

Government of India  
Ministry of Finance  
Department of Economic Affairs

\*\*\*\*\*

**Press Release on the Report of the Working Group for setting up Computer Emergency Response Team in the financial sector**

---

The Financial Stability & Development Council (FSDC), the apex financial sector body with Hon'ble Finance Minister in Chair and all financial sector regulatory heads as members, in its meeting held on 5<sup>th</sup> January 2017 recognized that a Computer Emergency Response Team in Financial Sector (CERT-Fin) needs to be established to work towards strengthening cyber security in the financial sector in close coordination with all financial sector regulators and national level CERT-In.

2. The Finance Minister in Para 101 of his Budget Speech 2017-18, had announced "Cyber security is critical for safeguarding the integrity and stability of our financial sector. A CERT-Fin will be established. This entity will work in close coordination with all financial sector regulators and other stakeholders".

3. Pursuant to the above announcement, a Working Group was set up with Director General, Indian Computer Emergency Response Team (CERT-In) as Chairperson on 6<sup>th</sup> March 2017, and Department of Economic Affairs, Department of Financial Services, Ministry of Electronics and Information Technology, Reserve Bank of India, Securities and Exchange Board of India, Insurance Regulatory and Development Authority of India, Pension Fund Regulatory and Development Authority of India, Institute for Development & Research in Banking Technology, Reserve Bank Information Technology Pvt Ltd and National Payment Corporation of India as members, to study and recommend measures for setting up of computer emergency response team in the financial sector, and submit its report to the Department within a period of three months.

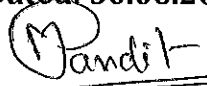
4. The Working Group has since submitted its report titled "Report of the working Group for setting up of Computer Emergency Response Team in the financial sector" along with recommendations arrived at unanimously after detailed discussions & deliberations. A copy of the Report of the Working Group are hosted on the home page of the Ministry of Finance at [www.dea.gov.in](http://www.dea.gov.in)

5. All stakeholders concerned/public are requested to forward their comments/suggestions that they may wish to submit on the report by 31<sup>st</sup> July 2017 by e-mail to [surjith.k@nic.in](mailto:surjith.k@nic.in) or in hard copy to Shri Surjith Karthikeyan, Deputy Director (FSDC), Department of Economic Affairs, Ministry of Finance, Room No. 269, North Block, New Delhi- 110001.

---

F. No. 18/06/2017-FSDC

New Delhi, Dated: 30.06.2017

  
(Dr. Manik Chandra Pandit)  
Joint Director (FSDC)

**REPORT OF THE WORKING GROUP  
FOR SETTING UP OF  
COMPUTER EMERGENCY RESPONSE TEAM  
IN THE FINANCIAL SECTOR (CERT-Fin)**



सत्यमेव जयते

**24<sup>th</sup> May 2017**

**FSDC Secretariat**

**Department of Economic Affairs**

**Ministry of Finance**

**Government of India**

## CONTENTS

Acronyms	ii
Acknowledgement	ix
Executive Summary	x
<b>1 Introduction</b>	<b>1</b>
1.1 Financial Sector In India	1
1.2 Emerging importance of Fin Tech and Cyber security	2
1.3 Discussions in international fora on Cyber Security	5
1.4. Addressing Cyber Security in Indian Financial Sector	8
1.5. Budget Announcement on CERT-Fin & setting up of Working Group	10
<b>2 Existing Cyber Security Structure in the Financial Sector in India</b>	<b>12</b>
2.1 CERT- In-An overview	12
2.2 National Critical Information Infrastructure Protection Centre (NCIIPC)	16
2.3 Existing Cyber Security structure in Financial Sector in India	19
2.3.1 Reserve Bank of India	19
2.3.1.1 National Payment Corporation of India	28
2.3.1.2 Institute for Development & Research in Banking Technology (IDRBT)	32
2.3.1.3 Reserve Bank Information Technology (ReBIT) Pvt. Ltd	34
2.3.2 Securities & Exchange Board of India	37
2.3.3 Insurance Regulatory & Development Authority of India	39
2.3.4 Pension Fund Regulatory & Development Authority of India	46
2.4 Other Sectoral CERTs	47
2.4.1 Telecom Sector and Financial Sector inter-linkages	48
2.4.2 Power & Defence CERTs	50
<b>3 Cyber Security and the Financial Sector – International Developments</b>	<b>55</b>
3.1 Computer Emergency Response Teams (CERTs) / Computer Security Incident Response Teams (CSIRTs)	55
3.2 International Practices in establishing CERT/ Fin-CERT	57
3.3 Relevant Lessons learnt for India- A discussion	60
3.4 CERT-Fin Model alternatives considered by the Working Group	64
<b>4 Conclusion and Recommendations of the Working Group</b>	<b>67</b>
<b>Annexes</b>	<b>81</b>

## Acronyms

ABS	Association of Bankers in Singapore
AEPS	Aadhaar-Enabled Payments System
AFA	Additional factor authentication
AIs	Authorized Institutions
APCERT	Asia Pacific Computer Emergency Response Team
ASTRI	Applied Science and Technology Research Institute
ATMs	Automated teller machine
BankSETA	Banking Sector Education and Training Authority
Bank CSIRT	Bank Computer Security Incident Response Team
BCMS	Business Continuity Management Standard
BCP	Business Continuity Planning
BCPs	Business Continuity Plans
BCP-DR	Business Continuity Planning and Disaster Recovery
BFS	Board for Financial Supervision
BFSI	Banking, Financial services and Insurance
BHIM	Bharat Interface For Money
BIS	Bureau of Indian Standards
BoE	Bank of England
BOI	Bank of India
BPO	Business process outsourcing
BPSS	Board for Regulation and Supervision of Payment and Settlement Systems
BSBDA	Basic Savings Bank Deposit Account
CA	Certifying Authority
CBEST	Controlled, bespoke, intelligence-led cyber security tests
CCA	Centre for Cyber Assessment
CCIRC	Canadian Cyber Incident Response Centre
CCRA	Certified Credit Research Analyst
CCTV	Closed-circuit television
CEA	Central Electricity Authority
CEO	Chief Executive Officer
CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Response
CERT	Computer Emergency Response Team
CERT.br	Computer Emergency Response Team Brazil
CERT-EU	Computer Emergency Response Team for the EU institutions, agencies and bodies
CERT-In	Indian Computer Emergency Response Team
CERT-Fin	Computer Emergency Response Team in the Financial Sector
CERT-NZ	Computer Emergency Response Team of New Zealand
CERT-SE	Computer Emergency Response Team of Sweden
CESG	Communications Electronics Security Group
CFI	Cyber-security Fortification Initiative
CGI.br	Brazilian Internet Steering Committee
CIA	Confidentiality, Integrity, and Availability

CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CINS	Critical Infrastructure Notification service
CIO	Chief Information Officer
CISA	Certified information system auditor
CISOs	Chief Information Security Officers
CMM-WG	Cyber security Maturity Model Development Working Group
CMP	Crisis Management Plan
CMU	Carnegie Mellon University
CNAP	Cyber-security National Action Plan
CNCERT/CC	National Computer Network Emergency Response Technical Team/Coordination Center of China
COBIT	Control Objectives for Information and Related Technologies
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPMI	Committee on Payments and Market Infrastructures
CPNI	Centre for the Protection of National Infrastructure
CRAs	Central Recordkeeping Agencies
CREST	Council of Registered Ethical Security Testers
CSA	Cyber Security Agency
CSIRT	Computer Security Incident Response Team
CSIRT.CZ	Computer Security Incident Response Teams of the Czech Republic
CSIS	Center for Strategic and International Studies
CSITE Cell	Cyber Security & IT Examination Cell
CSOC	Cyber Security Operations Centers
CTOs	Chief technology officers
CTS	Cheque Truncation System
CTS	Craftsmen Training Scheme
CWC	Cyber-Watch Centre
DBS	Department of Banking Supervision
DCS	Distributed Control System
DDG	Deputy Director General
DDoS	Distributed Denial-of-Service
DEA	Department of Economic Affairs
DFS	Department of Financial Services
DG	Director General
DGET	Director General of Employment & Training
DHS	Department of Homeland Security
DIA	Department of Internal Affairs
DIARA	Defence Information Assurance and Research Agency
DISA	Diploma in Information System Audit
DIT	Department of Information Technology
DLP/DRM	Data Loss Prevention/Digital Rights Management
DMA	Direct Market Access
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Naming System
DOS	Disk Operating System

DoT	Department of Telecommunications
DPI	Deep Packet Inspection
DPSS	Department of Payment and Settlement Systems
DR	Disaster Recovery
DRDO	Defence Research and Development Organisation
DRP	Disaster Recovery Plan
DSCI	Data Security Council of India
DTCC	Depository Trust & Clearing Corporation
DUKPT	Derived Unique Key per transaction
EC3	European Cybercrime Centre
ECB	European Central Bank
ECS-CSIRT	Electronic Communications Security - Computer Security Incident Response Team
ECU	Edith Cowan University
ED	Executive Director
EDP	Entrepreneurship Development Programme
EFI-ISAC	European Financial Institutes – Information Sharing and Analysis Centre
EMV	Europay, Mastercard and Visa
EMS	Element Management Systems
ENISA	European Union Agency for Network and Information Security
EIRM	Enterprise Integrated Risk Framework
EPC	European Payments Council
ERM	Enterprise Risk Management
ERP	Enterprise resource planning
EU	European Union
FBIIC	Financial and Banking Information Infrastructure Committee
FedCIRC	Federal Computer Incident Response Center
FIs	Financial Institutions
FI-ISAC	Financial Institutes – Information Sharing and Analysis Centre
Fin Tech	Financial Technology
Fin CERT	Computer Emergency Response Team in Financial Sector
FIRST	Financial Industry - Research in Security and Technology
FISC	Center for Financial Industry Information Systems
FMI	Financial market infrastructures
FRM	Fraud Risk Monitoring
FS	Financial Stability
FSA	Financial Services Agency
FSB	Financial Stability Board
FSDC	Financial Stability and Development Council
FS-ISAC	Financial Sector - Information Sharing Analysis Center
FSOR	Financial Sector forum for Operational Resilience
FSSCC	Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security
GLBA	Gramm-Leach-Bliley Act
GCHQ	Government Communications Head Quarters

GIS	Gas Insulated Substation
GovCERT.HK	Government Computer Emergency Response Team Hong Kong
HKCERT	Hong Kong Computer Emergency Response Team Coordination Centre
HKIB	Hong Kong Institute of Bankers
HKMA	Hong Kong Monetary Authority
HPSC-CS	High Powered Steering Committee on Cyber Security
IACS	Industrial Automation & Control Systems
IAIS	International Association of Insurance Supervisors
IB-CART	Indian Banks–Center for Analysis of Risks and Threats
IBA	Indian Banks’ Association
IBM	International Business Machines
IBT	Internet Based Trading
iCAST	Intelligence-led cyber-attack simulation testing
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICT	Information and Communication Technology
ICERT	Indian Computer Emergency Response Team
IDA	Infocomm Development Authority of Singapore
IDRBT	Institute for Development & Research in Banking Technology
IDS/IPS	Intrusion Defence Systems / Intrusion Prevention Systems
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IFTAS	Indian Financial Technology and Allied Services
IITs	Indian Institutes of Technology
IMPS	Immediate Payment Service
INFINET	Indian Financial Network
IOC	Indicators of Compromise
IOSCO	International Organization of Securities Commissions
IP	Internet Protocol
IRDAI	Insurance Regulatory and Development Authority of India
IS	Information Security
ISAC	Information Sharing and Analysis Centre
ISACA	Information Systems Audit and Control Association
ISAC-JP	Information Sharing and Analysis Centre - Japan
ISAI	Information and Security Audit for Insurers
ISC	Information Security Committee
ISEA	Information Security Education and Awareness
ISGF	India Smart Grid Forum
ISIRTs	Information security incident response teams
ISNP	Insurance Self-Network Platform
ISO	International Organization for Standardisation
ISPs	Internet service providers
IST	Information Security Team
IT	Information Technology
ITeS	Information Technology Enabled Services
ITI	Industrial Training Institute
JS	Joint Secretary

JCB	Japan Credit Bureau
JWG	Joint Working Group
KRIs	Key Risk Indicators
LEA's	Law Enforcement Agencies
LITD	Electronics & Information Technology Department
MAS	Monetary Authority of Singapore
MBIE	Ministry of Business, Innovation & Employment
MCA	Ministry of Corporate Affairs
MCI	Ministry of Communications and Information
MEA	Ministry of External Affairs
MeitY	Ministry of Electronics & Information Technology
MES	Modular Employable Skills
MHA	Ministry of Home Affairs
MIIs	Market Infrastructure Institutions
MoU	Memorandum of Understanding
MPIN	Mobile Personal Identification Number
NABARD	National Bank for Agriculture and Rural Development
NACH	National Automated Clearing House
NASSCOM	National Association of Software & Services Companies
NATO	North Atlantic Treaty Organization
NBFCs	Non-banking finance companies
NCAP	National Cybercrime Action Plan
NCAS	National Cyber Awareness System
NCCIC	National Cyber-security Communication Integration Center
NCFE	National Centre for Financial Education
NCII	National Critical Information Infrastructure
NCIIPC	National Critical Information Infrastructure Protection Centre
NCIRC	North Atlantic Treaty Organization (NATO) Computer Incident Response Capability
NCSC	National Cyber Security Centre
NCSC-UK	National Cyber Security Centre-United Kingdom
NCSP	National Cyber Security Policy
NEFT	National Electronic Funds Transfer
NFC	Near field communication
NFS	National Financial Switch
ngCERT	Nigerian Computer Emergency Response Team
NHB	National Housing Bank
NHPC	National Hydroelectric Power Corporation
NIPP	National Infrastructure Protection Plan
NISC	National Center of Incident Readiness and Strategy for Cyber-security
NIST	National Institute of Standards & Technology
NMS	Network Management System
NPCI	National Payments Corporation of India
NSC	National Security Council
NSCS	National Security Council Secretariat
NSDC	National Skill Development Corporation



NSOC	Network security operations center
NSS	National Security Strategy
NTPC	National Thermal Power Corporation
NTRO	National Technical Research Organisation
OEM	Original Equipment Manufacturer
OGCIO	Office of the Government Chief Information Officer
PA-DSS	Payment Applications - Data Security Standards
PCI-DSS	Payment Card Industry - Data Security Standards
PDCA	Plan-do-check-act
PDP	Professional Development Programme
PFMI	Principles for Financial Market Infrastructures
PFRDA	Pension Funds Regulatory and Development Authority
PGCIL	Power Grid Corporation of India Limited
PIN	Personal Identification Number
PKI	Public key infrastructures
PMJDY	Pradhan Mantri Jan-Dhan Yojana
PMO	Prime Minister's Office
PoS	Point of Sale
POSOCO	Power Operation System Corporation Ltd.
PPD	Presidential Policy Directive
PPIs	Prepaid Payment Instruments
PPP	Public Private Partnership
PSUs	Public Sector Undertakings
QMS	Quality Management Standard
QUT	Queensland University of Technology
RBI	Reserve Bank of India
ReBIT	Reserve Bank Information Technology Pvt Ltd
RFC	Request for Comments
RHQ	Registration Headquarters
RI	Regulated Institutions
RMI	Readiness Maturity Index
RRBs	Regional Rural Banks
RTGS	Real Time Gross Settlement
RVDP	Remote Vulnerability Disclosure Programme
S-CERT	Computer emergency response team of the German Sparkassen-Finanzgruppe
SABRIC	South African Banking Risk Information Centre
SCADA	Supervisory control and data acquisition
SEBI	Securities and Exchange Board of India
SEI	Software Engineering Institute
SFMS	Structured Financial Message System
SIEM	Security Information Event Management
SingCERT	Singapore Computer Emergency Response Team
SISTA	Singapore Infocomm Technology Security Authority
SLTT	State, Local, Tribal And Territorial
SMS	Short Message Service

SOC	Security Operation Center
SOP	Standard operating procedure
SPOC	Single Point of contact
SSA	Sector specific agency
STIX	Structured Threat Information eXpression
SWIFT	Society for the Worldwide Interbank Financial Telecommunication
TAC	Technical Advisory Committee
TAXII	Trusted Automated eXchange of Indicator Information
Tel-CERT	Telecom Sector Computer Emergency Response Team
TLE	Terminal line encryption
TLP	Traffic Light Protocol
TRAI	Telecom Regulatory Authority of India
TSP	Telecom Service Provider
UCBs	urban cooperative banks
UIDAI	Unique Identification Authority of India
UKPT	Unique Key per terminal
UPI	Unified Payments Interface
US-CERT	United States Computer Emergency Readiness Team
USD	United States Dollar
USSD	Unstructured Supplementary Service Data
VAPT	Vulnerability Assessment and Penetration Testing
VET	Vocational Education and Training
WG	Working Group
WLAOs	White Label ATM Operators

## Acknowledgements

*I feel thankful for having the opportunity to head this Working Group that was entrusted with the vital job of studying the existing national and international structure on Cyber Security and facilitating setting up of a CERT-Fin, as announced in FM's Budget Speech 2017-18. The Working Group after detailed discussions & deliberations, has unanimously finalised this report titled "Report of the working group for setting up of Computer Emergency Response Team in the financial sector". The FSDC Secretariat had assisted in the work of the Group with an admirable speed and promptness. Contribution of each of the members of the Group, their extended teams and specifically, Adviser (FS), Member Convener has been substantial.*

*The Working Group, to start with initially attempted to understand the working of various sectoral CERTs operating in the country and international best practices in the field of cyber security. A sub-group was formed with representatives from all financial sector Regulators, and the telecom sector (DoT & TRAI) to study the inter- linkages and suggest a coordination mechanism for the telecom and financial sector. A separate sub group was also formed within the working group with representation from all financial sector Regulators and National Payment Corporation of India which studied the international best practices in the field of cyber security. The contributions of these sub groups are highly appreciated. Specific inputs were also received from Group members which were helpful in rich discussion improving the quality of the report.*

*This also gave me the opportunity to highlight the working of our organization 'CERT-In', its roles and functions and could create awareness on cyber security among all members of the Working Group through a dedicated workshop held in CERT-In office.*

*The Working Group initially had two months' time, which was too short for the subject. Department of Economic Affairs (DEA) has been kind to consider extension of tenure of the Working Group by a month ie; till end May 2017.*

*I hope this report should be able to generate public awareness on the need for a comprehensive cyber security framework in the financial sector and pave the way for setting up CERT-Fin, a mandate that was assigned to the Group.*

*The role and importance of setting up CERT-Fin is reflected in the recommendations of the Group for immediately establishing the same with RBI as the lead regulator under the advice and guidance of the Inter Regulatory Technical Group that is already in place in the FSDC architecture with the involvement of related Ministries and Departments.*

*However, the Group recognizes that in this dynamic changing world, it would remain a challenge to manage newer form of cyber security risks in future recognizing which the Group also has recommended for the review of the functioning of CERT-Fin in two to three years' time.*

New Delhi



Dr Sanjay Bahl

Chairman of Working Group & DG-CERT-IN

## Executive Summary

### Mandate and Work process

1. The Financial Stability & Development Council (FSDC), the apex financial sector body with Hon'ble Finance Minister in Chair and all financial sector regulatory heads as members, in its meeting held on 5<sup>th</sup> January 2017, deliberated on a DEA agenda on "Fin Tech, digital innovations and Cyber security" agreed that a Computer Emergency Response Team in Financial Sector (CERT-Fin) needs to be established to work towards strengthening cyber security in the financial sector in close coordination with all financial sector regulators and national level CERT-In.
2. Subsequently, in FM's Budget Speech 2017-18, it was announced that "cyber security is critical for safeguarding the integrity and stability of our financial sector and announced that a CERT- Fin will be established. This entity will work in close coordination with all financial sector regulators and other stakeholders". Pursuant to the above announcement, a Working Group was set up with DG, CERT-In as Chairperson, on 6<sup>th</sup> March 2017 to study and recommend measures for setting up of computer emergency response system in the financial sector and submit its report to the Department within a period of two months, which was later extended by a month.
3. The terms of reference of this Working Group included (i) To study the existing cyber security measures and Computer Emergency Response system in the Financial Sector in India (ii) To study the best practices followed in the field of cyber security in financial sector across the World vis-à-vis Indian scenario, (iii) To suggest a suitable structure for setting up a CERT-Fin to strengthen the cyber security in the financial sector to work as sectoral CERT under close coordination with all financial sector related stakeholders & the CERT-In, which is the umbrella organization created under the Information Technology Act. FSDC Secretariat, DEA provided secretarial assistance to the Working Group with Adviser (FS) as Member-Convener of the Group.
4. The Working Group held its meetings on 22<sup>nd</sup> March 2017, 5<sup>th</sup> April 2017, 5<sup>th</sup> May, 2017 and 24<sup>th</sup> May 2017, besides a workshop held for all members to develop further clarity on the functioning of CERT-In and the existing framework, in the office of DG, CERT-In, on 5<sup>th</sup> April 2017. The Working Group finalised its report titled "Report of the working Group for setting up of Computer Emergency Response Team in the financial sector" along with recommendations arrived at unanimously after detailed discussions & deliberations.
5. The Report of the Group is broadly structured under four chapters viz; (i) Introduction (ii) Existing Cyber Security Structure in the Financial Sector in India (iii) Cyber Security and the Financial Sector – International Developments and (iv) Conclusion and Recommendations.

6. The first chapter discusses the emerging importance of Fin Tech and Cyber security in national and international arena including discussions in international fora such as G-7, G-20, & FSB on Cyber Security and the need for a comprehensive framework for cyber Security in Indian Financial Sector.

7. The second chapter describes the existing Cyber Security Structure in the Financial Sector in India, highlighting various initiatives of Working Group members in the cyber security front. The Working Group attempted to understand the working of various sectoral CERTs operating in the country, as also cyber security measures taken by financial sector Regulators in order to design the structure of CERT in the financial sector. The Group, noting the strong inter-linkages between telecom sector and finance sector, invited representatives from telecom sector for attending the Working Group held meetings and held discussions with a view to study the linkages and suggest a coordination mechanism for the same. A sub group was also formed on the same with representatives from all financial sector Regulators, and the telecom sector.

8. The third chapter describes the international developments in Cyber Security and the Financial Sector as the Working Group was of the view that the international experience of Financial CERTs needs to be studied thoroughly before reaching a final decision on the structure of CERT-Fin for India. A sub group was formed within the Working Group with representation from all financial sector Regulators and National Payment Corporation of India, studied the international best practices in the field of cyber security.

9. The fourth chapter while concluding the discussion of the Group, delineates a set of recommendations that it believes will lead to setting up a strong framework for addressing financial sector cyber security related issues.

### **Gist of Recommendations**

The Working Group, recognizing the criticality of cyber security for safeguarding the integrity and stability of India's financial sector and having studied the existing cyber security measures taken in the financial sector in India and international best practices in the field, unanimously recommends setting up of CERT-Fin, that will work in close coordination with all financial sector regulators and other stakeholders, on the lines delineated in this report. The recommendations of the Working Group can be summarized as follows:

- A nodal sectoral CERT ie; CERT-Fin to act as an umbrella CERT for the financial sector and report to CERT-In at the national level in accordance with IT Act and Rules.
- Sub sectoral CERTs may be set up and housed in each of the financial sector Regulators and below those, in major financial institutions, feeding information on real time basis to the proposed CERT-Fin. The diagrammatic representation of the

proposed model of CERT-Fin as recommended by the Working Group is depicted at Chapter 3 of the report.

- To facilitate smooth functioning in coordination with CERT-In, an MoU/legal arrangement in accordance with the Rules and IT Act clearly outlining the area of coverage/sharing protocol of proposed CERT-Fin and CERT-In, should be put in place. MoU may also be signed by proposed CERT-Fin with each of the sub sectoral regulator CERTs clearly outlining the role, functions & responsibilities of each of the parties.
- Proposed CERT-Fin should seek to complement the overarching mandate of CERT-In, keeping in view the following principles:
  - ✓ Financial services are offered by a large number of businesses that encompass the finance industry. These include Regulated Institutions (RIs) in each of key sectors of the financial system governed by various regulators. These regulators, viz. the RBI, SEBI, IRDAI and PFRDA have, for the last few years, been working through regulations needed to make their regulated entities better prepared for dealing with cyber risk. It is essential that all regulators should take adequate measures and enforce regulations for stronger cyber security architecture.
  - ✓ The approach also needs to take into account the differing levels of maturity of technology management across different types of regulated entities.
- CERT-Fin should be an independent body to be set up as a company under Section 8 of the Companies Act, 2013 with a Governing Board. An Advisory Board may be set up for, inter-alia, providing strategic direction, review of performance and recommendations for allocation of budget/resources. Keeping in view that this highly technical coordinating body may take time to be set up as a fully functional Company, it is necessary that during transition, RBI may act as the lead regulator in terms of setting up CERT-Fin.
- The Advisory Board for CERT-Fin may comprise all members of the Inter Regulatory Technical Group (under aegis of FSDC architecture), with ED (RBI) as Chairperson, and Adviser (FS), JS (MeitY), DDG/JS (DFS), DDG (DoT), representative of CERT-In and the CEO/Director, CERT-Fin also as members. The Advisory Board may also invite experts for discussion on need basis. The Advisory Board may meet frequently at the initial stage of setting up of CERT-Fin & thereafter, on quarterly basis. The Governing Body may be set up with nominees of shareholding institutions; i.e. the Regulators, CERT-In, two independent and technically qualified members and the CEO/Director, CERT-Fin. RBI may act as the lead Regulator till CERT-Fin is fully set up & functional as a Company.
- CERT-Fin may do analysis of financial sector cyber incidents, understand the pattern and nuances across financial sectors and envisage basic functions for CERT-Fin as delineated by the Working Group, while reporting the cyber security incidents to CERT-In.
- CERT-Fin should create awareness on security issues through dissemination of information on its website and operate 24x7 incidence responses Help Desk. CERT-

Fin may provide Incident Prevention and Response services as well as Security Quality Management Services. It may carry out functions similar to CERT-In that operate at a national level, for priority cyber security in financial sector.

- There are a number of processes which need to be established by CERT-Fin in order to deliver its services. These processes and services should be in the lines of the objectives defined for CERT-Fin and its constituency as delineated in the Report.
- CERT-Fin should offer policy suggestions for strengthening financial sector cyber security to all stakeholders including Regulators/Government.
- To promote cyber-security awareness on a mass scale, various public and private organizations may be involved in this regard to take forward the cause of promoting cyber security in the financial sector, in specific areas.
- CERT-Fin should be sufficiently equipped with state-of-the-art infrastructure to cater to the requirements of cyber security in the financial sector. Technology components for each area need to be identified and deployed appropriately as per the process set up for the various services, It should be ensured that state of the tools and technologies are deployed and these go through proper maintenance regularly.
- The software used by all stakeholders need to be updated (OEM standard) on regular basis to make up with modern technology, if the financial sector regulators want to remain ahead of cyber security attacks.
- The proposed CERT-Fin may be funded by all financial sector regulators. This may continue initially, say for five years or so till its maturity, after which CERT-Fin can chalk out a feasible long-term self-reliant funding strategy looking at FS-ISAC, EFI-ISAC, ISAC-JP models. RBI may act as a lead regulator and can play an active role in conceptualising, rolling out and steering the activities of the CERT-Fin in the initial years as an incubator. A Techno-Economic analysis of the proposed alternative 2 mentioned in chapter 3 of the report may be carried out to assess the requirements related to funding, manpower, infrastructure, etc. The analysis may articulate the parameters for manner and quantum of contribution which may in turn determine the structure of governance of the proposed CERT Fin.
- There is an urgent need to give attention (i) for more quality training and certification programs including online programs in the cyber security area (ii) to develop manpower with expertise in cyber security product development and cyber operations (iii) to conduct research programs and develop curriculum in order to innovate research deliverables in cyber security space to protect Indian infrastructure.
- Utilize the expertise in the leading institutions in the process of building up CERT-Fin and that wider consultation with leading technology institutes including IITs, Indian Institute of Science, etc may be useful to work out the technical details and chart out a long term plan in Indian context. All the financial sector regulators may train their manpower on cyber security in their respective domains in leading technology institutions.

- To develop necessary critical manpower infrastructure as also to improve the employability of youth at the bottom of the pyramid, the nation should optimally utilize the infrastructure available in Government, private institutions and the Industry by developing appropriate courses that can be worked out in consultation with CERT-In.
- The proposed CERT-Fin may be equipped with best available talent with highly skilled professionals, who may either be deputed from Regulators or other leading institutions, specialized in cyber security in our Country at market linked rates as per the requirements. The proposed CERT-Fin and sub sectoral financial CERTs may have at least one IT expert and one domain expert for reporting cyber security incidents to CERT-In/CERT-Fin. The personnel may have in-depth expertise in IT security and analysis. To start with, one domain expert and one subject expert from each sub-sector CERTs may be deputed to CERT-Fin for facilitating information sharing. A CEO/Director may also be sent on deputation basis to proposed CERT-Fin at the initial stage. In addition, CERT-Fin may have a representative not below the rank of Deputy Secretary from DG, CERT-In's office to further guide the activities of CERT-Fin, in accordance with IT Rules 2014.
- There is a need to identify protected systems/ critical infrastructure in the financial sector, for which CERT-Fin should play an important role in coordination with sub-sectoral CERTs and NCIIPC.
- A workshop may be held with all stakeholders and scholars specialized in the area of cyber security, leading academic and technology institutions for feedback on the recommendation of the Working Group. Public consultations on the Report may be considered by placing the Report in public domain for comments/ feedback.
- Major activities and processes to implement and operationalize CERT-Fin, with RBI as lead Regulator has been provided at Annex-II of the report. All the financial sector regulators may complete simultaneously strengthening of their cyber security framework in their respective domain including setting up sub-sectoral CERT-Fins by the time CERT-Fin is functional, in a time bound manner.
- After say, two to three years, a comprehensive review of CERT-Fin should be done in FSDC forum. The FSDC-SC may closely monitor on a regular basis and guide the advisory board in this regard
- CERT-Fin shall have tie-ups with various financial CERTS/FS-ISACs operating internationally to adopt international best practices in its functioning. To achieve this objective, CERT-In and MeitY can play a significant role.
- A Standing Technical Sub Committee on CERT-Fin & Tel-CERT may be operationalized so that there is continuous flow of information between these CERTs to address the inter-linkages between financial and telecom sector cyber incidents and develop ways and means to address the telecom related cyber security issues in the financial sector.
- There is a need to safeguard financial infrastructure from cyber security risks, which require coordinated efforts throughout, including cyber risk insurance.



# **CHAPTER 1**

## CHAPTER 1

### Introduction

#### 1.1. Financial Sector In India

1.1.1 India's diversified financial sector that includes institutions, markets and infrastructure has been expanding rapidly, especially over the recent past. Institutions comprise banks, insurance companies, non-banking financial companies, stock exchanges, clearing corporations, depositories, mutual funds, pension funds and other financial entities<sup>1</sup>.

1.1.2 Ours is a bank dominated financial sector and commercial banks account for over 60 per cent of the total assets of the financial system followed by the Insurance. Other bank intermediaries include regional rural banks and cooperative banks that target under serviced rural and urban populations. Under the differentiated licensing approach adopted by the Reserve Bank of India, Payment Banks and Small Finance Banks have also been licensed and a few of them are in their first year of operations. Many non-banking finance companies (NBFCs) operate in specialized segments (leasing, factoring, micro finance, infrastructure finance), though some can accept deposits<sup>2</sup>. There are Development Financial Institutions and housing finance companies as well. Major markets include Foreign Exchange Market, Call money market, Government Securities market, Capital Market – equity as well as debt and Commodities market. The financial system also includes a range of financial market infrastructures (FMIs), such as payment systems, clearing houses, central counterparties, securities settlement systems, and securities depositories. The sectoral composition of the Indian financial system is as below<sup>3</sup>:

<b>Institution</b>	<b>Share in combined financial assets</b>
Banking system	63%
Insurance companies	19%
Non-banking financial institutions	8%
Mutual funds	6%
Provident and pension funds	4%
<b>Total</b>	<b>100%</b>

Source: FSB Peer Review Report of India 2016

1.1.3 The regulation and supervision of the financial system in India is carried out by different regulatory authorities. The supervisory role of the RBI covers commercial banks, urban cooperative banks (UCBs), some financial institutions and non-banking finance companies (NBFCs). Some of the financial institutions, in turn, regulate or

<sup>1</sup> India.RBI, Perspective on Banking in India, May 2013

<sup>2</sup> IMF. India: Financial System Stability Assessment update, January 2013

<sup>3</sup> FSB Peer Review Report of India 2016

supervise other institutions in the financial sector, for instance, Regional Rural Banks and the rural Co-operative banks are supervised by National Bank for Agriculture and Rural Development (NABARD); and housing finance companies by National Housing Bank (NHB). Ministry of Company Affairs (MCA), Government of India regulates deposit taking activities of corporate, other than NBFCs registered under the Companies Act, but not those which are under separate statutes. The Registrar of Cooperatives of different States in the case of single State cooperatives and the Central Government in the case of Multi-State Cooperatives are joint regulators, with the RBI for UCBs, and with NABARD for rural cooperatives. Whereas RBI and NABARD are concerned with the banking functions of the cooperatives, their management control rests with the State/ Central Government. The capital market, mutual funds, and other capital market intermediaries are regulated by Securities and Exchange Board of India (SEBI) whereas insurance sector and pension funds are regulated by Insurance Regulatory and Development Authority (IRDA) and the Pension Funds Regulatory and Development Authority (PFRDA) respectively.<sup>4</sup> All these regulators have a key mandate to protect the interests of customers - who could be depositors, investors, policy holders or pension fund subscribers, depending on the product. Some of the functions carried out by banks and other financial institutions at times come under the purview of different regulators. As the financial system evolves, the interdependence among various institutions, markets and other critical infrastructure increases.

## **1.2. Emerging importance of Fin Tech and Cyber security in India**

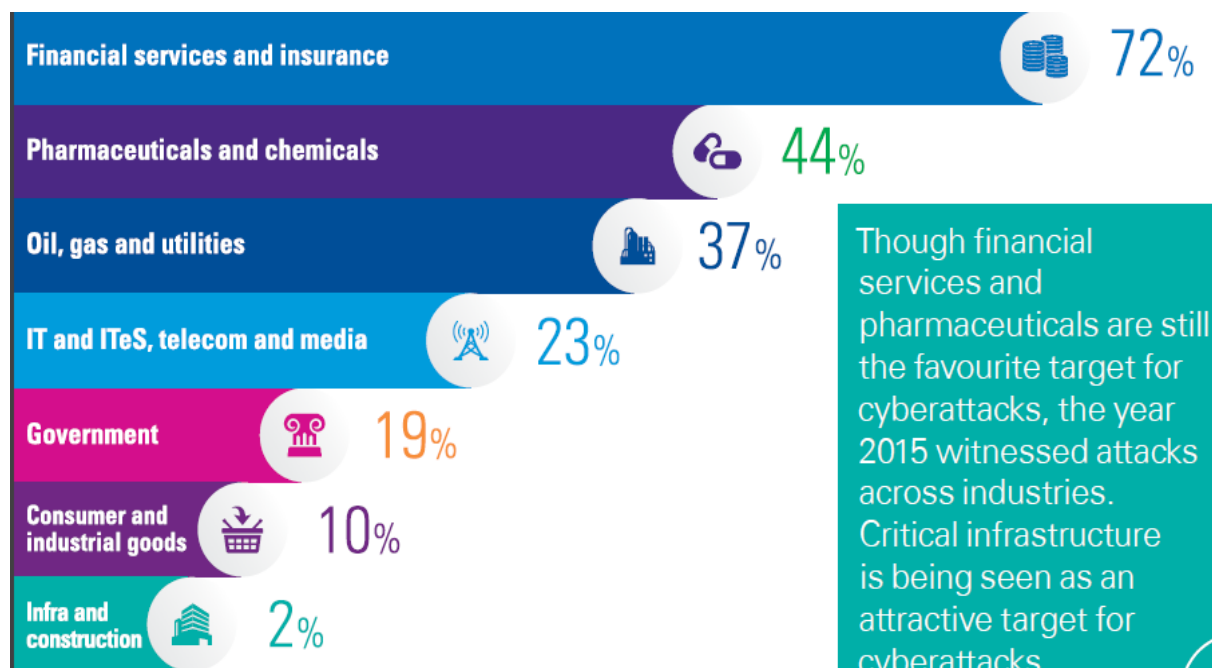
1.2.1. The financial sector plays a crucial role in the socio-economic progress of India. In the recent times, the financial sector has become increasingly dependent on the Information and Communication Technology (ICT), offering new and innovative delivery channels for customers. Customer expectation is driving further changes in the way in which banks operate and offer various products. The Working Group noted that the exponential pace of penetration of technology in the financial sector is leading to a perceived democratization of financial services through technology-driven innovation in the sector.

1.2.2. At the same time, financial sector cyber security concerns, both in India and abroad is increasing and several cyber incidents have come to notice in recent times. The same ICT which facilitates innovation is also being used by malicious actors for carrying out cyber-attacks and other malicious cyber activities. Cyber-attacks and malicious cyber activities in the financial sector have the potential of loss of money to the customer and/or bank, it affects institution's reputation, impacts the economy, besides creating trust deficit. Financial Institutions are conscious of such potential threats and have been taking several measures to protect the customers as well as their systems. Regulators world over are mandating several security related measures on their regulated entities. As such, banks and other financial institutions have stepped up

---

<sup>4</sup> Working Paper on Benchmarking Indian Regulatory Practices to the G20 Financial Reforms by RBI

their focus on cyber security and have been allocating higher budgets for cyber-security. Forbes has estimated the combined spending on cyber security of just a few major banks (J.P. Morgan, Bank of America, Citibank and Wells Fargo) was to the tune of US \$500 billion in 2016<sup>5</sup>. According to a research report from IBM approximately 20 million financial records were breached in 2015 and it costed the financial institutions an average of US\$ 215 per stolen record<sup>6</sup>. The following diagram shows the industry/sectors that are targets of cyber-crime as per the analysis carried out on the basis of KPMG India's cybercrime survey, 2015.



Source: KPMG India's crime survey 2015

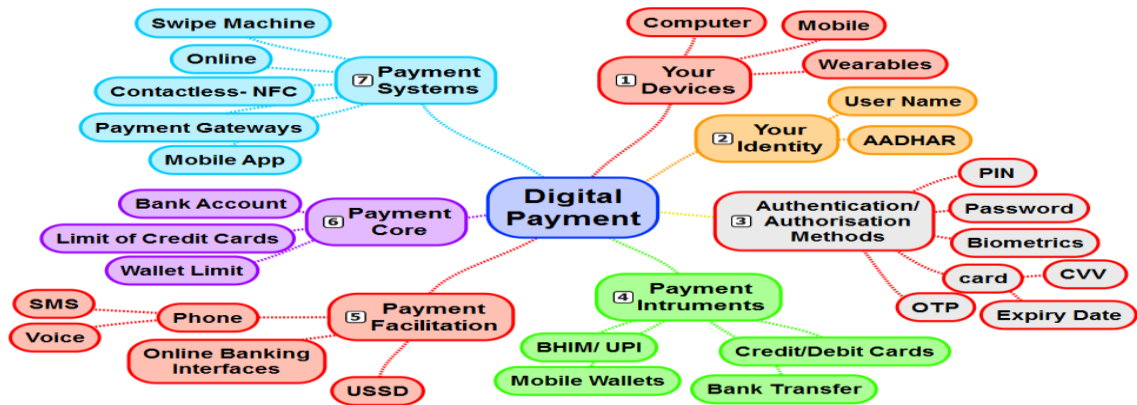
1.2.3. In India, we are going through a special phase in the digitisation process. As indicated in the Economic Survey 2016-17, Government has been encouraging to adopt digital payments and receipts. Digital transactions help bring people into the modern "wired" era and they bring people into the formal economy, thereby increasing financial saving, reducing tax evasion, and leveling the playing field between tax-compliant and tax-evading people. Digitalization can broadly impact three sections of society: the poor, who are largely outside the digital economy; the less affluent, who are becoming part of the digital economy having acquired Jan Dhan accounts and RuPay cards; and the affluent, who are fully digitally integrated via credit cards. One simple measure that illustrates the size of these three categories is cell phone ownership. There are approximately 350 million people without cellphones (the digitally excluded); 350 million with regular "feature" phones, and 250 million with smartphones.<sup>7</sup>

<sup>5</sup> <https://www.massivealliance.com/2016/07/27/4-largest-cyber-threat-fears-banking-industry/>

<sup>6</sup> <https://securityintelligence.com/the-new-bank-heist-the-financial-industrys-top-threats/>

<sup>7</sup> Economic Survey 2016-17

### Digital Payments Ecosystem

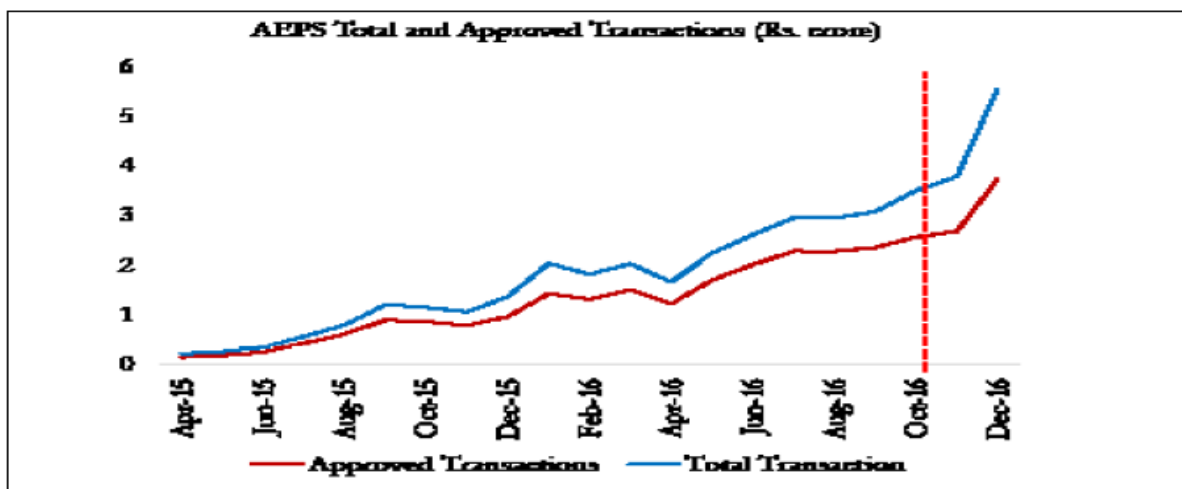


Source: MeitY

1.2.4. Recently, Government has taken a number of steps to facilitate and incentivize the move to a digital economy which include (a) Launch of the BHIM (Bharat Interface For Money) app for smartphones which is based on the new Unified Payments Interface (UPI). This has created inter-operability of digital transactions. The 250 million digital-haves can use their smartphone to make simple and quick payments (b) Launch of BHIM USSD 2.0, a product that allows the 350 million feature phone users to take advantage of the UPI (c) Launch of Aadhaar Merchant Pay, aimed at the 350 million who do not have phones. (d) Reductions in fees (Merchant Discount Rate) paid on digital transactions and transactions that use the UPI (e) Encouraging the adoption of Point of Sale (POS) devices beyond the current 1.5 million, through tariff reductions. There have also been relaxations of limits on the use of payment wallets. Tax benefits have also been provided for to incentivize digital transactions.

1.2.5. It is observed that Aadhaar-Enabled Payments System (AEPS) transactions have been steadily rising.

Digital transactions (Rs crore) of digitally excluded



Source: Economic Survey & NPCI

1.2.6. As people have started to use such e-payment systems, they have discovered that it is more convenient to conduct financial activities electronically. Eventually with the process gaining momentum, technology would be adopted by a large section of population for which the digital payments are to be made secure. With literacy levels of people adopting technology not being at the same level and with increased volume and velocity of the digital data in the financial sector attributable to the ICT penetration and innovation, the Working Group noted that the sector needs to address this growing and challenging need of ensuring adequate cyber security. Therefore, the stakeholders need to proactively embrace cyber-hygiene on the one hand and a formal and professional approach to prevent, monitor, detect, respond and recover from cyber-incidents, apart from having a state of the art cyber security infrastructure, in financial institutions.

### **1.3. Discussions in international fora on Fin Tech and Cyber Security**

1.3.1. Cyber Security as a topic is in the mainstream in the recent past and likely to continue so in the coming days. Many studies reveal that cyber security is one of the aspects receiving the attention of most of the Boards of companies. World Economic Forum 2017<sup>8</sup> held in Switzerland observed that cyber-security is at the top of the list of business risks and not just for the financial sector. This underlines the vulnerabilities faced by the financial sector. World Economic Forum<sup>9</sup> 2017 held in Davos discussed cyber-security related issues at length and published a document<sup>10</sup> titled “Advancing Cyber Resilience: Principles and Tools for Boards,” put together by a Working Group including many stakeholders in collaboration with the Boston Consulting Group and Hewlett Packard Enterprise. ‘Promote Cyber Resilience’ is one of the themes advocated by the publication<sup>11</sup>.

1.3.2. Building on President Obama and President Xi’s historic agreement on state activity in cyberspace during President Xi’s State Visit to Washington, D.C. in September 2015, G20<sup>12</sup> acknowledged the risk of cyber threats to the collective ability to use the Internet to bolster economic growth and development. The G7 also identified Cyber-security Strategy and Framework, Governance, Risk and Control Assessment, Monitoring, Response, Recovery and Information Sharing as the fundamental elements of cyber security.

1.3.3. The Committee on Payments and Market Infrastructures (CPMI) and the Board of the International Organization of Securities Commissions (IOSCO) released the final report on ‘Guidance on cyber resilience for financial market infrastructures’ (“Cyber

---

<sup>8</sup> World Economic Forum, Why India’s move toward a cashless society could increase cybercrime, 2017, <https://www.weforum.org/agenda/2017/03/why-indias-move-toward-a-cashless-society-could-increase-cybercrime>

<sup>9</sup> World Economic Forum, Advancing Cyber Resilience: Principles and Tools for Boards, 2017, [http://www3.weforum.org/docs/IP/2017/Adv\\_Cyber\\_Resilience\\_Principles-Tools.pdf](http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf)

<sup>10</sup> World Economic Forum, What cyber security insiders discussed at davos, 2017, <https://www.weforum.org/agenda/2017/02/what-cyber-security-insiders-discussed-at-davos-2017>

<sup>11</sup> World Economic Forum, The year cybersecurity went mainstream, 2017 <https://www.weforum.org/agenda/2017/03/cyberattacks-are-everybodys-business-why-cybersecurity-is-now-top-of-the-agenda-for-the-worlds-decision-makers>

<sup>12</sup> Whitehouse.gov, FACT SHEET: The 2015 G20 Summit in Antalya, Turkey dated April 14, 2017

Guidance”) on 29 June 2016. The Cyber Guidance was the first internationally agreed guidance on cyber security for the financial industry. It has been developed against the backdrop of a rising number of cyber-attacks against the financial sector and in a context where attacks are becoming increasingly sophisticated. Key concepts built into the Cyber Guidance included the following:

- (i) Sound cyber governance is key. Board and senior management attention is critical to a successful cyber resilience strategy.
- (ii) The ability to resume operations quickly and safely after a successful cyber-attack is paramount.
- (iii) Financial market infrastructures (FMIs) should make use of good-quality threat intelligence and rigorous testing.
- (iv) FMIs should aim to instil a culture of cyber risk awareness and demonstrate ongoing re-evaluation and improvement of their cyber resilience at every level within the organisation.
- (v) Cyber resilience cannot be achieved by an FMI alone; it is a collective endeavour of the whole “ecosystem”.

1.3.4. Financial Technology (Fin Tech) is defined as technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions on provision of financial services. The financial technology (Fin Tech) landscape continues to evolve, with some new applications of technology already launched and others still in their infancy. In the first nine months of 2016, global investment in Fin Tech reached USD 21 billion, marking a five-fold increase over 2013<sup>13</sup>. Much of these investments are concentrated in the United States and in Asia, where large and successful Fin Tech firms operate in the payments and lending space, and new investment is going into insurance, block chain and wealth management. While there is currently limited evidence regarding risks to financial stability emanating from Fin Tech developments, changes in this regard is rapid and decisions taken at this early stage may set important precedents. Therefore, there is a need to assess how Fin Tech developments intersect with regulatory frameworks, with the objective of facilitating benefits while mitigating risks.

1.3.5 Fin Tech or the emerging integration of financial businesses and information technologies, could transform the industry and the market by providing a range of innovative services to customers. Today, cyber security is becoming one of the highest priorities in securing financial stability. To foster Fin Tech and maximize its contribution to the economy as a whole, constructive and interactive communication among wide range of players, including those affiliated with traditional finance industry is required. While Fin Tech is necessary to increase efficiency, manage risk better and create new opportunities, a smart financial centre must be a safe financial centre.

---

<sup>13</sup> Citi, “Digital Disruption – Revisited: What FinTech VC Investments Tell us About a Changing Industry,” January 2017; Accenture, “Fintech and the evolving landscape: landing points for the industry,” April 2016.

1.3.6. The Financial Stability Board (FSB) is an international body that promotes international financial stability; it does so by coordinating national financial authorities and international standard-setting bodies as they work toward developing strong regulatory, supervisory and other financial sector policies. It fosters a level playing field by encouraging coherent implementation of these policies across sectors and jurisdictions. The FSB, working through its members, seeks to strengthen financial systems and increase the stability of international financial markets.

1.3.7. FSB recognises that today, the susceptibility of financial activity to cyber-attacks is likely to be higher the more the systems of different institutions are connected. In general, greater use of technology and digital solutions expand the range and number of entry points cyber hackers might target. In this regard, some Fin Tech activities may spread data across a larger number of institutions, for example, via increased use of digital wallets and e-aggregators.

1.3.8. The risk of cyber threats to the collective ability to use the internet to bolster economic growth and development has also been recognised in G20 forum. It has been affirmed at this forum that the international law applies to state conduct in cyberspace and has been committed that all states should abide by norms of responsible state behaviour in cyberspace. It has also been affirmed that no country should conduct or support cyber-enabled theft of intellectual property with the intent of providing competitive advantages to companies or commercial sectors. The digitalisation of the finance branch is an inextricable part of globalisation with all its pros and cons. On the one hand it provides for swift and affordable access to cash and financial services, but on the other, cyber-attacks can seriously damage the global interconnected financial sector.

1.3.9. Recognising the serious ramifications of cyber-related incidents on the financial sector, group of G 7 Countries has also released a non-binding, high-level fundamental elements of cyber-security designed for financial sector in October 2016. It has identified Cyber-Security Strategy and Framework, Governance, Risk and Control Assessment, Monitoring, Response, Recovery and Information Sharing, continuous learning as the fundamental elements. Increasing sophistication, frequency, and persistence, cyber risks are recognised to be growing more dangerous and diverse, threatening to disrupt our interconnected global financial systems and the institutions that operate and support those systems. To address these risks, the above nonbinding, high-level fundamental elements are designed for financial sector private and public entities to tailor to their specific operational and threat landscape, role in the sector, and legal and regulatory requirements. G 7 feels that public authorities within and across jurisdictions can use the elements as well to guide their public policy, regulatory, and supervisory efforts and working together, informed by these elements, private and public entities and public authorities can help bolster the overall cybersecurity and resiliency of the international financial system.



## 1.4. Addressing Cyber Security in Indian financial sector

### 1.4.1 The Working Group took stock of the various initiatives taken towards cyber

#### *Government Initiatives for Indian Cyber Security Ecosystem – Current Status*

#### Cyber Security & Privacy: Ecosystem, Policies, Laws & Initiatives

##### National Cyber Security Framework

- 2008 Amendment to Information Technology Act, comprehensive provisions for cyber crimes
- 2012 Joint Working Group for P-P-P on cyber security
- 2013 Recognition of country as 'authorizing nation' under CCRA product certification scheme
- National cyber security policy
- 2013 to 2015 NCIIPC- Critical Infrastructure Protection
- National Cyber Security Coordinator
- 2016 RBI Cyber Security Framework
- 2016 State Cyber Security Policies – Telangana and AP
- 2017 IRDAI Cyber Security Framework

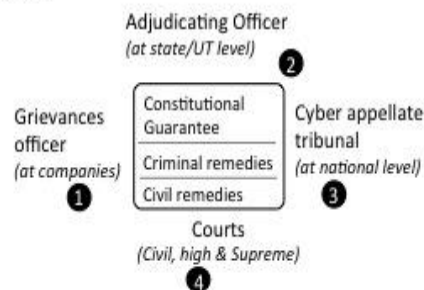
##### Law enforcement capability building (Industry Contribution)

- Last 3 years
- Capability building program for handling cyber crime / security breach
  - Technical infrastructure, skills and facilities
  - Public-private- partnership model in training police officers

##### Data Protection

- 2008 IT (Amendment) Act has specific clauses for clauses for privacy
- 2011 Notification of privacy rules, defining content, enforcement & compliance norms
- 2017 New Data protection law in making

##### Elements of protection & tiered structure for data protection



#### Existing Cyber Security Initiatives-India

##### Policy Initiatives & Guidelines

- National Policies on IT, Telecom and Electronics - 2012
- National Cyber Security Policy -2013
- Guidelines for Critical Information Infrastructure Protection -2013
- National Information Security Policy & Guidelines - 2014
- Draft IoT policy - 2014
- M2M (machine-to-machine) Roadmap document – 2015
- Security and Privacy Framework for Smart Cities (2016)
- State Cyber Security Policies (Telangana and AP) – 2016
- MeitY Cloud Accreditation Framework - 2017

##### Regulatory Framework

- Information Technology (Amendment) Act, 2008
- Regulatory Framework issued by regulators such as
  - Reserve Bank of India (RBI),
  - Telecom Regulatory Authority of India (TRAI),
  - Securities and Exchange Board of India (SEBI),
  - Insurance Regulatory and Development Authority (IRDA)

##### Institutional Mechanisms

- NCSC (PMO); NCIIPC (NTRO)
- CERTs (Fin-CERT and Power Sector CERT announced)
- Industry - DSCI (Policy, Assurance, Capacity Building and Awareness)
- Joint Working Group (PPP)
- Sector Skill Council (Skills)
- IB-CART (Information Sharing)
- ISEA (Capacity Building and Awareness)
- Cyber Forensic Lab (Capacity Building)
- LITD 17 Committee of BIS (Standards)

Source: Ministry of Electronics & Information Technology

security in India, in general and in the financial sector, in particular. The Indian Computer Emergency Response Team (CERT-In) was formed in the year 2004 to

respond to computer security incidents and it derives its power from Information Technology Act. The IT Act empowers CERT-In to carry on the following functions:

- i. Collection, analysis & dissemination of information on cyber incidents.
- ii. Forecast and alerts on cyber security incidents.
- iii. Emergency measures on cyber security incidents.
- iv. Coordination for cyber incident response activities.
- v. Issue guidelines, advisories, vulnerability and white papers relating to information security
- vi. Such other functions relating to cyber security as may be prescribed.

1.4.2. The National Cyber Security Policy for India was released by Ministry of Communication and Information Technology in the year 2013 with a vision to build a secure and resilient cyberspace for citizens, businesses and Government. The mission of the Policy is to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation. A detailed discussion on CERT-In and other sectoral CERT that exists in India is dealt in chapter 2.

1.4.3. Recognising that Cyber Security is a growing area of concern and priority in the emerging scenario, to get clarity on the need and role of financial sector CERT, a meeting on Fintech, Digital Innovations and Cyber Security was convened in Department of Economic Affairs (DEA) on 3rd January, 2017 with DG, CERT-In wherein it was informed that the CERT-In is in operation since 2004 and Section 70 B of the IT Act 2000 provides for CERT-In to serve as the National agency for cyber security incident response.

**Section 70 B of the IT Act 2000** provides for CERT-In to serve as the National agency for cyber security incident response. The National Cyber Security Policy (NCSP) 2013, Section IV – Strategies, Part E, Point 3 envisages to operationalize 24x7 sectoral CERTs for all coordination and communication actions within the respective sectors for effective incidence response & resolution and cyber crisis management. The NCSP recognizes the importance of sectoral CERTs as a ‘Strategy’ for ‘Security threat early warning, vulnerability management and response to security threats.’ It also envisages CERT-In to function as a nodal agency for coordination of all efforts for cyber security emergency response and crisis management and CERT-In will function as an umbrella organization in enabling creation and operationalization of sectoral CERTs as well as facilitating communication and coordination actions in dealing with cyber crisis situations. Rule 10 of the IT (CERT-In – manner of performing function and duties) Rules 2013, mentions that CERT-In shall interact with and seek assistance from the sectoral CERT for cyber security incident response and prevention.

1.4.4. It was observed that sector specific CERTs have been permitted under the Information Technology Act, 2000 and Rules framed under the Act, and CERT-In assists the Ministries and Departments of the Central Government and the Central Public Sector Undertakings to establish sectoral CERTs. Such sectoral CERTs need to have a fair degree of independence in its functioning to timely report back all cyber incidents to

CERT-In. It was felt that CERT-In and the Ministry of Electronics & Information Technology (MeitY) need to work in close coordination with DEA for strengthening the financial sector cyber security through helping in setting up of financial sector specific CERT i.e., CERT-Fin, the need for which was felt unanimously.

1.4.5. Subsequently, Financial Stability & Development Council (FSDC), the apex financial sector body under Chairmanship of Hon'ble Finance Minister and all financial sector regulatory heads as its members, in its 16<sup>th</sup> meeting held on 5<sup>th</sup> January 2017, deliberated on a DEA agenda on "Fin Tech, digital innovations and Cyber security" and recognised the need for a fully functional Computer Emergency Response Team in Financial Sector (CERT-Fin). The Council agreed that CERT-Fin needs to be established to work towards strengthening cyber security in the financial sector in close coordination with all financial sector regulators and CERT. It advised that detailed modalities may be worked out in consultation with Ministry of Electronics & Information Technology (MeitY) and all financial sector Regulators.

### **1.5 Budget Announcement on CERT-Fin & setting up of Working Group on CERT-Fin**

1.5.1. The Hon'ble Finance Minister in Para.101 of his Budget Speech 2017-18, announced that "cyber security is critical for safeguarding the integrity and stability of our financial sector and announced that a Computer Emergency Response Team for our Financial Sector (CERT- Fin) will be established. This entity will work in close coordination with all financial sector regulators and other stakeholders".

1.5.2. Pursuant to the above announcement, a Working Group was set up to study and recommend measures for setting up of computer emergency response system in the financial sector and submit its report to the Department within a period of two months, with the composition as below:-

<i>Dr. Sanjay Bahl, Director General, CERT-In, Ministry of Electronics &amp; Information Technology, Government of India</i>	<i>Chairperson</i>
<i>Dr. C. S. Mohapatra, Advisor (Financial Sector), Department of Economic Affairs, Ministry of Finance, Government of India</i>	<i>Member</i>
<i>Smt. Anjana Dube, Deputy Director General, Department of Financial Services, Ministry of Finance, Government of India</i>	<i>Member</i>
<i>Ms. Tulika Pandey, Scientist 'F', Ministry of Electronics &amp; Information Technology, Government of India</i>	<i>Member</i>
<i>Smt. Meena Hemchandra, Executive Director, Reserve Bank of India</i>	<i>Member</i>
<i>Shri. S. V. Murali Dhar Rao, Executive Director, Securities &amp; Exchange Board of India</i>	<i>Member</i>
<i>Shri A.R. Nithyanantham, Chief General Manager, Insurance Regulatory &amp; Development Authority of India</i>	<i>Member</i>
<i>Shri Satya Ranjan Prasad, Executive Director, Pension Fund Regulatory &amp; Development Authority of India</i>	<i>Member</i>
<i>Dr. A.S. Ramasastri, Director, Institute for Development &amp; Research in</i>	<i>Member</i>

<i>Banking Technology</i>	
<i>Shri A.P. Hota, Managing Director &amp; Chief Executive Officer, National Payment Corporation of India</i>	<i>Member</i>
<i>Shri Nandkumar Saravade, Chief Executive Officer, Reserve Bank Information Technology Pvt Ltd</i>	<i>Member</i>

1.5.3. The terms of reference of the Working Group include (i) To study the existing cyber security measures and Computer Emergency Response system in the Financial Sector in India (ii) To study the best practices followed in the field of cyber security in financial sector across the World vis-à-vis Indian scenario, (iii) To suggest a suitable structure for setting up a CERT-Fin to strengthen the cyber security in the financial sector to work as sectoral CERT under close coordination with all financial sector related stakeholders & the CERT-In, which is the umbrella organization created under the Information Technology Act. While, CERT-In will provide necessary technical inputs, FSDC Secretariat, DEA will provide secretarial assistance to the Working Group.

1.5.4. The Working Group held its meetings on 22<sup>nd</sup> March 2017, 5<sup>th</sup> April 2017, 5<sup>th</sup> May, 2017 and 24<sup>th</sup> May 2017, besides a workshop for all financial sector Regulators to develop clarity on the functioning of CERT-In and the existing framework, in the office of DG, CERT-In, on 5<sup>th</sup> April 2017. The Working Group submitted its report titled “Report of the working Group for setting up of Computer Emergency Response Team in the financial sector” along with recommendations arrived at unanimously, by all the members, after detailed discussion & deliberations.

## **CHAPTER 2**

## CHAPTER 2

# Existing Cyber Security Structure in India

The Working Group in its first meeting held on 22<sup>nd</sup> March 2017 decided to study the existing cyber security structure in Indian financial sector. It noted that Indian Computer Emergency Response Team (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC) are the national agencies with latter taking all measures including associated research and development for protected systems of Critical Information Infrastructures in India. The Group also noted that the financial sector regulators have been taking various initiatives to address cyber security in their respective domain, in consultation with CERT-In. In this context, the Group developed understanding on the working of CERT-In and NCIIPC in general and the initiatives taken by financial sector regulators such as RBI, SEBI, IRDAI & PFRDA in addressing cyber security.

### 2.1. CERT- In- An overview

2.1.1. As indicated in para 1.4.1 of chapter 1, the CERT-In under the Ministry of Electronics and Information Technology (MeitY) was established in 2004, to help organisations / departments handle and respond to cyber security incidents. Section 70 B of the IT Act 2000 (amended 2008) provides for CERT-In to serve as the National agency for cyber security incident response. As already highlighted in chapter 1, it is entrusted with the following functions:-

- i. Collection, analysis & dissemination of information on cyber incidents.
- ii. Forecast and alerts on cyber security incidents.
- iii. Emergency measures on cyber security incidents.
- iv. Coordination for cyber incident response activities.
- v. Issue guidelines, advisories, vulnerability and white papers relating to information security
- vi. Such other functions relating to cyber security as may be prescribed.

2.1.2 CERT-In creates awareness on security issues through dissemination of information on its website ([http:// www. cert-in.org.in](http://www.cert-in.org.in)) and operates 24x7 incidence response Help Desk. (Toll free number +91-1800-11-4949; [incident@cert-in.org.in](mailto:incident@cert-in.org.in)). CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services. It carries out the following roles:

#### Reactive

- Provide a single point of contact for reporting local cyber security incidents.
- Assist the organisational constituency and general computing community in preventing and handling computer security incidents.

- Share information and lessons learned with other CERTs, response teams, organisations and sites.
- Incident Response.
- Provide a 24 x 7 security service.
- Offer recovery procedures.
- Artifact analysis
- Incident tracing

#### Proactive

- Issue security guidelines, advisories and timely advice.
- Vulnerability analysis and response
- Risk Analysis
- Collaboration with vendors
- National Repository of, and a referral agency for, cyber-intrusions.
- Profiling attackers.
- Conduct Training
- Interact with vendors and others at large to investigate and provide solutions for incidents.

#### Reporting

- Central point for reporting incidents
- Database of incidents

#### Analysis

- Analysis of trends and patterns of intruder activity
- Develop preventive strategies for the whole constituency
- In-depth look at an incident report or an incident activity to determine the scope, priority and threat of the incident.

#### Response

- Incident response is a process devoted to restoring affected systems to operation
- Send out recommendations for recovery from, and containment of damage caused by the incidents.
- Help the System Administrators take follow up action to prevent recurrence of similar incidents.

2.1.3. Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre <http://www.cyberswachhtakendra.gov.in>) has been launched by CERT-In on February 21, 2017 for detection of compromised systems in India and to notify, enable cleaning and securing systems of end users to prevent further malware infections. The centre is working in close coordination and collaboration with Internet Service Providers, Academia and Industry. The centre is providing detection of malicious programs and free tools to remove the same for common users. The centre is also working with 37 Banks to detect malware infections in their networks and enable remedial actions.

2.1.4. As part of Cyber Security Assurance, under Security Assurance Framework, CERT-In has empanelled 32 auditors to carry out information security audit, including the vulnerability assessment and penetration test of the networked infrastructure of government and critical sector organizations. Government and critical sector organizations are implementing the security best practices in accordance with ISO 27001 standard and as per the advice issued by CERT-In. Services of CERT-In empanelled IT security auditors are being used to verify compliance.

2.1.5. CERT-In has requested RBI to carry out audits through empanelled auditors for all digital wallets to ensure their security posture. CERT-In has sent an advisory to the banks to put in place robust mechanisms to detect and report cyber security incidents to CERT-In by ensuring round the clock monitoring and surveillance and to periodically conduct audits, vulnerability assessment and penetration testing for all the critical systems. Letter has also been sent by CERT-In to Payment Banks and PPIs to nominate Chief Information Security Officers and report cyber security incidents without delay.

2.1.6. A Crisis Management Plan (CMP) for countering cyber-attacks and cyber terrorism for implementation by all Ministries/Departments of Central Government, State Governments/UTs and their organizational units in critical sectors has been formulated. In addition, several guideline documents and templates have been published to assist development and implementation of sectoral Crisis Management Plans. CMP for countering Cyber-Attacks and Cyber Terrorism is updated periodically on annual basis to take into account changing scenario of cyber threat landscape. The 6th version of CMP (2015 version) has been circulated to all the key Central Government Ministries/Departments and States/UTs. CERT-In is regularly conducting workshops for Central Ministries, Departments, States & UTs and critical organizations to sensitize them about the cyber security threat landscape and enabling them to prepare and implement the Cyber Crisis Management Plan.

2.1.7. Cyber Security Mock Drills are being conducted by CERT-In to help the organisations to assess their preparedness to withstand cyber-attacks. These drills have helped tremendously in improving the cyber security posture of the information infrastructure and training of manpower to handle cyber incidents, besides increasing the cyber security awareness among the various sectors of Indian economy i.e. Defence, Paramilitary forces, Space, Atomic Energy, Telecommunications (ISPs), Finance, Power, Oil & Natural Gas, Transportation (Railways & Civil Aviation), IT/ITeS/ BPO sectors and Data Centres from Government/Public/ Private. The mock drill helps the participating organizations to:

- Evaluate the effectiveness of their security processes and procedures
- Measure their attack detection, response, mitigation and recovery capabilities
- Create awareness besides imparting training and education for responding to cyber security incidents
- Promoting cross-sector and critical infrastructure relationships/ partnerships



- Identifying preparedness gaps
- Addressing gaps by improving processes, communication and information sharing
- Enhancing response to cyber incidents
- Reducing cyber risk

2.1.8. As part of security awareness, skill development and training, CERT-In is regularly conducting trainings / workshops to train officials of Government, critical sector, public/industry sectors, financial & banking sector and ISPs on various contemporary and focused topics of Cyber Security. CERT-In conducts regular training programme to make the network and system administrators aware about securing the IT infrastructure and mitigating cyber-attacks. CERT-In has published guidelines for securing IT infrastructure, which are available on its website ([www.certin.org.in](http://www.certin.org.in)).

2.1.8.1. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities along with countermeasures to create awareness among stakeholders to take appropriate measures to ensure safe usage of digital technologies. These advisories also cover security safeguards for POS, Micro ATMs, electronic wallets, online banking, smart phones, unified payment interface, wireless access points/routers, mobile banking and cloud. The specific advisories issued for these are - securing mobile banking; mobile and cloud security; online payments through Unified Payment Interface (UPI); securing biometric devices; personal online security; securing wireless hotspots; Aadhaar Enabled Payment System; securing web browsers; multiple vulnerabilities in Google Android OS and Apple IOS; security of POS Systems; securing online banking; security of e-wallets; securing Wireless Access Points/Routers, secure payment through Rupay card; security of Micro ATMs; safeguarding smartphones against cyber-attacks, USSD based mobile banking, securing USB Devices, securing SIM cards, secure use of credit/debit cards, safeguarding online identity and mobile payment channels.

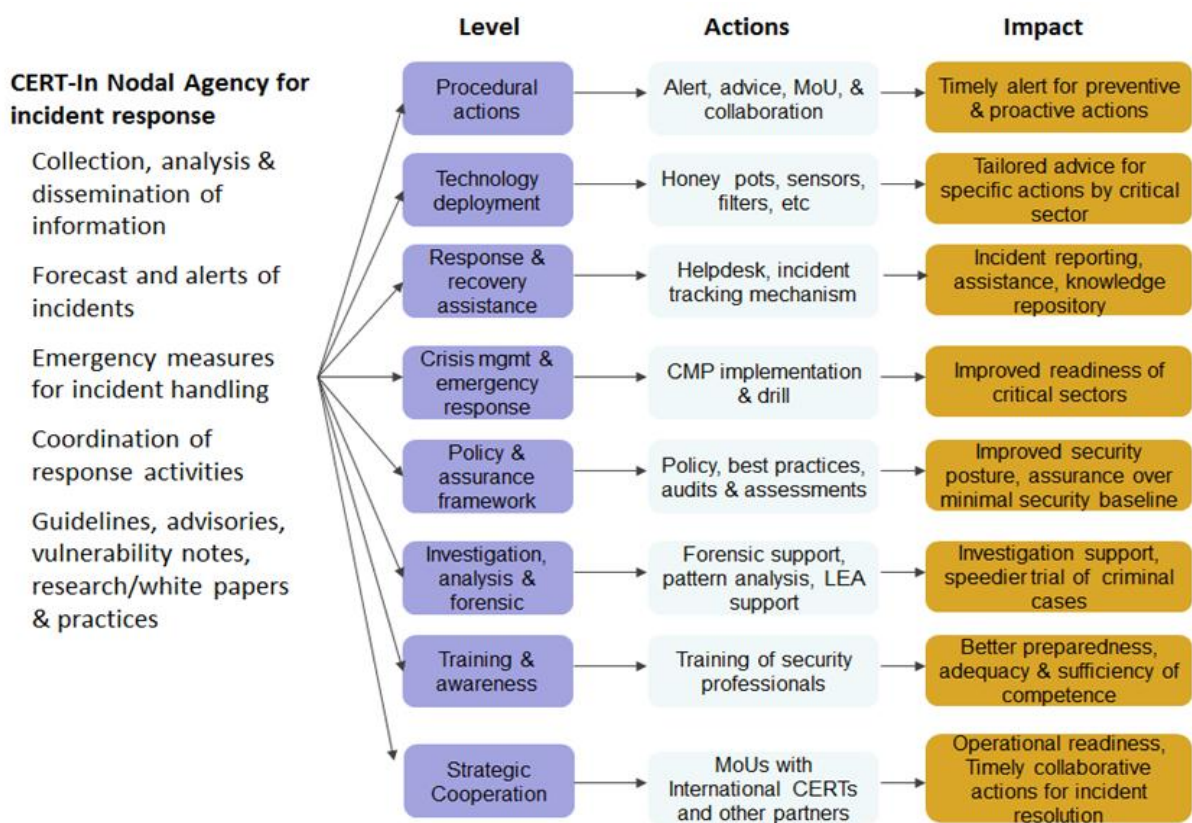
2.1.8.2. Workshops and meetings have been held regarding security in digital payments for banks, Internet Service Providers (ISPs) and Prepaid Payment Instruments (PPIs) entities along with active participation from RBI, Department of Financial Services, Law Enforcement Agencies and companies providing cyber security solutions. CERT-In has also recorded cyber security awareness sessions under the DigiShala Awareness Campaign, a free Doordarshan DTH channel, for educating citizens and create awareness amongst internet users so that they do not fall prey to online frauds.

2.1.9. CERT-In is equipped with cyber forensic and mobile device forensic analysis facility to extract and analyse the data from the digital devices involved in the cyber security incidents and cyber-crimes. CERT-In has imparted training on cyber forensics and mobile device forensics through lectures, demonstrations and hands on practical training sessions during the training workshops, which covers handling, seizing, preservation, imaging and analysis. CERT-In has also provided support to the state

police departments and other training institutes in imparting training on investigation of cyber-crimes, cyber security incidents using Cyber Forensic Techniques.

2.1.10. Strategic cyber security cooperation by CERT-In with the other countries enables creation of a security ring of like-minded and ICT dependent nations around the world that can help safety and security of cyber space. Accordingly, CERT-In enters into international cyber security cooperation arrangements with organizations engaged in similar activities, in the form of Memorandum of Understanding (MoU), to enhance its operational readiness.

The activities of CERT-In are summarised below:



Source : CERT-In

## 2.2. National Critical Information Infrastructure Protection Centre' (NCIIPC)

2.2.1. National Critical Information Infrastructure Protection Centre ("NCIIPC") with registered address at Block-III, JNU Campus, New Delhi-110067 is an organisation under the administrative control of National Technical Research Organisation ("NTRO") and is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection ("CIIP"). NCIIPC was constituted vide a Gazette Notification on 16th January 2014 issued under the Section 70A of the Information Technology Act, 2008.

2.2.2. Key responsibilities of NCIIPC are summarized as follows:

- (i) National Nodal Agency to protect National Critical Information Infrastructure (NCII).

- (ii) Deliver advice to reduce vulnerabilities.
- (iii) Identify all Critical Information Infrastructure (CII) elements for notification.
- (iv) Provide strategic leadership and coherent Government response.
- (v) Coordinate, share, monitor, collect, analyse and forecast threats.
- (vi) Develop plans, adopt standards, share best practices and refine procurement processes.
- (vii) Evolve protection strategies, policies, vulnerability assessment and auditing methodologies and plans for CII.
- (viii) Undertake R&D to create, collaborate and develop technologies for growth of CII protection.
- (ix) Develop training programs for CII protection.
- (x) Develop cooperation strategies.
- (xi) Issue guidelines, advisories etc. in coordination with CERT-In and other organisations.
- (xii) Exchange knowledge and experiences with CERT-In and other organisations.
- (xiii) NCIIPC may call for information and give directions to CII.

2.2.3. Major Initiatives taken by NCIIPC are as follows:

- (i) NCIIPC is operating a 24X7X365 Helpdesk with Toll Free Number 1800114430 for assisting organizations in critical sectors.
- (ii) NCIIPC has initiated Critical Information Infrastructure Protection activities with six Critical Sectors: Power & Energy Sector, Banking, Finance and Insurance Sector, Telecommunication Sector , Transportation Sector (air, surface, rail & water), Government Sector - Central Government (MHA, MEA, UIDAI etc.) & State Governments (Central Zone, East Zone, West Zone, North Zone, South Zone) and Strategic & Public Enterprises (PSUs & Heavy Industries).
- (iii) NCIIPC is currently engaging more than 300 organisations for critical information infrastructure protection activities.
- (iv) NCIIPC has published CII related documents and Frameworks. Some of these are as follows:
  - a. NCIIPC Controls Guidelines
  - b. NCIIPC Framework for Protection of CII
  - c. NCIIPC Framework for Evaluation and Enhancement of Cyber Security in CII
  - d. Training Curriculums for CISOs and Mid-Level Management
- (v) NCIIPC issues regular Advisory and Alerts. Actionable alerts are sent through SMS. NCIIPC also operates 'whatsApp' group for Chief Information Security Officers sharing and discussing knowledge and topics related to CIIP.
- (vi) NCIIPC is involved in R&D and coordinated CIIP activities with Industries, academia and PPP entities

- (vii) NCIIPC in collaboration with India Smart Grid Forum (ISGF) has conducted Cyber Security Preparedness Survey of Power Sector and finalized the following:
  - a. Top 10 Findings and recommendations circulated by Ministry of Power to its constituent organisations/agencies.
  - b. Cyber Security manual Prepared by ISGF in guidance of NCIIPC.
- (viii) NCIIPC has also conducted Cyber Security Preparedness Survey of Banking Sector and the findings were circulated across stake holders.
- (ix) NCIIPC conducts workshops for CIIP awareness.
- (x) NCIIPC carries out Incident Response for CII in coordination with CERT-In.
- (xi) NCIIPC operates a Remote Vulnerability Disclosure Programme (RVDP) for encouraging disclosure of vulnerabilities in CII.
- (xii) NCIIPC is assisting organisations in development of Secure Architecture for their CII.

2.2.4. Cyber Security Awareness: There are 80 Chief Information Security Officers (CISO) of Banking, Financial services and Insurance (BFSI) registered with NCIIPC and they are kept abreast of the changes in threat landscape through various means including email, messages and through whatsapp groups. Some of the recent additions are IDBI Federal Life Insurance Company Ltd, DHFL Pramerica Life Insurance Company Ltd, Ujjivan Financial Services, RBL Bank, IDFC Bank, Edelweiss Tokio Life Insurance, Star Union Dai-Chi Life Insurance and partnerships with key stakeholders

2.2.5. Cyber Security Preparedness Survey has been conducted in respect of Bank of India (BOI) on 5 - 6 June 2016 and report has been shared with BOI on 21 July 2016. Sectoral Coordinator – BFSI is the member of IT Committee of the board of NABARD and provides inputs on crucial issues and policy decisions of the Board. CISO Forum meeting was organized by IDRBT on 6 March 2017 in Hyderabad. BFSI Sectoral Coordinator has conducted a discussion and workshop focused on the initiatives taken by NCIIPC for the BFSI sector, necessity of identification and notification of CII and expectations from the stakeholders of BFSI sector. Inputs from the stakeholders are solicited on the concept note on CII and Criticality Matrix for the BFSI Sector. NPCI shared list of designations authorize to access CII on 15th Dec 2016. Process of analysing the cyber security posture of the NPCI is underway. NCIIPC works closely with Sectoral Regulators to facilitate them in identification of the Critical Information Infrastructure (“CII”) in their systems and also the sectors. Various cases of Notification of the CII pertaining to the RBI, SEBI and key stakeholders of the sector such as BSE, NSE, Payments agencies such as NPCI are at various stages.

2.2.6. NCIIPC has facilitated removal of multiple phishing sites to prevent any threat of loss of credentials by innocent citizens. NCIIPC issues periodical advisories to the sectoral members to keep them prepared for the ever changing threat landscape. Incidents reported to NCIIPC Incident Response Team by stakeholders are 25 in number.

## 2.3. Existing Cyber Security structure in financial sector in India

### 2.3.1. Reserve Bank of India initiatives on cyber security:

(i) Reserve Bank of India has been taking several initiatives in promoting computerization in Indian banks and in adopting technology. RBI had set up several working groups / committees to evaluate technological developments, its adoption in regulated entities and concerns arising out of information security. Some of the major initiatives are captured in the table below:

Sl No	Details	Year
1	In the wake of adoption of technology by banks, RBI issued a circular on Risk and Controls in Computer and Telecommunication Systems	1998
2	On the basis of recommendations of Working Group on Internet Banking, RBI issued guidelines on Internet Banking. Banks were advised to seek prior permission of RBI before rolling out internet banking to customers for carrying out transactions. Security issues were highlighted and system audit by qualified personnel was mandated.	2001
3	Guidance Note to banks was issued on digital record management	2002
4	In view of the growing computerisation, a working group on computer audit was set up. On the basis of the recommendation of the WG, Checklists for Computer Audit was issued.	2002
5	Business Continuity Planning (BCP) guidelines were issued to banks	2005
6	Need for obtaining prior permission to roll out internet banking was done away with. However, certain pre-conditions were set.	2005
7	Considering the growing incidents of frauds in electronic banking, a reporting framework for reporting frauds in Internet Banking / Debit / Credit cards was issued	2005
8	In view of the extensive use of outsourcing by banks, Reserve Bank issued guidelines for laying down a framework for managing the attendant risks in outsourcing. Responsibility and accountability for outsourced activity remains with the banks. Banks have been advised to take steps to ensure that the service provider employs the same high standard of care in performing the services as would be employed by the banks, if the activities were conducted within the banks and not outsourced.	2006, 2015

9	Following the announcement in the April 2010 Monetary Policy Statement, the Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds was constituted, under the Chairmanship of Executive Director, RBI. The Group examined various issues arising out of the use of Information Technology in banks and made its recommendations in nine broad areas. These areas are IT Governance, Information Security, IS Audit, IT Operations, IT Services Outsourcing, Cyber Fraud, Business Continuity Planning, Customer Awareness programmes and Legal aspects. Based on the recommendations of the WG, RBI issued detailed guidelines on the subject. The compliance of banks was monitored at the Board level of individual banks. The same was assessed as part of RBI's inspection of banks. Even today, these guidelines are considered as a reference document on the subject.	2011
10	<p>As stated in the Monetary Policy Statement of April 2012, banks were advised to put in place appropriate Information Security (IS) framework and IT governance structures to enable, <i>inter alia</i>, better alignment between IT and business. In order for banks to secure their ISSs, ensure their continuity, and check their robustness, they are required to put in place appropriate business continuity plans (BCPs) and test them periodically. These ISSs should be subjected to vulnerability assessment and penetration testing. Policies governing the above need to be approved at the board level. <i>Suitable guidelines in this regard issued to banks by end-June 2013.</i></p> <p>Accordingly, banks were mandated to conduct Vulnerability Assessment and Penetration Testing for Cyber Defence (VAPT) and report the findings on a quarterly basis to RBI</p>	2013

(ii) In the wake of rising concerns on cyber security incidents in banks, in its meeting held on December 24, 2014, Board for Financial Supervision (BFS) directed that RBI should have a thorough supervisory insight into the banks' IT systems. Pursuant to the direction, a dedicated Cyber Security & IT Examination Cell (CSITE Cell) was established in June 2015 in Department of Banking Supervision (DBS). Simultaneously, an Expert Panel on Cyber Security and IT Examination under the Chairmanship of the Executive Director with heads of DBS and DIT (Department of Information Technology) as also external members from the Academics, CERT-In and industry experts was set up to guide the cell on the approach to IT Examination, to review the guidelines pertaining to cyber security and to suggest appropriate capacity building in the area of cyber security. Subsequently, a group of officials with IT background were posted to the Cell after an internal selection based on applications received through Enterprise Knowledge Portal. The selected officials were provided intensive and customized training programmes.

(iii) CSITE Cell performs the following functions:

- a) As part of policy Initiatives, the Cell reviews the extant instructions on cyber security, emerging developments and concerns and accordingly, necessary policy initiatives are taken. A comprehensive circular on Cyber Security Framework in Banks was issued on June 2, 2016 (<https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF>) covering best practices pertaining to various aspects of cyber security. The circular requires banks to have, inter alia, a cyber-security policy, cyber crisis management plan, gap assessment vis-à-vis the baseline requirements indicated in the circular, monitoring certain risk indicators, board involvement in the matter, robust vendor risk management and reporting within 2-6 hours of unusual cyber security incidents. Compliance to the instructions is monitored. Various instructions are issued on an ongoing basis. CERT-In has been a member and contributed to this framework formulation.
- b) Beginning 2015, IT Examinations are being conducted to perform an in-depth assessment of the banks' IT infrastructure, their cyber security preparedness and resilience. These Examinations are independent of the financial supervision under the Risk Based Supervision. The IT Examination is performed on the lines of some of the best international standards on cyber security assessment and the gaps in compliance to the circular dated June 2, 2016 are also looked into. The examination reports are edited and issued to banks (also marked to Senior Supervisory Managers), post-which, compliance to the action points is monitored.
- c) CSITE Cell also carries out thematic studies on various cyber security issues. Themes vary from products, to delivery channels/systems. For instance, a study on Society for Worldwide Interbank Financial Telecommunication (SWIFT) operations in 10 banks were conducted to assess the security, organization and technologies employed immediately after a SWIFT related cyber-incident came to RBI's notice. The findings of the scrutiny were shared with all the banks so as to improve the security position of banks, particularly pertaining to SWIFT related operations
- d) With guidance of the Expert Panel, the Cell has developed the Key Risk Indicators (KRIs) in Cyber Security to evaluate the cyber risk profile of banks. The indicators have both the inherent and control gap components. Bank-wise heat maps are proposed to be drawn which may be used to decide on concomitant IT supervisory stance. A heat map is a graphical representation of data where the individual values contained in a matrix are represented as colours. This would facilitate immediate focus on risky banks on the basis of various indicators.
- e) Banks are required to report all the unusual cyber security incidents within 2-6 hours of detection to CSITE Cell through an online platform devised for the purpose.

These incidents are also reported to CERT-In. The reported incidents are examined for necessary follow up action with the banks till their resolution. The reported incidents are analysed to understand the modus operandi of incidents, possible control gaps that came to light and necessary action is taken to ensure containment of damages from the incidents and to pre-empt such incidents in future. The cell maintains an up-to-date contact details of CEOs and CISOs of banks in order to facilitate quick communication with them in case of emergency

- f) The Cell has constituted a Cyber Crisis Emergency Response Group comprising of the heads of Departments of Banking Supervision, Information Technology and Payment and Settlement Systems (DBS, DIT, DPSS) and the CEO of ReBIT to examine and offer guidance to swiftly handle major cyber incidents which may have potential systemic concerns.
- g) As part of offsite Monitoring of Cyber Risks, periodic returns have been devised (and being refined) to obtain various details like summary of cyber incidents, Technology implementations, self-assessed gaps in cyber security preparedness, action taken to address security concerns in specific areas, etc. Continuous assessment of risks in cyber security preparedness is ensured based on the reports and engagements with banks.
- h) During the year 2016, the Cell conducted a Cyber Drill across 6 banks in coordination with CERT-In to assess their incident response preparedness. This was followed up by another Cyber Drill across 9 banks in April 2017. These exercises involve hypothetical scenarios conducted in non-intrusive, table top format with real time communications between the Department and the banks. Vulnerabilities that get exposed during the drills are shared with banks for remedial action. The exercise, on a periodic basis, will cover all the large banks.
- i) On an ongoing basis, the Cell gathers market intelligence on cyber-attacks/threats/vulnerabilities with potential to cause damage to the banking sector. Various formal and informal sources are tapped for the purpose. Regular Advisories are issued to banks, as required, to caution and to take necessary action based on the intelligence gathered/incidents reported. The inputs are also kept in view during IT Examinations of banks.
- j) The Cell has been continuously interacting with ReBIT, CERT-In, IDRBT, ISACA, various Government entities and industry experts to evolve coordinated approach in strengthening cyber ecosystem in banks. Apart from one-to-one interactions with banks on continuous basis, formal meetings with the CISOs of banks are held periodically to: Discuss the various supervisory concerns; Take stock of the new technology developments and their deployment by banks; Elicit views on emerging



threats and action taken/proposed thereon. The Cell is also in touch with other departments like DPSS, DIT, etc. as necessary.

- k) As part of capacity building & continuous updation, the subject of IT Security being quite complex which requires intensive skill upgradation on an on-going basis, various initiatives are taken. The officials are deputed for regular and customized training/seminar, etc..
- l) An announcement was made in Bank's sixth bi-monthly monetary policy statement for 2016-17 to set up an inter-disciplinary Standing Committee on Cyber Security to review the threats inherent in the existing/emerging technology; study adoption of various security standards/protocols; interface with stakeholders; and to suggest appropriate policy interventions to strengthen cyber security and resilience. The 11 member Standing Committee, headed by the Executive Director with various external and internal members including CERT-In having expertise on relevant areas, would meet on an on-going basis to examine and recommend appropriate policy and supervisory interventions. As necessary, sub-groups may be formed to assist the Standing Committee on specific issues needing in-depth examination. The Cell acts as the Secretariat for the Standing Committee. The committee has already constituted three sub-groups to look at security aspects of card based transactions, mobile banking and vendor risk management
- m) In accordance with the mandate, the Terms of Reference, inter alia, include the following:
  - (i) Review the threats inherent in the existing/emerging technology;
  - (ii) Study adoption of various security standards/protocols;
  - (iii) Interface with stakeholders; and
  - (iv) Suggest appropriate policy interventions to strengthen cyber security and resilience.
- n) With regard to coverage of the institutions, the Cyber Security & IT Examination Cell has been established within the Department of Banking Supervision. The policy instructions, advisories and IT Examinations cover the scheduled commercial banks (excluding RRBs), Small Finance Banks, Payment Banks and Local Area Banks. The modalities of implementation of the recommendations, as applicable, to other RBI regulated entities are being examined by the Bank.
- o) The measures taken by the RBI pertaining to security related instructions for payment systems is given below:
  - (i) Reserve Bank of India has been formulating / reviewing its policies to promote migration towards less cash mode of payments at the same time ensuring that the electronic transactions are safe, secure and convenient. The DPSS is accordingly

constantly reviewing the challenges emerging in the Payments Ecosystem and accordingly has been framing policies to address those challenges. It is an on-going process.

- (ii) The instructions and directions encompass different stages as well as entities and instruments involved in a payment transaction chain.
  - (iii) Cards being widely used as a payment instrument – both for withdrawal of cash at ATMs as well as for purchase of goods and services – many of these instructions focus on card payments. In this regard, the globally accepted standards for cards (EMV) have been prescribed.
  - (iv) An additional aspect necessitating focus on card payments is that, in open system card payments (typically a four-party model consisting of card holder, merchant, acquirer and the issuer, in addition to the card network), the payments are made and accepted on the basis of trust and confidence in the system where the infrastructure put in place by different sets of banks are used by customers who have cards issued by different sets of banks.
  - (v) Unlike card payments, the payments made through net banking or mobile banking facility involves three parties – the customer, merchant and the account holding bank.
  - (vi) In case of remittances or funds transfers using net banking / mobile banking, the transactions are usually effected on other payment systems like RTGS / NEFT / IMPS etc.
  - (vii) Many of these payments – card as well as net banking - are facilitated by payment gateway providers / payment aggregators who link the customers making payments (using different payment instruments) with banks (who provide the payment instruments).
- p) On security instructions related to Card payments, to ensure end to end security in the ecosystem, instructions have been issued to banks in 3 broad areas – at infrastructure level, instrument level and transaction level.
- i. Infrastructure level
    - a) September 22, 2011: In order to strengthen the technology infrastructure, Unique Key per terminal (UKPT) or Derived Unique Key per transaction (DUKPT), and Terminal line encryption (TLE) needs to be implemented.
    - b) Sep 22, 2011: Enablement of all POS terminals to accept debit card transactions with PIN.
    - c) Sep 22, 2011: POS infrastructure to be ready for accepting EMV Chip cards.
    - d) Feb.28, 2013: Banks should ensure that the terminals installed at the merchants for capturing card payments (including the double swipe terminals used) should be certified for PCI-DSS (Payment Card Industry - Data Security Standards) and PA-DSS (Payment Applications - Data Security Standards)-

- e) Feb.28, 2013: Banks should ensure that all acquiring infrastructure that is currently operational on IP (Internet Protocol) based solutions are mandatorily made to go through PCI-DSS and PA-DSS certification. This should include acquirers, processors / aggregators and large merchants
  - f) May 26, 2016: In order to enhance the safety and security of transactions at ATMs, it has been mandated that EMV Chip and PIN cards used at ATMs should be processed on the basis of Chip content. Banks and WLAOs have been advised to ensure that all the existing ATMs installed and operated by them are enabled for processing of EMV Chip and PIN Cards by September 30, 2017.
- ii. Instrument level (security at card level)
- a) September 22, 2011: EMV Chip Card and PIN to be issued to customers who have evidenced at least one purchase using their debit/credit card in a foreign location.
  - b) February 28, 2013: all new debit and credit cards to be issued only for domestic usage unless international use is specifically sought by the customer. Such cards enabling international usage will have to be essentially EMV Chip and Pin enabled.
  - c) August 27, 2015: banks and Authorized card Payment networks (Rupay, Visa, Master Card, American Express, Diners) have been advised that with effect from February 01, 2016 all new cards issued – debit and credit , domestic and international (Other than Cards issued under PMJDY, BSBDA/Other Government Schemes) - by banks shall be EMV Chip and PIN based cards. Regarding the migration plan for existing magnetic stripe to EMV Chip and PIN cards, the time line is December 31, 2018. For cards issued under PMJDY/BSBDA/Other Government Schemes all new cards issued should be EMV Chip and PIN after September 30, 2016. EMV Chip and PIN cards are less prone to fraudulent activities.
- iii. Transaction level (ATM, POS and online card transactions): Instructions have been issued from time to time on Security and Risk mitigation measures to enhance the security of card transactions. India has been the leader in implementing some of these measures. Some details are given below:
- a) Banks have been advised to provide online alerts to customers for all card transactions (card present and card not present), vide, RBI circular dated February 18, 2009 and March 29, 2011.
  - b) Banks have been advised, vide, circular February 18, 2009 and December 31, 2010 to put in place a system of providing additional factor of authentication / validation (2FA) for all card not present transactions using the information which is not available on the card.
  - c) Entry of PIN has been mandated for all debit card transactions at POS for both magstripe and Chip and PIN cards. (Circular dated Sep 22, 2011)

- d) February 28, 2013 - All the active MagStripe International cards used by banks should have threshold limit for international usage which is to be determined by the bank based on the risk profile of the customer and accepted by the customer.
  - e) Circular dated May 14, 2015 - Guidelines have also been issued for issuance of Contactless cards using Near field communication (NFC) technology for small value transaction (maximum Rs. 2,000) without additional factor authentication (AFA) to foster innovative payment products as also to enhance the convenience factor in certain types of card uses.
  - f) Circular dated August 1, 2013 mandates requirement of PIN entry for each and every transaction, including balance enquiry transactions. As an additional safety measure, banks have also been advised that time out sessions should be enabled for all screens / stages of ATM transaction keeping in view the time required for such functions in normal course.
- iv. Electronic banking and funds transfer transactions:** For securing electronic payment transactions, vide Circular dated 28.2.2013, banks were advised to follow the under mentioned best practices:
- a) Customer induced options may be provided for fixing a cap on the value / mode of transactions/beneficiaries. In the event of customer wanting to exceed the cap, an additional authorization may be insisted upon.
  - b) Limit on the number of beneficiaries that may be added in a day per account could be considered.
  - c) A system of alert may be introduced when a beneficiary is added.
  - d) The banks may put in place mechanism for velocity check on the number of transactions effected per day/ per beneficiary and any suspicious operations should be subjected to alert within the bank and to the customer.
  - e) Introduction of additional factor of authentication (preferably dynamic in nature) for such payment transactions should be considered.
- v. Real Time Gross Settlement (RTGS) transactions:** In order to ensure that the communication infrastructure for RTGS transactions is secure, the RTGS Regulations requires:
- a) that each member will communicate from their Member Interface to the Central System through the INFINET or any other network permitted by the Bank.
  - b) the interactions between the Member Interface and the Central System will be through pre-defined message format (ISO 20022 – the latest messaging standard) only.
  - c) every message will be digitally signed and encrypted.
  - d) The Institute for Development and Research in Banking Technology (IDRBT) will be the Certifying Authority (CA) for digital certificates.
- vi. National Electronic Funds Transfer (NEFT) transactions:**

- a) The NEFT system uses the Structured Financial Messaging System (SFMS) for communication.
  - b) The security aspect of SFMS is taken care of using PKI based security environment.
  - c) Authentication, Confidentiality, Non-Repudiation and Integrity is taken care of by PKI based security features. Under Public Key Infrastructure each entity will have a public key and a private key.
  - d) Digital Signature will be a part of every message sent on SFMS. Smart card based access at the point of message generation provides additional security and audit trail.
- q) As part of System Audit, for Non-Bank Entities operating Payment Systems in India, RBI vide circular DPSS.AD.No.1206/02.27.005/2009-2010 dated December 7, 2009 and [DPSS.1444/ 06.11.001/ 2010-2011 dated December 27, 2010](#) which was subsequently amended vide circular DPSS.CO.OSD.No.2374/06.11.001/2010-2011 dated April 15, 2011(<https:// www.rbi.org.in/ scripts/FS Notification.aspx? Id=6344&fn=9&Mode=0>) has mandated System Audit to be done on an annual basis by CISA/DISA certified auditor. Further, the scope of the System Audit should include evaluation of the hardware structure, operating systems and critical applications, security and controls in place, including access controls on key applications, disaster recovery plans, training of personnel managing systems and applications, documentation, etc. The audit should also comment on the deviations, if any, in the processes followed from the process flow submitted to the Reserve Bank while seeking authorization. The objective of the IS audit is to ensure that the technology deployed to operate the payment system/s authorised is/are being operated in a safe, secure, sound and efficient manner and as per the process flow submitted by various authorised entities. Further, in view of the recent withdrawal of legal tender character of Rs.500 and Rs.1000 denomination notes and the stress on digital transactions, to address the issue of cyber resilience, RBI vide circular DPSS.CO.OSD.No.1485/06.08.005/2016-17 dated December 9, 2016 (copy is available on <https:// www.rbi.org.in/ scripts/FS Notification.aspx? Id=10772&fn=9&Mode=0>) had instructed all authorised entities / banks issuing PPIs in the country to:
- (i) Carry out a special audit by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In) on a priority basis and take immediate steps thereafter to comply with the findings of the audit report. The audit should cover compliance as per security best practices, specifically the application security lifecycle and patch/vulnerability and change management aspects for the system authorised and adherence to the process flow approved by the Reserve Bank. Banks may also be guided by the circular [DBS.CO/CSITE/BC.11/33.01.001/2015-16](#) on Cyber Security Framework in Banks dated June 02, 2016.

- (ii) Take appropriate measures on mitigating phishing attacks considering that the new customers are likely to be first time users of the digital channels. Safety and security best practices may be disseminated to the customers periodically.
  - (iii) Implement additional measures dynamically depending upon the risk perception or threats as they emerge.
- r) Reserve Bank of India enjoys statutory powers to issue various directions, circulars, instructions and guidelines to banks on an ongoing basis. Non-compliance with RBI's instructions might attract penalties under Banking Regulation Act 1949 as well as Payment and Settlement Systems Act 2007. Recently, Reserve Bank has established an Enforcement Department to look at various non-compliance by banks with the instructions and to initiate suitable penal measures independently

### **2.3.1.1. National Payment Corporation of India (NPCI) initiatives on Cyber Security**

2.3.1.1.1. National Payments Corporation of India (NPCI) is an umbrella organization for all retail payments system in India. It was set up with the guidance and support of the Reserve Bank of India (RBI) and Indian Banks' Association (IBA). The RBI, after setting up the Board for Regulation and Supervision of Payment and Settlement Systems (BPSS) in 2005, released a vision document incorporating a proposal to set up an umbrella institution for all the RETAIL PAYMENT SYSTEMS in the country. During the last six years, the organization has grown multi-fold from 2 million transactions a day to 20 million transactions now. From a single service of switching of inter-bank ATM transactions, the range of services has grown to Cheque Clearing (CTS), Immediate Payments Service (IMPS), Automated Clearing House (NACH), Electronic Benefit Transfer, Aadhaar Enabled Payment System (AePS), Unified Payment Interface (UPI), Bharat Bill Payment System (BBPS) and a domestic card payment network named RuPay to provide an alternative to international card schemes.

2.3.1.1.2. The management of risks is core to NPCI's vision mission and objectives of ensuring safety, security and sustainability of national retail payment systems. Effective risk management is fundamental to being able to generate critical mass and optimum risk-reward and is thus considered to be the epicentre of decision making at NPCI.

2.3.1.1.3. NPCI strongly believes that sound risk management and effective governance play a crucial role in mitigating risks and meeting the expectations of its stakeholders. At NPCI, risk management, governance and internal controls are the most effective tools to enhance service levels and enterprise value. A comprehensive risk management process allows management to take risks in a controlled manner. In order to provide all-inclusive view of retail payment systems, risks and opportunities are assessed and identified in a seamless manner using elements of top-down and bottoms-up approach. As part of the risk management framework we use a set of principles that entails the risk management culture we wish to promote, preach and practice at NPCI. NPCI has designed the Enterprise Integrated Risk Framework (EIRM) drawing guidance from

regulatory guidelines of Reserve Bank of India, guidelines from Bank for International Settlements (PFMI), COSO ERM and ISO31000.

2.3.1.1.4. NPCI offers best-in-class secured environment many of which are extended to all its products and services, those key common controls are as follows:

*Security Governance:*

- (i) Best in class policies and processes aligned with global standards for compliance and enforcement (Information Security Management, Business Continuity Management & Quality Management)
- (ii) Every new product, services and major changes goes through rigorous security assessment, certification and testing procedures before moving into production go-live environment. It involves test scenarios from banks and NPCI end as well.
- (iii) Source-code review, system readiness and operation preparedness review programs are performed before launch of any new product and services or before any major change into the system.
- (iv) NPCI has rolled out RuPay Card Manufacture and Personalisation vendor audit and certification program; all empanelled vendors must certify before offering their services to Bank for RuPay card.
- (v) NPCI has Third Party IT security Assessment program which essentially ensure that all out sourcing agencies follows defined controls.
- (vi) ATM Security Guidelines are framed by NPCI Task Force across bank for standardisation in minimum mandatory control i.e. those become default controls for banks and White Label Operator to follow.

*Security Technology Implementation:*

- (i) NPCI has implemented the world-class technological products to address any latest cyber security attacks. From the network perimeter level to the end user level machine with deployment of security solutions such as Firewall (acting as gatekeeper for all the data traffic moving in and out of NPCI), Antivirus, Data Leakage Prevention, Web application firewall, Advanced Persistent Threat (host and network based)
- (ii) Distributed Denial of Service, Security Analytics & Packet Capture (which delivers advanced packet capture and deep packet Inspection (DPI) that also indexes, classifies and enriches all network traffic data with the latest threat intelligence) and web proxy.
- (iii) Encryption in transit (over network) & in store (database) i.e. data remains always secured and protected.
- (iv) Robust and Scalable System Infrastructure - Handles 20 Million Online Transaction per day at present

- (v) Resilient Network Infrastructure – NPCINET (ensures uptime of 99.99%) supported by three Data-Center having High Availability of Systems with Secured and Multiple Telecom network connectivity ensure uninterrupted services.

*Continuous Security Threat Monitoring:*

- (i) NPCI has a strong application vulnerability management program conducted by 3rd party vendor, which includes application source code review, penetration testing, configuration audit, web application security assessment, mobile app security assessment (all Operating Systems). This program helps us to identify all the web application / mobile app level threats and also closes it in timely manner. The program is conducted on regular basis.
- (ii) NPCI infrastructure is regularly assessed by third party assessors including ethical hackers for any security vulnerabilities.
- (iii) Continuous monitoring through Anti-phishing service provider to identify any UPI rogue app and phishing websites.
- (iv) Continuous Monitoring (24/7-365 days) by Skilled Resources (application, security and infrastructure - Operations, Support Maintenance
- (v) Real time Transaction monitoring through “Fraud Risk Monitoring” tool to detect and prevent any fraudulent transaction
- (vi) NPCI performs annual system audit of entire environment and report of which is submitted to RBI for compliance. Annual System Audit exercise is performed by external qualified assessor as per RBI Guidelines. It covers the entire IT Infrastructure and System under scope and reviews according to RBI Guidelines and Industry best practices.
- (vii) Monitoring of the security tools and incidents is the strength of NPCI, which is done with the help of world class Security Information Event Management (SIEM) tool. Technically strong monitoring team is stationed at NPCI for 24x7x365 to monitor all the security real time events.
- (viii) Associated with Cert-In and IDRBT for participating in cyber security drills.

*RuPay Card Scheme:*

- (i) Local infrastructure for card scheme and card acceptance network leading to lean cost model and domestic transaction data residing in the country
- (ii) Global Partner with Discover Finance, JCB and Union-Pay for international acceptance and usage (Due diligence through partner review programs & interactions)
- (iii) All card manufactures in country only hence no data going out even for card manufacturing and personalization.

*UPI – Unified Payments Interface:*



- (i) UPI does the finger printing of device and verifies it for every subsequent transaction initiated by customer using tokenization as back end technology. The Parameters used for first level authentication are Mobile number, Device Id – Device ID and APP Id – Application ID that ensures that the transaction is fully secured. The second factor is the MPIN registered by the user.
- (ii) UPI assigns virtual address to customer and maintains a secure database for address resolution, such that customer bank account information remains confidential and he/she has to share only virtual address with others.
- (iii) Thus, UPI Solution provides strong end-to -end security and data protection.

2.4.1.1.5. In today's age when the country is speedily adopting electronic modes of payments like Cards, IMPS, UPI & mobile payment systems; it has become highly imperative to reassure the customer that these are indeed the safest mediums to transact.

- (i) NPCI also provides a state of the art Fraud Risk Monitoring (FRM) as a value added service to its member banks.
- (ii) FRM solution is designed to facilitate real time transaction monitoring for its member banks. It is a rule-based system wherein predefined criteria are set to identify abnormal transactions and set early warning signals to mitigate fraudulent transactions.
- (iii) The FRM tool also has the ability to block or decline transactions, which are deemed to be highly suspicious in nature. In addition this tool also provides flexibility to maintain watch lists / blacklists to track transactions based on predefined criteria. The system also allows a very flexible mechanism to modify rules or parameters, which may be required from time to time so as to address the dynamically changing fraud trends.
- (iv) NPCI's Risk Monitoring team evaluates transactions round the clock for all its member banks and flags suspicious transactions to verify with their customers. Additionally training & access is also provided as a value added feature to member banks who are interested in have a real time monitoring system to safeguard the interest of their customers.

2.3.1.1.6. Considering this dynamic shift where the country is moving towards the objective of a less cash society, having a robust fraud risk monitoring system has become very significant. This is where NPCI as an organization provides total reassurance to the end user that this new way of transacting electronically is rather safe than conventional means and that there is a round the clock monitoring of their transactions so as to safeguard their interest.

2.3.1.1.7. Audits and Assurance by External Parties and Certifications agencies:

- (i) Awarded with 'Certificate of Merit - 2015' and winner of "Making Quality Happen – Best practices" in Service Category by Indian Merchants' Chamber Ramkrishna Bajaj National Quality Award

- (ii) NPCI has been awarded with the Information Security Management System ISO/IEC 27001:2013 certification for all offices.
- (iii) NPCI has received ISO 9001:2008 certification for Quality Management Standard (QMS) that defines implementation on customer satisfaction, process approach, conformance to regulatory requirements and active involvement of top management and employees.
- (iv) NPCI has achieved ISO 22301:2012 certification for Business Continuity Management Standard (BCMS). The certification demonstrates that it can protect against, prepare for, respond to, and recover when disruptive incidents arise.
- (v) NPCI has also been certified by PCI DSS v 3.1 standard, which is mandated by the card brands to increase controls around cardholder and maintaining payment security for all entities that store, process or transmit cardholder data. NPCI was first in the country to get this certification.

2.3.1.1.8. Given the rapid change, NPCI continuously upgrades its security posture to meet the challenges of today and tomorrow. Some of the key initiatives currently in progress are:

- (i) Transform data into intelligence - Moving forward, the data must be transformed into intelligence and the enterprise needs to be aligned with data and context-centric security. We are in process of developing intelligence that shall help in reconstruct activities, determine if an incident is in progress and provide network and systems usage baselines.
- (ii) Transform to the Next Generation Security Model - Redefine the defence-in-depth approach to defence-in-context. Moving the protection strategy from focusing on systems to concentrating on the data.
- (iii) NPCI have already tied up our relationship with NCIIPC and CERT-IN and are in process of working more closely with their team for continuous monitoring of our infrastructure and threat assessment of the same.

### **2.3.1.2. Institute for Development & Research in Banking Technology (IDRBT) initiatives on cyber security**

2.3.1.2.1 Institute for Development & Research in Banking Technology (IDRBT) was established by the Reserve Bank of India in March 1996 as an Autonomous Centre for Development and Research in Banking Technology located at Hyderabad as 70% of the financial sector in India is dominated by banking sector. IDRBT has carved a niche for development and hosting of financial sector infrastructure, research in banking technology and conduct of training programmes on IT security. IDRBT formed the Chief Information Security Officers (CISO) Forum in the year 2010 with a view to provide a platform for CISOs of all banks to discuss common security concerns in the Indian Banking and Financial Sector and collaboratively provide solutions. The Reserve Bank of India's Working Group on Information Security, Electronic Banking, Technology Risk

Management and Cyber Frauds, in its Report issued in 2011, recommended that IDRBT may set up a body like the Financial Services Information Sharing Analysis Center (FS-ISAC) in the US that can enable sharing of security events amongst banks. As banks were well ahead in implementing information security and IDRBT had already set up a CISO Forum for banks, the task of setting up this body for information sharing was entrusted to IDRBT. Accordingly, IDRBT established the Indian Banks–Center for Analysis of Risks and Threats (IB-CART) in March 2014. The IB-CART now has more than 90 users from over 60 public, private and foreign banks in India. The IB-CART advisory council has 9 members with representation from public and private sector banks and CERT-In.

2.3.1.2.2 IB-CART is essentially functioning as an anonymous reporting platform for reporting of cyber security events. It is observed that, over time, the forum has been serving a useful purpose. In order to strengthen the reporting mechanism, RBI as part of its circular on Cyber Security Framework in Banks advised banks to report cyber-incidents invariably to IB-CART. Currently only banks are reporting to IDRBT and other financial sector players such as NBFCs, Insurance companies, Pension companies, SEBI regulated entities, etc. are not required to report to IB-CART.

2.3.1.2.3. Setting up of National Financial Switch (NFS), Indian Financial Network (INFINET) and Structured Financial Message System (SFMS) for the critical payment systems in India were some of the important initiatives of IDRBT. In order to focus exclusively on research and development, IDRBT has since transferred its service functions to Indian Financial Technology and Allied Services (IFTAS), a company promoted by it.

2.3.1.2.4. The Institute is currently focusing mainly on research, training, consultancy and coordination with banks. The focus areas of the Institute are cyber security, analytics, cloud computing, financial inclusion, payment systems and open sources. There are centers exclusively for each of the focus areas, managed by faculty, research scholars and research assistants.

2.3.1.2.5. The Center for Cyber Security carries out the following activities for Banks and Financial Institutions:

- (i) Executive Development Programme (EDP) programs in the area of Cyber Security - Cyber defence, Vulnerability Assessment and Penetration Testing, Malware Analysis, Cyber Forensics, and related customised programs
- (ii) Quarterly Cyber Drills for banks on the lines of level 2 cyber drill of CERT-in.
- (iii) IB-CART, Indian Banks - Center for Analysis of Risks and Threats
- (iv) Cyber crisis and cyber security workshops for bankers are carried out with the help of CERT-In two to three times in a year.

2.3.1.2.6. It is a Threat Intelligence Sharing platform for Indian Banks and FIs

- (i) IB-CART platform is developed using the automated and standardised exchange of cyber threat information which is the Trusted Automated Exchange of Indicator Information (TAXII) and Structured Threat Information Expression (STIX) standard
- (ii) Banks furnish incident details, anonymously
- (iii) Reports are shared amongst RBI, banks, Cert-In and NCIIPC.

#### 2.3.1.2.7. CISO Forum

- (i) All Bank CISOs are members of this forum.
- (ii) Meets every quarter, at IDRBT and other places hosted by Banks.
- (iii) Discussion on results of Cyber drill, IB-CART updates.
- (iv) Experience sharing and cyber security concerns amongst CISOs

#### **2.3.1.3. Reserve Bank Information Technology (ReBIT) Pvt. Ltd initiatives on cyber security**

2.3.1.3.1. Reserve Bank of India has recently established an IT subsidiary viz. Reserve Bank Information Technology (ReBIT) Pvt. Ltd. to focus on IT and cyber security related issues of the financial sector. ReBIT will focus on IT and cyber security (including related research) of the financial sector and assist in IT systems audit and assessment of the RBI regulated entities; advise, implement and manage internal or system-wide IT projects (both the existing & the new) of the Reserve Bank as mutually decided between the Reserve Bank and ReBIT.

2.3.1.3.2. ReBIT will act as a catalyst for innovation, big systems and new ideas apart from having the capability to guide the regulated entities in the IT areas of their operations as also for the RBI's IT related functions and initiatives. Given the need for inter-operability and cross-institutional cooperation, ReBIT will effectively participate in setting up of standards to strengthen Reserve Bank's role as regulator.

2.3.1.3.3. ReBIT will have the following four verticals to support its mission: (i) Cyber Security: To enhance the trust and reliability of RBI's infrastructure for assurance and resilience (ii) Research and Innovation: To empower Indian banking industry through creative technology solutions based on research, and by tapping the synergy among key stakeholders (iii) Systems Audit: To support validation and enforcement of regulatory guidance on cyber security for the banking sector, through excellence in audit, analytics and forensics (iv) Project Management: To leverage lean and agile development capability for creating and operating reliable and empowering systems, and delivering delightful user experience.

2.3.1.3.4. The main objectives of ReBIT are as follows:

- (i) To provide to Reserve Bank of India (RBI), Information Technology (IT) services as may be required by it, including but not limited to Cyber Security services to meet the requirements of RBI and the Indian Financial System.
- (ii) To assist RBI in carrying out IT Systems and Security Audit and Assessment of the regulated and/or supervised entities and potential entrants or applicants.
- (iii) To assist RBI in vulnerability assessment and penetration testing and forensic audit of the regulated and/or supervised entities and potential new entrants.
- (iv) To assist RBI in enhancing IT Management skills including but not limited to Project Management and Data Centre management.
- (v) To commission or facilitate high quality research in various IT related areas pertaining to the financial Sector with focus on Cyber Security and render advice to RBI for IT Security including Cyber Security related aspects.
- (vi) To act as a think-tank for innovation, big systems and new ideas in the financial sector and make recommendations to RBI for implementation of IT solutions to enhance the robustness and safety of the Indian Financial System.
- (vii) To participate in deliberations of IT Standard setting bodies to achieve robust and inter-operable Standards for the Indian financial Sector.
- (viii) To advise, provide consultancy services, develop and implement products for RBI and the Indian Financial System on all matters related to the implementation of computer software and hardware systems, management of data processing and information systems and data communication systems and such other components which may comprise part of the IT systems or updation or improvements thereof used by the Indian Financial system.
- (ix) To undertake, engage in, promote, assist, conduct scientific and technical research, developments, experiments, investigations, inquiries, studies, projects, analysis, examinations, surveys and tests of all kinds including, but not limited to those related to telecommunications, computers, electronic data processing equipment, software, hardware whether in India or abroad.
- (x) To provide consultancy, information processing, hardware, software and network system management as well as business advisory services related to cyber security, statistical, scientific or mathematical information and reports, data processing, preparing, collection and data of every kind and description, systems or aiding commerce, industry, scientific and research problems and for all other related businesses.
- (xi) To collaborate with other institutions / agencies including but not limited to the IDRBT, Hyderabad for achievement of its objectives.

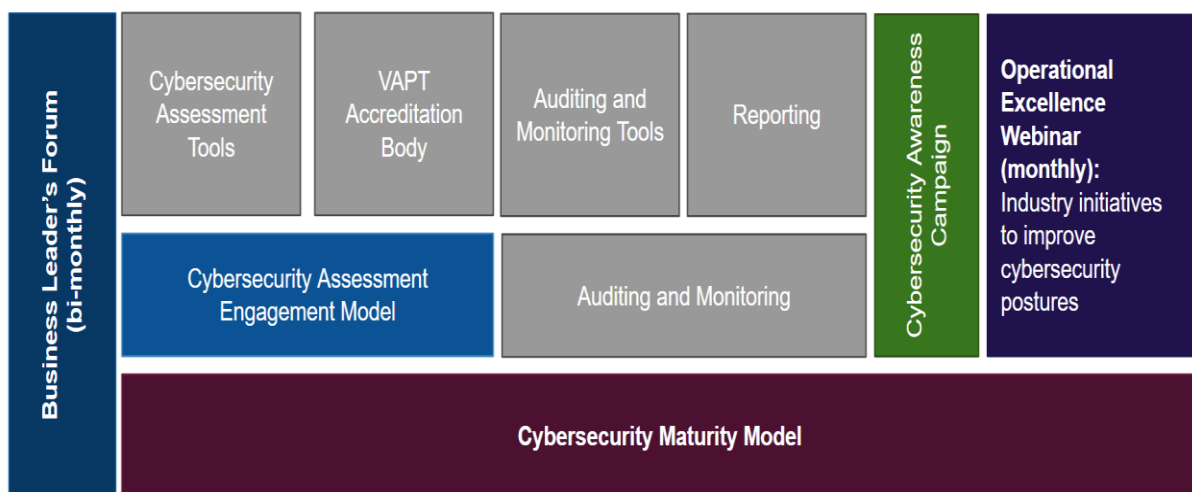
- (xii) To depute one or more IT experts of the Company to RBI, if so requisitioned by RBI, on such terms and conditions as may be mutually agreed between the Company and RBI, for assisting the Principal Inspection Officer of RBI conducting inspection of regulated and/or supervised entities.
- (xiii) To perform any other Information technology related activity relevant to the Indian financial system as RBI may, after consultation with the CEO, require the company to perform

2.3.1.3.5. ReBIT’s industry side initiatives: ReBIT plans to engage with the industry stakeholders and academic institutions to improve overall cyber resiliency of the financial sector. This requires multi-pronged initiatives towards developing common standards through a collaborative approach in the area of policy research, specification development, establishment of best practices, promoting industry adoption of right kind of tools and technologies, encourage cyber security awareness and creating a culture of security. To achieve these objectives, ReBIT sees its role as a facilitator and driving the collaborative engagement at various levels, as shown in the following diagram:



- (i) ReBIT has kicked-off an Operational Excellence Webinar Series recently that strives to engage with sub-CISO community and operational personnel in the financial sector and promote execution and excellence focussed knowledge sharing and promoting standards adoption. In the first webinar, ReBIT started an industry wide “Anti-Phishing campaign” and is working on Domain-based Message Authentication, Reporting & Conformance (DMARC) implementation. A recent survey covering 36 institutions that ReBIT did, it found that only 22% of the financial institutions have implemented DMARC. The industry objective that ReBIT has set is to achieve 100% DMARC compliance within a period of 1 year. For this, ReBIT will be building industry level tools/platform to reduce adoption cost and promote uniformity.

- (ii) The second initiative of ReBIT focuses on community leadership. ReBIT is establishing a consortium called FIRST (Financial Industry - Research in Security and Technology) within which it plans to start several industry led collaboration activities in form of various focussed working groups. For example, ReBIT surveyed the industry stakeholders and found gaps and inconsistency in how firms assess their maturity levels and identified a need for a common cyber security maturity assessment standard. ReBIT has launched a Cyber security Maturity Model Development Working Group (CMM-WG) to help the banking industry define a uniform yardstick to measure their maturity, establish cyber security maturity roadmap, perform industry benchmark and prioritize risk-driven investment in security. The working Group studied maturity models proposed and used in various countries and is working on coming up with a maturity model suited to the Indian financial institutions. The WG is adopting a consensus based approach and will be seeking feedback by coordinating with other institutional bodies as well as will open the cyber security maturity model for stakeholder comments.
- (iii) ReBIT also realizes that currently the financial institution do not look at cyber security as a business imperative. There is a need to highlight the criticality of cyber security risks and their impact on normal operations of the business, security of the customer assets and maintain public trust. ReBIT plans to equip business leaders to understand cyber risks more accurately and craft their response through a risk-based approach. This will help gather support and momentum for the industry initiatives and CISO functions within the regulated entities. ReBIT will shortly be launching the “Business Leader’s Forum” with these objectives.
- (iv) Within the framework mentioned above, ReBIT will be initiating other programs. The following diagram provides a broader perspective of initiatives that ReBIT has planned for within the next year of its operations.



### **2.3.2. Securities & Exchange Board of India initiatives on Cyber Security:**

2.3.2.1 Principle 17 of PFMI (CPMI-IOSCO Principles for Financial Market Infrastructures) that relates to management and mitigation of 'Operational risk' requires that systemically important market infrastructures institutions *"should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption."*

2.3.2.2. Accordingly, Market Infrastructure Institutions (MIIs) have been directed to have a robust cyber security framework as part of their operational risk management. SEBI has laid down a detailed framework in the circular dated July 06, 2016 with regard to cyber security and cyber resilience that MIIs (Stock Exchanges, Clearing Corporation and Depositories) are required to adopt<sup>14</sup>. The framework inter-alia covers areas such as Governance, Identification of critical assets and cyber risks (threats and vulnerabilities), Access Controls, Physical security, Network Security Management, Security of Data, Hardening of Hardware and Software, Application Security and Testing, Patch Management, Disposal of systems and storage devices, Vulnerability Assessment and Penetration Testing (VAPT), Monitoring and Detection, Response and Recovery, Sharing of information, Training, and Periodic Audit. The implementation of the said framework by MIIs is monitored through the requirement of (a) Quarterly reports on information on cyber-attacks and threats experienced by MII and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats, and (b) annual system audit undertaken by an independent auditor.

2.3.2.3. Prior to issuance of the aforementioned circular, the regulatory framework specified by SEBI through various circulars on Internet Based Trading (IBT), DMA (Direct Market Access), Algorithmic trading, BCP-DR (Business Continuity Planning and Disaster Recovery), System Audit, Testing of software used or provided by stock brokers, Outsourcing, etc. has been an effort to encourage Financial Market Infrastructures (FMIs) such as stock exchanges, clearing corporations and depositories and intermediaries to implement robust information technology risk management practices to ensure that trading, clearing and settlement systems are secure, reliable and resilient. With the view to strengthen cyber security and cyber resilience frameworks of the MIIs, SEBI in October 2013 had advised MIIs to assess their level of preparedness vis-à-vis the critical controls and the guiding principles mentioned in the report 'Guidelines for protection of National Critical Information Infrastructure, June 2013' of

<sup>14</sup> Weblink to SEBI circulars:

[http://www.sebi.gov.in/cms/sebi\\_data/attachdocs/1436179654531.pdf](http://www.sebi.gov.in/cms/sebi_data/attachdocs/1436179654531.pdf)

[http://www.sebi.gov.in/cms/sebi\\_data/attachdocs/1459250540053.pdf](http://www.sebi.gov.in/cms/sebi_data/attachdocs/1459250540053.pdf)



National Critical Information Infrastructure Protection Centre (NCIIPC), National Technical Research Organisation (NTRO).

2.3.2.4. In addition to the above, SEBI has issued various advisories to MIIs in the area of incident reporting, monitoring and surveillance of IT assets including website and network traffic, strengthening of cyber security framework of their websites, etc.

2.3.2.5. With the view to further strengthen the aforementioned framework, SEBI is institutionalizing / has institutionalised the following three-tier structure in securities market *to monitor cyber security related events and take actions as deemed necessary* in the interest of the securities market:

- (a) Tier 1: High Powered Steering Committee on Cyber Security chaired by a Whole Time Member of SEBI,
- (b) Tier 2: Cyber Security Centre / Lab,
- (c) Tier 3: A Cyber Cell in SEBI to coordinate with the Steering Group, Cyber Security Lab / Center and Security Operations Centres (at SEBI and respective MIIs).

2.3.2.6. The High Powered Steering Committee on Cyber Security (HPSC-CS) is chaired by Whole Time Member, SEBI. Other members of the committee are: a member of SEBI's Technical Advisory Committee (TAC), a cyber-security expert from a Government organization [DG (CERT-In)], and Executive Director of SEBI's Market Regulation Department. The panel will oversee and provide overall guidance on cyber security initiatives to SEBI and for the entire capital market

### **2.3.3.. IRDAI initiatives on Cyber Security:**

**2.3.3.1.** The insurance market has various layers namely the insurers, the insurance intermediaries and insurance agents. Each of them is at a different level of maturity. The insurers being the risk carriers and storekeepers of customer information are expected to have the highest standards of cyber-security. The next are the insurance intermediaries who also deal with customer/ client information. The risks which these insurers and insurance intermediaries face in the cyber world include the risk to their own system being hacked and the other is the customer personal information relating to his health and assets being compromised in such cyber-attacks. The insurers and insurance intermediaries are therefore expected to have systems which are secure against such cyber-attacks. The insurers and insurance intermediaries exchange information between themselves and the customers. Therefore, the information exchange has to be secure and safe. This would require sending encrypted messages, having firewalls, encrypted storage, etc. The second risk is the leakage of the personal information of the customer for which the insurer or the insurance intermediary could be sued. This requires a very high degree of security on part of the insurer and insurance intermediary.

2.3.3.2. In order to have a better understanding and an overview of Fin-Tech developments and possible implications in particular in insurance, International Association of Insurance Supervisors (IAIS) is going to establish a task force to (i) do a stock take of Fin-Tech developments and possible implications that are relevant to the insurance industry and insurance supervision, (ii) present a report with findings and recommendations for a strategic approach and possible follow-up work.

2.3.3.3. Further, in order to strengthen the existing cyber security framework and to put in place a more comprehensive framework, IRDAI has recently constituted two working groups for life and general (including Health) insurance sectors involving Chief Information Officers (CIO) of all insurers to deliberate and decide on various issues related to cyber security. The working groups of CIOs met and decided on the approach methodology for drafting of proposed framework. The Working Group decided to form three sub-groups comprising of CISOs, IT Experts and Cyber Law experts of Insurance companies to work on various issues related to Information and Cyber Security: (i) Group-1 All four layers of security (Data, Applications, Operating systems and Network layers), (ii) Group-2 (Security Audit), Group-3 (Legal aspects on Cyber Security)

2.3.3.3.1. The working group of CIOs also decided to include both information and cyber security aspects in the proposed framework. The subgroups were led by Chief Information Security Officers of IRDAI.

2.3.3.4. National Security Council (NSC) recently reviewed a few of the insurance companies on their IT infrastructures, the steps taken by them to secure their data & IT infrastructures, from various types of cyber-attacks being faced; and provided their formal recommendations to further strengthen the cyber security aspects of insurers. The summary recommendations of NSC are as follows:

- (i) Adequate protection and care is needed for transactions from Mobile.
- (ii) Systems need to be in place for updating and hardening of software and devices with respect to updates and upgrades.
- (iii) An integrated system needs to be in place to capture the data from devices to monitor and analyze the threats.
- (iv) Comprehensive audit to be done to identify the gaps in IT Security.
- (v) Sharing of logs (related to attacks) with CERT -  
Conducting of Regular Audits.
- (vi) While drafting the policies, the requirements of the company should be studied thoroughly and policies should be implemented in tune with the practical needs of the organizations.
- (vii) Having discreet policies should be minimized.
- (viii) All applications must be tested thoroughly for cyber security before deployment.

**2.3.3.5.** The sub groups formed by IRDAI reviewed various international standards on Information & Cyber security, and formulated the draft information and cyber security frame work by adopting the following approach

- (i) The existing frame works like ISO 27001 and the Guidelines of RBI may be taken as basis.
- (ii) Risks which are exclusive to the insurance sector need to be assessed and framework needs to be made accordingly.
- (iii) Risks related to adoption of new technology such as cloud computing, Mobile computing etc. need to be assessed.
- (iv) Best practices adopted by Insurers (originated from foreign partners / Group companies) to be studied and incorporated.
- (v) Prepare a list of audit controls using the best practices adopted by insurers
- (vi) Formulate a comprehensive reference document for the use of regulated entities by combining various laws / guidelines on Information & Cyber Security in India.

2.3.3.6. Exposure draft on Information and Cyber Security framework for insurance sector: The sub-groups had several rounds of discussions and came out with draft framework for insurance sector including a control check-list and a reference document containing various legal provisions available in India related to information and cyber security. The exposure draft on Information and Cyber security framework for insurance sector was issued by IRDAI on 2nd March 2017 for comments of all regulated entities and connected stakeholders. The comments received were deliberated and incorporated wherever appropriate. The recommendations of NSC and CERT-In were also incorporated in the framework. During the evaluation of draft framework, it was felt that the cyber risk related issues of intermediaries and other regulated entities with whom policy holder information is being shared by insurers, should be handled by insurers as they mainly deal with insurers. It was also decided to issue the framework as a guideline document through appropriate sections of IRDA Act 1999.

2.3.3.7. The Guidelines on Information and Cyber Security for insurers was issued by IRDAI on 7<sup>th</sup> April 2017 under Sub-section (1) of Section 14 of IRDA Act 1999 with strict timelines for implementation of various aspects of the guideline document. Insurers who have not completed three years from the date of commencement of business have been exempted from the requirement of a full-time person appointed as Chief Information Security Officer (CISO). However, the CISO responsibility may be taken care of by any of the functionaries reporting to the Board. All other requirements stipulated in the guidelines document shall be applicable to these insurers.

**2.3.3.8.** Objectives of Information and Cyber Security Guidelines are as below:

- (i) To ensure that a Board approved Information and Cyber Security policy is in place with all insurers.

- (ii) To ensure that necessary implementation procedures are laid down by insurers for Information and Cyber Security related issues.
- (iii) To ensure that insurers are adequately prepared to mitigate Information and cyber security related risks.
- (iv) To ensure that an in-built governance mechanism is in place for effective implementation of Information and cyber security frame work.

2.3.3.9. Salient aspects of the Guidelines are as below:

- (i) Mandating insurers to have Board approved Information and Cyber Security policy.
- (ii) Establishment of appropriate self-governance mechanism at insurer level for effective implementation of IS policy.
- (iii) Appointment of Chief Information Security Officer (CSIO) who will be responsible for designing, enforcing IS policy and also who will act as a Single Point of contact (SPOC) for IRDAI.
- (iv) Involvement of Board in designing and enforcement of Information and Cyber Security policy.
- (v) Formation of Information Security Committee (ISC) with a senior level executive with Information Security Audit background with a reporting line to the Board to take overall responsibility for the information security governance framework.
- (vi) Formation of Information Security Team to implement and to focus exclusively on information security management.
- (vii) Internal Audit for ensuring compliance of IS Policy.
- (viii) Annual mandatory Information Security Audit for all insurers.
- (ix) Mandating insurers to establish a Security Operation Center (SOC) at Insurer level for monitoring of Network Security.

2.3.3.10. The guidelines broadly cover the aspects such as access control management, vendor/third party Risk Management, business continuity plan and disaster recovery, information security risk management, data security, application security, cyber-security, infrastructure security, network security, cryptography and key management, security logging and monitoring, incident management, end-point security, virtualization, cloud security and mobile security

2.3.3.11. Every Insurer has been mandated to appoint/designate a suitably qualified and experienced senior level officer exclusively as Chief Information Security Officer (CISO)

who will be responsible for articulating and enforcing the policies to protect their information assets. The policy for Information and Cyber Security shall be established by Insurers based on the Guidelines issued in this document. CISO would be responsible for the following activities:

- (i) Articulating Information and Cyber Security policy for the Organisation and getting the same approved from Board through Information Security Committee (ISC).
- (ii) Preparing an Information and Cyber Security Assurance Programme (implementation plan/ Implementation guidelines) based on the approved Policy.
- (iii) Building and leading the information security team with appropriate competencies and attitude to deliver the information security program.

2.3.3.12. Insurers have been advised to form an Information Security Committee (ISC) headed by a senior level executive with a reporting line to the Board to take overall responsibility for the information security governance framework. Members of ISC shall include functional heads from Operations, Information Technology, Legal, Compliance, Finance, HR, Risk etc.

2.3.3.13. Role of Information Security Committee is as below:

- (i) Review and recommend to the Board necessary changes to the high level IS Policy.
- (ii) Approve standards and procedures in line with the Board-approved IS policy.
- (iii) Review and approve exceptions to the Information Security Policy, any significant risk to be reported to the Board. However, operational level exceptions can be approved by respective business owner in consultation with CISO.
- (iv) Recommend changes to the constitution and functioning of the committee.
- (v) Review, discuss and direct information security risk mitigation (which includes reporting security incidents).
- (vi) Ensure that risks are accurately reported and appropriately dealt with.
- (vii) Ensure compliance to regulatory and statutory requirements related Information Security.
- (viii) Be responsible to ensure management of cyber security initiatives and incident management.
- (ix) Ensure that the information security governance framework is supported by an information security assurance programme (Implementation Plan).
- (x) Report to Risk Management Committee of the Board a minimum of two times in a year.
- (xi) CISO shall be convener of the Information Security Committee.

2.3.3.14. Insurers have been advised to form a separate information security Team to focus exclusively on information security management. The constitution of the IST would be commensurate with the nature and size of activities of the organization. The information security team 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.

2.3.3.15. Roles and responsibilities of Information Security Team are as below:

- (i) Develop and maintain IS policy, standards, procedures and guidelines to support the organization's information security program.
- (ii) Translate the information security program into specific actions which shall include awareness, security infrastructure, security incident response and risk management.
- (iii) Work closely with IT and other functional teams and monitor implementation of information security projects and controls for new or identified deficiencies.
- (iv) Identify current and potential legal and regulatory issues affecting information security and assess their impact in conjunction with legal and compliance team.
- (v) Act as consultants and advisors to different stakeholders for information security matters.
- (vi) Perform information security risk assessments on an on-going basis and report any significant risks to ISC.
- (vii) Monitor information security incident management i.e. identification, response, remediation and reporting.

2.3.3.16. Insurers have been advised to conduct annual audit which shall be through qualified external systems Auditor holding certifications like CISA/ DISA /Cert-In empanelled Auditor etc. The Annual IS Audits shall also cover branches on sample basis. The assurance audit shall be primarily driven by the Information Security Team.

2.3.3.17. Insurers have been directed to complete the following activities in a stipulated time frame:

- (i) Appointment/ designation of a suitably qualified and experienced Senior Level Officer exclusively as Chief Information Security Officer (CISO) who will be responsible for articulating and enforcing the policies to protect their information assets and formation of Information Security Committee (ISC)
- (ii) Preparation of Gap Analysis report (as-is vs, requirements stated in the guidelines document)
- (iii) Formulation of Cyber Crisis Management Plan
- (iv) Finalization of Board approved Information and Cyber Security Policy

- (v) Formulation of Information and Cyber Security assurance programme (implementation plan / guidelines) in line with Board approved Information and Cyber security policy
- (vi) Completion of first comprehensive Information and Cyber Security assurance audit by 31st March 2018.

2.3.3.18. IRDAI is also in the process of formulation of a separate team headed by a General Manager level officer for Information and Security Audit for Insurers (ISAI), to take care of the following activities:

- Periodical assessment of Information & Cyber Security status of Insurers.
- Review Audit reports on Cyber Security Audit.
- Conduct inspections on Cyber Security, if necessary.
- Provide periodical updates to entities on latest threats, prevention and mitigation solutions by co-ordination with other agencies in financial and other sectors.

2.3.3.19. The team will have divisions to take care of life, non-life insurers and intermediaries separately. Through the Information and Cyber Security Guidelines, IRDAI has mandated the insurers that appropriate governance is in place at their level to handle the information and cyber security related issues on an ongoing basis. The proposed mandatory annual IS audit through an effective control check list will ensure that guideline document is fully implemented.

2.3.3.20. Insurance Regulatory and Development Authority of India (Insurance e-commerce) Regulations, 2016: IRDAI recently issued guidelines on e-commerce to promote insurance business through Insurance Self-Network Platform (ISNP) which is a technology platform to undertake Insurance e-commerce activities in India such as selling and servicing of insurance products.

2.3.3.21. ISNPs have also been mandated to ensure compliance on the following:

- (i) ISNP is protected against unauthorized access, alteration, destruction, disclosure or dissemination of records and data;
- (ii) The network through which electronic means of communications are established amongst the market participants on applicant's ISNP is secure against unauthorized entry or access;
- (iii) ISNP has standard transmission and encryption formats amongst the market participants on the platform in order to protect the information from any disruption, hacking, etc;
- (iv) the applicant's ISNP has established adequate procedures and facilities to ensure that it is protected against loss or destruction; and arrangements have been made for disaster recovery at a location different from the existing place;
- (v) the applicant's ISNP has a mechanism in place to ensure that the interests of the persons buying policies or other services under insurance policies including their privacy on the ISNP are adequately protected

- (vi) ISNP has Management Information System supporting internet based insurance business operations in order to realize a real-time connection with insurance core systems; and of ensuring effective isolation between other application systems of the insurers, avoiding the external transmission and spread of information security risks for insurers;
- (vii) ISNP has robust firewall, intrusion detection, data encryption, disaster recovery and other internet information security management systems;
- (viii) ISNP has the domain name of the website registered and with servers hosting them located within India;
- (ix) ISNP has specialized internet insurance business administration, equipped with appropriate professionals.

2.3.3.22. A review on the controls, systems, procedures and safeguards put in place by the insurance Self-Network platform, shall be carried out, at least once a year by ISNP through an external certified information system auditor (CISA) at their cost.

#### **2.3.4. PFRDA initiatives on Cyber Security**

##### **2.3.4.1 Proposed Cyber security policy for intermediaries registered with PFRDA**

2.3.4.1.1 Applicability: The policy guidelines shall be applicable to Central Recordkeeping Agencies (CRAs), Pension Funds and Custodian which form part and parcel of the critical Information Technology infrastructure under the National Pension System (NPS). The intermediaries as mentioned above shall comply with the framework as provided below on cyber security of the critical IT infrastructure being developed and maintained by them:

- (i) As part of the operational risk management framework to manage risk to systems, networks and databases from cyber-attacks and threats, intermediaries shall formulate a comprehensive cyber security and cyber resilience policy document encompassing the framework mentioned hereunder. The policy document should be approved by the Board, and in case of deviations from the suggested framework, reasons for such deviations should also be provided in the policy document. The policy document should be reviewed by the Board of the intermediary at least annually with the view to strengthen and improve its cyber security and cyber resilience framework.
- (ii) The Cyber security policy should encompass the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organisation (NTRO), the nodal agency under Section 70A(1) of the Information Technology (Amendment) Act 2008 in the report titled 'Guidelines for Protection of National Critical Information Infrastructure' and subsequent revisions, if any, from time to time.

2.3.4.1.2. Broadly, the following steps shall be undertaken by the intermediary to arrive at the comprehensive cyber security and cyber resilience policy document:



- (i) Risk assessment: Intermediary shall 'Identify' critical IT assets and risks associated with such assets,
- (ii) Security design and implementation: Intermediary shall plan for all efforts to 'Protect' assets by deploying suitable controls, tools and measures. In order to protect the assets, policies with respect to the following shall be clearly laid down and adhered to by the intermediary at all times: (a) Access Controls (b) Physical security (c) Network Security Management (d) Security of Data (e) Hardening of Hardware and Software (f) Application Security and Testing (g) Patch Management (h) Disposal of systems and storage devices (i) VAPT
- (iii) Security management: Intermediary shall plan for all efforts to 'Detect' incidents, anomalies and attacks through appropriate monitoring tools / processes,
- (iv) Response: Intermediary shall "respond" by taking immediate steps after identification of the incident, anomaly or attack.
- (v) Recover: Intermediary shall "Recover" from incident through incident management, disaster recovery and business continuity framework.
- (vi) Reassessment: Intermediary should also conduct suitable periodic drills to test the adequacy and effectiveness of response and recovery plan.

2.3.4.1.2. The cyber security policy of the intermediary should incorporate best practices from standards such as ISO 27001, ISO 27002, COBIT 5, etc., or their subsequent revisions, if any, from time to time.

2.3.4.1.3. Intermediary should designate a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify and reduce cyber security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cyber security and resilience policy approved by the Board of the intermediary. Intermediary should establish a reporting procedure to facilitate communication of unusual activities and events to CISO or to the senior management in a timely manner. The aforementioned committee and the senior management of the intermediary, including the CISO, should periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen cyber security framework in a holistic manner.

2.3.4.1.4. Quarterly reports containing information on cyber-attacks and threats experienced by intermediary and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs / vulnerabilities / threats that may be useful for other intermediaries shall be submitted to the Authority (PFRDA).

2.3.4.1.5. Intermediaries should conduct periodic training programs to enhance awareness level among the employees and outsourced staff, vendors, etc. on IT / Cyber security policy and standards. Special focus should be given to build awareness levels

and skills of staff from non-technical disciplines. Such training program should be reviewed and updated at periodic intervals to ensure that the contents of the program remain current and relevant.

## **2.4. Other Sectoral CERTs**

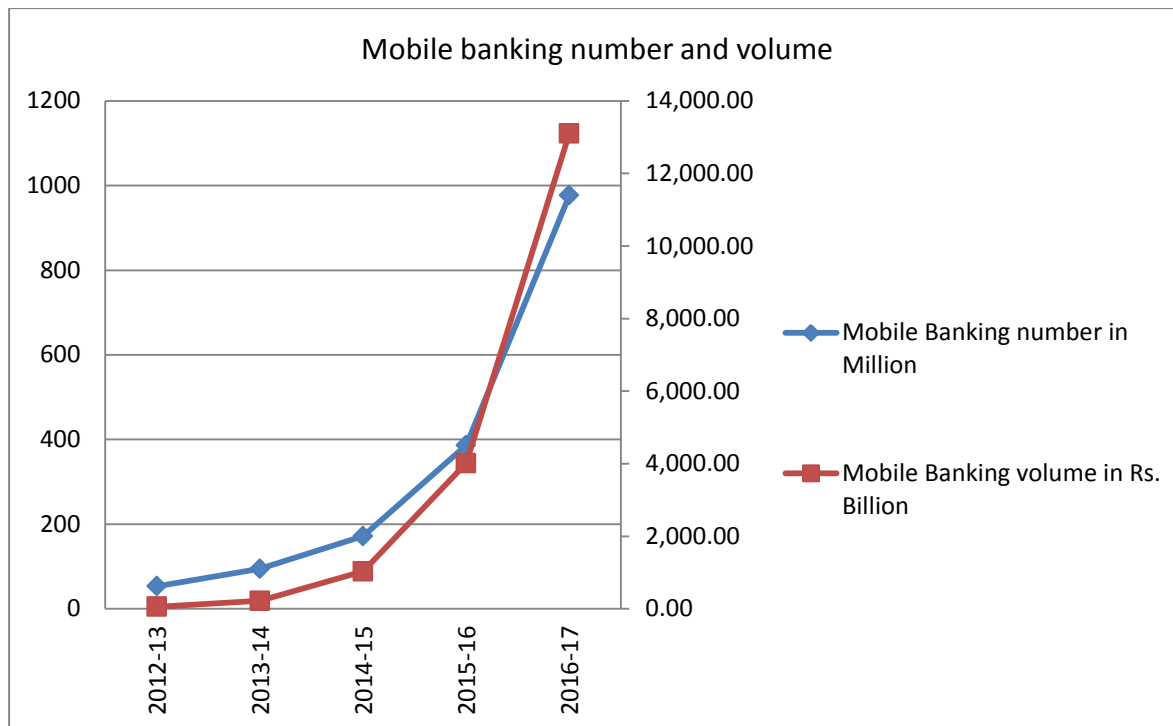
The Working Group in its first meeting attempted to understand the working of various sectoral CERTs operating in our country, in order to design the structure of CERT in the financial sector, wherein it was noted that Power CERT and Defence CERT are already operating in the Country and Department of Telecommunications is in the process of establishing a telecom CERT. A workshop was also held with all the working Group members, under the chairpersonship of DG (CERT-In), to understand the working of CERT-In and various sectoral CERTs. The Group in its second meeting noted the interlinkages between telecom and financial sector and decided to invite representatives from telecom sector who were invited for the third meeting of the Working Group held on 5<sup>th</sup> May 2017. While TRAI representative couldn't attend the meeting and was briefed on its limited role in cyber security for telecom sector, in a separate meeting in DEA, DoT representative attended the third meeting of the Working Group and highlighted the activities undertaken by DoT in the cyber security space. Also the strong linkages of telecom sector and finance sectors were highlighted and status of telecom CERT was informed to the Working Group. The detailed analysis of the various sectoral CERTs including the inter-linkages between telecom and financial sector are as below:

### **2.4.1. Telecom Sector and its inter-linkages with Financial Sector**

2.4.1.1. As on December, 2016<sup>15</sup>, the country had 1.1 billion mobile connections and 390 million internet subscribers. The growth in number of mobile connections as well as internet subscribers has seen phenomenal growth in the recent years. As per the NASSCOM-AKAMAI report 70% of E-commerce transactions will happen on mobile by 2020. As per the BCG Google Report (BCG & Google, Digital Payment 2020 - The making of the \$500 Billion Ecosystem in India, July 2016), the total conducted via digital payments will be in the range of USD 500 billion. By 2020, India will have 1150 million mobile phones; 25-30% of them will have Internet connections on them. The use of Indian digital payment markets will reach \$500 Billion by 2020 (Rebello, July, 2016), from 9% in 2010. It is estimated that the same will reach to 48% by 2025. With the Government announcing use of mobile apps for digital payment transactions, these numbers are likely to increase significantly in times to come. Aadhaar Enabled Payment Services (AEPS) is also triggering large scale migration to digital payments. One of the features of the payment channels is that they are inter-operable to facilitate customer ease.

---

<sup>15</sup> Data released by Telecom Regulatory Authority of India (TRAI)



Source: DFS

2.4.1.2. The Working Group was informed that the Central Government has exclusive privilege of establishing, maintaining and working telegraphs under Section 4 of the Indian Telegraph Act 1885. Accordingly the services are provided in India through licensed operators within a framework of the license conditions. Security has been an important item for engagement with the telecom industry and especially with the service providers. After detailed consultations with the industry and intra-government consultations Department of Telecommunications (DoT) had earlier amended the Service License Agreements for various categories of services incorporating clauses for security related concerns in May/June, 2011. As per the conditions the licensees are completely and totally responsible for the security of their networks. They shall have an organisational policy on security and security management of their networks. network forensics, network hardening, network penetration test, risk assessment, actions to fix problems and to prevent such problems from reoccurring etc should be part of the policy. The license condition mandates the service providers to audit their networks or get their network audited from security point of view once a year from a network audit and certification agency.

2.4.1.3. Further, the licensee is mandated to induct only those network elements into his network which have got security tested and copies of test results and test certificates are to be kept by the licensee for a period of 10 years from the date of procurement of the equipment. The licensee is to employ only resident, trained Indian nationals as CTOs, CISO, and as in-charges of identified important technical installations. A record of all operation and command logs is required to be kept for a period of 12 months, which should include the actual command given, who gave the command, when it was given and from where. For the next 24 months the same information is required to be

stored/retained in non-online mode. A record is to be kept of all software updates and changes. Detailed guidelines on Remote Access have been issued and the licensees are to comply with the conditions set out therein. The licensees are also required to create facilities for monitoring all intrusions, attacks and frauds and report to Licensor and CERT-In

2.4.1.4. In case of inadvertent inadequacies in precaution on the part of licensee as prescribed in the licence conditions, a provision has been kept to levy up to Rs.50 crore penalty for any security breach. A five member committee shall examine the nature of the breach and quantum of penalty. In case of inadequate measures, act of intentional omissions, deliberate vulnerability left in the equipment or in case of deliberate attempt for a security breach, penalty amount will be Rs. 50 crores per breach. This is in addition to any liability and criminal proceedings under relevant acts.

2.4.1.5. The Group was also informed that DoT prepared 16 templates which are based on the above mentioned license amendments, inter-ministerial consultations, and discussions with various TSPs for DoT teams to conduct security audit of the Telecom networks in India from network security angle. In March 2016, DoT conducted a joint Security Audit which included Officers of DoT, HQ, field Units and members of TSPs/ISPs to understand the security scenarios of Telecom networks in India. Thereafter, Field Units have conducted 14 Security Audits of TSPs/ISPs networks in 2016-17. DoT will soon conduct a workshop with all field Units to share their experiences and evolve mechanism to further harden telecom networks in India.

2.4.1.6. After release of National Cyber Security Policy, 2013 (NCSP-2013), which has provision for setting up of sectoral CERTs, a committee has been formed in DoT including members from DoT, CERT-In, NCIIPC and NSCS. The terms of reference of the committee are as follows:

- i. To suggest an organizational structure for the proposed Telecom-CERT.
- ii. To suggest the functionalities and responsibilities of proposed Telecom-CERT.
- iii. To identify the infrastructure requirements for creation of the Telecom –CERT.

2.4.1.7. The establishment of the Telecom CERT is a work in progress with active cooperation from CERT-In. DoT has communicated email address [cert-telecom@gov.in](mailto:cert-telecom@gov.in) to TSP/ISPs, CERT-In and NCIIPC for communication regarding security incidents, frauds, intrusions in the telecom network and advisories, if any.

## **2.4.2. Power CERT & Defence CERT**

2.4.2.1. Keeping in view the importance of cyber security, it is learnt that the Ministry of Power has constituted following four domain specific CERTs in Power Sector:

- (i) CERT-Thermal – Coordinated by designated officer of NTPC (PSU engaged primarily in thermal generation)
- (ii) CERT-Hydro – Coordinated by designated officer of NHPC (PSU engaged in hydro generation)
- (iii) CERT-Transmission – Coordinated by designated officer of Power Grid Corporation of India Ltd. (PSU engaged in the activities related to transmission of power)
- (iv) CERT-Distribution – Coordinated by designated officer of Distribution Planning & Development Division of CEA

2.4.2.2. The information of Chief Information Security Officers of respective sectoral CERTs is available on [http://www.cea.nic.in/isac\\_nodalofficers.html](http://www.cea.nic.in/isac_nodalofficers.html). The co-ordination work between the Ministry and respective Sectoral Power CERT is undertaken by Director (IT) of Central Electricity Authority. The activities of Sectoral Power CERTs are discussed and reviewed during meetings held on quarterly basis. The actions taken by Sectoral Power CERTs are as under:

- i. Proper publicity of contact details of Sectoral CERT so that utilities can contact as and when required - Sectoral CERTs have sought nominations of nodal officers from Power Sector utilities by sharing their contact details. The contact details of Sectoral CERTs have been made available on the webpage of ISAC-Power (<http://www.cea.nic.in/isacpower.html>). The list of power utilities (sector-wise) was initially circulated among Sectoral Power CERTs. Thereafter, CISO of respective Sectoral Power CERT contacted the top management of power utilities for getting nomination of organization level CISO. Moreover, power utilities have been requested to formulate IT Security policy, create Incident Response Team for handling Cyber Security incidents at entity/plant level, conduct vulnerability assessment audit exercise and establish disaster recovery plan in their respective organization. By the beginning of this year, nominations from more than 85 power utilities (comprising of both private and government) have been received by Sectoral Power CERTs.
- ii. All advisories received from CERT-In and NCIIPC are timely shared with sectoral Power CERTs and thereafter with the nodal officers of power utilities.
- iii. Identification of cyber infrastructure: NTPC, NHPC, PGCIL including POSOCO Ltd have identified their cyber infrastructure. These organizations have laid down policy & procedure for ensuring protection & availability of both businesses as well as information infrastructure.
- iv. Coordination with CERT-In by sectoral CERTs: IT cyber security audit & Vulnerability Assessment Analysis of 'IT Cyber Security implementation & IT Network infrastructure' at NHPC Ltd. was done by CERT-In empaneled IT Security Auditing organization. In PGCIL, audit was undertaken by internal and external

auditors, for the compliance of ISO 27001 certification requirements. NTPC has been in touch with CERT-In for Incidence Reporting and remedial advisory.

- v. Crisis Management Plan (CMP) of sectoral CERTs: CMP of NHPC has been shared with CERT-In. NTPC is following the Crisis Management Plan (CMP) for countering cyber-attacks and cyber-terrorism, issued by CERT-In. PGCIL has obtained ISO-27001:2013 certification and CMP of POWERGRID is defined as part of its ISO-27001:2013 Information Security Management System.
- vi. Information Sharing and Analysis Centre (ISAC): The concept of Information Sharing and Analysis Centre (ISAC) was formulated by Data Security Council of India (DSCI). ISACs have to evolve from sharing of information to information analysis and maintaining of inventory of Critical Information Infrastructure (CII), issuing standards and guidelines, standardizing audit standards and procedures.
  - a. As per recommendations of the Joint Working Group (JWG) Sub-Group on 'Vulnerabilities in Critical Information Infrastructure' submitted to JWG on Public Private Partnership (PPP) in Cyber Security, Sectoral ISACs to start with, should only provide information sharing services. Only when this service becomes successful, should it extend its service portfolio to include information analysis, threat determination of a Sector, Sector specific studies and surveys, creating and maintaining inventory of Critical Information Infrastructure (CII) within the Sector, security standards and audit processes, among others. The ISAC should not be legally responsible for handling security incidents but should only facilitate incident response, under the directions of CERT-in. It was decided to entrust the responsibility of establishing ISAC on Sectoral Power CERTs. Presently, the ISACs are envisaged to provide a platform for sharing of cyber security related information.
  - b. Webpage for ISAC-Power for Power Sector CERTs was initially developed and hosted on CERT-In website (<http://www.cert-in.org.in>) on 10<sup>th</sup> September, 2014. Later, ISAC-Power section has also been made part of CEA website (<http://www.cea.nic.in/isacpower.html>).
- vii. Cyber Security Training Programme: Cyber Security related sensitization programmes are being attended by the officials of Sectoral Power CERTs and CEA. NHPC has conducted Cyber Security awareness session for NHPC officials and CERT-Hydro constituent CPSUs. In NTPC, IT awareness guidance to employees is given to mitigate security breaches. In PGCIL, various state utilities have been sensitized on cyber security matters. The concerned officers regularly attended training programme / workshops conducted by MeiTY/CERT-In, MHA, NCIIPC, etc.
- viii. Sharing of common incident reporting template amongst the Sectoral CERTs: The template in the CERT-in document "Crisis Management Plan for Countering Cyber Attacks and Cyber Terrorism has been shared amongst the Sectoral CERTs.

2.4.2.3. Defence CERT: Defence Information Assurance and Research Agency (DIARA) is the apex CERT for the Defence Services and functions as mother CERT for the three Services. It regularly engages with CERT-In as well as interacts with CERTs of the Army, Navy, Air Force and all other departments of Ministry of Defence. Additionally, as mother Defence-CERT, DIARA also has interactions with civil organizations dealing with cyber security such as NSCS/NCSC, NTRO, NCIIPC, DRDO etc. The activities of CERT-DIARA are as summarized below:-

#### 2.4.2.4. Interaction with CERT-In

- a) Information Sharing: CERT-In issues various advisories and alerts pertaining to Indian cyber space in its website as well as by email to nominated-group members. CERT DIARA receives these alerts/advisories and disseminates the relevant alerts to organizations under it as well as to the Services CERTs.
- b) Participation in National Level Drills: DIARA is regularly participating in the National Level Cyber Drills conducted by CERT-In. Participation in these Drills has helped formulate and validate various plans including Crisis Management Plan (CMP) and Disaster Recovery Plan (DRP).
- c) Training: CERT-In conducts training on various cyber security topics. DIARA has been sending its representatives for the same and thus utilizing these lectures for its capability enhancement

2.4.2.5. Interaction With Services CERTS: CERT-DIARA regularly interacts with the services CERT in various formal and informal forums. A functional level committee meeting is held and points of common interests are discussed. The interactions with the Services CERTs are in the following areas:-

- a) Information Sharing: Advisories, information, alerts etc. are shared between the Services CERTs.
- b) Sharing of Resources: The services share their resources. This helps in optimum utilization of resources and in overcoming limitations of any specific resources possessed by any individual CERT/Service.
- c) Training: DIARA plans and coordinates training of cyber security personnel. The courses are conducted through reputed institutes.

2.4.2.6. DIARA as the apex organization has permanent representation at national level forums. These interactions help in sharing of information as well as facilitating a common understating of current cyber security situation of the National cyber space.



## **CHAPTER 3**

## CHAPTER 3

# Cyber Security and the Financial Sector – International Developments

### 3.1. Computer Emergency Response Teams (CERTs) / Computer Security Incident Response Teams (CSIRTs)<sup>16</sup>

3.1.1. Given the concerns on cyber-security, several countries have established Computer Emergency Response Teams. The CERT (Computer Emergency Response Team) name is registered in the U.S. Patent and Trademark Office and was coined by Carnegie Mellon University (CMU) and subsequently has been adopted by organizations around the world. The name CERT requires permission from CMU. A more specific term CSIRT (Computer Security Incident Response Team) is also widely used<sup>17</sup>. Today, the Software Engineering Institute at CMU manages the CERT program and provides training and support for setting up a CSIRT. In addition, Network Security Group at Internet Engineering Task Force (IETF) has issued an RFC-2350 that describes the “Expectations of Computer Security Incident Response”. These works were done in late 1990s and even though the awareness and number of cybercrime incidents have subsequently grown exponentially, these references still provide a good overview and understanding of a CERT’s role and responsibility. (Terms CERT and CSIRT are interchangeably used in this document)

3.1.2. The scope of a CERT is organized around a constituency and depending upon the definition of a ‘constituency,’ CERTs can be created at different levels to service their constituencies. The CERT needs to clearly define procedure and policies and expectations from the constituent participants. A good clarity around what values the response team bring to the constituency is important. Typically, the CSIRT’s constituency will fund the team, determining who it provides services to as well as the kinds of services it will offer. However, some CSIRTs are funded by other organizations or institutions. For example, CGI.br provides CSIRT services to the government of Brazil, but it is not a national CSIRT. To maintain this independence, CGI.br receives its funding from domain name registration in Brazil (Best Practice Forum 2015).

3.1.3. A Handbook for CSIRTs (2<sup>nd</sup> Edition – 2003) has been published by the Carnegie Mellon University – SEI, clearly articulating the role of CSIRTs<sup>18</sup> and how they are to be set up. This document provides guidance on forming and operating a computer security incident response team (CSIRT). In particular, it helps an organization to define and document the nature and scope of a computer security incident handling service, which

---

<sup>16</sup> <https://www.enisa.europa.eu/publications/nis-directive-and-national-csirts>

<sup>17</sup> NIS Directive and national CSIRTs, February 2016, Info Note, ENISA. <https://www.enisa.europa.eu/topics/national-csirt-network/capacity-building/european-initiatives/cert-eu>

<sup>18</sup> Bradshaw, Samantha, Combating Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity (December 8, 2015). Global Commission on Internet Governance Paper Series, Paper no. 23. Available at SSRN: <https://ssrn.com/abstract=2700899> or <http://dx.doi.org/10.2139/ssrn.2700899>

is the core service of a CSIRT. The document explains the functions that make up the service; how those functions interrelate; and the tools, procedures, and roles necessary to implement the service. This document also describes how CSIRTs interact with other organizations and how to handle sensitive information. In addition, operational and technical issues are covered, such as equipment, security, and staffing considerations.

3.1.4. CSIRT services can be grouped into three categories:

- (i) Reactive services. These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system. Reactive services are the core component of CSIRT work.
- (ii) Proactive services. These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future.
- (iii) Security quality management services. These services augment existing and well established services that are independent of incident handling and traditionally performed by other areas of an organization such as the IT, audit, or training departments. If the CSIRT performs or assists with these services, the CSIRT’s point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses. These services are generally proactive but contribute indirectly to reducing the number of incidents.

3.1.5. The services that each CSIRT provides should be based on the mission, purpose, and constituency of the team. List of Common CSIRT Services is given in the Table below:

Reactive Services 	Proactive Services 	Security Quality Management Services 
<ul style="list-style-type: none"> <li>+ Alerts and Warnings</li> <li>+ Incident Handling                             <ul style="list-style-type: none"> <li>– Incident analysis</li> <li>– Incident response on site</li> <li>– Incident response support</li> <li>– Incident response coordination</li> </ul> </li> <li>+ Vulnerability Handling                             <ul style="list-style-type: none"> <li>– Vulnerability analysis</li> <li>– Vulnerability response</li> <li>– Vulnerability response coordination</li> </ul> </li> <li>+ Artifact Handling                             <ul style="list-style-type: none"> <li>– Artifact analysis</li> <li>– Artifact response</li> <li>– Artifact response coordination</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>○ Announcements</li> <li>○ Technology Watch</li> <li>○ Security Audit or Assessments</li> <li>○ Configuration &amp; Maintenance of Security Tools, Applications, &amp; Infrastructures</li> <li>○ Development of Security Tools</li> <li>○ Intrusion Detection Services</li> <li>○ Security-Related Information Dissemination</li> </ul>	<ul style="list-style-type: none"> <li>✓ Risk Analysis</li> <li>✓ Business Continuity &amp; Disaster Recovery Planning</li> <li>✓ Security Consulting</li> <li>✓ Awareness Building</li> <li>✓ Education/Training</li> <li>✓ Product Evaluation or Certification</li> </ul>

Source : CSIRT Services published by CMU-SEI

3.1.6. ‘Paper series: no. 23-December 2015 - Combatting Cyber Threats: CSIRTs and Fostering international Cooperation on Cybersecurity’ by Samantha Bradshaw and

published by Global Commission on Internet Governance breaks down the classification of teams into three major categories, based on the parent organization. These categories are:

- a. **National CSIRTs:** National CSIRTs are the national point of contact for incident response. Broadly speaking, they carry out certain aspects of a state's cyber defence policy -usually by issuing various alerts and warnings, handling aspects of cyber incidents or providing training and education to government constituents. Some national CSIRT capabilities are very advanced and are part of a larger national security operations centre; others are less developed and operate within a particular government department such as law enforcement, military or the ministry of technology or telecommunications. In some countries, more than one national CSIRT exists. Examples of national CSIRTs include the CERT Coordination Centre of Korea, the Canadian Cyber Incident Response Centre, CERT-SE of Sweden and the Chilean Computer Emergency Response Team.
- b. **Private CSIRTs:** These CSIRTs operate for or within a private organization and respond to incidents for their defined constituents. Private CSIRTs could serve a company internally, such as a bank, Internet service provider, or a chemical or Petroleum Company, or they could be a public-facing for-profit vendor that sells CSIRT services to individuals or companies that do not have in-house security functions. Private CSIRTs can also operate across private companies or across a particular industry category such as banking or e-commerce. Examples of private CSIRTs include the Amazon Security Incident Response Team, the Financial Services Information Sharing and Analysis Centre, the Canadian Imperial Bank of Commerce Incident Response Team, the Symantec CERT and the Verizon CSIRT.
- c. **Technical or Academic CSIRTs:** CSIRTs in this category serve a university or a technical organization, or promote research, education and information sharing within a non-governmental organization. Examples include the Internet Corporation for Assigned Names and Numbers CIRT, the CERT/CC and the Oxford University CERT. Regional organizations such as Asia Pacific CERT (APCERT) or Africa CERT are also included in this category.

### **3.2. International Practices in establishing CERT/ CERT-Fin**

3.2.1. In the second meeting of the Working Group, it was decided that the international experience of Financial CERTs need to be studied thoroughly before reaching a final decision on the structure of CERT-Fin for India. This section describes how the CERTs are structured in other countries. It is not possible to provide comprehensive information and few major CERT formulations in other countries have been documented which is at Annex 1. The status on cyber security set up from various Countries, considered by the Working Group, can be summarized as below:

S.N	Countries	Key lessons
1	United States	President's Cyber-security National Action Plan (CNAP) <sup>19</sup> directs the Federal Government to take new action now and fosters the conditions required for long term improvements in their approach to cyber-security across the Federal Government, the private sector, and personal lives. President on February 9, 2016 established a Commission on Enhancing National Cyber-security <sup>20</sup> that bring top strategic, business, and technical thinkers from outside the government to make critical recommendations on how to use new technical solutions and best practices to protect privacy and public safety. Computer Emergency Readiness Team, United States of America (US-CERT) established in 2003, the Financial Sector - Information Sharing Analysis Center (FS-ISAC) established in 1999.
2	Canada	<i>Canadian Cyber Incident Response Centre (CCIRC)</i> is Canada's national coordination centre responsible for reducing the cyber risks and all CCIRC's cyber awareness products for their partners have one of four information sharing levels (Ex: Public/Private), commonly known as the Traffic Light Protocol (TLP) Viz., Red, Amber, Green and White
3	European Union	EU has a permanent Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies since 2012. The European Union Agency for Network and Information Security (ENISA) set up in 2004 with overall goal of ensuring a high level of network and information security within the EU. In 2016, EU brought out a directive to establish CSIRTs network. The European FI-ISAC, the European Financial Institutes – Information Sharing and Analysis Centre was founded in 2008. <i>Members of the European FI-ISAC must sign the Traffic Light Protocol (TLP)</i> . The TLP is an agreement to ensure that sensitive information is shared according to requirements defined by the source individual/organisation. 32 Financial CERTs are operating in Europe
4	Germany	The S-CERT, are the computer emergency response team of the German Sparkassen-Finanzgruppe (Savings Banks Financial Group)
5	Denmark	The Financial Sector forum for Operational Resilience (FSOR) was set up in 2016. It is a forum for collaboration between authorities and key financial sector participants in Denmark aiming to increase operational resilience when using IT across the sector, including resilience to cyber-attacks. FSOR has arrangements to conduct cyber-stress tests etc.
6	United Kingdom	The National Cyber Security Centre (NCSC) is the UK's authority on cyber security. NCSC exchange talent with other organizations through secondments and interchanges; this allows them to foster the technical

<sup>19</sup>Michael Daniel, Tony Scott, Ed Felten, The President's National cybersecurity Plan: What You Need to Know, February 9, 2016

<sup>20</sup> Whitehouse.gov, Administration Efforts on Cybersecurity: The Year in Review and Looking Forward to 2016, February 2, 2016.

		innovation needed to succeed in an ever changing landscape. In 2013, CBEST Framework of UK was set up to put in place a programme of work to improve and test resilience to sophisticated cyber-attacks.
7	Australia	CERT Australia (the CERT) is the national computer emergency response team. They are the point of contact in Government for cyber security issues affecting major Australian businesses
8	Japan	The Financial Services Agency (FSA) has been conducting the supervision and inspection regarding cyber security management as a part of system risk control, etc. The Center for Financial Industry Information Systems (FISC) raise the level of FISC Security Guidelines, and publish the answers to inquiries from financial institutions regarding the interpretation of FISC Security Guidelines as “Cyber Security reference information.
9	New Zealand	CERT NZ was formed on April 11, 2017 at Ministry of Business, Innovation & Employment (MBIE), New Zealand Government to support businesses, organisations and individuals who are affected (or may be affected) by cyber security incidents.
10	Singapore	The Singapore Computer Emergency Response Team (SingCERT) was set up in October 1997. In 2015, a Cyber Security Agency (CSA) was established under the Prime Minister’s Office (PMO) and is managed administratively by the Ministry of Communications and Information (MCI). CREST (Council of Registered Ethical Security Testers) examination facility was opened in Singapore which offers penetration testing certifications and accreditations.
11	Hong Kong	In Hong Kong, the OGCIO (The Office of the Government Chief Information Officer) is responsible for articulating government-wide IT security policy and guidelines. Hong Kong Monetary Authority (HKMA) has undertaken a Cyber-security Fortification Initiative (CFI)
12	Brazil	CGI.br in 1997 created CERT Brazil (CERT.br) which is the national CERT for Brazil with responsibilities to collect public statistics on the incidents that are reported to them voluntarily.
13	Russia	The Russian Central Bank has established a centre ‘FinCERT’ for dealing with cyber-attacks in Russia's financial sector. This centre is responsible for collection and sharing of cyber-attack information in the Russian banking and financial sector.
14	South Africa	The Electronic Communications Security - Computer Security Incident Response Team (ECS-CSIRT), established in 2003 serves as the South African Government Computer Security Incident Response Team. South African Banking Risk Information Centre (SABRIC) was setup in 2002 by four major banks to track & respond to cybercrime targeting the banking sector.
15	China	The National Computer Network Emergency Response Technical

		Team/Coordination Center of China (known as CNCERT or CNCERT/CC) was founded in September 2002. As of 2016, CNCERT has established “CNCERT International Cooperation Partnership” with 185 organizations in 69 nations and regions.
16	Czech Republic	CSIRT.CZ is the National CSIRT of the Czech Republic. CSIRT.CZ fulfills the role of National CERT team as defined in the Act on Cyber security.
17	Nigeria	ngCERT (Nigerian Computer Emergency Response Team) is the National CERT for Nigeria which is domiciled in the Office of the National Security Adviser.
18	Sri Lanka	Bank Computer Security Incident Response Team (Bank CSIRT) is a joint initiative of the Central Bank of Sri Lanka and the Sri Lanka Computer Emergency Response Team (Sri Lanka CERT) and is hosted under Lanka Clear (Private) Limited, the national payment infrastructure provider.

### 3.3. Relevant lessons learnt for India-A discussion

3.3.1. The international best practices in Financial CERTS was studied by the Working Group in great detail and it was understood that major developed countries attach significant importance to cyber-security as may be seen from various initiatives taken by North America as well as at EU level. Cyber security related initiatives are getting reviewed periodically and improvements are brought about on a continuous fashion. In general, these countries have a strong National level CERT similar to CERT-In and this CERT coordinates its activity along with Industrial Control Systems at national level. Developed world does not operate a Fin-CERT generally. However, the financial sector has been identified as one of the critical infrastructure invariably by all these countries and as such an Information Sharing and Coordination Centre focused on financial sector is fully functional (e.g FS-ISAC, EFI-ISAC, ISAC-JP etc) and such arrangements are generally voluntary from the financial sector participants.

3.3.2. The Working Group noted that another unique aspect in these countries is the establishment of CSIRTs by individual institutions – in US it is mandated for all federal agencies and in Europe more than 30 CSIRTs are established by the constituency members as well as technology service provider firms. These CSIRTs coordinate their activities with the CERT as well as ISACs and have capacity to respond to cyber-incidents within their organisations effectively. In some countries, like Hong Kong, there are multiple National CERTs. One CERT takes care of all the public sector agencies and another CERT takes care of all the private sector agencies and citizens in general. Government CERTs play a lead role and the other CERT play along the Government CERTs. Broadly speaking, these countries have their cyber-security strategy finalised by their Government (through Ministry of IT or Electronics or Home), supported by a critical infrastructure monitoring arrangement, a CERT at National level, an ISAC at the

financial sector level, regulatory oversight over cyber-security related aspects by respective regulators and respective large institutions having capacity to handle cyber incidents on their own.

3.3.3 The Working Group also identified that in Sri Lanka, Fin-CERT (Bank-CERT) look at the financial sector exclusively. The arrangement is made by the CERT-Sri Lanka in coordination with the Central Bank of Sri Lanka. Italy has also set up a separate Fin-CERT to take care of the cyber-security issues among financial sector participants. In Italy, the arrangement has been put in place by the Central Bank of Italy in association with the Bankers' Association of Italy. The funding has been arranged voluntarily by the participants and the management is carried out by a steering committee. Central Bank has guided this arrangement so as to ensure that the Fin-CERT is effective. The Fin-CERT works in coordination with the country CERT as well as EFI-ISAC.

3.3.4. The Working Group viewed that, the most elaborate arrangement for financial sector has been put in place by Russia. Central Bank of Russia has set up a Fin-CERT exclusively for the financial sector. The difference here is the scope of activities defined for the Fin-CERT and its capacity to coordinate with various government agencies. This Fin-CERT is expected to work in close coordination with Ministry of Interior, Investigation agencies and External affairs. The scope includes monitoring the international transfer of money, monitoring money laundering activities as well as power to decide whether an account is to be frozen or not, certain fraud risk management activities etc. in addition to the technical activities of Fin-CERTs in general.

3.3.5. FSA, Japan, in terms of cyber security conducts a range of activities such as (a) constructive dialogue with financial institutions and grasp of their current condition regarding cyber security (b) improvement of the information sharing framework among financial institutions (c) continuous implementation of industry-wide cyber security exercises (d) cyber-security human resource development in financial sector (e) arrangement of cyber security initiatives in the FSA – A separate division; Expert panel. Indian financial system also at present conducts similar range of activities, for example; RBI hold (a) dialogue with regulated entities on a regular basis; IT examination reports discussed with banks; (b) cyber incident reporting framework; summary data on cyber security on a quarterly basis; Threat intelligence shared among banks (c) cyber-drills conducted periodically; based on hypothetical scenarios; Table top exercise prepares banks to face actual incidents;(d) IDRBT plays an important role in this. RBI also conducts seminars on important topics including cyber security; Top Management speeches focus on this area; (e) CSITE Cell at DBS focuses only on cyber-security; Standing Committee on Cyber-security. SEBI (a) periodically interacts with CISOs of the Market Infrastructure Institutions (MIIs) to discuss developments and challenges in the areas of cyber security, (b) has institutionalised the process of incident reporting by MIIs, (c) has constituted a *Cyber Security Cell* under its Market Regulation Department that focuses on strengthening of cyber-security framework of MIIs, the *High Powered Steering Committee on Cyber Security* to advise SEBI in developing and maintaining cyber



security and resilience requirements in Indian securities market.

3.3.6. A similar comparison between Danish arrangement and arrangements in India is also interesting. Financial Sector forum for Operational Resilience (FSOR) was set up in 2016 as a forum for collaboration between authorities and key financial sector participants in Denmark aiming to increase operational resilience when using IT across the sector, including resilience to cyber-attacks. This, in a way is comparable to the FSDC taking keen interest in ensuring cyber-security in the financial sector from a stability angle

3.3.7. The Working Group noted that India compares reasonably well with other international jurisdictions in bits and pieces. India has a national CERT in the form of CERT-IN. Private sector CSIRTs are not common in India and Academic CSIRTs in some form or the other are there in a few technical institutions like Indian Institute of Science or IDRBT. National CERT here means that the response arrangements are for the country as a whole –either for all sectors or for individual sector and Private sector CSIRT would mean that it is only for the institution. As far as banks are concerned, the predominant institutions in the financial sector of India, the current arrangements have been strengthened in the recent past and are comparable to other well regulated jurisdictions.

3.3.8. The Working Group unanimously felt that the challenges faced by India, in particular financial sector in India are significantly different from other jurisdictions. India is the seventh largest country having a diverse population of 1.3 billion. The dispersal of technical resources is concentrated at major cities and not evenly spread. On the ground, even if a lot of initiatives have been taken by various financial sector stakeholders, the preparedness of the financial sector to meet the cyber challenges from different threat vectors cannot be considered robust. The challenge is significant for public sector entities – be it banks, insurance companies or any other. Appreciation at the Board / senior management level is considered to be low and focus on cyber aspects is seen, generally as nominal and threats are increasing with state actors and non-state criminal actors turning their attention to this fastest growing economy in the world. The dependence on outsourced vendors for day to day operations in the financial sector is ever increasing and is a source of risk in the absence of appropriate as also adequate security controls to mitigate threats. Some members of the Working Group felt that at times, by outsourcing, the job ultimately gets done by resources which receive paltry salary thereby mis-aligning the incentives for better management of technology.

3.3.9. Parallely, the innovations in the payment and settlement systems in India have been phenomenal. As noted in chapter 1, with the digital push announced by the Government post November 8, 2016, the thrust is to digitally include the entire population as early as possible. Government allocating significant incentives to promote BHIM application is likely to deliver the desired results. Thus there is enormous pressure on the financial sector to support the nation at this crucial juncture.

3.3.10. Given the above, a need was felt by the Group to look for solutions that would be apt for the country at this stage while reckoning the international best practices. This brings to the fore as to what should be the structure, role and constituency of the proposed CERT-Fin and what would be the funding arrangements. It was agreed that the fundamental role of CERT-Fin should include the following:

- Threat intelligence sharing among constituents
- Information collation and sharing on real time basis
- 24/7 Vulnerability Assessment
- Conducting assessment / Provision of response
- Bringing down rogue sites / apps
- Developing Standard for data protection (encryption, access rights etc.)
- Analysis of incidents, response & policy suggestions for promoting financial sector cyber security.

3.3.11. Considering the country specific situation, it was felt that the CERT-Fin need to be vested with some additional responsibilities. Banks often mention that VAPT is better carried out by the Regulator in order to be sure that the exercise itself does not add risk. Financial products that are used by the financial institutions need to be seen closely from the cyber-security point of view. Similarly, members felt that outsourced vendors dealing with day to day operation in financial sector as well as their systems need to be assessed impartially and professionally. The current arrangement of getting certain audits done on the above aspects was considered by some members in not being able to providing full confidence. Scanning internet facing applications of the financial institutions as well as infrastructure 24/7 is another requirement. Malware /artifact analysis capabilities are also required.

3.3.13. Given the growing list of needs as outlined above, the CERT-Fin needs to be fully empowered and enabled to deliver quality services and hence has to be set up as state of the art facility. We need to aim for best in class as far as the services delivered by CERT-Fin is concerned.

3.3.14. The Working group reviewed the structure of CERT/CERT-Fins in various countries and unanimously identified the following lessons, which can be adopted in India, subject to Indian conditions:

- (i) India need to further strengthen cyber-security in financial sector, in a coordinated manner through setting up of CERT-Fin.
- (ii) India should identify financial sector as one of the critical infrastructure similar to other developed countries.
- (iii) CERT-Fin should provide seamless integration for information dissemination to other nodal agencies using standard protocols. It may support a collaborative approach to gather threat intel information, in addition to developing its own independent capability to research and identify threat information to the financial sector.

- (iv) There is a need for training and certification programs in the cyber security area for key personnel in the financial sector and for developing manpower with necessary skill, expertise in cyber security product development and cyber operations.
- (v) There is a need for better cyber security awareness in the Country to be done through potential resources, financial sector intermediaries, Regulators etc.
- (vi) The functions of CERT-Fin should be well defined in consonance with international best practices.
- (vii) CERT-Fin should adopt international best practices in its functioning and be dynamic in adopting state of the art technology.
- (viii) Information Sharing and Coordination Centre focused on financial sector, successful in developed countries (e.g FS-ISAC, EFI-ISAC, ISAC-JP etc) may be adopted in India at a matured stage.
- (ix) International interface with similar financial sector CERT is required.

### **3.4. CERT-Fin Model alternatives considered by the Working Group**

3.4.1. The Working Group viewed that the CERT-Fin may be designed to support programmatic and rapid information sharing with right set of stakeholders. This requires leveraging open standards and existing protocols used internationally by similar such agencies. This would ensure inter-operability. The platform must provide mechanisms for managing the incident lifecycle through a case driven approach. In addition, there should be provision for managing incident tickets, assigning ownership, tracking the incidents through its various progressive stages always keeping the right stakeholders involved through a collaborative platform. It may support maintenance of all artefacts, their classification and categorization etc. It may be available through access control and visibility of data based on authorization level. It should support, alert notifications via email, SMS, automated voice calls etc.

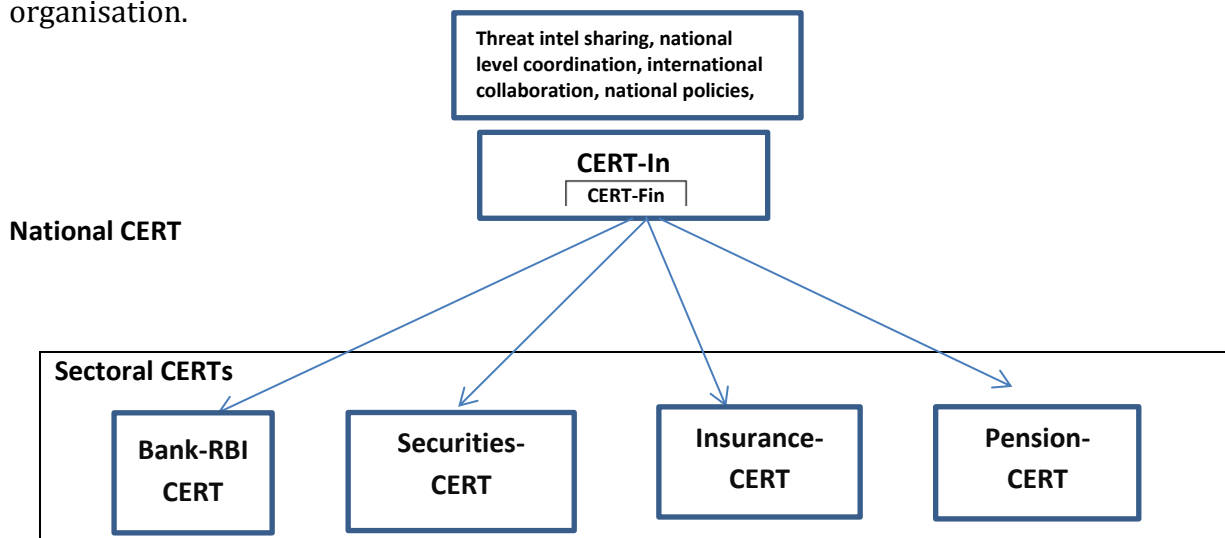
3.4.2. CERT-Fin may provide seamless integration for information dissemination to other nodal agencies using standard protocols. It may support a collaborative approach to gather threat intel information, in addition to developing its own independent capability to research and identify threat information to the financial sector.

3.4.3. A hierarchical structural model should be instituted to establish clear roles and responsibilities between various nodal agencies. A good coordination should exist between the various nodal agencies and right model of information exchange should be established to mitigate reporting burden on the constituency members and help concentrate right skills and capabilities at the right hierarchy. The Working Group considered basically the following two alternatives for CERT-Fin, in the Indian context.

**3.4.3.1 Alternative-1: CERT-Fin within CERT-In with sub sectoral CERTs:** This structure is slightly similar to the structure proposed for the Power sector, where there is no separate CERT-Fin for coordinating power CERTs. In this scenario, the CERT-Fin becomes a part of CERT-In as a department within CERT-In and each of the regulator

operates their own sub sector specific CERTs (bank, securities, insurance, payments & pensions), reporting to CERT-Fin located within CERT-In. The advantages of this model is that (a) it enables each of the regulators to maintain control, build specialized expertise in the cyber-incident handling, build advanced capabilities and track the pertinent threat intel effectively (b) reduces reporting levels as the sub sector CERTs report directly to an arm of CERT-In.

3.4.3.2. The disadvantages of this model includes (a) inefficiencies in handling of threat intelligence especially for attacks affecting more than one financial sub-sector (b) CERT-In handling various sector CERTs cannot devote time dedicatedly for the financial sector (c) Lack of proper cyber incident analysis in the financial sector as a whole (d) as CERT-In is already stretched handling different types of threats across heterogeneous sectors, they may not be able to have dedicated full time attention specific to financial sector (e) as a government organisation, they may be constrained to execute the action plan envisaged for CERT-In free of cost. (f) challenges in attracting best of talent also would be considerable as it will be difficult to provide market linked salary being a government organisation.



**Individual BFSI Firms**

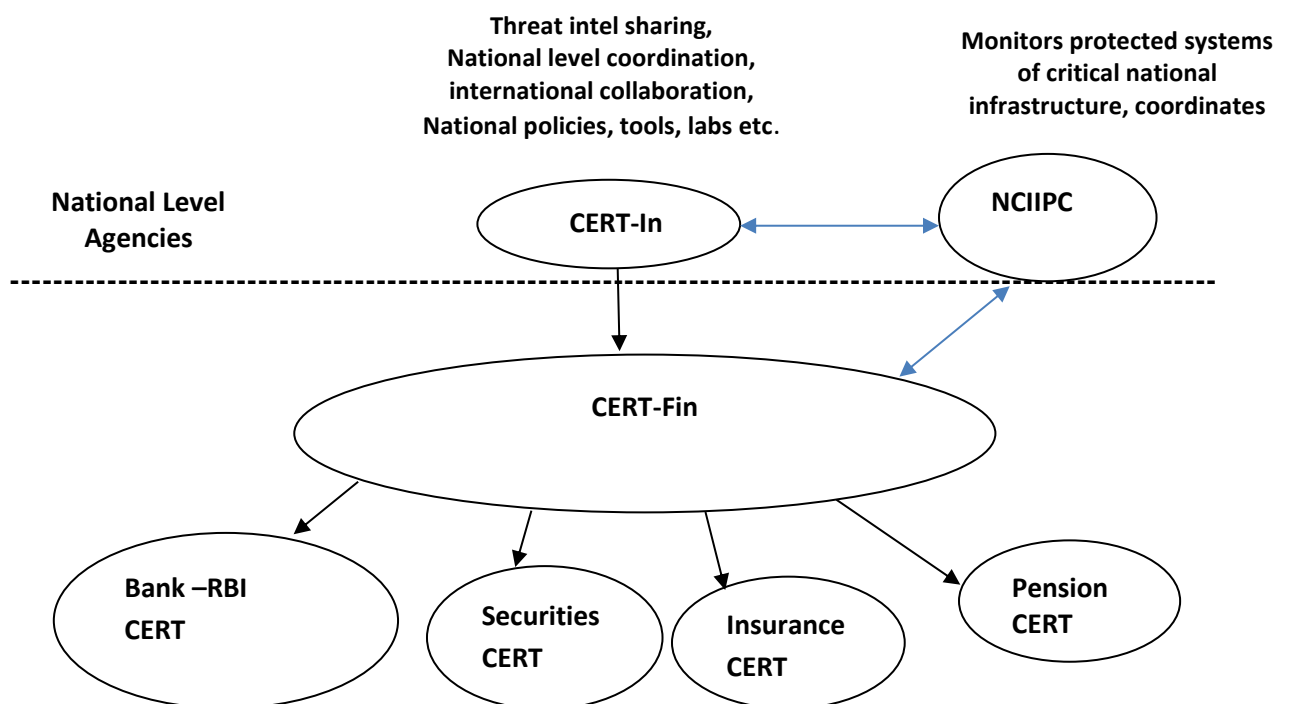
**3.4.4. Alternative-2: One overall financial CERT across sub sector CERTs:** In this model, the CERT-Fin will be a single body supporting all sub sectoral CERTs in regulatory authorities, viz, RBI, SEBI, IRDAI and PFRDA, and also will play a role in monitoring the effectiveness of their regulatory responsibilities in the area of cyber security. In this structure, the CERT-Fin, will function under the overall guidance and framework as an extension of CERT-In becomes an entity that manages incidents and coordinating responses across banking, securities market infrastructure, insurance and pension funds. The payment system is governed under PSS Act 2007, which is overseen by RBI .Therefore, RBI through its Bank CERT will monitor and report all payment and settlements related cyber security incidents/issues.

3.4.4.1. This model envisages to set up the CERT-Fin as a separate independent

institution initially funded by Regulators, say, for the first five years till its maturity and thereafter to be jointly funded by the stakeholders (banks & other regulated entities). After 5 years, it may provide different types of memberships commensurating with the fee/non-fee based service opted. It needs to establish a strong working relationship & guidance seeking mechanism from CERT-In for analysis of threats affecting the sectors & infrastructure beyond the control of FIs. RBI may act as lead regulator and can play an active role in conceptualising, rolling out and steering the activities of the CERT-Fin in the initial years as an incubator and lead the overall management in an advisory committee of the stakeholders, and a well-qualified Governing Board with experts as independent members. Funding and recruitment of personnel/experts maybe done with a pooled approach by regulators

3.4.4.2. It was also discussed whether RBI may operate the CERT-Fin within RBI as the around 60% of the financial sector is bank dominated. Then CERT-Fin becomes a banking-specific specialized CERT, operated under the aegis of RBI with additional capacity to cater to other sector requirements. Other regulators, viz. SEBI, IRDAI and PFRDA do not set up separate CERTs, but leverage the capabilities of CERT-Fin to meet their requirements and will continue to report the incidents directly to CERT-In. However the disadvantage of this model was considered to have potential conflict of interest. Moreover, the role of CERT-Fin as envisaged above could compromise the efficacy of supervisory role of RBI in independently evaluating the responsibilities/functions of CERT-Fin as per the defined terms & conditions. Therefore, the Group unanimously supported the proposition of setting up of CERT-Fin as described in para 4.3 and 4.8 with broad roles and functions as delineated at para 4.10.

**CERT-Fin model recommended by the Working Group**



## **CHAPTER 4**

## CHAPTER 4

# Conclusion and Recommendations of the Working Group

### I. Establishment and structure of CERT-Fin

4.1. The international best practices in Financial CERTs were studied by the Working Group and it was understood that major developed countries attach significant importance to cyber-security and have taken various initiatives in that regard. (refer para 3.3.1 to 3.3.2). Fin-CERT work in coordination with the country CERTs as well as EFI-ISAC in Europe. The Working Group also observed that, the most elaborate arrangement for financial sector has been put in place by some jurisdictions such as Russia. Central Bank of Russia has set up a Fin-CERT exclusively for the financial sector. The Working Group noted that in Sri Lanka and Italy, Fin-CERTs (Bank-CERT) look at the financial sector exclusively (para 3.3.3 of this report).

4.2. India compares reasonably well with other international jurisdictions in bits and pieces. India has a national CERT in the form of CERT-In. Private sector CSIRTs are not common in India and Academic CSIRTs in some form or the other exist in a few technical institutions like Indian Institute of Science/IDRBT. The Working Group unanimously felt that the challenges faced by India, in particular financial sector in India are significant (refer para 3.3.5 to 3.3.7), as enormous pressure is there on the financial sector to support the nation's development as also in ensuring a secure digital India. The Working Group considered various models for CERT-Fin as detailed in Chapter 3 based on international best practices.

**4.3. *The Working Group recognised the importance of setting up a financial sector CERT soon and recommended a nodal sectoral CERT ie; CERT-Fin to act as an umbrella CERT for the financial sector and report to CERT-In at the national level in accordance with IT Act and Rules. The Group, after detailed deliberations, recommended that the sub sectoral CERTs may be set up and housed in each of the financial sector Regulators and below those, in major financial institutions, feeding information on real time basis to the proposed CERT-Fin. The diagrammatic representation of the proposed model of CERT-Fin as recommended by the Working Group is depicted at Chapter 3 of the report.***

4.4. The Working Group observed that Section 70 B of the IT Act 2000 provides for CERT-In to serve as the National agency for cyber security incident response as highlighted in chapter 1 of this report. It also envisages CERT-In to function as a nodal agency for coordination of all efforts for cyber security emergency response and crisis management and CERT-In will function as an umbrella organization in enabling creation and operationalization of sectoral CERTs as well as facilitating communication and coordination actions in dealing with cyber crisis situations. Rule 10 of the IT (CERT-In – manner of performing function and duties) Rules 2013, mentions that CERT-In shall interact with and seek assistance from the sectoral CERT for cyber security incident

response and prevention. ***To facilitate smooth functioning in coordination with CERT-In, the Working Group recommended that an MoU/legal arrangement in accordance with the Rules and IT Act clearly outlining the area of coverage/sharing protocol of proposed CERT-Fin and CERT-In should be put in place. MoU may also be signed by proposed CERT-Fin with each of the sub sectoral regulator CERTs clearly outlining the role, functions & responsibilities of each of the parties.***

4.5. India's financial sector is diversified and expanding rapidly. The regulation and supervision of the financial system in India is carried out by different regulatory authorities as highlighted in para section 1.1 of this report. As the financial system evolves, the interdependence among institutions, markets and critical infrastructure are increasing. ***Therefore, the Working Group recommended that Proposed CERT-Fin should seek to complement the overarching mandate of CERT-In, keeping in view the following principles:***

***(i) Financial services are offered by a large number of businesses that encompass the finance industry. These include Regulated Institutions (RIs) in each of key sectors of the financial system governed by various regulators. These regulators, viz. the RBI, SEBI, IRDAI and PFRDA have, for the last few years, been working through regulations needed to make their regulated entities better prepared for dealing with cyber risk. It is essential that all regulators should take adequate measures and enforce regulations for stronger cyber security architecture.***

***(ii) The approach also needs to take into account the differing levels of maturity of technology management across different types of regulated entities.***

4.6. The Working Group observed that in developed world, the financial sector has been identified as one of the critical infrastructure invariably by all countries. As such, an Information Sharing and Coordination Centre focused on financial sector is functional in major jurisdictions (e.g FS-ISAC in US, EFI-ISAC in Europe, ISAC-JP in Japan etc) and such arrangements are generally voluntary from the financial sector participants.. Financial sector participants become members and avail whatever services they need as explained in para 3.3.1 of the report. In some countries, like Hong Kong, there are multiple National CERTs. One CERT takes care of all the public sector agencies and another CERT takes care of all the private sector agencies and citizens in general. Government CERTs play a lead role and the other CERTs play along with the Government CERTs.

4.7. Broadly, the Working Group noted that these countries have their cyber-security strategy finalised by their Government (through Ministry of IT or Electronics or Home), supported by a critical infrastructure monitoring arrangement, a CERT at National level, an ISAC at the financial sector level and regulatory oversight over cyber-security related aspects by respective regulators as noted in para 3.3.2 of this report. Besides, in developed countries, respective large institutions have the capacity to handle cyber incidents on their own. In India, management of CERT-Fin is better left with



Regulators/Government as private sector managed CERTs do not exist in India. Therefore, a privately managed CERT-Fin in a developing country like India may not be suitable. To leverage the best of the models of CERT-Fin as detailed in chapter 3, the Working Group considered a model that is best suitable for Indian conditions.

**4.8.** The Working Group therefore, recommends that *the CERT-Fin should be an independent body to be set up as a company under Section 8 of the Companies Act, 2013 with a Governing Board. An Advisory Board may be set up for, inter-alia, providing strategic direction, review of performance and recommendations for allocation of budget/resources. Keeping in view that this highly technical coordinating body may take time to be set up as a fully functional Company, it is necessary that during transition, RBI may act as the lead regulator in terms of setting up CERT-Fin.*

**4.9.** *The Advisory Board for CERT-Fin may comprise all members of the Inter Regulatory Technical Group (under aegis of FSDC Architecture), with ED (RBI) as Chairperson, and Adviser (FS), JS (MeitY), DDG/JS (DFS), DDG (DoT), representative of CERT-In and the CEO/Director, CERT-Fin also as members. The Advisory Board may also invite experts for discussion on need basis. The Advisory Board may meet frequently at the initial stage of setting up of CERT-Fin & thereafter, on quarterly basis. The Governing Body may be set up with nominees of shareholding institutions; i.e. the Regulators, CERT-In, two independent and technically qualified members and the CEO/Director, CERT-Fin. RBI may act as the lead Regulator till CERT-Fin is fully set up & functional as a Company.*

## **II. Role and Functions of CERT-Fin**

**4.10.** The Working Group considered the functions assigned to CERT-In and other existing sectoral CERTs and the existing initiatives taken by the financial sector Regulators prior to identifying the role and functions of CERT-Fin. It also noted that the functions of CERT-Fin should be well defined in consonance with international best practices where core functions of incident reporting, response coordination, readiness support, vulnerability identification and threat identification are given more importance. Para 3.1.3 of this report focus on a Handbook for CSIRTs which provides guidance on forming and operating a computer security incident response team (CSIRT). Thus the Working Group *recommends that the CERT-Fin may do analysis of financial sector cyber incidents, understand the pattern and nuances across financial sectors envisage basic functions for CERT-Fin as delineated by the Working Group, while reporting the cyber security incidents to CERT-In:*

- i. Collection, analysis & dissemination of information on cyber incidents.*
- ii. Forecast and alerts on cyber security incidents.*
- iii. Emergency measures on cyber security incidents.*

- iv. Coordination for cyber incident response activities.*
- v. Issue guidelines, advisories, vulnerability and white papers relating to information security*
- vi. Monitor sectoral efforts in financial sector towards maintaining dynamic and modern cyber security architecture, developing awareness amongst regulated entities and public in general.*
- vii. Such other functions relating to cyber security in financial sector, as may be prescribed*

**4.11. The Working Group suggested that CERT-Fin should create awareness on security issues through dissemination of information on its website and operate 24x7 incidence responses Help Desk. CERT-Fin may provide Incident Prevention and Response services as well as Security Quality Management Services. It may carry out functions similar to CERT-In that operate at a national level, for priority cyber security in financial sector.**

**4.12. The Working Group also noted that there are a number of processes which need to be established by CERT-Fin in order to deliver its services. These processes and services should be in the lines of the objectives defined for CERT-Fin and its constituency as delineated in the Report at Annex III, provided by CERT-In.**

**4.13. The Working Group viewed that there is a need for policy suggestions for strengthening financial sector cyber security. An analysis by the OECD of a new generation of national cyber-security strategies<sup>21</sup> reveals that cyber-security policy making is at a turning point. In many countries, it has become a national policy priority supported by stronger leadership. All new strategies are becoming integrated and comprehensive. *Considering this, the Working Group recommended that CERT-Fin should offer policy suggestions for strengthening financial sector cyber security to all stakeholders including Regulators/Government.***

4.14. The Working Group recognized the importance of customer education especially cyber security education and the importance of education and awareness among the regulated entities. There is also need for awareness among Bank and Financial Sector employees. Workshop need to be held with all stakeholders/public to facilitate aspects such as developing awareness and importance of cyber security by the regulated entities and other stakeholders as also developing necessary framework by the regulated entities. The Working Group also noted the importance of public private partnership for customer education and awareness as promotion of financial literacy ultimately results in cyber security awareness among the people, thereby understanding the need for

---

<sup>21</sup> Cyber-security Policy Making at a Turning Point: Analysing a New Generation of National Cyber-security Strategies for the Internet Economy-OECD

CERT-Fin. In this regard, the proposed CERT-Fin may make use of the potential resources including existing funding facilities for financial education and awareness, and institutions available in our Country such as National Centre for Financial Education, leading technology institutes focused on cyber security, state specific agencies etc.

**4.15. In view of the above, *the Working Group recommends that as part of financial literacy programs, cyber security awareness should also be equally promoted. In this regard, all financial sector regulators including RBI may promote cyber security awareness and various sources of funds available from Government and Regulators may be used.***

**4.16. *To promote cyber-security awareness on a mass scale, the Working Group suggested that various public and private organisations may be involved in this regard to take forward the cause of promoting cyber security in the financial sector, specifically in areas such as:***

- ***Financial sector threat intelligence and business resilience***
- ***Insider threats, anti-fraud and cyber-crime including money laundering***
- ***Compliance, audit, frameworks, standards, guidelines and best practices from security and privacy perspective***
- ***Regulatory, legal and media response***
- ***Cyber risk (including threats and vulnerabilities) and awareness for – clearing house, depository services, card issue / reissue, insurance, payment processors, asset managers, investors, brokers / dealers, treasury, banks, etc***
- ***Supply chain risk, audit, compliance and awareness***
- ***Standardisation with respect to automation, incident detection, incident response and information sharing***

### **III. State of the Art Infrastructure**

4.17. The Working Group in its various meetings noted that the proposed CERT-Fin should be designed to support programmatic and rapid information sharing with right set of stakeholders learning from the international best practices This requires leveraging open standards and existing protocols (such as STIX and TAXII) used internationally by similar such agencies. This would ensure inter-operability. The platform must provide mechanisms for managing the incident lifecycle through a case driven approach. In addition, there should be provision for managing incident tickets, assigning ownership, tracking the incidents through its various progressive stages always keeping the right stakeholders involved through a collaborative platform. It should support maintenance of all artifacts, their classification and categorization etc. It

should be available through the Internet and provide access control and visibility of data based on authorization level. It should allow some administrative functions to members to manage their own set of users and extend access to the SOCs within the firm. It should support, alert notifications via email, SMS, automated voice calls etc.

4.18. CERT-Fin should provide seamless integration for information dissemination to other nodal agencies using standard protocols. It may support a collaborative approach to gather threat intel information, in addition to developing its own independent capability to research and identify threat information to the financial sector.

**4.19. Taking into consideration the above aspects, the Working Group recommends that CERT-Fin should be sufficiently equipped with state-of-the-art infrastructure to cater to the requirements of cyber security in the financial sector. Technology components for each area need to be identified and deployed appropriately as per the process set up for the various services. It should be ensured that state of the tools and technologies are deployed and these go through proper maintenance regularly. The Working Group also recommended that the software used by all stakeholders need to be updated (OEM standard) on regular basis to make up with modern technology, if the financial sector regulators want to remain ahead of cyber security attacks.**

**Box-1. Indicative Areas with associated Technology Components of CERT-Fin**

S. No.	Areas	Technology Component
1	Incident Handling	Service desk & reporting platform, Website monitoring solution, Spam Traps, Sandbox platform, System & Network forensics platform, Net flow & traffic analysis, DNS Monitoring, Botnet & DOS detection platform, Network/Server Honeypot, SMS & Email gateways, Incident & Report Archiving, CERT-Fin Lab (Mobile Platforms, OS Platforms, Network Devices, Security Devices, Virtualization Platform, and Simulation Platform)
2	Threat Intelligence	Threat Feed Aggregation Platform, Automated Parser, Security Incident and Event Management Solution, Asset Inventory Solution, Portal, Email Setup, and SMS Gateway Integration
3	Security Operations Centre	SIEM Solution, DLP/DRM Tool, Encryption Tool, Firewall, IDS/IPS, Proxies, Web Application Firewall, Identity & Access Management Tool, End Point Monitoring Tool, Asset management & Inventory tool, Security Analytics Tool, DDoS Tool, among others
4	Security Audits and Assessments	Dedicated Internet Leased Line, Vulnerability Assessment Tools, Network scanning or Monitoring Tools, Penetration Testing Tools, Reporting Dashboards, Web Application Assessment

		Tools, Virtual Private Networks, Intruder Detection/Prevention Systems, Security Baseline documents & scripts, Patch Development & Distribution Systems, and Debugger for detection of Vulnerabilities
5	Information Sharing	Knowledge Management Platform

#### IV. Funding of CERT-Fin

4.20. The Working Group considered various options for funding of CERT-Fin. It was discussed that when the funds are generated from users, the organization delivering the services becomes more responsible. Same is the case with beneficiaries, ie; people, when they pay for it, they become more responsible. Given the above, the Working Group looked for solutions that would be apt for the country at this stage while reckoning the international best practices. A view was that the CERT-Fin may be set up as a separate independent institution jointly funded by the stakeholders (banks & other regulated entities) with different types of memberships commensurating with the fee/non-fee based service opted. In this scenario, initial budget support may come from Government and subsequent management to be done by private sector.

4.21. Members however strongly felt that, cyber-literacy is at its infancy now in India and some institutions are still not following adequate cyber-hygiene. Therefore, expecting a privately led CERT-Fin is asking too much at this stage. Banks and financial institutions are also used to the regulator led model where desired changes are brought about by regulations rather than as a voluntary measure.

4.22. The Working Group also considered the pattern of National Centre for Financial Education (NCFE) which is supported by all the financial sector regulators, and one successful model operating in India, under the guidance of a Technical Group on Financial Inclusion and Financial Literacy under the aegis of the Financial Stability and Development Council (FSDC), which would cater to all sections of the population in the country. The main role of NCFE is however to create financial education materials and conduct financial education campaigns across the country for all sections of the population along with awareness campaigns at different levels for existing and potential customers so as to improve their knowledge, understanding, skills and competence. ***After detailed discussions, the Working Group recommended that the proposed CERT-Fin may be funded by all financial sector regulators. This may continue initially, say for five years or so till its maturity, after which CERT-Fin can chalk out a feasible long-term self-reliant funding strategy looking at FS-ISAC, EFI-ISAC, ISAC-JP models. RBI may act as lead regulator and can play an active role in conceptualising, rolling out and steering the activities of the CERT-Fin in the initial years as an incubator. A Techno-Economic analysis of the proposed Alternative 2***

***mentioned in Chapter 3 of the report may be carried out to assess the requirements related to funding, manpower, infrastructure, etc. The analysis may articulate the parameters for manner and quantum of contribution which may in turn determine the structure and governance of the proposed CERT Fin.***

## V. Capacity Building

4.23. The Working Group had detailed discussions in its various meetings on demand supply gap of experienced Cyber Security Professionals. One of the views was that IT managers face challenges in defending their network as shortage of talent is leaving them vulnerable to attack. As per the report published by Intel Security in partnership with the Center for Strategic and International Studies (CSIS)<sup>22</sup>, 82% of the respondent reported a lack of cyber security skills within their organization. The global cyber-security workforce will have 1 to 2 million jobs unfilled by 2022<sup>23</sup>. The global survey<sup>24</sup> of more than 3,400 ISACA members in 129 countries found that 86% of respondents see a global cyber security skills gap—and 92% of those planning to hire more cyber security professionals this year say they expect to have difficulty finding a skilled candidate. In India itself, the National Cyber Security Policy, 2013, recognizing the need to address this burgeoning skill gaps, called for creating a workforce of 5 lakh cyber security skilled professionals<sup>25</sup>. A recent report by a leading recruitment website points out that there is significant mismatch in demand and supply<sup>26</sup>.

4.24. The Working Group viewed that the cyber security skill gap challenges are exacerbated as India is fast becoming a strategic target, in part because of the potentially sensitive information that is being digitized as part of the Digital India and India is also seeing higher than global average attacks on organizations<sup>27</sup>. Majority of the course offerings in cyber security is at the Masters level. The Group felt that there is a need for more affordable vocational trainings and certification programs in the cyber security area. There have been some efforts in this direction such as efforts by NSDC<sup>28</sup> to create qualification packs that outlines the job profiles and job requirements for various cyber security roles required. A broader adoption of such programs, creation of more affordable training programs combined with robust pipelines of jobs in the cyber security area through well-defined cyber security roles within the organizations would bolster the capacity building required for cyber security jobs. In the interim, the organizations requiring cyber security professionals may need to hire talent based on

<sup>22</sup> <https://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf>

<sup>23</sup> <http://www.crn.com/news/security/300083904/study-cybersecurity-skills-gap-to-widen-to-a-massive-1-8-million-worker-shortfall-by-2022.htm>

<sup>24</sup> <https://www.isaca.org/pages/cybersecurity-global-status-report.aspx>

<sup>25</sup> [http://meity.gov.in/sites/upload\\_files/dit/files/National\\_cyber\\_security\\_policy-2013\(1\).pdf](http://meity.gov.in/sites/upload_files/dit/files/National_cyber_security_policy-2013(1).pdf)

<sup>26</sup> <http://blog.indeed.com/2017/01/17/cybersecurity-skills-gap-report/>

<sup>27</sup> <http://www.livemint.com/Politics/3lIPntavAkp5i3uZseTUnl/India-sees-increasing-targeted-cyber-attacks.html>

<sup>28</sup> <http://www.sscnasscom.com/ssc-projects/cyber-security-skills/>

their aptitude and provide right kind of training opportunity and talent management environment to build internal capability and use a balanced sourcing strategy<sup>29</sup>.

4.25. In the second meeting of the Working Group, it was highlighted that over the years, there is rapid increase of technology in the Banking, Financial, Securities and Insurance (BFSI) sector. The Working Group identified that the following technology areas are critical to the sector (i) Cyber Security (ii) Computer Networks and Network Security (iii) Internet and Web Security Technology (iv) Online Databases and eCommerce (v) Vulnerability Assessment and Penetration testing (vi) Cyber Security Monitoring Analysis (also called CSOC/NSOC) (vii) Digital Forensics and Proactive Approaches to cyber security (viii) Advanced Malware Threats, Targeted Attacks (ix) Cyber Crimes and Counter Measures (x) Security Attack Surface Measurements and Analysis (xi) System Hardening and Cyber defence (xii) Proactive approaches to Cyber security (xiii) Cyber Security Incidents/Events - Management and Planning (xiv) Business Continuity and Resilience Planning (v) Security Analytics and Visualization Techniques.

**4.26.** The Working Group observed that the dependence on outsourced vendors for day to day operations in the financial sector is ever increasing. At times, by outsourcing, the job ultimately gets done by resources which receive paltry salary thereby mis-aligning the incentives for better management of technology. Thus, in India we need research programmes and curriculum in order to innovate research deliverables in cyber security space to protect Indian infrastructure and to develop manpower with expertise in cyber security product development and cyber operations. Taking into consideration the above, ***the Working Group recommends that there is an urgent need to give attention (i) for more quality training and certification programs including online programs in the cyber security area (ii) to develop manpower with expertise in cyber security product development and cyber operations (iii) to conduct research programs and develop curriculum in order to innovate research deliverables in cyber security space to protect Indian infrastructure.***

4.27. The Working Group took note of the fact that IDRBT's mandate is research, training, consultancy for Banks. The focus areas of the Institute are cyber security, analytics, cloud computing, financial inclusion, payment systems and open sources. There are Centers exclusively for each of the focus areas, managed by faculty, research scholars and research assistants. IDRBT conducts about 100 programs every year in various topics. The Center for Cyber Security in IDRBT carries out various activities for Banks and Financial Institutions such as EDP programs in the area of Cyber Security - Cyber Defense, Vulnerability Assessment and Penetration Testing, Malware Analysis, Cyber Forensics, and related customised programs, Quarterly Cyber Drills for banks on the lines of level 2 cyber drill of CERT-In. Cyber crisis and cyber security workshops for banks are carried out with the help of CERT-In regularly.

---

<sup>29</sup> <https://manpowergroup.co.in/MEOS/2016%20Information%20Security%20Whitepaper%20-low%20res.pdf>

**4.28.** The Working Group also noted that IDRBT manages IB-CART, Indian Banks - Center for Analysis of Risks and Threats which is a Threat Intelligence Sharing platform for Indian Banks and FIs where reports are shared amongst RBI, banks, CERT-In and NCIIPC. IDRBT also coordinates Banks' CISO Forum where all Bank CISOs are members, which discusses on results of Cyber drills, IB-CART updates and experience sharing and cyber security concerns amongst CISOs. In addition to the Cyber Security Programs, IDRBT also conducts special Programs for SEBI and RBI such as customized Programme on Vulnerability Assessment and Penetration Testing for SEBI and Customized Programme on Vulnerability Assessment and Penetration Testing for RBI. Besides, IDRBT carries out International programs in the area of Information Assurance and Management. In addition to IDRBT, there are leading technology institutes in our Country such as IITs offering courses on cyber security, and the Working Group felt that we should tap the potential of these leading institutes for developing CERT-Fin. ***In view of the above, the Working Group suggests utilizing the expertise in the leading institutions in the process of building up CERT-Fin and recommends that wider consultation with leading technology institutes including IITs, Indian Institute of Science, etc may be useful to work out the technical details and chart out a long term plan in Indian context. All the financial sector regulators may train their manpower on cyber security in their respective domains in leading technology institutions.***

**4.29.** Today, Vocational Education and Training (VET), also called Career and Technical Education (CTE), prepares learners for jobs that are based in manual or practical activities, traditionally non-academic and totally related to a specific trade, occupation or vocation. As the labor market becomes more specialized and economies demand higher levels of skill at the bottom of the pyramid, governments and businesses are increasingly investing in the future of vocational education through publicly funded training organizations and subsidized apprenticeship or traineeship initiatives for businesses. Today VET as a model is well established internationally in Australia, Commonwealth of Independent States, European Union, Finland, Germany, Hong Kong, Hungary, India, Japan, South Korea, Mexico, The Netherlands, New Zealand, Norway, Paraguay, Russia, Sweden, Switzerland, Turkey, United Kingdom, and United States.

**4.30.** ***The Working Group recommends that to develop necessary critical manpower infrastructure as also to improve the employability of youth at the bottom of the pyramid, the nation should optimally utilize the infrastructure available in Government, private institutions and the Industry by developing appropriate courses that can be worked out in consultation with CERT-In.***

## **VI. Staffing in CERT-Fin**

**4.31.** In order to ensure that the services of the CERT-Fin are being properly delivered, resources with right skill set need to be deployed. This would ensure in having the correct governance for running the CERT-Fin operations with properly defined roles and responsibilities. There is also need for resource capability with adequate experience and educational background with defined roles and responsibilities. Adequate staff with



required technical Skills (Security Principles, Risks, Network Protocols, Network Applications and Services, Network Security Issues, Host/System Security Issues, Malicious Code, Programming Skills, etc) Incident Handling Skills (Policies and Procedures, Understanding/ Identifying Intruder Techniques, Communicating with Sites, Incident Analysis, Maintenance of Incident Records, etc) and Personal Skills (Communication, Presentation skills, Diplomacy, team skills, problem solving, etc) are vital in this regard. There is also need to formulate teams pertaining to incident management, threat management, audit & vulnerability assessment; such as head of the service/ process, subject matter experts (Incident, Vulnerability, Malware, Analysis and others), manager or Team Lead (Coordinator, Principal Investigator or Senior Technical Lead), Quality Team Lead, Assistant Manager, Supervisor or Group Leads, Technical Staff (Incident Handlers, Vulnerability Assessment or Artefact Analysts, SOC Team, Audit), First Responders (Hotline, Help Desk, or Triage Staff), Vulnerability handlers, Technical Writers, Web Developers and Maintainers, Network or System Administrators, Platform Specialists and other Professional or Administrative Support Staff. Training courses should also be specifically designed for managers and technical staff of CERT-Fin and sub-sectoral financial CERTs.

**4.32.** Taking into consideration the facts mentioned above, *the Working Group recommends that the proposed CERT-Fin may be equipped with best available talent with highly skilled professionals which may either be deputed from Regulators or other leading institutions specialized in cyber security in our country at market linked rates as per the requirements. The Group also recommends that the proposed CERT-Fin and sub sectoral financial CERTs may have at least one IT expert and one domain expert for reporting cyber security incidents to CERT-In/CERT-Fin. The personnel may have in-depth expertise in IT security and analysis. The Working Group also recommend that, to start with, one domain expert and one subject expert from each sub-sector CERTs may be deputed to CERT-Fin for facilitating information sharing. A CEO/Director may also be sent on deputation basis to proposed CERT-Fin at the initial stage. In addition, CERT-Fin may have a representative not below the rank of Deputy Secretary from DG, CERT-In's office to further guide the activities of CERT-Fin, in accordance with IT Rules, 2014.*

## **VII. Identifying protected system in the financial sector.**

4.33. The Working Group took note of the fact that with the advancement of convergent communication technologies and shared Information system in India, critical sectors are becoming more dependent on their Critical Information Infrastructures (CIIs). These CIIs are interconnected, interdependent, complex and distributed across various geographical locations. Various inherent threats exist to CIIs, ranging from terrorist attacks to organized crimes to espionage, malicious cyber activities, which are growing rapidly”.

**4.34.** The Working Group also noted that NCIIPC is an organization of the Government of India created under Sec 70A of the Information Technology Act, 2000 (amended 2008), through a gazette notification on 16th Jan 2014 based in New Delhi, India, it is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection. The detailed role and functions of NCIIPC is stated at chapter 1. ***In the above context, the Working Group recognizes that there is a need to identify protected systems/ critical infrastructure in the financial sector, for which CERT-Fin should play an important role in coordination with sub-sectoral CERTs and NCIIPC.***

#### **VIII. Consultation Workshops to be held with experts/stakeholders concerned**

**4.35.** The working group has considered various models of CERT-Fin operating domestically and internationally and has come out with a set of recommendations in the Indian context. . The recommendations of the Working Group can be thrown open for discussion in a Workshop that can be held with all stakeholders specialized in cyber-security area. These may include scholars in the area of cyber security, leading institutions specialized in cyber security, and leading technology institutes of the Country. This open house discussion with the stakeholders may be useful in further refining and implementing the recommendations of the Group. Therefore, ***the Working Group recommend that a workshop may be held with all stakeholders and scholars specialized in the area of cyber security, leading academic and technology institutions for feedback on the recommendation of the Working Group. Public consultations on the Report may be considered by placing the Report in public domain for comments/ feedback.***

#### **IX. Major activities and processes involved**

**4.36.** The Working Group considered the importance of establishing a CERT-Fin on an urgent basis and in this context, delineated the major activities and processes involved for setting up CERT-Fin- in a time bound manner. ***The Working Group recommends major activities and processes to implement and operationalize CERT-Fin, with RBI as lead Regulator, as has been provided at Annex-II of the Report. All the financial sector regulators may complete simultaneously strengthening of their cyber security framework in their respective domain including setting up sub sectoral CERT-Fins by the time CERT-Fin is functional in a time bound manner.*** The Working Group feels, the success of CERT-Fin would depend upon the value that it creates for its constituency. clarity, transparency, project management and awareness will be critical to build momentum and consequently the effectiveness of the CERT-Fin. ***After say, two to three years, a comprehensive review of CERT-Fin should be done in FSDC forum. The FSDC-SC may closely monitor on a regular basis and guide the advisory board in this regard.***

#### **X. International Interface:**

**4.37.** Today, the threats of cyber terrorism and cyber-crimes have emerged as new threats, for which businesses and Governments need to incorporate new security

measures into its governance procedures. CERT-Fin need to be aware about the cyber security related affairs at the international arena and the measures being taken to cope with it, including building alliances and tie ups for information. Therefore, the Working Group recommends that ***CERT-Fin shall have tie-ups with various financial CERTS/FS-ISACS operating internationally to adopt international best practices in its functioning. To achieve this objective, CERT-In and MeitY can play a significant role.***

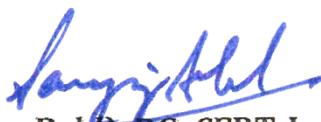
#### **XI. Telecom and Financial Sector Inter-linkages:**

**4.38.** The Working Group discussed at length on the strong inter-linkages between the telecom sector and the Financial Sector as highlighted in para 2.3.1 of the report. There is therefore, a need for simultaneous action and coordinated effort to be taken by both these sectors for ensuring secure and fool proof financial transactions, on the basis of state of art technology. After release of National Cyber Security Policy, 2013 (NCSP-2013), which has provision for setting up of sectoral CERTs, a committee has been formed in DoT including members from DoT, CERT-In, NCIIPC and NSCS. The establishment of the Telecom CERT is a work in progress with active cooperation from CERT-In. ***In view of the above, the Working Group recommends that a Standing Technical Sub Committee on CERT-Fin & Tel-CERT may be operationalized so that there is continuous flow of information between these CERTs to address the inter-linkages between financial and telecom sector cyber incidents and develop ways and means to address the telecom related cyber security issues in the financial sector.***

#### **XII. Cyber Security Governance**

**4.39.** In present times, when cyber risks loom large, it is very important to have a strong Cyber Security Governance in place. ***Taking this into account, the Working Group recommends that there is a need to safeguard the financial infrastructure from cyber security risks, which require coordinated efforts throughout, including cyber risk insurance.***

The Working Group recognizing the criticality of cyber security for safeguarding the integrity and stability of India's financial sector and having studied the existing cyber security measures taken in the financial sector in India and international best practices in the field, unanimously recommends setting up of CERT-Fin, that will work in close coordination with all financial sector regulators and other stakeholders, on the lines delineated in this report.



(Dr. Sanjay Bahl), DG, CERT-In  
Chairman



(Dr. C. S. Mohapatra),  
Adviser (FS), DEA  
Member & Convener



(Smt. Anjana Dube)  
DDG, DFS, Member



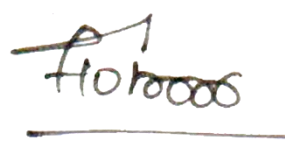
(Ms. Tulika Pandey)  
Scientist 'F', MeitY,  
Member



(Smt. Meena Hemchandra)  
ED, RBI, Member



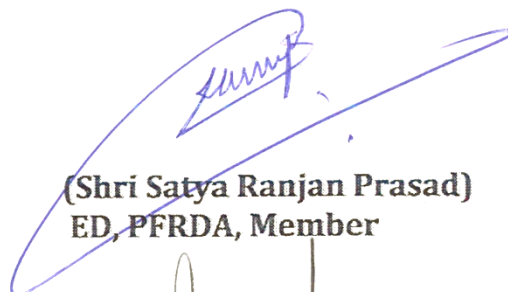
(Shri. S. V. Murali Dhar Rao)  
ED, SEBI, Member



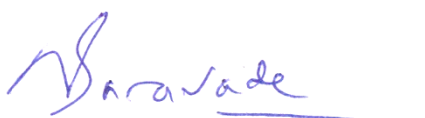
(Shri A.P. Hota)  
MD & CEO, NPCI, Member



(Shri A.R. Nithiyantham)  
CGM, IRDAI, Member



(Shri Satya Ranjan Prasad)  
ED, PFRDA, Member



(Shri Nandkumar Saravade)  
CEO, ReBIT, Member



(Dr. A.S. Ramasastri)  
Director, IDRBT, Member

## **ANNEXES**

**Annex-I****International practices in establishing CERT/CERT-Fin-Structure in different Countries****1. Major developed economies****a) United States: Computer Emergency Readiness Team, United States of America (US-CERT)**

1.1. The President's Cyber-security National Action Plan (CNAP)<sup>30</sup> directs the Federal Government to take new action now and fosters the conditions required for long term improvements in their approach to cyber-security across the Federal Government, the private sector, and personal lives. Highlights of the CNAP include inter alia empowering Americans to secure their online accounts by moving beyond just passwords and adding an extra layer of security and investing over \$ 19 billion for cyber-security as part of the President's Fiscal Year (FY) 2017 Budget.

1.2. President on February 9, 2016 established a Commission on Enhancing National Cyber-security<sup>31</sup> that bring top strategic, business, and technical thinkers from outside the government to make critical recommendations on how to use new technical solutions and best practices to protect privacy and public safety. On December 1, 2016 the Commission submitted their report on securing and growing the digital economy. The Commission identified main challenges to achieving cybersecurity as under:

- (i) Technology companies are under significant market pressure to innovate and move to market quickly, often at the expense of cybersecurity.
- (ii) Organizations and their employees require flexible and mobile working environments.
- (iii) Many organizations and individuals still fail to do the basics.
- (iv) Both offense and defense adopt the same innovations
- (v) The attacker has the advantage
- (vi) Technological complexity creates vulnerabilities
- (vii) Interdependencies and supply chain risks abound
- (viii) Governments are as operationally dependent on cyberspace as the private sector
- (ix) Trust is fundamental

1.3. US-CERT (*it is a readiness team and not response team*) strives for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cyber security information with trusted partners around the world. US-CERT's critical mission activities include:

- Providing cyber security protection to Federal civilian executive branch agencies

<sup>30</sup>Michael Daniel, Tony Scott, Ed Felten, The President's National cyber security Plan: What You Need to Know, FEBRUARY 9, 2016

<sup>31</sup> Whitehouse.gov, Administration Efforts on Cybersecurity: The Year in Review and Looking Forward to 2016, February 2, 2016.

through intrusion detection and prevention capabilities.

- Developing timely and actionable information for distribution to federal departments and agencies; state, local, tribal and territorial (SLTT) governments; critical infrastructure owners and operators; private industry; and international organizations.
- Responding to incidents and analyzing data about emerging cyber threats.
- Collaborating with foreign governments and international entities to enhance the nation's cyber security posture.

1.4. In early 2000, Federal Government networks began to experience an alarming number of cyber breaches. In response, Congress created the Federal Computer Incident Response Center (FedCIRC) at the General Services Administration as a centralized hub of coordination and information sharing between federal organizations. With the creation of the Department of Homeland Security in 2002, Congress transferred these responsibilities to the new Department. In 2003, FedCIRC was renamed "US-CERT," and its mission was expanded to include providing boundary protection for the federal civilian executive domain and cyber security leadership. This shared responsibility has evolved over time to make US-CERT a trusted partner and authoritative source in cyberspace for the Federal Government; SLTT governments; private industry; and international organizations. It is the 24-hour operational arm of the National Cyber-security Communication Integration Center (NCCIC) which accepts, triages, and collaboratively responds to incidents, provides technical assistance to information system operators, and disseminates timely notifications regarding current and potential security threats, exploits, and vulnerabilities to the public via its National Cyber Awareness System (NCAS). US-CERT operates side-by-side with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) which deals with security related to industrial control systems. Both entities operate together within NCCIC to provide a single source of support to critical infrastructure stakeholders.

1.5. FS-ISAC and other developments<sup>32</sup>: In US, the Financial Sector - Information Sharing Analysis Center (FS-ISAC) was established in 1999. It is a membership driven non-profit organization. The FS-ISAC gathers threat, vulnerability, and risk information about cyber and physical security risks faced by the financial services sector around the world. Sources of information include commercial companies who gather this type of information, government agencies, CERTs, academic sources, and other trusted sources. After analysis by industry experts, alerts are delivered to participants based on their level of service.

1.6. U.S. Department of Treasury is the official government sponsor and has provided substantial project funding to meet the requirements of the FS-ISAC. FS-ISAC membership is also recommended by:

---

<sup>32</sup> <https://www.soltra.com/en/about/>

- The United States Treasury
- The Office of the Controller of Currency
- The United States Secret Service
- The Department of Homeland Security
- The Financial Services Sector Coordinating Council, which represents 26 Financial Services Associations and Utilities representing over 25,000 eligible firms.

1.7. Additionally, the FS-ISAC has the endorsement of its members and continues to garner endorsement from relevant agencies, organizations and associations representing the best interests of the financial services industry world-wide. FS-ISAC membership and participants include eligible firms in the financial services sector world-wide such as Banking Firms & Credit Unions. Securities Firms, Insurance Companies, Credit Card Companies, Mortgage Banking Companies, Financial Services Sector Utilities, Financial Services Service Bureaus, Appropriate Industry Associations, Hedge Fund IT and Security Service Providers

1.8. The FS-ISAC is managed by member financial services organizations, and is entirely funded by the private sector. The FS-ISAC offers a variety of value-added information sharing and analysis tools which include the following: Cyber and physical alerts, member surveys, anonymous submissions, bi-weekly threat conference calls, Critical Infrastructure Notification service (CINS), crisis conference calls, membership meetings, and webinar training, all at no additional cost to membership (depending on your membership level).

1.9. The current FS-ISAC database has thousands of threats, vulnerabilities, and events dating back to 1999. Premier and above members may use this database to do research and investigations. The FS-ISAC analysts use the database to establish trends, do research, and investigations. Over time the FS-ISAC is expecting to offer advanced analytics to Premier and above members to study multiple firm IDS data and other sophisticated programs to predict the likelihood of events.

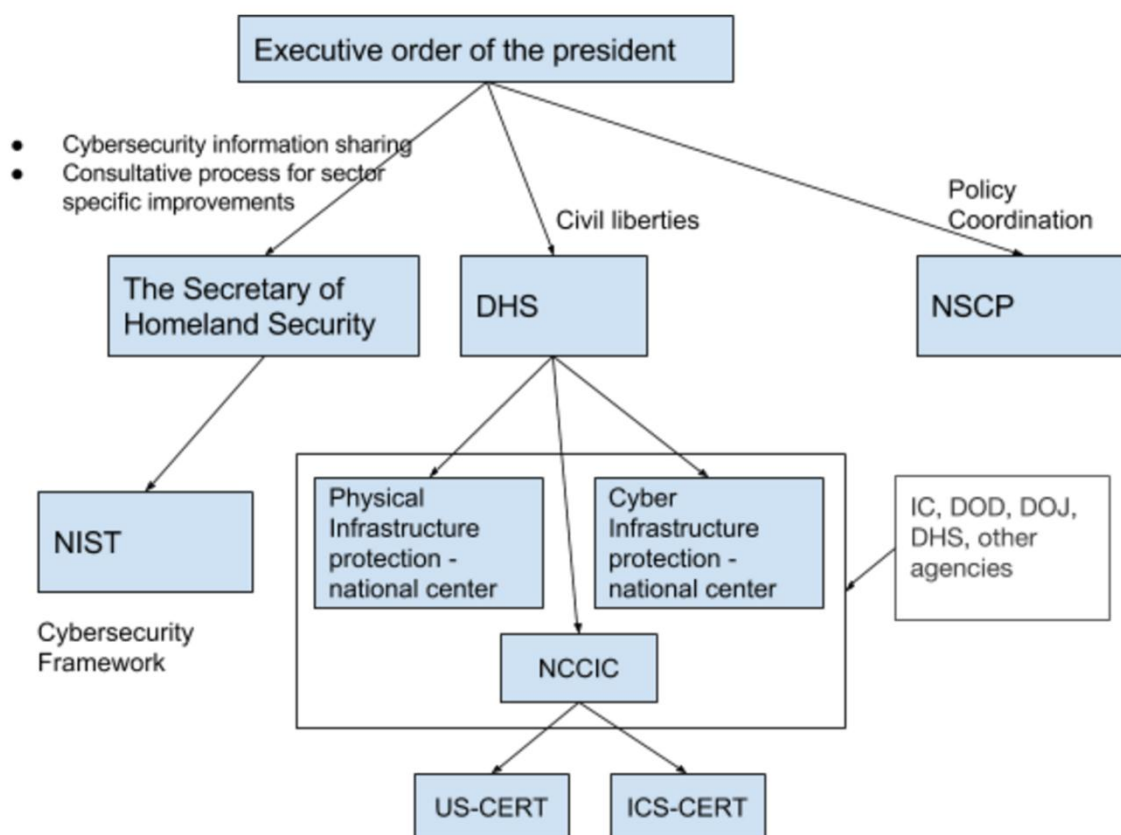
1.10. In addition to work in the financial sector a national level plan and structure of nodal agencies and clarification of roles and responsibilities was undertaken under an executive order of the President. The President of US issued an order on Feb 12, 2013 to strengthen the cyber-security for critical infrastructure (Executive Order 13636, Improving Critical Infrastructure Cyber-security).

1.11. In the US, the laws addressing cyber-security expectations and requirements include Gramm-Leach-Bliley Act (GLBA), the Bank Secrecy Act, the USA PATRIOT Act, the identity theft red flag rule, and Sarbanes Oxley. Financial sector in US are amongst the most aware, most organized and most sophisticated industries facing the cyber-security threat. The executive order to improve critical infrastructure cyber-security,



2013 identified the following:

- i. Policy coordination - to be performed by National Security Council System
- ii. Cyber-security information sharing – Secretary of Homeland Security and Director of National Intelligence to issue unclassified reports, establish process to disseminate the information to the targeted entity. Assist the operators and owners of critical infrastructure through Enhanced Cyber-security services program.
- iii. Department of Homeland Security (DHS) to assess and mitigate civil liberties risk.
- iv. National Institute of Standards & Technology (NIST) under the Secretary was asked to work on putting together Cyber-security Framework.
- v. The Secretary was given a task to identify the critical sectors based on risk based model.



1.12. Based on this directive 16 critical sectors were identified and for each sector, sector-specific plan was developed. For e.g., Financial Services Sector Specific plans was developed through collaboration between: U.S. Department of the Treasury (Treasury), the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC), the Financial and Banking Information Infrastructure Committee (FBIIC), and the U.S. DHS. There are many partners engaging formally and informally.

1.13. In addition to the executive order, a NIPP (National Infrastructure Protection Plan)

and a Presidential Policy Directive (PPD-21) was issued. NIPP was developed in collaboration with these 16 different sectors in all 50 states, all levels of government and states. The PPD-21 assigns a sector specific agency (SSA) to each of these 16 sectors. The PDD-21 also clarifies roles of various federal agencies for cybersecurity resiliency.

1.14. In joint venture with Depository Trust & Clearing Corporation (DTCC), FS-ISAC has built a platform called Soltra that was made available in December of 2014 for real-time threat information sharing to its members. The FS-ISAC remains a separate body and provides cyber threat exchange solution along with US-CERT. The Cyber Threat Exchange Platform for both FS-ISAC and US-CERT is provided by NC4. The Soltra was acquired by NC4 in November.

## **b) Canada**

1.15. The Government of Canada is currently reviewing its approach to cyber security to maximize the benefits of digital technologies for Canadians and businesses, and to advance its cyber security capability, resilience and innovation. *Canada's Cyber Security Strategy* outlines how the Government of Canada is working with all levels of government, private sector organizations and international partners to strengthen cyber security in Canada. It is focused on three pillars: securing Government systems, partnering to secure vital cyber systems outside the federal Government and helping Canadians to be secure online.

1.16.. Get Cyber Safe provides information on cyber security to help Canadians protect themselves, their families, and their small and medium businesses online. Learn more about the tools and tips to help you stay cyber safe. Public Safety Canada's Cyber Incident Response Centre coordinates Canada's response to serious cyber security incidents. It works with partners, both inside and outside Canada, to take action on cyber threats and to protect the important systems Canadians rely on, such as banks and telecommunications service providers. The Cyber Security Cooperation Program supports projects through grants and contributions to improve the security of Canada's vital cyber systems. Find out if you qualify and how to apply. Cyber Security Awareness Month is an internationally recognized campaign held each October to promote cyber security and inform Canadians on how to be more secure online.

**1.17. Canadian Cyber Incident Response Centre (CCIRC):** CCIRC is Canada's national coordination centre responsible for reducing the cyber risks faced by Canada's key systems and services. These systems, such as banks or phone service providers, are known as critical infrastructure. CCIRC works within Public Safety Canada in partnership with provinces, territories, municipalities, private sector organizations and international counterparts. It also coordinates the national response to any serious cyber security incident.

1.18. Products and services available to CCIRC partners:

**(a) Advice and support to prepare for and mitigate cyber events.**

In addition to the technical advice and guidance, partners also receive early detection indicators, summary, trend and operational analysis. They also regularly send out technical information on cyber threats, vulnerabilities, risks and incidents. These information resources help partners better understand the cyber risks and make informed decisions.

**(b) Technical advice and support to respond to and recover from targeted attacks.**

CCIRC provides its partners with technical advice, and performs malware analysis and forensics. In addition to its own expertise, CCIRC can draw on broader Government expertise and resources to help develop timely mitigation and recovery advice.

**(c) Access to trusted forum for information sharing and collaboration.**

CCIRC partners have access to the Community Portal, a collaboration tool for organizations, where they can share information and gain access to expertise and peer support. This portal is used to share CCIRC's documents and publications and, in turn, partners can post documents of their own or report cyber incidents.

**1.19. Information sharing levels:** All CCIRC's cyber awareness products for their partners have one of four information sharing levels (Ex: Public/Private), commonly known as the Traffic Light Protocol (TLP) Viz., Red, Amber, Green and White.

**c) European Union<sup>3334</sup>**

1.20. EU has a permanent Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies since 2012. The team is made up of IT security experts from the main EU Institutions (European Commission, General Secretariat of the Council, European Parliament, Committee of the Regions and Economic and Social Committee). It cooperates closely with other CERTs in the Member States and beyond as well as with specialised IT security companies.

1.21. In response to growing worries concerning global cyber threats, in February 2016, the European Union (EU) and NATO have stepped up their cyber defence cooperation and signed a Technical Arrangement between the North Atlantic Treaty Organization (NATO) Computer Incident Response Capability (NCIRC) and CERT-EU. The milestone agreement signed enables technical information sharing as well as best practices exchanges between NCIRC and CERT-EU to advance cyber incident prevention, detection and response in both organisations, in line with their decision making autonomy and procedures.

<sup>33</sup>EU cyber security initiatives, January 2017.

[http://ec.europa.eu/information\\_society/newsroom/image/document/2017-3/factsheet\\_cybersecurity\\_update\\_january\\_2017\\_41543.pdf](http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf)

<sup>34</sup> Raluca Csernatonu, Time to Catch Up: The EU's Cyber Security Strategy, March 4, 2016, European Public Affairs.eu <http://www.europeanpublicaffairs.eu/time-to-catch-up-the-eus-cyber-security-strategy/>

1.22. The European Union Agency for Network and Information Security (ENISA) set up in 2004 with an objective to contribute to the overall goal of ensuring a high level of network and information security within the EU, supports CERTs cooperation in the Member States apart from collecting and analysing data on security incidents in Europe and emerging risks, promoting risk assessment and risk management methods to enhance capability to deal with information security threats etc.

1.23. In 2016, EU brought out a directive to establish CSIRTs network "in order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation". It is composed of representatives of the EU Member States' CSIRTs and a CSIRT for EU institutions CERT-EU.

**1.24. EFI-ISAC:** The European FI-ISAC, the European Financial Institutes – Information Sharing and Analysis Centre, is an independent organisation that was founded in 2008. Membership consists of country representatives coming from the financial sector, national CERT's (GovCerts) and Law Enforcement Agencies (LEA's). Other organisations represented are: ENISA, Europol, the European Central Bank (ECB), the European Payments Council (EPC) and the European Commission. The European FI-ISAC is actively supported by ENISA.

1.25. Mission statement: The mission of the European FI-ISAC is information exchange on e- and m-channel, cards, central systems and all ICT related topics including (i) Cyber-criminal activity affecting the financial community (ii) Vulnerabilities, technology trends and threats (iii) Incidents and case-studies. This information exchange helps each member and the banks in its member state, to raise awareness on potentials risks, and provides an early warning on new threats and MO's.

1.26. Co-operation model: The members share information by (i) Meeting twice per year (hosted by members, in different European cities) (ii) Forwarding continuously relevant information via the EU FI-ISAC list server (iii) Direct individual communication between member organizations/individuals. Trusted relationships are the key to successful co-operation and exchange between members. Members represent their country and should actively participate in the information exchange. Members cannot send non-members as substitutes in a meeting.

**1.27. Members of the European FI-ISAC must sign the Traffic Light Protocol (TLP).** The TLP is an agreement to ensure that sensitive information is shared according to requirements defined by the source individual/organisation. Europol is the European Union's law enforcement agency set up to achieve a safer Europe for the benefit of all EU citizens. Europol set up the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime. The European FI-

ISAC has signed a Memorandum of Understanding with Europol EC3 seeking the mutual interest for co-operation between the European FI-ISAC and EC3, a step to improve co-operation between the European banking community and European Law Enforcement Agencies. There are 32 financial CERTS operating in Europe (These are either country specific or within a country, institution specific).

1.28. The following 32 Financial CERTs are operating in Europe:

<b>Country</b>	<b>Region</b>	<b>Name</b>
Austria	EU	R-IT CERT
Belgium	EU	KBC Group CERT
Czech Republic	EU	CSOB-Group-CSIRT
France	EU	CERT Groupe BPCE
France	EU	CERT Caisse des Depots (CERT-CDCFR)
France	EU	CSIRT La Poste
France	EU	CSIRT BNP Paribas
France	EU	CERT-Societe Generale
France	EU	CERT-BDF
France	EU	CERT Credit Agricole
Germany	EU	S-CERT
Germany	EU	Deutsche Bank
Germany	EU	CSIRT-ECB
Germany	EU	ComCERT
INT	Europe	ISPIRIT
Luxembourg	EU	DBG-CERT
Netherlands	EU	Rabobank Group CSIRT
Netherlands	EU	ING CCERT
Netherlands	EU	ABN AMRO Global CIRT (AAB GCIRT)
Norway	EFTA	FinansCERT
Norway	EFTA	DnB IRT
Spain	EU	BBVA CERT
Spain	EU	MAPFRE-CCG-CERT
Spain	EU	e-LC CSIRT
Sweden	EU	SEB Computer Security Incident Response Team
Sweden	EU	Swedbank SIRT
Sweden	EU	Handelsbanken SIRT
Switzerland	EFTA	Bank Vontobel CERT (VTCERT)
Switzerland	EFTA	BVCERT
United Kingdom	EU	RBSG-ISIRT
United Kingdom	EU	MLCIRT
United Kingdom	EU	Citi SIRT (formerly Citigroup)

#### **d) Germany**

1.29. The S-CERT, are the computer emergency response team of the German Sparkassen-Finanzgruppe (Savings Banks Financial Group). S-CERT consists of members

drawn from savings banks, Landesbanken and insurers as well as IT service providers affiliated directly with the Sparkassen-Finanzgruppe. S-CERT is a service of SIZ GmbH. It serves not only members of the Sparkassen-Finanzgruppe, but other German financial institutes too. S-CERT also provides its international partners with a central point of contact with the German finance industry, and as such, forms an important first point of contact for all IT-security-related issues.

#### **e) Denmark**

1.30. In 2015, citing the increasing cyber related attacks and its potential threat to financial stability, Denmark's National bank raised this issue in Systemic Risk Council and as an outcome, the Financial Sector forum for Operational Resilience (FSOR) was set up in 2016. FSOR is a forum for collaboration between authorities and key financial sector participants in Denmark aiming to increase operational resilience when using IT across the sector, including resilience to cyber-attacks. Broadly its task are to (i) ensure a common overview of operational risks that may have cross sector impact (ii) ensure implementation of joint measures to ensure financial sector resilience to major operational incidents, including cyberattacks and (iii) create a framework for collaboration and information sharing.

1.31. The FSOR with special focus on cyber resilience works on establishment of national cross-sector crisis response for the financial sector, conducting a Danish cyber stress test, mapping and risk-assessing the financial infrastructure, and general stocktaking of the cyber resilience capability of key participants in relation to cyber-attacks. Articulating its vision, the FSOR has observed as under: The Danish financial sector should be best in class in Europe when it comes to countering the threat from cybercrime, so that it (a) continues to provide a secure and efficient infrastructure, and (b) supports the Danes' continued trust in the digital solutions of the Danish financial sector.

1.32. It is essential that financial sector customers have trust in the sector and in the digital solutions it uses. This is a precondition for realising the growth and innovation potential that lies in the digitisation of society. FSOR has identified three measuring points in order to measure whether the vision is realised, with attached indicators. The measuring points suggested are:

- (i) Denmark is in the top 5 in international benchmarks for cyber security among financial firms in Europe.
- (ii) Danish citizens and firms continue to have great trust in the sector's digital solutions.
- (iii) The sector's losses as a result of cybercrime are in the bottom 5 in Europe.

1.33. These indicators are currently being clarified. In its vision document, inter alia it has discussed on working on possibilities of setting up a Nordic financial CSIRT, risk assessment, cyber stress test and setting up collaboration with a future Nordic financial CSIR, relevant FSOR counterparts in other countries by 2020. Thus, Denmark is in early stages of preparation in setting up necessary systems and procedures in the overall

cyber security framework. To implement the vision, a three pronged strategy has been suggested:

- (i) Strengthened collaboration within the sector and improved scope for action for individual sector participants: The FSOR should create the framework for strengthened collaboration within the sector and improve the sector's scope for action in relation to cyber threats and IT security threats. They want to be best in class in Europe when it comes to optimising and testing operational resilience capability across the sector. Stronger sector collaboration should also contribute to improving the individual participants' ability to address cyber threats and IT security threats.
- (ii) Stronger collaboration with relevant stakeholders both nationally and internationally: The FSOR should strengthen collaboration with relevant stakeholders, both nationally and internationally, with a view to sharing experience and best practice for countering cybercrime. This should improve the scope for specific action for FSOR members and for other stakeholders.
- (iii) Increased awareness and knowledge of cyber security: The FSOR should help to ensure that all financial sector participants have the necessary knowledge and skills so that they will be able to protect themselves against cyber threats and IT security threats. At the same time, the FSOR's work should contribute to improving the individual participants' efforts to increase customer awareness and competencies as regards cyber security.

**f) United Kingdom: National Cyber Security Centre-United Kingdom (NCSC-UK)<sup>35</sup>**

1.34. The NCSC was set up to help protect critical services from cyber-attacks, managing major incidents and improve the underlying security of the UK Internet through technological improvement and advice to citizens and organizations. Vision is to help make the UK the safest place to live and do business online. The National Cyber Security Centre (NCSC) is the UK's authority on cyber security. They are a part of Government Communications Head Quarters (GCHQ). The NCSC brings together and replaces CESG (the information security arm of GCHQ), the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT UK) and the cyber-related responsibilities of the Centre for the Protection of National Infrastructure (CPNI). The NCSC has access to some of the most sophisticated capabilities available to government.

1.35. The NCSC is open and accessible. They work collaboratively with other government agencies and departments, law enforcement, defense, the UK's intelligence and security agencies and international partners. NCSC exchange talent with other organizations through secondments and interchanges; this allows them to foster

---

<sup>35</sup>([https://www.theregister.co.uk/2016/03/23/new\\_uk\\_cyber\\_security\\_centre\\_to\\_work\\_with\\_bank\\_of\\_england/](https://www.theregister.co.uk/2016/03/23/new_uk_cyber_security_centre_to_work_with_bank_of_england/))

the technical innovation needed to succeed in an ever changing landscape.

1.36. Purpose: The NCSC's main purpose is to reduce the cyber security risk to the UK by improving its cyber security and cyber resilience. It work together with UK organizations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management. This is underpinned by world class research and innovation. They recognize that, despite all their efforts to reduce risks and enhance security, incidents will happen. When they do, the NCSC will provide effective incident response to minimize harm to the UK, help with recovery, and learn lessons for the future. The 2015 National Security Strategy (NSS) reaffirmed the cyber threat as one of the most significant risks to UK interests. The NSS set out the Government's determination to address cyber threats and put in place tough and innovative measures as a world leader in cyber security. To deliver on that commitment, on 1st November 2016 the Government published the 2016-2021 National Cyber Security Strategy. The National Cyber Security Centre is a key means for government to deliver many elements of strengthened cyber security for the UK.

1.37. Guidance: The NCSC guidance is a crucial part of ensuring that the UK has the capacity to manage the increasing cyber threat. Based on unique perspective that they provide through their global intelligence insight, they publish practical and proportionate security guidance to protect both new and existing IT systems, and the UK's critical national infrastructure. Their approach to guidance is that they provide *advice*, not standards or policy. And because their guidance is advisory in nature, it provides a sound basis from which to make your own, informed decisions that are right for organization. With help from their colleagues in CPNI providing expert protective security advice, we take an experienced, balanced view of risk to identify appropriate countermeasures. Their aim is to provide the best possible cyber security advice and information to everyone in the UK, including the public and members of organizations of all kinds. Ten Steps to Cyber Security outlines the basic cyber security procedures to protect an organization from cyber-attacks, while Cyber Essentials allows organizations to advertise that they meet a government endorsed standard of cyber hygiene. Ten Steps to Cyber Security as suggested by NCSC-UK are as follows: Risk Management Regime, Secure configuration, Network security, Managing user privileges, User education and awareness, Incident management, Malware prevention, Monitoring, Removable media controls and Home and mobile working

1.38. CBEST Framework of UK: CBEST is a framework to deliver controlled, bespoke, intelligence-led cyber security tests. In 2013, the Financial Policy Committee issued a recommendation to HM Treasury requesting that they and regulators work with the core UK financial systems and the infrastructure providers that support them, to put in place a programme of work to improve and test resilience to sophisticated cyber-attacks. The Committee also noted it was important that boards of financial firms and infrastructure providers recognized their responsibility for responding to attacks, which requires a combination of continuous vigilance and investment to strengthen



operational resilience.

1.39. The UK Financial Authorities – Bank of England (BoE), Her Majesty’s Treasury, and the Financial Conduct Authority - have taken steps to address these issues<sup>36</sup>. They have consulted with financial services organizations, while also working with the penetration testing and cyber threat intelligence services industry to develop a scheme that is sympathetic to the concerns raised by the financial services industry and the risks associated with testing critical assets. It is through these consultations that the Financial Authorities have defined the CBEST testing framework. The implementation of CBEST will help the boards of financial firms, infrastructure providers and regulators to improve their understanding of the types of cyber-attack that could undermine financial stability in the UK, the extent to which the UK financial sector is vulnerable to those attacks and how effective the detection and recovery processes are. CBEST, with the support of industry, puts in place measures to ensure that targeted tests can be conducted on critical assets without harm.

1.40. CBEST replicate behaviors of threat actors, assessed by Government and commercial intelligence providers as posing a genuine threat to systemically important financial institutions. CBEST differs from other security testing currently undertaken by the financial services sector because it is threat intelligence based, is less constrained and focuses on the more sophisticated and persistent attacks on critical systems and essential services. CBEST provides a holistic assessment of financial services or infrastructure provider’s cyber capabilities by testing people, processes and technology in a single test which will be less time constrained than traditional penetration testing.

1.41. The inclusion of specific cyber threat intelligence will ensure that the tests replicate, as closely as possible, the evolving threat landscape and therefore will remain relevant. CBEST will utilize key performance indicators to measure capability and maturity in this important area and provide benchmark information to the industry and regulators. This benchmark information will not only improve the position of those that have been subject to CBEST but will also help to inform where effort needs to be focussed to improve all aspects of the financial services industry’s ability to protect itself from cyber-attacks and to be able to detect and respond appropriately.

#### **g) Australia**

1.42. CERT Australia (the CERT) is the national computer emergency response team. They are the point of contact in Government for cyber security issues affecting major Australian businesses. The CERT is part of the Federal Attorney-General’s Department, with offices in Canberra and Brisbane. They are also a key element in the Australian Cyber Security Centre, sharing information and working closely with the Australian Security Intelligence Organization, the Australian Federal Police, the Australian Signals

---

<sup>36</sup> <https://www.ncsc.gov.uk/>  
 Cabinet Office National security and intelligence HM Treasury The Rt Hon Philip Hammond MP, National Cyber Security Strategy 2016 to 2021, November 1, 2016. <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>

Directorate, the Defence Intelligence Organization and the Australian Criminal Intelligence Commission. In addition, the CERT has direct working relationships and a range of bilateral and multilateral agreements with government and business computer emergency response teams around the world. Their partnerships with government agencies and international counterparts mean they are well connected and informed, so they are best placed to help businesses protect themselves from cyber-attacks.

1.43. The CERT provides advice and support on cyber threats and vulnerabilities to the owners and operators of Australia's critical infrastructure and other systems of national interest. A compromise of these systems could result in significant impacts on Australia's economic prosperity, social wellbeing, national defence and security. These businesses and industries underpin essential service delivery across Australia, including banking and finance, communications, energy, resources, transport and water. To date, they have partnerships with around 500 businesses. By using the government, industry and international networks, the CERT provides the partners with the most useful and effective advice possible, as soon as possible.

1.44. In addition, they advise businesses to implement the Strategies to Mitigating Cyber Security Incidents released by the Australian Signals Directorate. The advantage of this guidance is that it is customizable to each organization based on their risk profile and the threats they are most concerned about. The CERT issues advisories which are detailed and time sensitive information on action that can be taken in regard to vulnerabilities and/or mitigation strategies – e.g., a security flaw or vulnerability in a particular product. For advice on how to better protect information and/or systems, the Guidelines are issued.

1.45. An overview of the services offered by the CERT Australia: CERT Australia is a trusted source of information and advice on cyber security issues. They provide advice in many forms, from written advisories to sectoral briefings, and if needed onsite consultation and support. They offer a range of services including a hotline, email support, technical guidance on mitigating cyber threats, incident response support and coordination, information sharing and capability building. Small businesses and home users are encouraged to use the Stay Smart Online service.

#### **General guidance**

- (i) provide locally relevant, closed-source information regarding vulnerabilities and software platforms, and threats
- (ii) provide technical guidance on mitigating threats and vulnerabilities, including on system architecture
- (iii) verify proposed controls and response activities undertaken by in-house experts
- (iv) provide high level architecture guidance and a security sounding board to help in-house experts

- (v) provide details on malicious infrastructure currently used to target Australian interests.

### **Denial of service mitigation**

- (i) identify attack controllers
- (ii) reach out to international partners to request takedown of attack controllers and mitigate attack traffic
- (iii) provide specific advice based on the particular attack being employed.

### **Incident response support**

- (i) provide rapid access to initial advice and assistance during an incident, while other support and clean-up is being arranged
- (ii) access whole-of-government specialist skills, expertise and information to help in mitigating threats and vulnerabilities
- (iii) work with international partners to seek remediation of attacks originating overseas, and to respond to attacks originating in Australia that are targeting infrastructure overseas
- (iv) provide preliminary malware, log file and other artefact analysis to offer advice on optimal response activities
- (v) coordinate the disclosure of vulnerabilities between individuals, businesses and vendors. For further information, see our Vulnerability disclosure coordination policy.

### **Incident response coordination**

- (i) coordinate the Government's response with industry during a significant incident
- (ii) provide an initial point of contact and coordination for threats with an international dimension
- (iii) notify Australian websites and businesses of system network compromises based on information feeds from a variety of sources.

### **Information sharing and capability building**

- (i) provide one-on-one briefings to businesses about the current cyber threat environment
- (ii) provide businesses with unique and sensitive information through sector specific, regional and national information exchange programs
- (iii) contribute to and present at the cyber security training course for control systems held by the Queensland University of Technology (QUT) and Edith Cowan University (ECU)
- (iv) conduct and contribute to cyber security exercises – nationally and

internationally.

## **h) Japan**

1.46. The Financial Services Agency (FSA) has been conducting the supervision and inspection regarding cyber security management as a part of system risk control, etc. The Cyber Security Basic Act enacted in November 2014 discusses the cyber security of critical infrastructure including the financial sector. FSA has five policies to strengthening cyber security in the financial sector from the financial regulator's perspective as under:

- (i) Constructive dialogue with financial institutions and grasp of their current condition regarding cyber security
- (ii) Improvement of the information sharing framework among financial institutions
- (iii) Continuous implementation of industry-wide cyber security exercises
- (iv) Cyber-security human resource development in financial sector
- (v) Arrangement of cyber security initiatives in the FSA

**1.47. Constructive Dialogue with Financial Institutions and Grasp of their Current Condition regarding Cyber Security:** The FSA will continue constructive dialogues to enhance the effectiveness of cyber security management systems of financial institutions. As a part of this process, the FSA will grasp the current condition regarding the cyber security of the whole financial sector this year through a questionnaire, and analyze issues associated with each type of financial institution. The FSA will give the financial institutions feedback through dialogue with them and encourage the financial institutions to conduct self-checks, etc.

**1.48. Improvement of Information Sharing Framework among Financial Institutions:** The FSA will continuously raise awareness to financial institutions regarding the importance of collecting/providing information and strengthening measures (immediate grasp of vulnerabilities, introduction of security control technology, etc.) through utilizing the information sharing institution (Financials ISAC Japan, etc.). The FSA will voluntarily provide information through industry groups (CEPTOAR) as necessary in addition to the information provided by the National Center of Incident Readiness and Strategy for Cyber-security (NISC) under Cabinet Secretariat. The Center for Financial Industry Information Systems (FISC) will drastically raise the level of FISC Security Guidelines, and will publish the answers to inquiries from financial institutions regarding the interpretation of FISC Security Guidelines as "Cyber Security reference information".

**1.49. Continuous Implementation of Industry-wide Cyber Security Exercises:** Conduct cyber security exercises, cultivate practical abilities, check the system, and conduct the PDCA cycle. To use exercises in foreign countries also as a reference.

**1.50. Cyber-security human resource development in financial sector:** To strengthen cyber security, financial institutions' staff such as not only IT engineers but also members of the board of directors and executives need to have a certain level of

awareness and knowledge about cyber security. Also, it is necessary to improve the quality of human resources in the supervisory authority. After July 2015, the FSA promotes the following measures:

- (i) Organize seminars to improve the awareness of Financial institution's
- (ii) Considering plans to develop human resources and to strengthen cyber security in the financial sector in cooperation with industry associations and information sharing institutions
- (iii) Improving the expertise of the FSA's human resources (adoption of outside experts and education of internal personnel)

**1.51. Arrangement of Cyber Security Initiatives in FSA:** To strengthen the cyber security of the whole financial system, the FSA immediately establishes a division which collects and unifies relevant information in the FSA, accumulates knowledge through utilizing outside experts, and coordinates the policy across the FSA. A timeline of Japan's CERT activities, as it ramped up its services:

#### Japan CERT Timelines



#### i) New Zealand<sup>37</sup>

<sup>37</sup> National Computer Emergency Response Team (CERT) to be established at MBIE, May 5, 2016. <http://www.mbie.govt.nz/about/whats-happening/news/2016/nationalcomputer-emergency-response-team-cert-to-be-established-at-mbie>  
Simon Bridges, New national cyber security unit launched, April 11, 2017, [beehive.govt.nz. https://www.beehive.govt.nz/release/new-national-cyber-security-unit-launched](https://www.beehive.govt.nz/release/new-national-cyber-security-unit-launched)

1.52. New Zealand framed its revised cyber security strategy<sup>38</sup>, accompanying Action Plan, and a National Plan to Address cybercrime in late 2015 based on which its CERT viz., CERT NZ was formed on April 11, 2017. It was formed at Ministry of Business, Innovation & Employment (MBIE), New Zealand Government to support businesses, organisations and individuals who are affected (or may be affected) by cyber security incidents. It provides trusted and authoritative information and advice, while also collating a profile of the threat landscape in New Zealand. The NZ Government announced an investment of \$22.2 million to set up a new national Computer Emergency Response Team (CERT) as part of Budget 2016. In establishing a CERT, New Zealand joins an international network of CERTs.

1.53. To meet the challenges in cyber threat landscape, CERT NZ would work with other organisations in the cyber security environment across the private, public and not-for-profit sectors in New Zealand including Department of Internal Affairs (DIA), Netsafe, National Cyber Security Centre (NCSC), and New Zealand Police. CERT NZ will function at the centre of New Zealand's cyber security architecture to deliver on five core functions of incident reporting, response coordination, readiness support, vulnerability identification and threat identification.

#### **j) Singapore<sup>39</sup>**

**1.54.** Singapore's cyber resilience strategy resides on four pillars viz., (i) Building a resilient infrastructure (ii) Creating a safer cyber space (iii) Developing a vibrant cyber-security ecosystem and (iv) Strengthening international partnerships. The Singapore Computer Emergency Response Team (SingCERT) was set up in October 1997 as a programme of the Infocomm Development Authority of Singapore (IDA), in collaboration with the National University of Singapore (NUS) to facilitate the detection, resolution and prevention of security related incidents on the Internet. SingCERT provides technical assistance and coordinates responses to security compromises, identifies trends in hacking activities, and works with other security agencies to resolve computer security incidents.

1.55. The gist of developments made by Singapore in combating cyber threat in the last decade is given here. In the ever increasing cyber threat landscape, Singapore launched its first infocomm security masterplan in 2005 and the second in 2008. A Cyber-Watch Centre (CWC) was established by IDA in 2007 to monitor cyber threats to government networks and provide early warning of impending cyber-attacks. This was further upgraded in 2015 with a wider range of detection capabilities and enhanced correlation capabilities. In 2009, Singapore Infocomm Technology Security Authority (SISTA) was

<sup>38</sup> N. Brownlee, The University of Auckland, E. Guttman, Sun Microsystems, Request for Comments: 2350, "Expectations for Computer Security Incident Response" June 1998

<sup>39</sup> (<https://www.out-law.com/en/articles/2012/june/singapores-mas-sets-out-it-security-standards-for-financial-institutions/>)

established to act as a national specialist authority included overseeing the preparation and securing of Critical Information Infrastructures (CIIs) against cyber threats. CIIs include global payment systems, port operations systems, and air-traffic control systems etc. To assess the readiness for CIIs for cyber risk preparedness, a cyber risk management framework and cyber-security maturity assessment model using Readiness Maturity Index (RMI) was introduced. In 2013, the cyber security master plan was expanded to include business and individuals in addition to CIIs. A cyber security R&D programme also was established in same year to improve the trustworthiness of cyber infrastructure, with emphasis on security, reliability, resilience and usability. A National Cyber Security Centre (NCSC) was formed as part of SISTA in 2014 to maintain cyber situational awareness, correlate cyber-security events across sectors, and coordinate with the respective lead agencies to provide a national-level response to large-scale, cross-sector cyber incidents.

1.56. In 2015, a Cyber Security Agency (CSA) was established under the Prime Minister's Office (PMO) and is managed administratively by the Ministry of Communications and Information (MCI). With its formation, all agencies and initiatives related to cyber-security such as SingCERT, IDA and SISTA are brought under this single agency.

1.57. The Singapore government is working to promote "Security by Design" as a best practice to ensure systems that are built are secure throughout its lifecycle. To this effect, the Monetary Authority of Singapore (MAS) has formed a Financial Technology & Innovation Group since August 2015 to design cyber security into FinTech. This Group is responsible for formulating regulatory policies and developing strategies to facilitate the use of technology and innovation to enhance efficiency and better manage risks in the financial sector. This include inter alia to (i) establish a FinTech Innovation Lab that allows stakeholders to experiment with FinTech solutions, including security solutions; (ii) establish "regulatory sandboxes" that can be used to carve out a safe and conducive space to experiment with FinTech solutions, and where the consequences of failure can be contained.

1.58. It is important to encourage the practice of penetration testing to discover vulnerabilities early for remediation at the design stage. To this effect, to raise the professional competency standard, the CREST (Council of Registered Ethical Security Testers) examination facility was opened in Singapore which offers penetration testing certifications and accreditations.

1.59. Recognising the need for concerted and coordinated efforts to deal with cybercrime, the Ministry of Home Affairs (MHA) launched the National Cybercrime Action Plan (NCAP) in July 2016. The NCAP sets out the Government's key principles and priorities in combating cybercrime. The Plan also details the Government's ongoing efforts and future plans to tackle cybercrime which has four priority areas viz., (i) Educating and empowering the public to stay safe in cyberspace (ii) Enhancing

Government's capacity and capability to combat cybercrime (iii) Strengthening legislation and the criminal justice framework and (iv) Stepping up partnership and international engagement.

1.60. While, there is no dedicated CERT set up to exclusively look into the financial sector in Singapore, the CSA coordinates the developments related to cyber security for all sectors including CIIs and is empowered to develop and enforce cybersecurity regulations, policies, and practices. However, Association of Bankers in Singapore (ABS) have released a Penetration Testing Guidelines For the Financial Industry in Singapore on 31 July 2015 for penetration testing to ascertain the effectiveness of the security controls put in place to preserve the confidentiality, integrity and availability of online systems.

1.61. Financial Sector related developments: The Singapore financial services regulator has published the IT security standards that financial services companies operating there must adhere to. The Notice on Technology Risk Management defines and enforces a set of mandatory IT requirements for the financial industry. The Notice stipulates requirements for a high level of robustness and integrity of critical IT infrastructure and systems. It also specifies the requirement for financial institutions to implement IT controls to protect customer information from unauthorised access or disclosure.

1.62. Notices impose legally binding requirements on a specified class of financial institutions or persons. Guidelines, such as the more general one published on technology risk management, are not binding but specified institutions or persons are encouraged to observe the spirit of these guidelines. Monetary Authority of Singapore (MAS) said in the consultation paper that it particularly invited comment from industry in relation to new proposals on data centre protection and controls; mobile banking and payment security; payment card system and ATM security, and combating cyber threats.

### **k) Hong Kong**

1.63. In Hong Kong, the OGCI (The Office of the Government Chief Information Officer) is responsible for articulating government-wide IT security policy and guidelines by providing technical advice and guidance to government agencies in respect of the protection of government information systems, etc. The OGCI in steering the implementation of the IT security standards and measures, also maintains a 24/7 monitoring and reporting system for government information security incident outbreaks. Further, in addition to the government-wide information security incident response teams (ISIRTs) and related mechanism, with increasing trend of cyber-attacks and in order to have closer collaboration both on local and global front, in 2005 the Hong Kong government established Government Computer Emergency Response Team Hong Kong (GovCERT.HK) to centrally coordinate information and cyber security incidents as well as to collaborate with other CERT organisations.



1.64. While, GovCERT.HK is the coordination centre for government, the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) performs similar role for private sectors and the community. Globally, GovCERT.HK collaborates with other governmental / national CERTs and international organisations with a view to facilitate exchange of information and knowledge needed to reduce vulnerabilities, mitigate risks, and react upon threats and attacks. Locally, GovCERT. HK works closely with HKCERT to share information on security threats and vulnerabilities, and provide recommendations to the public/private sectors and individuals in protecting their information systems and digital assets.

1.65. HKCERT also offers services such as (i) Security Alert Monitoring and Early Warning, (ii) Incident Report and Response (Advisory role on response and recovery), (iii) Publication of Security Guidelines & Information and (iv) Promotion of Information Security Awareness. It establishes co-ordination network with related parties, including the OGCIO, the Hong Kong Police Force, Internet Service Providers, Domain Name Registries in Hong Kong, Overseas Computer Emergency Response Teams and other information security vendors for effective response handling. To objectively measure its role, HKCERT has identified some performance indicators and set targets to assess its efficacy.

1.66. To raise public awareness and promote ethics on information security, the OGCIO has set up the InfoSec web site ([www.infosec.gov.hk](http://www.infosec.gov.hk)) which serves as a one-stop portal to facilitate the public's access to various information security related resources and updates.

1.67. Hong Kong Monetary Authority (HKMA) has undertaken a Cyber-security Fortification Initiative (CFI) in May 2016 emphasizing the need for the Authorised Institutions (AIs) Board & senior management to play proactive role in ensuring effective cyber security risk management in their institutions. To further enhance the cyber resilience of banking sector, CFI was developed broadly on three pillars viz., (i) cyber resilience assessment framework, a risk-based framework for AIs to assess their own risk profiles and benchmark the level of defense and resilience that would be required to accord appropriate protection against cyber-attacks (ii) Professional Development Programme (PDP), which seeks to increase the supply of qualified professionals in cyber-security going forward. (iii) Cyber Intelligence Sharing Platform, which provides an effective infrastructure for sharing intelligence on cyber-attacks. Through this platform, member banks of HKAB will be able to tap the latest threat scenarios and get prepared accordingly.

1.68. The HKMA through CFI envisages that AIs put in place proper governance arrangements and processes to achieve the level of resilience in cyber-security commensurating with their risk profile. The assessment framework identifies the

inherent risk based on cyber risk exposure assessed on factors such as technologies used, services offered, delivery channels operated in addition to the organisational character etc. Subsequent to this, the framework provides a measurable process to assess and determine the “actual maturity level” of AIs, which will be compared with the “required maturity level” of cyber resilience. This step is used for process improvement to move the maturity level from “assessed” to “required” level. Finally, the assessment framework has intelligence-led cyber-attack simulation testing (iCAST) to be applied on top of penetration testing (PT) based on specific and up-to-date threat intelligence. AIs, which aim to attain the “intermediate” or “advanced” maturity level are supposed to execute the cyber-attack simulation test.

1.69. In respect of PDP, the HKMA is working with Hong Kong Institute of Bankers (HKIB) and Hong Kong Applied Science and Technology Research Institute (ASTRI) to develop a localized certification scheme and training programme to train and nurture cyber-security practitioners in the AIs and the information technology industry, and to enhance their cyber-security awareness and technical capabilities of conducting cyber resilience assessments and simulation testing.

## **2. BRICS Countries/Economies**

### **a) Brazil<sup>40</sup>**

2.1. The Brazilian Internet Steering Committee (CGI.br) was created by the Brazilian government in 1995 with diverse responsibilities broadly to establish strategic directives related to the use and development of Internet in Brazil. CGI.br in 1997 created CERT Brazil (CERT.br) which is the national CERT for Brazil with responsibilities to collect public statistics on the incidents that are reported to them voluntarily. The data is collected on four categories viz., intrusions, web attacks, denial of service, and fraud.

2.2. CERT.br provides a focal point for incident notification, providing the coordination and necessary support for organizations involved in incidents. Besides doing Incident handling activities, network monitoring & trend analysis, CERT.br also works to increase security awareness, maintains an early warning project with the goal of identifying new trends and correlating security events, as well as alerting Brazilian networks involved in malicious activities.

2.3. Many states and institutions in Brazil have formed their own CSIRTs under the aegis of CERT.br. To raise the national capability in Incident Response CERT.br/CGI.br are a Software Engineering Institute (SEI) - Carnegie Mellon University (SEI/CMU) partner and have licensed 4 CERT/CC courses to deliver in Brazil for incident handling and response.

---

<sup>40</sup> <https://www.cert.br/docs/palestras/certbr-itu-americas2005.pdf>  
<https://www.cert.br/en/>

**b) Russia<sup>41</sup>**

2.4. The Russian Central Bank has established a centre for dealing with cyber-attacks in Russia's financial sector. This centre is responsible for collection and sharing of cyber-attack information in the Russian banking and financial sector. Established by the Russian Central Bank, the centre is called FinCERT. It has been set up following a December 2014 order by the Russian Security Council, a consultative body of the Russian President that implements the President's decisions on national security affairs. This order called for establishment of a centre to respond to cyber-fraud and cyber-attacks on the national financial sector including facilitating notification of possible cyber-threats.

2.5. The FinCERT has close cooperation with the Russian Ministry of Internal Affairs and Federal Security Services and is regarded as very important for the security of the entire Russian financial and banking system, taking into account that the number of cyber-attacks on Russian banks is growing by 20 percent each year. The cooperation between Russian banks and the new centre will be on a voluntary basis, however, in some cases the banks will be obliged to provide certain essential information to FinCERT. Russian banks are currently obliged to provide information about cyber-attacks to the Bank of Russia on a monthly basis.

2.6. The centre will focus on the development of recommendations and best practice to repel hacker attacks and prevent attempted cyber-fraud. It is planned that the centre will provide recommendations for banks when to suspend payments which have indicators of fraud, and will ask them for information about specific clients suspected of stealing. In addition, FinCERT will focus on analytical work, as well as the prevention of DDoS-attacks on the websites of banks. Russian analysts believe that the success of FinCERT will mostly depend on demonstrating its ability to respond effectively to cyber-attacks, as well as the number of banks that choose to cooperate with it.

2.7. The establishment of FinCERT is seen as very important for IT security in the domestic Russian financial and banking systems, as it will facilitate interaction with both law enforcement agencies and other banks. It is reported that 500 Russian banks have expressed their interest in cooperating with FinCERT. In future the ability to track all transactions in the international payment system will allow the FinCERT to take over operational functions, such as monitoring of activity by people previously convicted of fraud, and to inform banks about possible illegal activities and sources of such operations, which may result in their suspension until all the circumstances are clarified.

**c) South Africa<sup>42</sup>**

---

<sup>41</sup> (<https://www.scmagazineuk.com/fincert-to-help-russian-banks-respond-to-cyber-attacks/article/535448/>)  
(<https://www.scmagazineuk.com/russia-to-launch-banking-it-security-centre/article/540908/>)

2.8. The Electronic Communications Security - Computer Security Incident Response Team (ECS-CSIRT), established in 2003 serves as the South African Government Computer Security Incident Response Team. It is a member of FIRST. Africa Computer Emergency Response Team (AfricaCERT) is an umbrella body for CERTs or CSIRTs (Computer Security Incidence Response Team) in Africa, which aims to promote establishment of CERTs and their cooperation and coordination to maintain the health of Africa's Internet systems including South Africa.

2.9. South African Banking Risk Information Centre (SABRIC)<sup>43</sup> was setup in 2002 by four major banks to track & respond to cybercrime targeting the banking sector. A non profit company, it assists the banking and cash in transit companies to combat organised bank-related crimes. SABRIC coordinates closely with the South African Police Service (SAPS), the Directorate for Priority Crime Investigation ('the Hawks') and the Special Investigating Unit's Cyber Forensic Laboratory. Some of the current and future threats identified by SABRIC against secure e-banking include phishing, malwares, hacking, DDoS, Man-in-The-middle Attack etc.

2.10. SABRIC CSIRT became operational since beginning of 2015 under which banking CSIRTs are established as constituents. The establishment of a banking-sector computer security incident response team (CSIRT) at the South African Banking Risk Information Centre (SABRIC) supports a more integrated approach to their national strategy on cybercrime. The CSIRT facilitates early warnings, information sharing at a technical level and the sharing of best practices. The sector CSIRT also facilitates information sharing at a technical level and disseminating best practices.

2.11. The Objectives of the banking sector CSIRT is to

- (i) Combat cyber-crime as an industry
- (ii) To provide information and assistance to the members of the CSIRT in implementing proactive measures to reduce the risks of cyber crime and cyber security incidents as well as responding to such incidents when they occur.
- (iii) Lobby government for an improved environment to counter cybercrime

2.12. In this regard, SABRIC facilitates:

- (i) Cyber-security steering committee for interbank collaboration (which was

---

<sup>42</sup> <https://issafrica.org/iss-today/south-africa-must-pay-more-attention-to-cybercrime>  
<https://www.sabric.co.za/about-us/>  
[http://www.crime-prevention-intl.org/fileadmin/user\\_upload/Evenements/10th\\_ICPC\\_Colloquium/Proceedings/Kalyani\\_Pillay.pdf](http://www.crime-prevention-intl.org/fileadmin/user_upload/Evenements/10th_ICPC_Colloquium/Proceedings/Kalyani_Pillay.pdf)  
[http://www.gov.za/sites/www.gov.za/files/39475\\_gon609.pdf](http://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf)

<sup>43</sup> Dr Buks Louwrens, Mr Gideon Serfontein, Enabling services for secure eBanking in South Africa, ISSA 2011, SBRIC  
[http://www.bic-trust.eu/files/2011/09/South-Africa-Talk\\_6.pdf](http://www.bic-trust.eu/files/2011/09/South-Africa-Talk_6.pdf)  
<http://www.banking.org.za/docs/default-source/publication/annual-review/the-banking-association-south-africa---annual-review-2015.pdf>

established in early 2014). This committee enables participating members of the Financial Services Sector to mature their cyber resilience capabilities

- (ii) Banking Sector CSIRTs to share and respond to shared threats and intelligence
- (iii) SABRIC Cyber-security Assessment (Wolfpack threat framework) to measure the collective cyber resilience maturity of the sector and set a baseline
- (iv) Cyber threat repository, a recent initiative to gather incident and threat information from their members to build a local cyber threat picture - to be driven by a newly approved Cyber-security Reporting Workgroup.
- (v) Customer awareness programs using social media and other platforms
- (vi) Exploring collaborative models to source threat intelligence and up skill resources
- (vii) Working with The Banking Sector Education and Training Authority (BankSETA) and the CSH to promote a skills framework and hopefully define cyber as an occupation with recognized career path and accredited training

2.13. The objectives of SABRIC Cyber-security Steering Committee is to

- (i) Develop and mandate industry strategies to strengthen the banking sector cyber resilience
- (ii) Monitor and understand the international cybersecurity threat landscape
- (iii) Facilitate co-operation between banks in instances where an interchange of knowledge relating to criminal or potential criminal activities will benefit all banks
- (iv) Identify and propose new initiatives and projects to strengthen the banking sector cyber resilience
- (v) Explore proactive measures to countering cyber security threats, and direct the business priorities of SABRIC through agreeing on cybersecurity priorities

#### **d) China<sup>44</sup>**

2.14. The National Computer Network Emergency Response Technical Team/Coordination Center of China (known as CNCERT or CNCERT/CC) was founded in September 2002. It is a non-governmental non-profit cyber security technical center and the key coordination team for China's cyber security emergency response community. As the key coordination organization of China's cyber security emergency response system, CNCERT organizes enterprises, schools, non-governmental groups and research

<sup>44</sup> <http://shnuodi.com/baike.asp?iid=4458>  
<http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan016388.pdf>  
<https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2016/08/cyber-security-in-china.pdf>  
<http://www.cert.org.cn/publish/english/index.html>

institutes that are specialized in cyber security and coordinates ISPs, domain name registrars and other emergency response organizations in a joint effort to build the cyber security emergency response system of China and handle major cyber security incidents. It is also member of FIRST and one of the founders of Asia Pacific Computer Emergency Response Team (APCERT). As of 2016, CNCERT has established “CNCERT International Cooperation Partnership” with 185 organizations in 69 nations and regions.

2.15. CNCERT has established so far 31 branches across mainland china. CNCERT performs information collection, event monitoring, incident handling, data analysis, resource building, security research & training, technical consulting etc. It also organizes domestic CERTs to conduct international cooperation and exchange.

2.16. The Chinese government has revised its cyber security law in 2016, which will come into effect from June 2017. Security requirements for “network operators” is seen as one of the key considerations under cyber security law and the definition of network operators may also include Financial institutions that collect citizens’ personal information and provide online services, such as banking institutions, insurance companies, securities companies and foundations. China Banking Regulatory Commission (CBRC) has issued rules for the emergency management of banking important information systems. It specifies that information technology supervisory Department of CBRC security shall be the regular agency for emergency management of banking information systems and performs functions including emergency response, releasing early warning information, maintaining contacts with emergency management agencies etc.

### **3. Emerging economies**

#### **a) Czech Republic**

3.1. CSIRT.CZ is the National CSIRT of the Czech Republic. CSIRT.CZ fulfills the role of National CERT team as defined in the Act on Cyber security. The CSIRT.CZ team was established under the Cyber threats and Czech Republic’s security interests’ grant. Its aim was to establish a model CSIRT practice and to map the ability of network and service provider in the Czech Republic to cooperate in addressing security incidents.

3.2. The task was to establish a model CSIRT.CZ practice under the Cyber threats and Czech Republic’s security interest grant was assigned to the CESNET association. As CESNET had put together the first official CSIRT team in the Czech Republic – the CESNET-CERTS team, it had experience with both the establishment and functioning of a CSIRT team. Moreover, CESNET can also rely on its relations with the global community of CERT/CSIRT teams necessary to incorporate the new team into the global infrastructure. Once the technical and organisational background was set up (in 2007) and with the support of CESNET-CERTS, the CSIRT.CZ team was accepted by the global community – CSIRT.CZ was listed among teams officially recognised by the Trusted

Introducer. In the Czech Republic, CSIRT.CZ assumed the responsibility of the national and government CSIRT team as defined by the CERT/CSIRT terminology.

3.3. In December 2010, CSIRT.CZ was established as the National CSIRT of the Czech Republic. Their work was governed by a memorandum signed with the National Security Authority. The CSIRT.CZ team is responsible for the territory of the Czech Republic, i.e. all users and networks operated in the Czech Republic fall under the responsibility of CSIRT.CZ. The Cyber security Act of the country defines two high-level teams (governmental CERT and national CERT) and their competences. Governmental CERT is operated by National Cyber Security Centre which is part of National Security Authority. CSIRT.CZ was chosen for fulfilling the role of national CERT in August 2015.

**3.4. GOALS OF CSIRT:** Tasks of CSIRT.CZ in the Czech Republic are as follows:

- (i) To maintain foreign relations – with the global community of CERT/CSIRT teams as well as with organisations supporting the community.
- (ii) To cooperate with various entities across the country – ISPs, content providers, banks, security organs, institutions in the academic sphere, public authorities and other institutions.
- (iii) To provide security services such as:
- (iv) Addressing security incidents and coordination thereof – Receives cyber security incident reports and evaluates them. It also provides methodological support, assistance and cooperation in case of a cyber-security incident and also evaluates vulnerabilities in cyber security
- (v) Education and tutoring
- (vi) Proactive services in the area of security

3.5. Information on threats in the .CZ domain: CSIRT.CZ has developed an open source tracker called Malicious Domain Manager for central monitoring and addressing threats in the top level domain. This application acts as a central point for collecting and analyzing information on the malicious URL in the domain .CZ. It also supports the history of threats in the domains and can directly contact their holders from a dedicated address at [malware@nic.cz](mailto:malware@nic.cz).

3.6. Web Scanner: It offers services of website penetration testing that are primarily designed for public and not-for-profit sector. This service is offered free of charge. The testing consists of automated and manual tests aimed at finding security vulnerabilities in the website application. Each security finding is indicated with an estimated measure of potential risks and a description of recommendations for its correction is also provided.

3.7. Education: In cooperation with the CZ.NIC Academy it regularly organize trainings called "Computer security in practice" where participants can become familiar with the most common ways of cyber attacks. It provides training related to basic operation and requirements of CSIRT teams.

3.8. Working groups: The team holds regular meetings of security teams and members of the security community in the Czech Republic to discuss current trends in the field of security, security threats, the development of cooperation between security teams and exchange of experience with prevention and security incidents resolution.

3.9. Stress tests: CZ.NIC has set up a laboratory for stress tests to handle DoS attacks in cooperation with CSIRT.CZ.

3.10. Intrusion Detection System: In cooperation with CESNET, CSIRT.CZ operates a system for detecting suspicious behaviour of systems connected to the Internet.

3.11. Operation of honeypots: In the context of security research CSIRT.CZ runs a number of honeypots in cooperation with CZ.NIC Labs. Visualization of attacks in real time can be found at <https://honeymap.cz/>. Newly captured malware samples are analyzed and accordingly sent to antivirus companies.

3.12. Incident reporting: According to CSIRT.CZ, it should be regarded as the last resort to seek assistance and cooperation from when it comes to addressing security incidents relating to networks operated in the Czech Republic (i.e. the source or target network is operated in the Czech Republic). It holds network administrator as responsible for handling security incidents.

## **b) Nigeria**

3.13. ngCERT (Nigerian Computer Emergency Response Team) is the National CERT for Nigeria which is domiciled in the Office of the National Security Adviser. ngCERT's core value is to promote the philosophy of cybersecurity research initiatives in Nigeria. The Vision is "To achieve a safe, secure and resilient cyberspace in Nigeria that provides opportunities for national prosperity". The Mission is "To manage the risks of cyber threats in the Nigeria's cyberspace and effectively coordinate incident response and mitigation strategies to proactively prevent cyber-attacks against Nigeria"

3.14. Core Functions:

- To establish a shared Situation Awareness platform - Coordinate information sharing at the National Level
- Efficiently manage and coordinate management of incident of national interest
- Support the National Cyber Security Strategy
- To provide technical support and expertise to sectorial CSIRT's as and when required.
- International Point of contact for all Internet Security Incident in Nigeria.

## **c) Sri Lanka**



3.15. Bank Computer Security Incident Response Team (Bank CSIRT) is a specialized service unit that is responsible for receiving, reviewing, processing and responding to computer security alerts and incidents affecting the Banks and other Licensed Financial Institutions in the country. Bank CSIRT is a joint initiative of the Central Bank of Sri Lanka and the Sri Lanka Computer Emergency Response Team (Sri Lanka CERT) and is hosted under LankaClear (Private) Limited, the national payment infrastructure provider. Bank CSIRT is established as a centralized body to coordinate security efforts within the banking and financial sector, and as an entity steered and funded by the banks, they will have the prime responsibility and accountability towards them.

3.16. **Services:** The Bank CSIRT is structured and positioned to offer the following unique information security services.

- (i) Formulating and implementing of Baseline Security Standards for Banks.
- (ii) Sharing of de-sensitized Fraud, Cyber Crime Incidents and Threat Intelligence information anonymously among Bank CSIRT Members.
- (iii) Raising Vulnerability, Advisory and Informational Alerts.
- (iv) Incident Response Services.
- (v) Registration of Certified third Party Service Providers.

**Major activities and processes involved in setting up CERT-Fin**

<b>Phase</b>	<b>Features</b>
Phase-1  Establish	<ul style="list-style-type: none"> <li>● <b>Definition</b> <ul style="list-style-type: none"> <li>○ Develop policies and procedure</li> <li>○ Elucidate clear expectations from CERT-Fin</li> <li>○ Define constituency and engage with them</li> <li>○ Define relationships with other CERTs and nodal agencies through CERT-In</li> <li>○ Charter, Mission Statements, Contact information, Team structure</li> <li>○ Sponsoring organization, affiliations</li> </ul> </li> <li>● <b>Planning and Development</b> <ul style="list-style-type: none"> <li>○ Tools evaluation, scope and platform requirement elucidation</li> <li>○ Development and operationalization of the base platform</li> </ul> </li> <li>● <b>Onboarding of regulated entities</b> <ul style="list-style-type: none"> <li>○ Training for regulated entities on how to use the platform and report incidents</li> <li>○ Onboard regulated entities to report incidents to the platform</li> <li>○ Provide access as per the membership terms</li> <li>○ Training for nodal agencies on how to connect and exchange information.</li> </ul> </li> <li>● <b>Establish framework for threat exchange between nodal agencies</b> <ul style="list-style-type: none"> <li>○ Long term planning to automate and integrate threat intelligence information exchange between several nodal agencies. Define hierarchies and rules for automated and manual information exchange.</li> <li>○ Training on the platform</li> <li>○ Development of plan for real time information exchange</li> <li>○ Plan joint exercises to establish cohesion between nodal agencies</li> </ul> </li> </ul>
Phase-2  Collect   Coordinate	<ul style="list-style-type: none"> <li>● <b>Platform Enrichment</b> <ul style="list-style-type: none"> <li>○ Add BCP/DR capability</li> <li>○ Adding ticketing system for incident lifecycle management</li> <li>○ Adding knowledge management portal</li> </ul> </li> <li>● <b>Establish appropriate security controls for CERT-Fin systems to ensure CIA of data/incidents collected/reported</b></li> <li>● <b>CERT-Fin website development</b> <ul style="list-style-type: none"> <li>○ Policies and procedures</li> <li>○ Member supports</li> <li>○ Crowdsourcing of threat intel</li> <li>○ SOP for incident handling</li> </ul> </li> <li>● <b>Threat intelligence sources development</b> <ul style="list-style-type: none"> <li>○ Establish secure communication channels</li> <li>○ Obtain membership with available FS-ISACs</li> <li>○ Establish robust information exchange framework with</li> </ul> </li> </ul>

	<p style="text-align: center;">CERT-In</p> <ul style="list-style-type: none"> <li>● <b>Establish incident support capabilities</b></li> <li>● <b>Onboarding of partners and other nodal agencies</b> <ul style="list-style-type: none"> <li>○ Distribution lists, roles, establish protocols for information dissemination</li> </ul> </li> </ul>
Phase-3 Share Awareness	<ul style="list-style-type: none"> <li>● <b>Publishing case studies and lessons learnt</b> <ul style="list-style-type: none"> <li>○ Share through industry forums</li> <li>○ Website</li> </ul> </li> <li>● <b>Basic data analytics – reporting and industry health dashboard</b></li> <li>● <b>Enrich training and awareness programs</b> (training programs, webinars, industry forums, blogs and educational events)</li> </ul>
Phase-4 Exercise Educate	<ul style="list-style-type: none"> <li>● <b>Capability enrichment to enhance incident handling capability</b></li> <li>● <b>Incident handling drills plans</b></li> <li>● <b>Establish in collaboration with other institutions on providing certifications in area of cyber security</b></li> </ul>
Phase-5 Analyse Audit Respond	<ul style="list-style-type: none"> <li>● <b>Advanced data analytics</b></li> <li>● <b>Analyse the incidents (Malware)</b></li> <li>● <b>Conduct Forensic Audits</b></li> <li>● <b>Audit as Service</b> <ul style="list-style-type: none"> <li>○ Conduct VA-PT for RIs</li> <li>○ Conduct risk assessment including of of new financial products (to start with post launch evaluation)</li> <li>○ Conduct gap assessment with extant instructions – on need basis</li> </ul> </li> <li>● <b>Provide emergency response support</b></li> </ul>
Phase -6 Research Secure Benchmark	<ul style="list-style-type: none"> <li>● <b>Establish state of the art experimental hub for enabling “Regulatory sandbox” and lab for providing training on cyber security and related aspects (if required in collaboration with another entity) &amp; other relevant research aspects</b></li> <li>● <b>Work with various stakeholders to secure from extant cyber threats</b></li> <li>● <b>Establish a benchmark to rate the RIs</b></li> </ul>

**Minimum services that need to be offered by CERT-Fin**

<b>S.No. No.</b>	<b>Processes/ Services</b>	<b>Description</b>
1	Incident Handling	Defining processes for incident handling including but not limited to receiving, triaging, and responding to requests and reports, and analyzing incidents and events
2	Vulnerability Handling	Defining complete processes for vulnerability handling including receiving information and reports about hardware and software vulnerabilities, analyzing the nature, mechanics, and effects of the vulnerabilities, and developing response strategies for detecting and repairing the vulnerabilities. This should include scanning, assessment, and network mapping
3	Malware Handling	Defining processes for malware handling for managing any artifact that can be any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures
4	Threat Intelligence	Threat intelligence processes for aggregation of various threat feeds including feeds from other CERTs, OEM, Security Vendors, constituents, open source feeds, etc. This would include Collection, Analysis, Distribution, Creation, Fusion, Trending, and Assessment.
5	Security Operations Centre (SOC)	The process to include collection of logs and events from multiple sources, analyzing and correlating with internal and external infrastructure components and generating alerts providing insights of overall security posture. The various activities will include but not limited to – Real-time monitoring and triage/incident analysis, Border Protection Device operations and management, SOC Infrastructure operations and management, Sensor Tuning and Maintenance, Tool Deployment
6	Security Audits & Assessments	Detailed review and analysis of the critical constituent's security infrastructure, based on set standards need to be conducted on a regular basis. The review should include but not limited to Infrastructure Review, Best Practices Review, Scanning, Penetration Testing, Configuration and Maintenance of Security Tools, Applications and Infrastructures, development of security tools, intrusion detection services, etc.
7	Security Quality Management	Incorporate feedback and lessons learned based on knowledge gained by responding to incidents, vulnerabilities and attacks including Risk Analysis, Business Continuity Planning – Disaster Recovery, Awareness building, Security Awareness and Training, Product Evaluation and Certificate among others

8	CERT-Fin Portal	CERT-Fin Portal to include various provisions such as incident repository, Audit surveys, training content, reporting portal, weekly bulletins, advisories
9	Information Sharing	Enable information dissemination for other CERTs and coordination mechanism. This can be done through alerts and warnings on latest security threats
10	Security Standards	Defining sector or industry specific security standards which need to be followed to ensure security