directors, Top Management, Third Party Vendors, Customers, Employees.

How can Deloitte help?

Learning from global experience

Though banks acknowledge the magnitude of the problem that cyber risks pose, this imperative is not always adequately recognized or accounted for across the enterprise. A deeper analysis of the successes and failures of cyber security programs shows that Banks need to develop a more comprehensive approach to cyber risk management as also suggested by RBI in their guidelines for Cyber Security Framework:

01	Cyber risk strategy to be driven at the executive level as an integral part of the core company strategy
02	A dedicated cyber security management team to be established for a dynamic, intelligence-driven approach to security
03	A focused effort to be placed on automation and analytics to create internal and external risk transparency
04	The “people” link in the defense chain can be strengthened as part of a cyber risk-aware culture
05	Cyber security collaboration to be extended beyond company walls to address common enemies

Transforming to a Secure, Vigilant, and Resilient model

The very innovations that drive business growth and value also create first order cyber risks. A sound cyber risk program is an integral element of business success. While being secure is more important than ever, Deloitte emphasizes the need to also be constantly vigilant and resilient in the face of shifting cyber threats. We help organizations understand the current threat landscape, and develop strategies to manage cyber risks in line with business risk priorities.

Our framework is built on industry-leading practices, insights from cyber incidents, and awareness of regulatory standards. Deloitte helps organizations better prioritize program investments, improve threat awareness and visibility, and remain resilient when cyber incidents occur.

- What is my business strategy and related cyber risks?
- What is my risk appetite?

- Who are my adversaries?
- What critical assets are they interested in?

- What tactics might they use to attack?
- What strategies and solutions do I need?

What strategies and solutions do I need

Governance

SECURE

Established risk prioritized controls to protect against known and emerging threats, and comply with standards and regulations

VIGILANT

Establish situational risk and threat awareness across the environment to detect violations and anomaliesrisk prioritized controls to protect against known and emerging threats, and comply with standards and regulations

RESILIENT

Establish the ability to handle critical incidents, quickly return to normal operations, and repair damage to the business

	Cyber Security – Protection (CSP)	Cyber Vigilance & Operations (CVO)	Cyber Resiliency – Respond (CRR)
	Secure. Being secure means having risk-prioritized controls to defend against known and emerging threats.	**Vigilant.** Being vigilant means having threat intelligence and situational awareness to identify harmful behavior.	**Resilient.** Being resilient means having the ability to recover from, and minimize the impact of, cyber incidents.
Cyber Strategy and governance	*Achieving and maintaining a Secure.Vigilant.Resilient.™ posture requires ongoing effort to define an executive-led cyber risk program, track progress, and continuously adapt the program to shifting business strategies and the evolution of cyber threats.*		
	• Software License Review • Vendor Risk Management • Cyber Training, Education and Awareness • Cyber Strategy, Transformation & Assessments • Project Risk Services • Technology Governance, Social Media, Cloud & Mobility	• Infrastructure protection • Vulnerability management • Application Security • Application Integrity • Identity and access management • Information Privacy	• Advanced threat readiness and preparation • Cyber Security and Risk analytics • Threat intelligence and Analysis	• Cyber Crisis Management • Forensics & Malware Analysis • Disaster Recovery • Cyber Wargaming
Managed services	*Deloitte's tailored, high-touch managed and subscription services can help you operate more efficiently, address talent shortages, achieve more advanced capabilities, and keep on track with your overall cyber risk program objectives.*		
	• Governance, Risk and Compliance	• Application Monitoring • Data Loss Prevention	• Security operations center / CIC	• Cyber Incident Response

Contacts

To learn more about how your organization can become secure, vigilant and resilient, please contact:

National

Amry Junaideen
President
National Leader
Enterprise Risk Services

Shree Parthasarathy
Partner
National Leader
Cyber Risk Services

A. K. Viswanathan
Partner
Cyber Risk Services

Maninder Bharadwaj
Partner
Cyber Risk Services

Abhijit Katkar
Partner
Cyber Risk Services

Ramu N
Partner
Enterprise Risk Services

Priti Ray
Sr. Director
Cyber Risk Services

Ashish Sharma
Partner
Cyber Risk Services

Please mail your queries at incyberisk@deloitte.com

Deloitte.