Digital Trust & Information Security

23 March 2025

Dr. Srinivas Josyula

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

1

Outline

Governance Risk and Compliance

Reg Tech

Digital Trust and Information/ Cyber Security

Privacy / GDPR

2

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

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

Goals

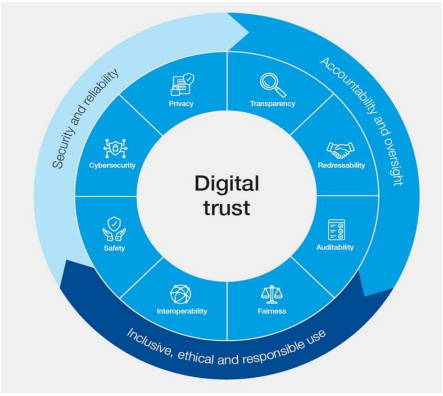
The digital trust framework defines shared goals or values that inform the concept of digital trust, including:

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

5

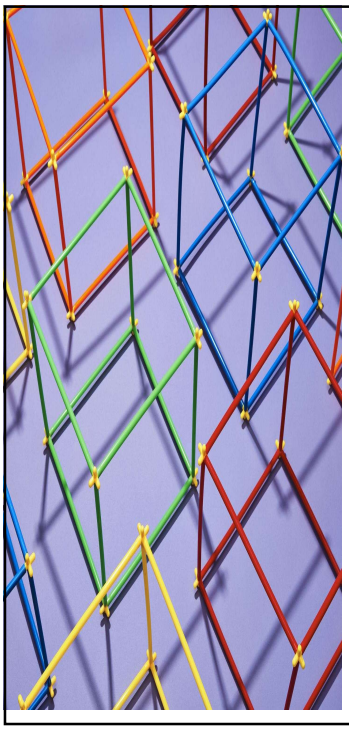
Digital Trust Framework

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.



6

6



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

7

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

8

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).

9

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.***

10

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

11

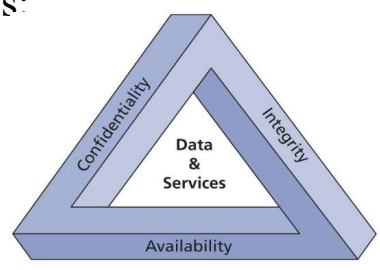
11

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



12

12

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)**

13

13

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"

14

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)

15

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.*

16

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).

17

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.

18

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***.

Deter Unethical and Illegal Behaviour

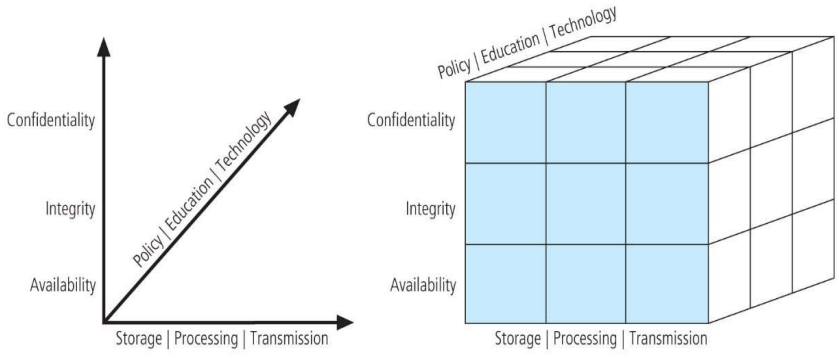
- It is the responsibility of InfoSec personnel to deter unethical and illegal acts, ***using policy, education and training, and technology as controls or safeguards, in order to protect the organization's information and systems.***
- There are three general categories of unethical behavior that organizations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

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

21

CNSS Security Model



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

22

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.

23

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***

24

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)"

25

IT-related Business Risk

26

26

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.

27

27

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.

28

28

Sources of Vulnerabilities

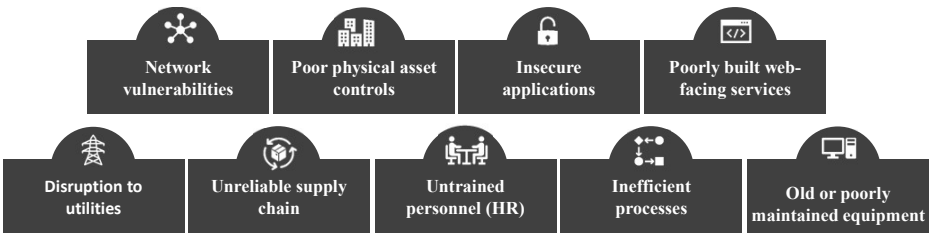
Network:	Misconfiguration of equipment, poor architecture or traffic interception protocols
Physical Access	Allows attackers to potentially bypass other types of controls
Apps/Web Services	Supports business function without due regard to security requirements
Utilities	Power failure or environmental 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

29

29

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



30

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)

31

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***

32

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

33

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

34

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.

35

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

36

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

37

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**

38

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

39

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***

40

Mandates and Guidelines

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

41

41

42

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

43

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.

44

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

45

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.

46

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)*

47

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

48

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.

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

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.

51

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**

52

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)

53

IT Act, 2000

Enabling Act

Facilitating Act

Regulatory Act

54

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.

55

55

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***

56

56

Q&A

57

58

Agenda

1. Data Protection
2. GDPR

59

What is Data protection?

- Data protection is the fair and proper use of information about people. It's part of the fundamental right to privacy – but on a more practical level, it's really about building trust between people and organisations. It's about treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others, and striking a balance with the wider interests of society.
- It's also about removing unnecessary barriers to trade and co-operation. It exists in part because of international treaties for common standards that enable the free flow of data across borders. The UK has been actively involved in developing these standards.
- Data protection is essential to innovation. Good practice in data protection is vital to ensure public trust in, engagement with and support for innovative uses of data in both the public and private sectors.
- The UK data protection regime is set out in the DPA 2018 and the GDPR (which also forms part of UK law).

60

What is GDPR?

- Is a new EU regulation to strengthen and control the use of personal data for all individuals within the EU
- In May 2018, GDPR replaced the Data Protection directive (DPA)
- Not just about Marketing, technology neutral
- GDPR will increase privacy for individuals and authorities will have greater powers against businesses that breach Data Protection laws

61

GDPR key drivers

Source: European Council
Council of the European Union

- Updates and modernizes the principles of the 1995 Data Protection Directive
- Sets out the rights of the individual and establishes the obligations of those processing and those responsible for the processing of the data.
- Establishes the methods for ensuring compliance as well as the scope of sanctions for those in breach of the rules.
- Applies to all organizations doing business in the EU regardless of location.

62

62

GDPR data definitions regardless of nationality or EU residence

Personal Data (from GDPR)

"…means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Examples:

- Name
- Identification number (e.g., SSN)
- Location data (e.g., home address)
- Online identifier (e.g., e-mail address, screen names, IP address, device IDs)
- Genetic data (e.g., biological samples from an individual)
- Biometric data (e.g., fingerprints, facial recognition)

"The GDPR also requires compliance from non-EU organizations that offer goods or services to EU residents or monitor the behavior of EU residents."

Source: *Brief: You Need An Action Plan For The GDPR*; Forrester Research; October 2016

63

GDPR compliance is a challenge for both controllers and processors

64

"By the end of 2018, over 50% of companies affected by the GDPR will not be in full compliance with its requirements."

Gartner - *Focus on Five High-Priority Changes to Tackle the EU GDPR*; September 30, 2016

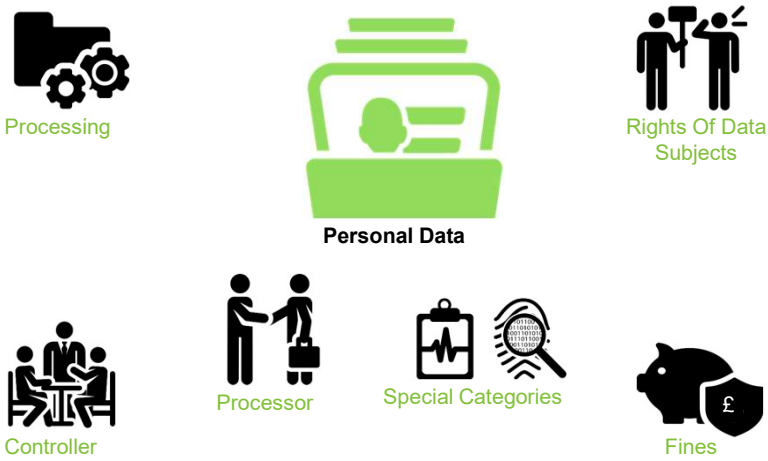
The General Data Protection Regulation (GDPR) imposes new rules on organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents, no matter where they are located.

- **Enhanced** personal privacy rights
- **Increased** duty for protecting data
- **Mandatory** breach reporting
- **Significant** penalties for non-compliance

64

GDPR impact?

If you process, either as a controller or a processor, personal data of any data subjects who are in the EU?



65

General overview

– Key changes brought in by GDPR:

- Direct accountability of data processors
  - » *Data controller/processor distinction*
- Consent requirements toughened up
  - » *"freely given, specific, informed and unambiguous indication … by a statement or clear affirmative action…"*
- Territorial extent
  - » *The "Global" Data Protection Regulation?*
- Breach notification and record keeping
  - » *Mandatory notification, document intensive*

66

What is Personal Data?

Any information relating to an identified or identifiable living person:

Personal Data

- Full name, maiden name, mothers maiden name or alias
- Date and place of birth, race, religion, weight, geographical indicators, employment, medical, education and financial information
- Address information, street, IP or email address
- Personal identification numbers: National Insurance, passport, drivers license, patient ID, financial accounts and credit numbers
- Vehicle registration number
- Telephone numbers including mobile, business and personal
- Personal characteristics, including photo (face or distinguishing features), finger prints, biometric data (retina scan, etc)

67

What is Processing?

Any operation performed on personal data whether or not by automated means:

Processing

- Collection
- Recording
- Organisation
- Structuring
- Storage
- Adaptation or alteration
- Retrieval
- Consultation
- Use
- Disclosure by transmission
- Dissemination or otherwise making available
- Alignment or combination
- Erasure or destruction

A processor is a separate person or organisation (not an employee) who processes data on behalf of the controller and in accordance with their instructions. Processors have some direct legal obligations, but these are more limited than the controller's obligations.

68

What is a Controller?

Natural or legal person, public authority, agency or other body which determines the purposes and means of the processing of personal data

Controller

Controllers determine:

- The legal basis for collecting data
- Which items of personal data to collect
- The content of the data
- The purpose or purposes the data are to be used for
- Which individuals to collect data about
- Whether to disclose the data, and if so, who to?
- Whether subject access and other individuals' rights apply
- How long to retain the data
- Whether to make non-routine amendments to the data

A controller is the person that decides how and why to collect and use the data. This will usually be an organisation, but can be an individual (eg a sole trader). If you are an employee acting on behalf of your employer, the employer would be the controller. The controller must make sure that the processing of that data complies with data protection law.

69

What is a Processor?

Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Processor

Within the terms of the agreement with the data controller, and its contract, a data processor may decide:

- What IT systems or methods to use
- How to store
- The detail of the security surrounding the data
- The means used to transfer from one organisation to another
- The means used to retrieve personal data about certain individuals
- The method for ensuring a retention schedule is adhered to
- The means used to delete or dispose of the data

70

Processor Contracts

New obligations require a greater need for contracts between controller and processor

Contract

The contract should specify:

- Will act only on the instructions of the controller
- Guarantee to both parties that the other is abiding by GDPR
- Require the processor to comply with data security obligations equivalent to those imposed on the controller
- Set out what happens in the event of a breach of security
- Set out the processor's obligations for data retention and destruction
- Specify the mechanisms for exchange of data between the parties

71

What are Special Categories ?

Processing is prohibited* of any personal data that reveals:

Special Categories

- Race
- Ethnic origin
- Political opinions
- Religion
- Philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Data concerning sex life
- Sexual orientation

* Some exceptions apply

72

Individuals Rights

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the Data Protection Act:

Rights Of Data Subjects

- Right to be informed
- Right off access
- Right to rectification
- Right to erasure
- Right to restriction
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

73

What Are The Penalties?

ICO (Information Commissioner's Office) is the UK's supervisory authority. Their role is to supervise and enforce the GDPR and have the power to conduct investigations and deal with complaints

ICO's enforcement powers include administrative fines:

Fines

- €20m or 4% of global turnover, whichever is higher, in cases where the data subject's rights have been infringed
- €10m or 2% of global turnover, whichever is higher, in cases where data controllers or processors have not met the obligations of the regulation

74

GDPR Principles

1. Fair & Lawful	• Processed lawfully, fairly and in a transparent manner
2. Legitimate	• Collected for specified, explicit and legitimate purposes
3. Limited	• Adequate, relevant and limited to what is necessary
4. Accurate	• Accurate and, where necessary, kept up to date
5. Retention	• Retained only for as long as necessary
6. Security	• Processed in an appropriate manner to maintain security

Accountability

75

Areas of Risk

Risks are evident in any function within a business, wherever personal data is processed

HR

- Key employee data
- Financial information
- Staffing procedures
- Accident book
- Medical details
- Criminal records
- Trade Union involvement
- Visitor book / mailroom

Sales & Marketing

- Customer data
- Bank details
- Purchase history
- Personal identifiers
- Payment history
- Delivery records

Others

- Supplier information
- Shared data

76

Checklist

Data Flow Audit

- Conduct a data flow audit
- What, where, why, who, retention

Data Protection Policy / Statement

- Amount of information has increased
- Needs to be clear, concise, for internal/external

Subject Access Requests

- Understanding individual rights
- Process in place for providing within 1 month

Consent

- Individuals can withdraw previous consent
- Process in place and parental if applicable

77

Checklist

International Transfer

- Consider cloud storage
- Process and contracts in place

Data Protection Impact Assessments

- Conduct for new systems and projects
- Regularly review

Processor Agreements

- Contracts in place for all third parties
- Mitigate your liability

Data Breach Process

- Understand your obligations
- Consider data breach register

78

ICO Advice

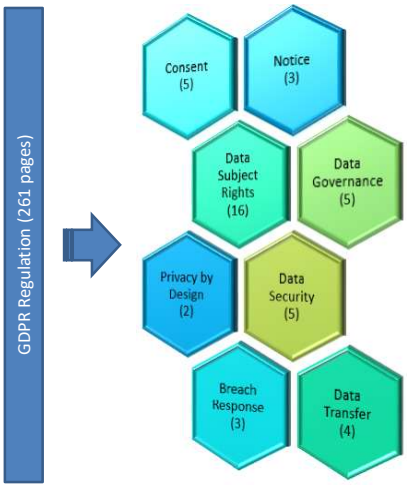
- Documenting policies alone is often not enough
- Ensure that you have a process to monitor compliance
- You should regularly test measures
- You should brief all staff handling personal data on their data protection responsibilities
- You should also consider specialist training for staff with specific duties
- You need to have a senior staff member with responsibility for managing information risks

79

Controller's GDPR compliance model

European Council
Council of the European Union

43 GDPR Requirements*



"…organizations must demonstrate that they have implemented appropriate measures to mitigate privacy risks. Even in the absence of a privacy breach or customer complaint, regulators may require firms to exhibit evidence of their compliance and risk management strategies, including a privacy impact assessment (PIA) when appropriate."

80

Thank You