Regulatory Technologies Information Security

Dr. Srinivas Josyula

IIM
भारतीय प्रबंध संस्थान विशाखापट्टनम
Indian Institute of Management Visakhapatnam
विद्या परं देवत्वम्

1

Course Outline

- Future of Banking
- Digital Transformation in Banking Sector
- Governance Risk and Compliance
- Reg Tech
- Digital Trust and Information/ Cyber Security

2

Agenda

- Background
- Regulations and Compliance
- Demystifying Reg Tech
- Global and Indian Context
- Reg Tech use cases
- Reg Tech Adoption
- Implementation Approach
- Issues and Challenges
- Way forward

3

Regulations and Compliance

4

Regulations …

Regulation is central to governmental management of complex system,.

Primary objectives of Banking Regulations include, ***ensuring financial stability, prudential safety and soundness, protecting consumers, maintaining market integrity, and fostering market competition and development***

Strengthening the regulations of the complex financial system, and early warning and disposal of risks are the requirements for achieving financial stability (Battiston et al., 2016).

Governments routinely use regulation ***to boost market efficiency, ensure accountability, support, coordination and minimize risks***.

5

5

GFC and Regulatory overhaul

- The 2007 global financial crisis prompted a comprehensive overhaul of the financial regulatory framework led by the Financial Stability Board (FSB) and the Basel Committee.
- Poor risk data collection and reporting practices within banks were identified as vulnerabilities and addressed in 2013 when the BCBS released its *Principles for Effective Risk Data Aggregation and Risk Reporting.*
- Risk Management has become a focus are for Banks and Regulators. The BCBS principles ***set minimum criteria for establishing IT infrastructure and data collection and administration***.
- Regulatory compliance costs at financial institutions have skyrocketed due to the increasingly complex global regulatory framework, reporting requirements, and the risk of costly penalties due to stringent post-crisis standards, particularly for internationally active banks.

6

6

Regulatory Announcements

Source : Thomson Reuters , June 2021,

7

7

Regulations and Compliance

Explosive Growth in Regulations: a 2021 report estimated that financial institutions had 220 regulation revisions to keep track of daily on average

High Compliance Costs: from 2009 to 2021, regulatory fines exceeded $ 345 billion globally. increasing financial burden substantially on companies.

Compliance Staff: About 10% to 15% of financial institutions staff worked on Governance, Risk and Compliance function .

8

8

FinTech, Reg Tech & Sup Tech

9

Fin Tech

"Technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services" (FSB, 2017)

Fintech activities: Crowdfunding, digital currencies, mobile banks, robo-advice, high-frequency trading, and algorithmic trading

The biggest FinTech activities are in the areas of payments, clearing and settlement services with a 41 % share (BIS, 2018).

10

10

Emergence of Fin Tech

The emergence of FinTech is attributable to:

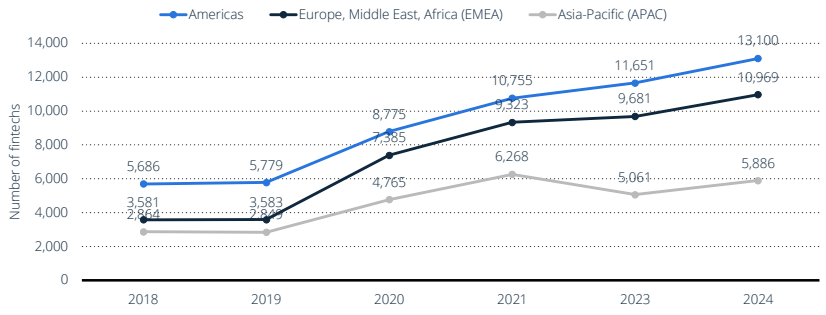
1. financial market deficiencies caused by the GFC and the regulatory response to it;
2. public distrust in the financial services industry, particularly in the United States and EU;
3. political pressure for alternative sources of finance for small and medium enterprises;
4. unemployed financial professionals looking to apply their talents; and
5. the commoditization of technology and the market penetration of the internet and mobile phones, particularly smart phones.

11

11

Number of fintechs worldwide from 2018 to 2024, by region

Number of fintechs worldwide 2018-2024, by region



Note(s): 2018 to 2024
Further information regarding this statistic can be found on page 8.
Source(s): BCG; CrunchBase; Statista; ID 893954

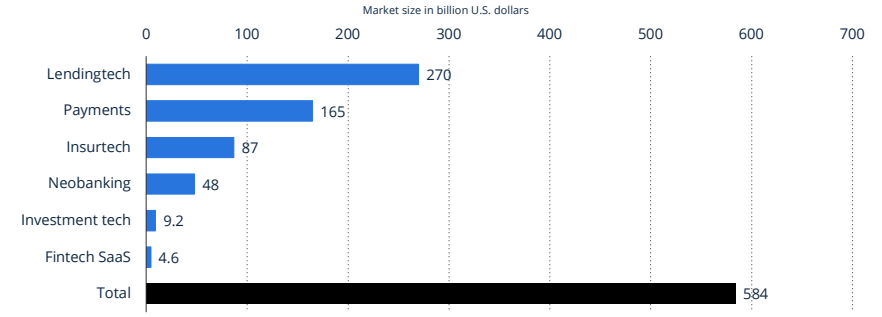
6

statista

12

Fintech market size in India in 2022, by segment (in billion U.S. dollars)

Fintech market size in India 2022, by segment

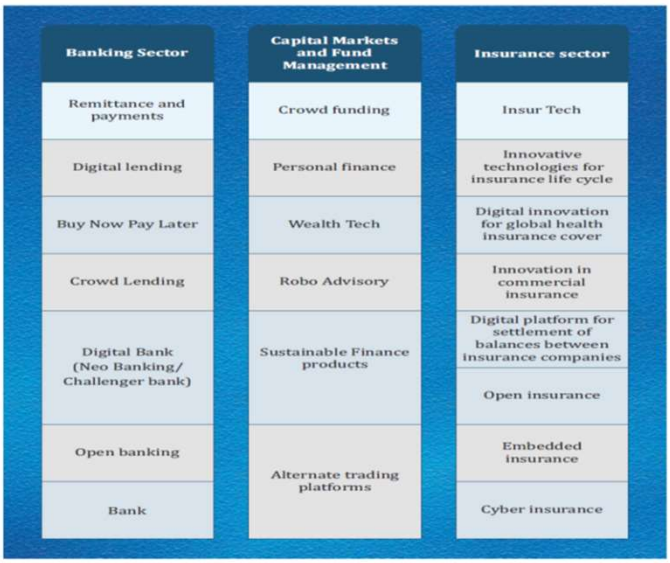


Description: The fintech market in India was valued at 584 billion U.S. dollars in 2022. Lendingtech sector accounted for 270 billion dollars of the total market size. Followed by insurtech with a market size of 165 billion dollars the same year. Read more
Note(s): India; 2022
Source(s): Inc42

statista

13

Fin tech focus Areas



14

14

Benefits and Risks …

FSB study highlighted benefits like:

- *Efficiency improvements, risk reduction and greater financial inclusion.*

And challenges like :

- *Difficulty of regulating an evolving technology with different use cases, monitoring activity outside the regulated sector, identifying and monitoring new risks arising from the technology*.

15

15

Reg Tech

FSB (2017) defines Reg Tech as "*any range of applications of FinTech for regulatory and compliance requirements and reporting by regulated financial institutions*."

FCA (2017) defines "Reg Tech is a sub - set of FinTech that focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities

Reg Tech describes the *use of technology in the context of regulatory monitoring, reporting, and compliance* (Arner, P.Buckley, & Barberis, 2019).

16

16

Emergence of Reg Tech

The emergence of Reg Tech is attributable to:

1. postcrisis regulatory changes requiring additional data disclosure from regulated entities;
2. developments in data science (for instance AI and deep learning);
3. Economic incentives for participants to minimize rapidly rising compliance costs; and
4. regulators' efforts to enhance the efficiency of supervisory tools to foster competition and uphold their mandates of financial stability and market integrity

17

17

Compliance Challenges …

The top 5 themes for Compliance Officers	The top five themes for the Board
• Volume and implementation of regulatory changes	• Balancing cost pressures
• Balancing budgets and resources	• Keeping up with regulatory change
• Retaining skilled resources	• Increased regulatory scrutiny
• Growing regulatory expectations	• Cyber risk
• Availability of skilled resources	• Retaining skilled resources

Source: Thomson Reuters, 2023

18

18

Sup Tech

- "Sup Tech (supervisory technology) is the use of technologically enabled innovation by supervisory authorities" (BIS, 2017)
- "Sup Tech is the use of Data Analytics, AI &ML by public sector regulators and supervisors."

19

19

SupTech Definition	Reference
"…harness technology to enhance the efficiency and effectiveness of supervision and surveillance."	Menon, Financial Regulation -the Forward Agenda (March 2017)
"…the use of new technologies for internal supervisory purposes." *"…the use of technologically enabled innovation by supervisory authorities."*	BIS, Basel Committee on Banking Supervision (August 2017) BIS, Basel Committee on Banking Supervision (February, 2018)
"Applications of FinTech by supervisory authorities." *"…the use of these technologies (AI/ML) by public sector regulators and supervisors."*	Financial Stability Board (November 2017)
"Technological solutions focused on improving the processes and effectiveness of financial supervision and regulation."	Dias & Staschen (CGAP, December 2017)
"…the use of technology to facilitate and enhance supervisory processes from the perspective of supervisory authorities".	Boeddu, Brix, Kachingwe, Lopes, & Randall (World Bank Group, June 2018)
"…the use of innovative technology by supervisory agencies to support supervision."	Dirk Broeders and Jermy Prenio (July 2018)
"…the use of innovative technology by financial authorities to support their work."	Castri, Hohl, Kulenkampff, & Prenio (October 2019)
"…the use of technology to carry out supervisory responsibilities."	Zeranski, S., & Sancak, I. E. (2020).

20

20

Objectives of Sup Tech

The objectives of Sup Tech are ***seamless and straight-through data collection / reporting, data analysis and decision making, streamlined licensing, market monitoring and surveillance, KYC / AML / CFT, cybersecurity data or evidence-based policy making*** (RBI, Keynote address by Governor, May 2019)

RBI Sup Tech Systems : Import Data Processing and Monitoring System (IDPMS), Export Data Processing and Monitoring System (EDPMS) and Central Repository of Information on Large Credits (CRILC)

21

21

Technologies deployed …

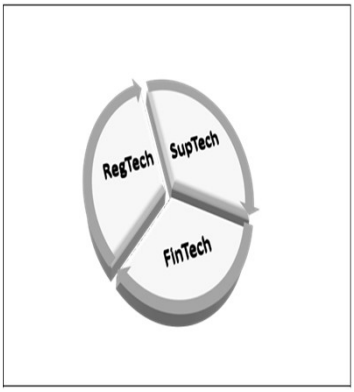
The technologies deployed in RegTech and SupTech include:

- Big data analytics,
- Artificial intelligence, Machine learning,
- Cloud computing,
- Geographic information system (GIS)
- API and data transfer protocols,
- Biometrics, etc.

22

22

Fin Tech, Reg Tech and Sup Tech - Conceptual Framework



- They have close connections, but each one needs different perspectives and approaches to produce sound policies.
- They all share "technology", but technological tools are used for various purposes in each area

Source: Zeranski, S., & Sancak, I. E. (2020). Digitalisation of financial supervision with supervisory technology (SupTech). *Journal of International Banking Law & Regulation*.

23

Reg Tech: As a tool to Manage Risks

24

Reg Tech

Reg Tech is defined as "*The application of various new technological solutions that assist highly regulated industry stakeholders, including regulators, in setting, effectuating and meeting regulatory governance, reporting, compliance and risk management obligations.*"

The goal of Reg Tech is to prioritize and improve the effectiveness of regulations and governance while reducing the risk and cost of compliance through modern technology.

~ WEF

25

25

Why Reg Tech ?

- The 21st century poses new challenges as regulatory systems struggle to keep up with the risks and opportunities of emerging technologies.
- It is important to recognize the challenges of balancing the need to innovate and the duty to protect and build trust among stakeholders.
- During the COVID-19 pandemic, economic conditions have required agile governance and technology deployment.
- Regulators and regulated industries have revealed a need for more agile and responsive regulation when faced with social, economic and political disruptions.
- Regulatory technologies support the shift from 'reactive' to 'dynamic' regulation – enabling regulatory formation and compliance to more effectively evolve with changing market dynamics.

26

26

Benefits of Reg Tech

- The global Reg Tech market stands at $ 8.7 billion in 2021, and it is forecasted to grow at a CAGR of 23% to reach USD 29.2 billion by 2027.
- Reg Tech use could provide upwards of 600% returns on investment with a payback horizon of fewer than three years.
- TRRI survey states that prominent Reg tech use cases are:
- Cyber resilience (20%),
- Compliance monitoring (16%),
- Financial crime/anti-money laundering/sanctions (14%), and
- Customer onboarding (14%)
- Others

27

27

Reg Tech - Success factors

Engagement with stakeholders

- PPP Model
- Champion led

Design

- Radical user centricity : transition from “regulate and forget” to “adapt and learn” era
- Dynamic : nurture experimentation, iteration and protyping via regulatory sand boxes.

Applications

- Human and Machine intelligence : Investment in AI, analytics and digitization

28

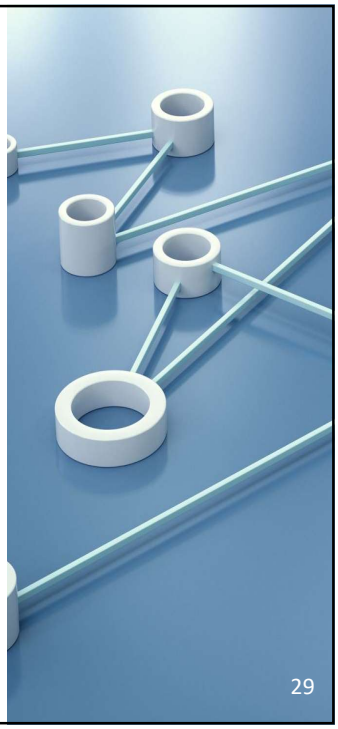
28

Reg Tech Categories

Reg Tech is still in a developing phase

Deloitte grouped Reg Tech into five sub categories

1. Regulatory Reporting
2. Risk Management
3. Identity Management and Control
4. Compliance
5. Transaction Monitoring



29

29

Reg Tech Focus Areas…

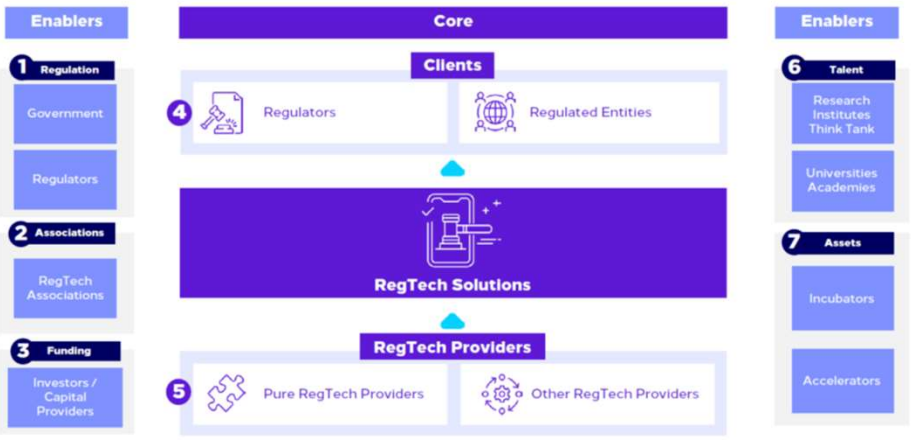
Consumer protection and market conduct
Data-driven financial system stability
Data collection and management
Detection and prevention of financial crimes
Remote supervision and reporting
Financial inclusion for disadvantaged groups and women

Reg-Tech's concept has been expanded to ***financial stability monitoring, including financial market risk early warning, digital financial risk identification, abnormal cross-border capital monitoring, anti-money laundering, monitoring, and many other fields*** (Kou, Chao, Peng, Alsaadi, & Herrera- Viedma, 2019; Souza, 2016; Zhou, 2013).

30

30

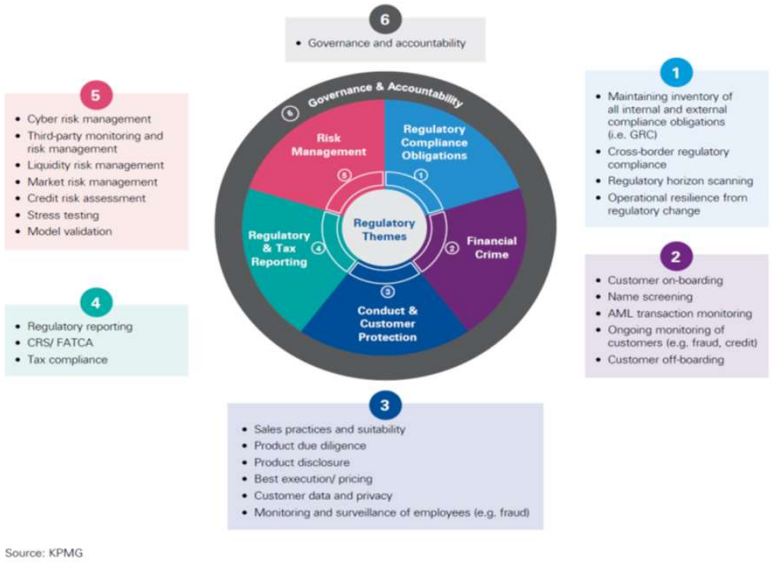
Reg Tech eco system



31

31

Reg Tech Application Areas



Source: KPMG

32

Reg Tech Implementation Approach

Foundations :

1. Leadership commitment and support
2. Governance
3. Capabilities and Skills

33

33

Adoption – Issues and Barriers
(indicative)

1. Leadership Support
2. Budget or resource constraints
3. Unattractive business case
4. Lack of available solutions/Available solutions do not meet needs
5. Lack of suitably skilled/experienced talent to develop and/or implement successfully
6. Complex legacy infrastructure
7. Reluctance/challenges around aligning decisions globally or regionally rather than locally
8. Lack of awareness of potential value of Regtech solutions
9. Data is not in a form that can be easily digitized
10. Policy Restrictions /Risk appetite

34

34

Global Reg Tech Adoption

Australian Securities and Investments Commission (ASIC) has taken a leading role in driving Regtech development and adoption within the sector.

The Singapore government and the Monetary Authority of Singapore (MAS) are actively collaborating with Singapore FinTech Association (SFA) to promote the use of Regtech solutions in Singapore.

MAS and the Financial Stability Board (FSB) supported the Saudi G20 Presidency and the Bank for International Settlements (BIS) Innovation Hub Singapore Centre in conducting the inaugural G20 Global Tech Sprint in 2020 s in the areas of Sup tech and Reg tech.

The Financial Conduct Authority (FCA) was an early supporter of and facilitate opportunities for the private sector to convene and overcome challenges.

35

35

Issues and Challenges

36

Regulatory landscape ….

- The Reserve Bank of India (RBI) is India's central bank. It manages credit supply, regulates bank operations, and helps maintain a healthy financial system.
- The Securities and Exchange Board of India (SEBI) is the regulatory authority responsible for overseeing the securities market in India.
- The Ministry of Corporate Affairs regulates the functioning of industrial and services sectors.
- National Housing Bank (NHB) is the apex regulatory body for the housing finance sector in India.
- Association of Mutual Funds in India (AMFI) is an industry association of mutual funds in India.
- IT Act
- Data Privacy Act

37

37

Reg Tech adoption in India

- The future of Reg Tech in India holds great promise.
- Indian banks operate in a regulatory environment characterized by a multitude of guidelines covering areas such as anti-money laundering (AML), know-your-customer (e- KYC), data privacy, and cybersecurity, IT Outsourcing, IT Governance, Compliance with these regulations is both a necessity and a challenge.
- Regulators are recognizing the potential of Reg Tech to enhance regulatory oversight.

38

38

Way forward…

1. **Investment in Reg Tech and Adoption** : Commitment to invest in and adopt Reg Tech solutions, Process Reengineering
2. **Encouraging the Growth of Reg Tech Startups** : Supporting startups with mentorship, funding, and regulatory assistance to foster a vibrant ecosystem.
3. **Investments and Funding for Startups :** Providing financial backing and resources to new Reg Tech ventures.
4. **Collaboration Between Regulators and Banks** : Promoting partnerships for seamless integration and innovation.
5. **Regulatory Recognition, Standardization, and Guidelines** : Establishing standards and guidelines to build confidence in adoption.
6. **Change Management Strategies** : Implementing effective change management to facilitate digital transformation and acceptance of automated compliance.
7. **Staff Education, Training, and Awareness** : Ensuring personnel are aware, trained and educated, about digital technologies and processes.
8. **Integrating with Legacy Technologies** :Addressing the challenges of integrating new solutions with existing legacy systems.

39

39

Thank You

40

40

IT Outsourcing

41

Outsourcing of IT Services

- Regulated Entities (REs) have been extensively leveraging Information Technology (IT) and IT enabled Services (ITeS) to support their business models, products and services offered to their customers.
- REs also outsource substantial portion of their IT activities to third parties, which expose them to various risks.
- In order to ensure effective management of attendant risks, the Statement on Developmental and Regulatory Policies dated February 10, 2022, proposed the issuance of suitable regulatory guidelines on Outsourcing of IT Services
- **Master Direction on Outsourcing of Information Technology Services:** RBI/2023-24/102 DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 dated April 10 2023
- The underlying principle of these Directions is to ensure that outsourcing arrangements neither diminish REs ability to fulfil its obligations to customers nor impede effective supervision by the RBI.

42

Outsourcing of IT Services Directions 2023.

- Chapter I: Preliminary
- Chapter II: Role of the Regulated Entity
- Chapter III: Governance Framework
- Chapter IV: Evaluation and Engagement of Service Providers
- Chapter V: Role of the Regulated Entity
- Chapter VI: Risk Management
- Chapter VII: Monitoring and Control of Outsourced Activities
- Chapter VIII: Outsourcing within a group/ Conglomerate
- Chapter IX: Cross Border Outsourcing
- Chapter X: Exit Strategy

43

Master Directions – Applicability

These Directions shall be applicable to the following entities, collectively referred to as 'regulated entities' or 'REs' in these directions:

i. All Banking Companies,

ii. Primary Co-operative Banks

iii. Non-Banking Financial Companies

iv. Credit Information Companies

v. EXIM Bank, NABARD, NaBFID, NHB and SIDBI respectively (hereinafter referred to as 'All India Financial Institutions or 'AIFIs').

- These Directions shall apply to Material Outsourcing of Information Technology ('IT') Services arrangements entered by the REs.

"Material Outsourcing of IT Services" are those which:

a) if disrupted or compromised shall have the potential to significantly impact the RE's business operations; or

b) may have material impact on the RE's customers in the event of any unauthorised access, loss or theft of customer information.

44

IT Services include ….

"Outsourcing of IT Services" shall include outsourcing of the following activities:

a) IT infrastructure management, maintenance and support (hardware, software or firmware);

b) Network and security solutions, maintenance (hardware, software or firmware);

c) Application Development, Maintenance and Testing; Application Service Providers (ASPs) including ATM Switch ASPs;

d) Services and operations related to Data Centers;

e) Cloud Computing Services;

f) Managed Security Services; and

g) Management of IT infrastructure and technology services associated with payment system ecosystem.

45

Comprehensive assessment

- REs shall evaluate the need for Outsourcing of IT Services based on comprehensive assessment of attendant benefits, risks and availability of commensurate processes to manage those risks.

- REs shall inter-alia consider:

a) determining the need for outsourcing based on criticality of activity to be outsourced;
b) determining expectations and outcome from outsourcing;
c) determining success factors and cost-benefit analysis; and
d) deciding the model for outsourcing.

- The RE shall consider all relevant laws, regulations, rules, guidelines and conditions of approval, licensing or registration, when performing its due diligence in relation to outsourcing of IT services.

46

Role of IT function in Governance

The responsibilities of the IT Function of the RE shall, inter alia, include:

a. Assisting the Senior Management in identifying, measuring, monitoring, mitigating and managing the level of IT outsourcing risk in the organisation;

a. ensuring that a central database of all IT outsourcing arrangements is maintained and is accessible for review by Board, Senior Management, Auditors and Supervisors;

b. effectively monitor and supervise the outsourced activity to ensure that the service providers meet the laid down performance standards and provide uninterrupted services, report to the Senior Management; co-ordinate periodic due diligence and highlight concerns, if any; and

c. putting in place necessary documentation required for contractual agreements including service level management, monitoring of vendor operations, key risk indicators and classifying the vendors as per the determined risk.

47

Due Diligence

- Due diligence shall take into consideration qualitative, quantitative, financial, operational, legal and reputational factors.
- Where possible, the RE shall obtain independent reviews and market feedback on the service provider to supplement its own assessment.
- REs shall also consider, while evaluating the capability of the service provider, risks arising from concentration of outsourcing arrangements with a single or a few service provider/s.

48

IV- Vendor Due Diligence .. considerations

Due diligence shall involve evaluation of all available information, as applicable, about the service provider, including but not limited to:

a. past experience and demonstrated competence to implement and support the proposed IT activity over the contract period;
b. financial soundness and ability to service commitments even under adverse conditions;
c. business reputation and culture, compliance, complaints and outstanding or potential litigations;
d. conflict of interest, if any;
e. external factors like political, economic, social and legal environment of the jurisdiction in which the service provider operates and other events that may impact data security and service performance;
f. details of the technology, infrastructure stability, security and internal control, audit coverage, reporting and monitoring procedures, data backup arrangements, business continuity management and disaster recovery plan;

49

IV- Vendor Due Diligence contd.. considerations

a. capability to identify and segregate REs data;
b. quality of due diligence exercised by the service provider with respect to its employees and sub-contractors;
c. capability to comply with the regulatory and legal requirements of the Outsourcing of IT Services arrangement;
d. information/ cyber security risk assessment;
e. ensuring that appropriate controls, assurance requirements and possible contractual arrangements are in place to ensure data protection and RE's access to the data which is processed, managed or stored by the service provider;
f. ability to effectively service all the customers while maintaining confidentiality, especially where a service provider has exposure to multiple entities; and
g. ability to enforce agreements and the rights available thereunder including those relating to aspects such as data storage, data protection and confidentiality.

50

BCP and DRP

a. REs shall require their service providers to develop and establish a robust framework for documenting, maintaining and testing Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) commensurate with the nature and scope of the outsourced activity as per extant instructions issued by RBI from time to time on BCP/ DR requirements.

b. In establishing a viable contingency plan, REs shall consider the availability of alternative service providers or the possibility of bringing the outsourced activity back in-house in an emergency, and the costs, time and resources that would be involved.

c. In order to mitigate the risk of unexpected termination of the outsourcing agreement or insolvency/ liquidation of the service provider, REs shall retain an appropriate level of control over their IT-outsourcing arrangement along with right to intervene, with appropriate measures to continue its business operations.

d. REs shall ensure that service providers are able to isolate the REs' information, documents and records and other assets. This is to ensure that, in adverse conditions or termination of the contract, all documents, record of transactions and information with the service provider and assets of the RE can be removed from the possession of the service provider, or deleted, destroyed or rendered unusable

51

IT GRCA guidelines

52

RBI - IT Governance, Risk, Controls and Assurance Practices

- (Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023.

Adobe Acrobat Document

53

AML – RBI

54

Money Laundering

- Money laundering involves taking criminal proceeds and disguising their illegal sources in order to use the funds to perform legal or illegal activities. Simply put, money laundering is the process of making dirty money look clean.
- Money Laundering is the process of converting the tainted property (referred to as Proceeds of Crime - POC) acquired/obtained by carrying out specific offences (referred to as "scheduled offences" or "predicate offences") as described in the Schedules under the **Prevention of Money Laundering Act 2002**, into the untainted property.
- All or Any acts, directly or indirectly related to such proceeds of crime such as ***concealment, possession, acquisition, use, projecting or claiming it as untainted property is treated as an act of Money Laundering Offences.***
- The offense of money laundering involves knowingly engaging in financial transactions that conceal, possess, acquire, use or disguise the origins of illicitly obtained funds. It typically involves three stages:

  i. **Placement** (introducing illicit funds into the financial system),
  ii. **Layering** (conducting complex transactions to obscure the audit trail),
  iii. **Integration** (legitimizing the illicit funds by integrating them back into the formal economy).

55

RE Obligations and data to be collected

Every RE must carry out its obligations as stated in Chapter IV (Sec. 11-A to 15) of the PMLA Act 2002 read with the PML (Maintenance of records) Rules 2005. This requires RE:

- **To verify the identity of its clients along with the beneficial owner.**
- **To maintain such records and for such period as prescribed**
- **To carry out enhanced due diligence**
- **To report to the concerned authorities (FIU)** – As per the prescribed Procedure and manner

Further as per the PML Rules, the RE must maintain records in terms of

- **Value and nature especially Cash Transaction Reports (CTR),**
- **Suspicious Transaction Reports (STR),**
- **Certain transactions by NPO,**
- **Cash Transactions where forged/counterfeit currency were used,**
- **Cross Border as well as Domestic wire Transfer of certain values & Purchase/sale of immovable property above certain values.**
- This is the critical reporting to be done by the RE as on date.
- RE need to undertake ***client due diligence and what documents are needed and other things***

56

RE Obligations and data to be collected

- Section 11A of the PMLA places *KYC obligations upon 'every' reporting entity* while Section 12AA provides for *"**enhanced due diligence" by 'every' reporting entity prior to the commencement of each specified transaction.***
- *Maintain a record of all transactions (five years from the date of the transaction), including information relating to transactions covered under clauses, in such manner as to enable it to reconstruct individual transactions*
- *Furnish to the Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed;*
- *Maintain a record of documents* (five years after the business relationship between a client and the reporting entity has ended or the account has been closed, whichever is later) evidencing the identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.

57

KYC Norms

58

KYC guidelines by RBI

- Banks and financial institutions (FIs) have been advised to follow certain customer identification procedure for opening of accounts and monitor transactions of suspicious nature for the purpose of reporting the same to appropriate authority.
- These 'Know Your Customer' (KYC) guidelines have been revisited in the context of the recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT).
- Detailed guidelines based on the recommendations of FATF and the paper issued on **Customer Due Diligence** (CDD) for banks by the Basel Committee on Banking Supervision (BCBS), with suggestions wherever considered necessary, have been issued.
- Banks/FIs have been advised to ensure that a proper policy framework on 'Know Your Customer' and Anti-Money Laundering measures is formulated and put in place with the approval of their Boards.

59

KYC

- KYC is an acronym for "**Know your Customer**" a term used for Customer identification process.
- It *involves making reasonable efforts to determine, the true identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business*,etc which in turn helps the banks to manage their risks prudently.
- The objective of KYC/AML/CFT guidelines is to prevent banks/FIs from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.
- KYC procedures also enable banks/FIs to know/understand their customers and their financial dealings better and manage their risks prudently.

60

KYC Policy

- KYC is an acronym for "**Know your Customer**" a term used for Customer identification process.
- It *involves making reasonable efforts to determine, the true identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business*,vetc which in turn helps the banks to manage their risks prudently.
- The **objective of the KYC guidelines is to prevent banks being used, intentionally or unintentionally by criminal elements for money laundering**.

As per RBI guidelines issued vide their circular dated July 2015 , all banks are required to formulate a KYC Policy with the approval of their respective boards.

The KYC Policy consists of the following four key elements.

1) Customer Acceptance Policy
2) Customer Identification Procedures
3) Monitoring of Transactions
4) Risk Management

61

KYC Policy

62

Regulatory Sand Box

63

Regulatory Sandbox

- To enable regulated and orderly growth of FinTech ecosystem in India, the Reserve Bank in August 2019 became one of the few countries that have their very own **Regulatory Sandbox** (RS) ecosystem.
- Regulatory Sandbox usually refers to live testing of new products or services in a controlled/test regulatory environment for which regulators may (or may not) permit certain regulatory relaxations for the limited purpose of the testing.
- The RS allows the regulator, the innovators, the financial service providers (as potential deployers of the technology) and the customers (as final users) to conduct field tests to collect evidence on the benefits and risks of new financial innovations, while carefully monitoring and containing their risks.
- It can provide a structured avenue for the regulator to engage with the ecosystem and to develop innovation-enabling or innovation-responsive regulations that facilitate delivery of relevant, low-cost financial products.
- Within the sandbox, **the eligible entities can live test their innovative products or services in a controlled environment.**
- The RS is an important tool which enables more dynamic, evidence-based regulatory environments which learn from, and evolve with, emerging technologies.

64

64

Regulatory Sandbox

I. The RS is based on thematic cohorts. The themes of the various cohorts under RS are as given below:

I. **Retail Payments**

II. Cross Border Payments

III. MSME Lending

IV. Prevention and Mitigation of Financial Frauds

V. Theme Neutral – Here innovative products/ services/ technologies cutting across various functions in RBI's regulatory domain would be eligible to apply.

Further to ensure continuous innovation in the closed themes, the RS also accepts 'On Tap' applications for the closed themes.

At present, themes of first two cohorts (viz. Retail Payments and Cross Border Payments) are open for 'On Tap' applications.

65

65

Governance

- Governance means administering the processes and systems placed for satisfying stakeholder expectations.
- Corporate Governance means *a set of systems, procedures, policies, practices, standards put in place by a corporate* to ensure that relationship with various stakeholders is maintained in transparent and honest manner.
- The phrase "corporate governance" describes *"the framework of rules, relationships, systems and processes within and by which authority is exercised and controlled within corporations. It encompasses the mechanisms by which companies, and those in control, are held to account."*
- "Corporate Governance is the application of best management practices, compliance of law in true letter and spirit and adherence to ethical standards for effective management and distribution of wealth and discharge of social responsibility for sustainable development of all stakeholders." (ICSI)

66

Thank You

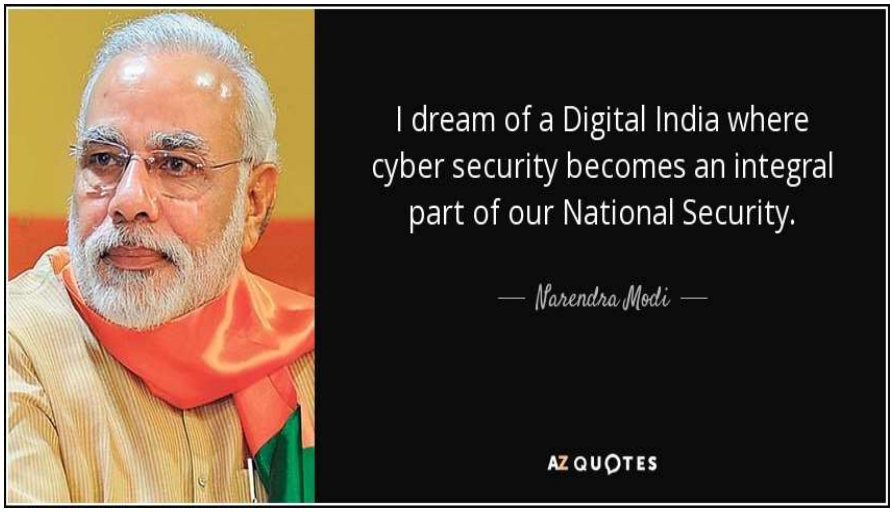
67

Cyber Security, IT Act, NCSP

Dr. Srinivas Josyula

IIM
भारतीय प्रबंध संस्थान विशाखापत्तनम
Indian Institute of Management Visakhapatnam
विद्या परं वैदत्म्

68



69

Therefore, I say:

One who knows the enemy and knows himself will not be in danger in a hundred battles.

One who does not know the enemy but knows himself will sometimes win, sometimes lose

One who does not know the enemy and does not know himself will be in danger in every battle

~ Sun Tzu

"It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it."

"Cyber-Security is much more than a matter of IT."

~ Stephane Nappo.

Global Head Information Security
Société Générale International Banking

70

70

Zero Trust Framework

- ***Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data***
- *Zero Trust is a go to framework for securing infrastructure and data for today's modern digitally transforming Banks .*
- *Zero Trust is a significant departure from traditional security which followed the "trust but verify" method."*

71

India ranks among top 10 in ITU's Global Cybersecurity Index-2020, Released on 29 June 2021

- The Global Cybersecurity Index (GCI) is a trusted reference that measures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue.
- As cybersecurity has a broad field of application, cutting across many industries and various sectors, each country's level of development or engagement is assessed along five pillars –
- (i) Legal Measures,
- (ii) Technical Measures,
- (iii) Organizational Measures,
- (iv) Capacity Development, and
- (v) Cooperation – and then aggregated into an overall score.

https://cybersecureindia.in/india-ranks-among-top-10-itus-global-cybersecurity-index-2020/

72

Digital Trust

Digital trust is individuals' expectation that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values.

~ WEF

73

Goals

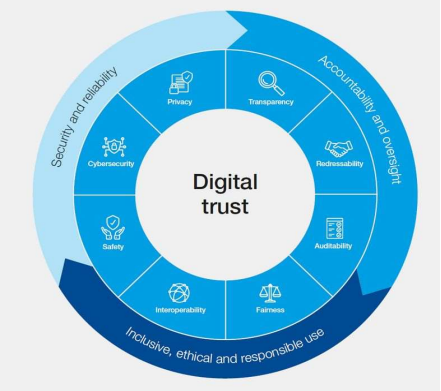
The digital trust framework defines shared goals or values that inform the concept of digital trust, including:

- Security and reliability
- Accountability and oversight
- Inclusive, ethical and responsible use

74

Digital Trust Framework

The digital trust framework defines shared goals or values that inform the concept of digital trust, as well as dimensions against which the trustworthiness of digital technologies can be operationalized and evaluated.



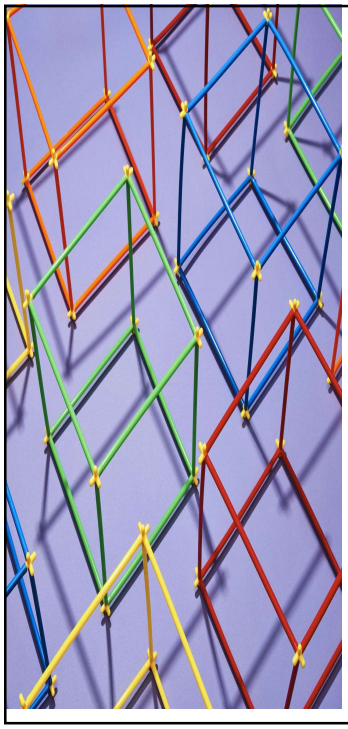
75

75

- Security and reliability
- organization's technology and data are well-protected against internal and external attacks, manipulations and interruptions while operating as designed according to a clearly defined set of parameters.

76

76



Digital Trust Dimensions

Dimensions : are the aspect of digital trust over which organizational decision-makers, such as CEOs and senior executives, have control and, if applied to a given technology with a human-centric approach, will promote digital trustworthiness.

- Cybersecurity
- Safety
- Transparency
- Interoperability
- Auditability
- Redressability
- Fairness
- Privacy

77

Cyber space

"A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

- NIST

78

Defining Cyber Security

- **Cyber security** is the ability to protect or defend the use of cyberspace from cyber attacks, damage, misuse, and economic espionage.
- **Cyber security** is all about the security of anything in the cyber realm.
- **Information security** is all about the security of information regardless of the realm.
- **Cyber security** refers to the protection of Internet-connected systems, such as hardware, software as well as data (information) from cyber attacks (adversaries).

79

Information Systems / Security?

- An Information System (IS) can be any ***organized combination of people, hardware, software, communications networks, data resources, and policies and procedures that stores, retrieves, transforms, and disseminates information in an organization***

- In general, ***security means being free from danger***. To be secure is ***to be protected from the risk of loss, damage, unwanted modification, or other hazards.***

80

Critical Infrastructure

Information Infrastructure is the term used to describe the totality of interconnected computers and networks, and information flowing through them.

Critical Information Infrastructure is defined as: ***"The computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety."***

~ Section 70 of IT Act 2000

NCIIPC has broadly identified the following as 'Critical Sectors' :-

- Power & Energy
- **Banking, Financial Services & Insurance**
- Telecom
- Transport
- Government
- Strategic & Public Enterprises

81

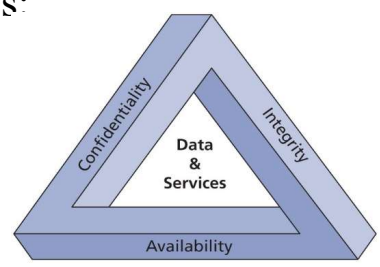
81

Components of an Information System

Information System (IS) is entire set of Software, Hardware, Data, People, Policies/Procedures, and networks necessary to use information as a resource in the organization

The value of information comes from the characteristics it possesses:

- Confidentiality
- Integrity
- Availability



82

82

Information Security - Objectives

For most computer users, the **security objective** is met when:

1. Information is accessible to, or disclosed to only those who have a right to know (**Confidentiality)**
2. Information is protected against unauthorized modification or error so that accuracy, completeness and validity are maintained (**Integrity)**
3. Information systems are available and usable when required, and can appropriately resist attacks and recover from failures (**Availability**)
4. Business transactions and information exchanges between enterprises, customers, suppliers, partners and regulators can be trusted (**Authenticity and Non-Repudiation)**

83

83

Information Security

Other principles include:

- **Authentication:** is a mechanism by which the identity of a user is verified. (Based on the number of factors used in authentication, it is termed a single-factor, two-factor, or multi-factor scheme.)
- **Non-repudiation:** refers to the assurance that a communicating party in the system cannot deny something.
- **Accountability:** "the access control mechanism that ensures all actions on a system—authorized or unauthorized—can be attributed to an authenticated identity. Also known as auditability"

84

Confidentiality

- Confidentiality is "**an attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems**"
- To protect the confidentiality of information, a number of measures are used:
  - Information classification
  - Secure document (and data) storage
  - Application of general security policies
  - Education of information custodians and end users
  - Cryptography (encryption)

85

Integrity

- Integrity is "**an attribute of information that describes how data is whole, complete, and uncorrupted**"
- The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state
- Integrity is the principle that information should be protected from intentional, unauthorized, or accidental changes. *Information stored in files, databases, systems, and networks must be relied upon to accurately process transactions and provide accurate information for business decision making.*

86

Availability

- Availability is "**an attribute of information that describes how data is accessible and correctly formatted for use without interference or obstruction**"
- Availability is the principle that ensures that information is available and accessible to users when needed.
- The two primary areas affecting the availability of systems are
  - Denial-of-Service attacks (DoS attack)
  - Loss of service due to a disaster, which could be man-made (e.g., poor capacity planning resulting in a system crash, outdated hardware, and poor testing resulting in system crash after upgrade) or natural (e.g., earthquake, tornado, blackout, hurricane, fire, and flood).

87

Privacy

- Privacy is, **"in the context of information security, the right of individuals or groups to protect themselves and their information from unauthorized access, providing confidentiality"**
- Information that is collected, used, and stored by an organization is to be used only for the purposes stated by the data owner at the time it was collected.

88

Identification

- Identification is **"the access control mechanism whereby unverified entities who seek access to a resource provide a label by which they are known to the system"**
- An information system possesses the characteristic of identification when it is able to recognize individual users
- **Identification and authentication are essential to establishing the level of access or authorization that an individual is granted**
- Identification is typically performed by means of a user name or other ID

89

Authentication

- Authentication is **"the access control mechanism that requires the validation and verification of an unauthenticated entity's purported identity"**
- It is the process by which a control establishes whether a user (or system) has the identity it claims to have.
- Individual users may disclose a personal identification number (PIN), a password, or a passphrase to authenticate their identities to a computer system

90

Authorization

- Authorization is **"the access control mechanism that represents the matching of an authenticated entity to a list of information assets and corresponding access levels"**
- After the identity of a user is authenticated, authorization defines what the user (whether a person or a computer) has been specifically and explicitly permitted by the proper authority to do, such as access, modify, or delete the contents of an information asset

91

Accountability

- Accountability is **"the access control mechanism that ensures all actions on a system—authorized or unauthorized—can be attributed to an authenticated identity. Also known as auditability"**
- Accountability of information occurs when a control provides assurance that every activity undertaken can be attributed to a named person or automated process
- Accountability is most commonly associated with system audit logs

92

Ethics and Education

- ***Employees must be trained and kept up-to-date on InfoSec topics, including the expected behaviors of an ethical employee.***
- Proper ***ethical and legal education, training and awareness are vital to creating an informed, well-prepared, and low-risk system user***.

93

Deter Unethical and Illegal Behaviour

- It is the responsibility of InfoSec personnel to deter unethical and illegal acts, ***using policy, education and training, and technology as controls or safeguards, in order to protect the organization's information and systems.***
- There are three general categories of unethical behavior that organizations and society should seek to eliminate:
  1. Ignorance
  2. Accident
  3. Intent

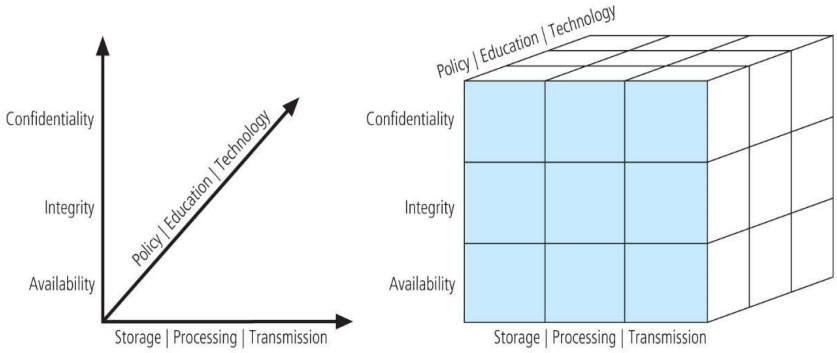
94

Functions of Information Security

- The unique functions of information security management are known as the **six Ps**:
  1. Planning
  2. Policy
  3. Programs
  4. Protection
  5. People
  6. Project management

95

CNSS Security Model



Source:
Management of Information Security: (6th Edition) by Michael E Whitman and Herbert J Mattord, Cengage Learning, USA , 2018

96

Areas of Security

Specialized areas of security include:

1. **Physical security:** protection of physical items, objects, or areas from unauthorized access and misuse
2. **Operations security:** protection of details of an organization's operations and activities
3. **Communications security:** protection of all communications media, technology, and content
4. **Cyber (or computer) security**: protection of information processing systems and the data they contain and process
5. **Network security**: a subset of communications and cyber security, the protection of voice and data networking components and connections.

97

Knowing Yourself and Knowing the Enemy

- When operating any kind of organization, a certain amount of risk is always involved.
- For an organization *to* ***manage risk properly, managers should understand how information is collected, processed, stored, and transmitted*** **.**
- Knowing yourself in this context requires ***identifying which information assets are valuable to the organization, categorizing and classifying those assets, and understanding how they are currently being protected.***
- Knowing the enemy means ***identifying, examining, and understanding the threats facing the organization's information assets***

98

Key Concepts of Information Security: Threats and Attacks

- A threat represents - a *potential* risk to an information asset, whereas an attack (or threat event) represents an ongoing act against the asset that could result in a loss.
- Threat agents damage or steal an organization's information or physical assets by using exploits to take advantage of a vulnerability where controls are not present or no longer effective
- **Attack:** "an intentional or unintentional act that can damage or otherwise compromise information and the systems that support it"
- **Exploit:** "a technique used to compromise a system… Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain"
- **Vulnerability:** "a potential weakness in an asset or its defensive control system(s)"

99

IT-related Business Risk

100

100

Assets Inventory and Documentation

Update to reflect items currently in use when implementing changes or updates

Common requirement in regulations, standards and agreements relating to privacy

Data/information assets

- System(s)
- Source
- Acquisition method
- Business use
- Business criticality
- Availability
- Completeness
- Processing
- Storage
- Transmission
- Sensitivity
- Classification
- Business owner

Hardware Assets

- Equipment
- Supplier
- Acquisition date
- Original cost
- Actual cost
- Location
- Equipment owner
- Maintenance details
- Insurance and warranty data

101

101

Threats Assessment

- Armed with a properly classified inventory, *you can assess potential weaknesses in each information asset - a process known as threat assessment.*
- Any organization typically faces a wide variety of threats; if you assume that every threat can and will attack every information asset, then the project scope becomes too complex.

102

102

Vulnerability Analysis

Vulnerabilities are weaknesses, gaps in an enterprise's people, processes or technologies that provide an opportunity for a threat actor to exploit, creating consequences that may impact the enterprise.

Many vulnerabilities are system conditions that must be identified to be addressed. The purpose of vulnerability identification is to find problems before an adversary finds and exploits them. An enterprise should conduct regular vulnerability assessments and penetration tests to identify, validate and classify its vulnerabilities. Where vulnerabilities exist, there is a potential for risk.

NIST Special Publication 800-30 Revision 1: Guide to Conducting Risk Assessments provides a list of vulnerabilities to consider with predisposing conditions that may lead to the rapid or unpredictable emergence of new vulnerabilities.

103

103

Sources of Vulnerabilities

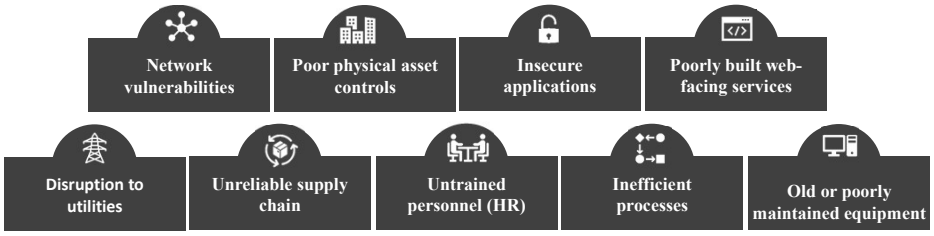
Network:	Misconfiguration of equipment, poor architecture or traffic interception protocols
Physical Access	Allows attackers to potentially bypass other types of controls
Apps/Web Services	Supports business function without due regard to security requirements
Utilities	Power failure or environmental conditions leading to system failure
Supply Chain	Reliance on products, raw materials and supplies from other locations
Equipment	Expectations, goals and objectives of programs and projects
Cloud Computing	Limited view on outsourced enterprise Data centers are large, visible targets
Big Data	Analyze structured and unstructured data for better business decisions

104

104

Vulnerabilities Assessment

- A process of identifying and classifying vulnerabilities
- Provides a careful examination of a target environment to discover any potential points of compromise or weakness



105

Policy

- Policy is the essential foundation of an effective information security program:
  - *The success of an information resources protection program depends on the policy generated, and on the attitude of management toward securing the information on automated systems*
  - ***Your primary responsibility is to set the information resource security policy for the organization with the objectives of reduced risk, compliance with laws and regulations and assurance of operational continuity, information integrity, and confidentiality***

(NIST, 1989)

106

Policies, Standards, Guidelines, Procedures, and practices

- **Policy** is a set of "*organizational guidelines that dictate certain behavior within the organization*"
- A **standard** is "*a detailed statement of what must be done to comply with policy, sometimes viewed as the rules governing policy compliance*"
- **Guidelines** are "*nonmandatory recommendations the employee may use as a reference in complying with a policy*"
- **Procedures** are "*step-by-step instructions designed to assist employees in following policies, standards, and guidelines*"
- **Practices** are "*examples of actions that illustrate compliance with policies*"
- **Policies define *what* you can do and not do, whereas the other documents focus on the *how***

107

Policy Centric Decision Making

- Bull's-eye model layers:
  - Policies—first layer of defense
  - Networks—threats first meet the organization's network
  - Systems—computers and manufacturing systems
  - Applications—all applications systems

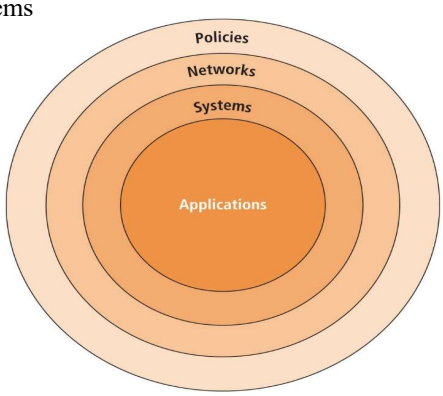


Figure 4-2 Bull's-eye model

Source:
Management of Information Security: (6th Edition) by Michael E Whitman and Herbert J Mattord, Cengage Learning, USA , 2018

108

Common Types of Fraud

- **Social engineering :**

Fraudsters will use a range of techniques to trick you into sharing banking information or transferring money – usually over the phone, by text message or email. Often criminals use more than one approach to build a level of trust. These tactics are known as social engineering.

E.g., Resist pressure, Beware of emotion, Check who you're talking to, Be suspicious of saviors, Don't divulge information

- **Invoice fraud :**

CEO frauds, Mandate frauds, SIM Swap frauds

https://www.cafonline.org/about-us/security-centre/be-aware---current-threats

https://www.ncsc.gov.uk/guidance/WannaCry-guidance-for-home-users-and-small-businesses

109

Common Types of Fraud

- **Malware and spyware :**

Malicious software, or malware, is software code or virus designed to disrupt the normal working of computer systems or mobile devices. Any exchange of data, such as opening an infected email attachment, visiting a malware-hosting website, or importing the content of a USB stick, carries the risk of transferring malware into an organization's systems and services.

Malware can be used by fraudsters to capture information from systems, PCs, laptops or portable devices, or to read data entered onto them such as passwords and log-on details.

Other names for malware include *viruses, worms, trojan horses, spyware and ransomware.*

Ransomware refers to a particular use of malware, in which a fraudster threatens to make public the victim's seized data or block access to it, unless a ransom is paid.

https://www.cafonline.org/about-us/security-centre/be-aware---current-threats
https://www.ncsc.gov.uk/guidance/WannaCry-guidance-for-home-users-and-small-businesses

110

Common Types of Fraud

Phishing :

Phishing is a technique of fraudulently obtaining private information like login ID and Password, Debit / Credit Card details, PIN, Date of Birth, and Mobile Number etc. This is one of the most common type of social engineering attack. Most Phishing scams endeavour to:

- Obtain personal information such as names, bank account details (User ID, Password, OTP), PAN, Aadhaar etc. by using the shortened or misleading link.
- Incorporate threats, fear, and a sense of urgency with phishing message/ email to manipulate the user into responding quickly.

Vishing

Vishing is the voice form of Phishing where frauds take place over phone calls. It is an act of using the telephone to trick the user into surrendering private information that will be used for fraudulent purposes. The scammer usually pretends to be from a legitimate entity and tries to befool the victim by luring or threatening him.

Smishing

Smishing uses cell phone text messages to lure users in a similar fashion like Phishing. They take the form of text messages that claim to be from legitimate entities and are often used in combination with other techniques to bypass inbuilt protections. They might also direct victims to malicious websites on their phones.

111

Espionage / Trespass

- Password attacks fall under the category of espionage or trespass.
- Attempting to guess or reverse-calculate a password is often called cracking.
- There are alternative approaches to password cracking:
  - Brute force attack :
  - Dictionary password attack
  - Social engineering password attack etc

112

Forces of Nature

Some typical force of nature attacks include the following:

- Fire
- Flood
- Earthquake
- Lightning
- Landslide or mudslide
- Tornados or severe windstorms
- Hurricanes, typhoons, and tropical depressions
- Tsunami
- Electrostatic discharge (ESD)
- Dust contamination
- Epidemics/ Pandemics

113

Human Errors / Failure

- This category includes acts performed without intent or malicious purpose or in ignorance by an authorized user.
- When people use information systems, mistakes happen; similar errors happen when people fail to follow established policy.
- Inexperience, improper training, and incorrect assumptions are just a few things that can cause human error or failure.
- *One of the greatest threats to an organization's information security is its own employees, as they are the threat agents closest to the information.*
- **Human error or failure often can be prevented with training, ongoing awareness activities, and controls**

114

Sabotage / Vandalism

- This category of threat involves the deliberate sabotage of a computer system or business or acts of vandalism to destroy an asset or damage the image of an organization.
- These acts can range from petty vandalism by employees to organized sabotage against an organization.
- Vandalism to a Web site can erode consumer confidence, diminishing an organization's sales, net worth, and reputation
- Activism in the digital age:
  - Online activism
  - Cyberterrorism and cyberwarfare
  - Positive online activism

115

Software Attacks

- Deliberate software attacks occur when an individual or a group designs and deploys software to attack a system.
- This software can be used to overwhelm the processing capabilities of online systems or to gain access to protected systems by hidden means
  - ***Malware—viruses, worms, Trojan horses, polymorphic threats and hoaxes***
  - ***Back doors, and maintenance hooks***
  - ***Denial-of-service (DoS) and distributed denial-of-service attacks (DDoS)***
  - ***E-mail attacks- spam,***
  - ***Communications interception attacks***

116

Mandates and Guidelines

- IT Act
- National Cyber Security Policy
- NCIIPC guidelines and Controls
- RBI guidelines and advisories (2016)
- Cyber / Ransomware attacks gaining attention

117

117

118

Cyber Laws in India

- Need for cyber law
- Information Technology Act, 2000
- Other laws amended by the IT Act, 2000
- Penalties and offences under the IT Act, 2000

119

The Information Technology Act, 2000 is the second technology related legislation in India.

The first one was the Indian Telegraph Act, 1885.

IT Act, 2000 was enacted on 17th May 2000 and India is 12th nation in the world to adopt cyber laws.

THE INFORMATION TECHNOLOGY ACT 2000 continues to be the ***omnibus legislation that governs cyber security policy in the country, and it includes provisions for digital signatures, e-governance, e-commerce, data protection, cyber offences, critical information infrastructure, interception and monitoring, blocking of websites and cyber terrorism. Rules under the Act are issued from time to time.***

IT Act , 2008: Information Technology (Amendment) Act, 2008 which has brought marked changes in the IT Act, 2000 on several counts was made effective from 27 October 2009.

120

Objectives

To provide legal recognition for transactions :- Carried out by means of electronic data interchange, and other means of electronic communication, commonly referred to as "electronic commerce".

To facilitate electronic filing of documents with Government agencies and

To amend the:

- Indian Penal Code, 1860
- Indian Evidence Act,1872
- The Banker's Books Evidence Act 1891
- Reserve Bank of India Act,1934 and for matters connected therewith or incidental thereto.
- Companies Act

121

Objectives of IT Act 2000

a) To give legal recognition to any transaction which is done by electronic way or use of internet?
b) To give legal recognition to digital signature for accepting any agreement via computer.
c) To provide facility of filling documents online
d) According to I.T. Act 2000, any company can store their data in electronic storage.
e) To stop computer crime and protect privacy of internet users.
f) To give more power to IPC, RBI and Indian Evidence act for restricting electronic crime.
g) To give legal recognition for keeping books of accounts by bankers and other companies in electronic form.

122

Notable features of the ITAA 2008

a) *Focusing on Data privacy*

b) *Focusing on Information Security*

c) *Making digital signature technology neutral*

d) *Defining reasonable security practices to be followed by corporate*

e) *Redefining the role of intermediaries*

f) *Recognizing the role of Indian Computer Emergency Response Team*

g) *Inclusion of some additional cyber crimes like child pornography and cyber terrorism*

h) *Authorizing an Inspector to investigate cyber offences (as against the DSP earlier)*

123

Data Protection: Sec 43A

Corporates are under an obligation to ensure adoption of reasonable security practices.

Reasonable Security Practices include:

a) Site certification
b) Security initiatives
c) Awareness Training
d) Conformance to Standards, certification
e) Policies and adherence to policies
f) Policies like password policy, Access Control, email Policy etc
g) Periodic monitoring and review.

The international Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub-rule

124

Offences as per IT Act

65. Tampering with computer source documents.
66. Computer related offences.
66A. Punishment for sending offensive messages through communication service, etc.
66B. Punishment for dishonestly receiving stolen computer resource or communication device.
66C. Punishment for identity theft.
66D. Punishment for cheating by personation by using computer resource.
66E. Punishment for violation of privacy.
66F. Punishment for cyber terrorism.
67. Punishment for publishing or transmitting obscene material in electronic form.
67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.
67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.
67C. Preservation and retention of information by intermediaries.
68. Power of Controller to give directions.
69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource.
69A. Power to issue directions for blocking for public access of any information through any computer resource.
69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security.

125

Protecting Critical Infrastructure

"Critical Information Infrastructure means the computer resource, the incapacitation or destruction of which , shall have debilitating impact on national security, economy, public health or safety. [*Explanation* section 70 (1)]

e-Governance information security will be covered under sections 70A (National Nodal Agency for protection of Critical Information Infrastructure) and 70B (CERT-IN to serve as national agency for incident response) of the Information Technology (Amendment) Act, 2008.

126

IPC amendments

- ITA 2000 has amended the sections dealing with records and documents in the IPC by inserting the word ‘electronic’ thereby treating the electronic records and documents on a par with physical records and documents.
- The Sections dealing with false entry in a record or false document etc (eg 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc) have since been amended as electronic record and electronic document thereby bringing within the ambit of IPC, all crimes to an electronic record and electronic documents just like physical acts of forgery or falsification of physical records.

127

The Indian Evidence Act - Amendments

- Prior to the passing of ITA, all evidences in a court were in the physical form only.
- With the ITA giving recognition to all electronic records and documents, it was but natural that the evidentiary legislation in the nation be amended in tune with it.
- In the definitions part of the Act itself, the “all documents including electronic records” were substituted. Words like ‘digital signature’, ‘electronic form’, ‘secure electronic record’ ‘information’ as used in the ITA, were all inserted to make them part of the evidentiary mechanism in legislations.

128

The Bankers' Books Evidence(BBE) Act 1891 - Amendments

- Prior to the passing of ITA, any evidence from a bank to be produced in a court, necessitated production of the original ledger or other register for verification at some stage with the copy retained in the court records as exhibits.
- With the passing of the ITA the definitions part of the BBE Act stood amended as: "'bankers ' books' include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device".

129

RBI Act , 1934 Amendments

Section 58 of the Act sub-section (2), after clause (p), a clause relating to the regulation of funds transfer through electronic means between banks (ie transactions like RTGS and NEFT and other funds transfers) was inserted, to facilitate such electronic funds transfer and ensure legal admissibility of documents and records therein.

130

India's approach to Cyber Security:

1. Enabling Legal Framework
2. Cyber Security Policy
3. Compliance and Assurance
4. Cyber Security R&D Security
5. Incident – Early Warning and Response
   a) National Cyber Alert System
   b) CERT-In and Sectoral CERTs
   c) Information Exchange with International CERTs
6. Security training
   a) Skill & Competence development
   b) Domain Specific training – Cyber Forensics, Network & System Security Administration
7. Collaboration
   a) International
   b) National

131

NCSP - 2013

The National Cyber Policy 2013 document outlines a road-map to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country.

Vision: To build a secure and resilient cyber space for citizen, businesses and Government.

Mission: To protect information and information infrastructure in cyberspace, build capacities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structure, people, process, technology and cooperation.

132

NCSP - Objectives

1. To create secure cyber-ecosystem and enable adequate trust and confidence in electronic transactions and also guiding stakeholders actions for protection of cyber space.
2. To create an assurance framework for design of security policies and enable actions for compliance of global standards.
3. To strengthen regulatory framework for ensuring secure cyber ecosystem.
4. To develop suitable indigenous technologies in ICT sector.
5. To increase the visibility of integrity of ICT product by establishing infrastructure for testing and validation of security of such product.
6. To create a workforce of 500,000 professionals skilled in cyber security in next five years.
7. To provide fiscal benefits for corporate for adoption of cyber security.
8. To safeguard the privacy of citizen's data.
9. To enable effective prevention, detection and investigation of cyber crimes
10. To create the culture of cyber security.
11. To enhance global cooperation in cyber security
12. To enhance protection and resilience of National Critical Information Infrastructure.
13. To enhance national and sectoral 24*7 mechanisms for monitoring cyber threats.

133

NCSP - Strategy

1. **Creating a secure cyber ecosystem** :
   a) Designate nodal agency for coordination in cyber security related issues
   b) Designate Chief Information Security Officer (CSIO) in all organization.
   c) Encourage all organization to come out with cyber security policy in line with national policy
   d) Ensure all organization allocate some part of their budget for cyber security
   e) Fiscal schemes for cyber security
   f) Encourage trustworthy and indigenous ICT products.
2. **Creating assurance framework**:
   a) To promote adoption of best practices
3. **Encouraging open standards**
4. **Strengthening the regulatory framework**
5. **Creating mechanisms for security threats early warning, vulnerability management and response to security needs**:
   a) Implement cyber crisis management plan.
6. **Securing e-governance services**
7. **Protecting and resilience of Critical Information Infrastructure**
8. **Promoting research and development in cyber security**
9. **Reducing supply chain risk**
   a) Create testing infrastructure and facilities for ICT products.
10. **Human resource development**
11. **Creating Cyber awareness**:
12. **Developing effective public-private partnership**
13. **Information sharing and cooperation**
    a) Bilateral and multilateral relationship in information sharing.
    b) Enhance national and global cooperation
    c) Mechanism for dialogue in the field of cyber security
14. **Prioritized approach for implementation**

134

Regulators guidelines

In addition to this legislation, regulatory guidelines are issued by sectoral regulators for organizations under their purview.

1. Reserve Bank of India (RBI- Banking Regulator)
2. Telecom Regulatory Authority of India (TRAI - Telecom Regulator)
3. Insurance Regulatory and Development Authority (IRDA -Insurance Regulator)
4. Securities and Exchange Board of India (SEBI - Capital markets Regulator)

135

IT Act, 2000

Enabling Act

Facilitating Act

Regulatory Act

136

RBI guidelines

1. The Reserve Bank, had, provided ***Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds*** (G. Gopalakrishna Committee) vide Circular DBS.CO.ITC.BC.No.6/31.02.008/2010-11 dated April 29, 2011.

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

137

137

Need ..

- According to RBI, ***the use of technology by banks has gained further momentum, the number, frequency and impact of cyber incidents / attacks have increased manifold in the recent past, more so in the case of financial sector including banks***, underlining the ***urgent need to put in place a robust cyber security/resilience framework at banks and to ensure adequate cyber-security preparedness among banks on a continuous basis.***

- In view of the low barriers to entry, evolving nature, growing scale/velocity, motivation, and resourcefulness of cyber-threats to the banking system, **it is essential to enhance the resilience of the banking system by improving the current defences in addressing cyber risks.**

- These would include, but not limited to, **putting in place an adaptive Incident Response, Management and Recovery framework to deal with adverse incidents/disruptions**, if and when they occur.

138

138

RBI Guidelines

1. *Need for a Board approved Cyber-security Policy*
2. *Cyber Security Policy to be distinct from the broader IT policy / IS Security Policy of a bank*
3. *Arrangement for continuous surveillance*
4. *IT architecture should be conducive to security*
5. *Comprehensively address network and database security*
6. *Ensuring Protection of customer information*
7. *Cyber Crisis Management Plan*
8. *Cyber security preparedness indicators*
9. *Sharing of information on cyber-security incidents with RBI*
10. *Supervisory Reporting framework*
11. *An immediate assessment of gaps in preparedness to be reported to RBI*
12. *Organisational arrangements*
13. *Cyber-security awareness among stakeholders / Top Management / Board*

139

139

NCIIPC: CII – Controls

The five families of controls into which the Guidelines for the protection of CII have been divided are:

1. **Planning Controls**:
2. **Implementation Controls**:
3. **Operational Controls**:
4. **Disaster Recovery/Business Continuity Planning (BCP) Controls**:
5. **Reporting and Accountability Controls**:

140

140

CII – Family of Controls

Planning Controls (12)

1. PC1: Identification of CII
2. PC2: Vertical and Horizontal Interdependencies
3. PC3: Information Security Department
4. PC4: Information Security Policy
5. PC5: Integration Control
6. PC6: VTR Assessment and Mitigation Controls
7. PC7: Security Architecture Controls including configuration Management and Mitigation Controls
8. PC8: Redundancy Controls
9. PC9: Legacy System Integration
10. PC10: Supply Chain Management – NDA's, Extensions and Applicability
11. PC11: Security Certifications
12. PC12: Physical Security Controls

Implementation Controls (6)

1. IC1:Asset and Inventory Control
2. IC2:Access Control Policies
3. IC3:Identification and Authentication Control
4. IC4:Perimeter Protection
5. IC5:Physical and Environmental Security
6. IC6:Testing and Evaluation of Hardware and Softwares

Operational Controls (11)

1. OC1:Data storage: Hashing and Encryption
2. OC2:Incident Management - Response
3. OC3:Training, Awareness and Skill up-gradation
4. OC4:Data Loss Prevention
5. OC5:Penetration Testing
6. OC6:Asset and Inventory Management
7. OC7:Network Device Protection
8. OC8:Cloud Protection
9. OC9:Critical Information Disposal and Transfer
10. OC10: Intranet Security
11. OC11: APT protection

Disaster Recovery/ Business Continuity Planning (BCP) Controls (3)

1. DR1:Contingency Planning – Graceful degradation
2. DR2:Data Back-up and Recovery Plan, Disaster Recovery Site
3. DR3:Secure and Resilient Architecture Deployment

Reporting and Accountability Controls (3)

1. RA1:Mechanism for threat reporting to Govt. Agencies
2. RA2:Periodic Audit and Vulnerability assessment
3. RA3:Compliance of Security Recommendation

141

141

Q&A

142

142