Learning Objectives

- DPDP Act & AI Act (EU)
- New Cyber Risks & their respective policies, controls and compliance
- Risk Control Matrix
- Audit tools & Techniques
- Crafting Audit Checklist for different Audits using Generative AI
- Case Studies on COBIT 2019, GDPR (DPDP), New Generation Cyber Frauds, Business continuity planning, Automation of a MSME (SDLC), Cloud Service Provider (SLA & Cloud Audit)

DPDP Act

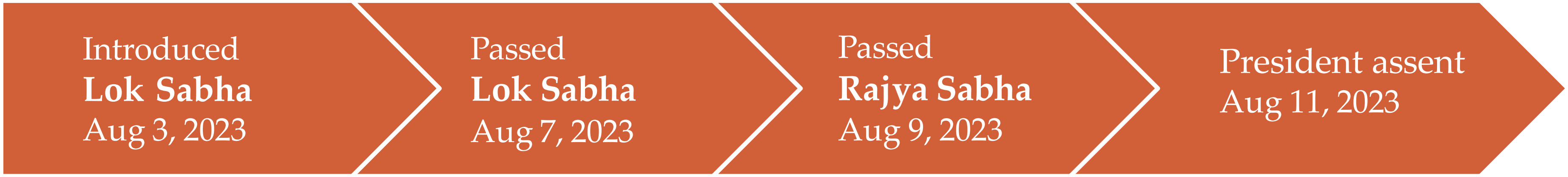
Brief History

- 2017 landmark SC judgement (*K.S. Puttaswamy vs Union of India*) recognised **privacy as a fundamental right** in India.

- First iteration of the law (Draft Personal Data Protection Bill, 2018) made by the Justice BN Srikrishna Committee.

- Three more iterations of the draft bill - released for public consultations in 2018, 2019 and 2022.

- The fifth iteration was introduced and passed by the Parliament as the Digital Personal Data Protection Bill, 2023 ("**DPDP Act**").



Introduced
Lok Sabha
Aug 3, 2023

Passed
Lok Sabha
Aug 7, 2023

Passed
Rajya Sabha
Aug 9, 2023

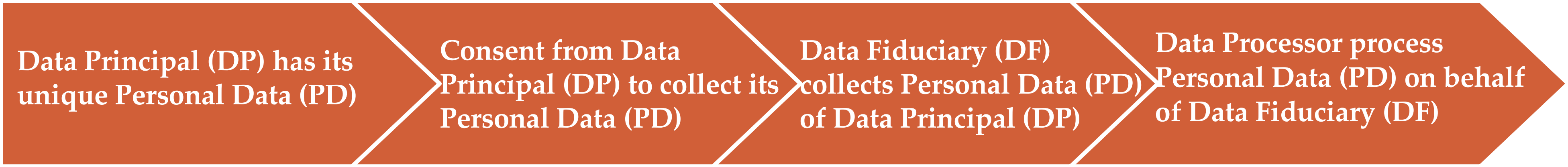
President assent
Aug 11, 2023

Timeline of DPDP Act

Key Definitions

- **Data**: Representation of information, facts, concepts, opinions or instructions suitable for communication or processing by humans or automated means.
- **Personal Data ("PD")**: Any data about an individual who is identifiable by or in relation to such data.
- **Digital Personal Data**: PD in digital form (collected in digital form or digitized subsequently).
- **Data Fiduciary ("DF")** - any person who alone or in conjunction with other persons determines the purpose and means of processing of PD.
- **Data Principal ("DP")** - individual to whom the PD relates. In case of a child/person with disability, the term includes the parent or lawful guardian of the child.
- **Processing** - means a wholly or partly automated operation – on digital personal data – includes collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.
- **Data Processor** - any person who processes PD on behalf of a data fiduciary

PD Processing



Data Principal (DP) has its unique Personal Data (PD)

Consent from Data Principal (DP) to collect its Personal Data (PD)

Data Fiduciary (DF) collects Personal Data (PD) of Data Principal (DP)

Data Processor process Personal Data (PD) on behalf of Data Fiduciary (DF)

Processing of PD

General Obligations

- **Baseline Compliance** – The DF must comply with its obligations such as notice, consent etc. regardless of whether the DP has adhered to its duties.
- **Integrity of PD:** Take reasonable efforts to ensure that the PD is accurate and complete if it is likely to be used by the DF to make a decision that affects the DP or is likely to be disclosed to another DF.
- **Technical & Organizational Measures:** Implement appropriate technical and organizational measures to comply.
- **Security of PD:** Protect PD under its possession or control & implement reasonable security safeguards to prevent personal data breach.

Duties of Data Principals

- Comply with applicable law while exercising rights under the DPDP Act.
- Not register false or frivolous grievances.
- Not furnish false data or suppress material facts or impersonate another person when applying for any document, service, unique identifier, proof of identity or proof of address.
- Furnish only verifiably authentic information while exercising right to correction and erasure.

Impact of rights & duties of data principals:

- Companies will have to maintain – i) a list of persons with whom the it shares any DP's PD; ii) summary of types of PD being processed and the types of processing being done on any DP's PD.
- Create effective responsive systems and mechanisms to address DP rights requests and grievances in the an effective & timebound manner.
- Adherence to the timelines for responding to requests, existing mechanisms in place needs to be relooked at.

Rights of Data Principals

- **Right to obtain information from the DF-** A DP has the right to – (i) obtain a summary of PD and details of processing (ii) a list of entities processing PD and the type of PD shared, (iii) any other information as maybe prescribed.

  Exception - Point (ii) and (iii) shall not apply in respect of sharing any PD with other DF, *IF authorized by law for prevention, detection or investigation of a cyber incident or for prosecution or punishment of offences.*

- **Right to ask for correction and erasure -**
  - DF must correct inaccurate or misleading data, complete a DP's incomplete data, update the DPs PD, and erase the PD of the DP that is no longer necessary unless retention is required for a legal purpose.

- **Right to ready and available grievance redressal-**
  - DP has the right to readily available grievance redressal mechanism by a DF or CM.
  - DF or CM must reply within prescribed period.
  - Mandatory to exhaust this remedy before approaching the Board.

- **Right to nominate-** The right of a DP to nominate another person who will be eligible to exercise the DP's right in the event of the DP's death or incapacity.

Data Protection Board

- Board to function as an **independent body**.
- **Powers:**
  - Conduct inquiry
  - Impose penalty
  - Advise the government regarding blocking of information
  - Issue interim orders
  - Powers of civil court
- **Functions:**
  - Inquire into non-compliances upon complaint, intimation or reference by Central Govt.
  - No *suo moto* power
  - Direct DF to adopt urgent, remedial or mitigation measures in case of personal data breaches
  - Issue directions to any person for effective discharge of its functions

- **Flow of appeal:**

Order of the Board >> TDSAT >> Supreme Court (only when substantial question of law involved)

(Telecom Disputes Settlement and Appellate Tribunal (TDSAT) has been designated as the appellate Tribunal under the DPDP Act)

- Civil courts cannot entertain suits or take action under the Act, although certain remedies, such as writs (where applicable) cannot be precluded.

Penalties

The Board, in arriving at the quantum of the penalties, may consider a number of factors such as the nature, gravity and duration of the contravention, types of personal data affected, implications of the contravention and mitigating measures adopted by the contravening party.

Non-Compliance	Penalty (in INR)
Failure of Data Processor or Data Fiduciary to take reasonable security safeguards to prevent personal data breach	Up to 250 Cr. (3 Bn USD)
Failure to report data breach	Up to 200 Cr. (2.41 Bn USD)
Processing of PD of child in violation of Bill	Up to 200 Cr (2.41 Bn USD)
Failure on part of SDF to comply with incremental obligations	Up to 150 Cr (1.8 Bn USD)
DP not complying with their duties	Up to 10,000 (120 USD)
Breach of voluntary undertaking accepted by Board	Up to the extent applicable for the breach
Residuary	Up to 50 Cr (60 Mn USD)

Important Sections

- **Section 2**: Definitions
- **Section 4 to 10**: Obligations of Data Fiduciary
- **Section 11 to 15** : Rights and Duties of Data Principal
- **Section 16 to 17** : Special Provisions
- **Section 18 to 26** : Data Protection Board of India
- **Section 27 to 28** : Power, Functions and Procedure to be followed by Board
- **Section 29 to 32** : Appeal and Alternate Dispute Resolutions
- **Section 33 to 34** : Penalties and Adjudication
- **Section 35 to 44** : Miscellaneous

AI Act (EU)

Introduction

- The EU AI Act, also known as the EU Artificial Intelligence Act, is the world's first concrete initiative for regulating Artificial Intelligence.

- The AI Act aims to ensure that AI systems in the EU are safe and respect fundamental rights and values.

- Its objectives are to foster investment and innovation in AI, enhance governance and enforcement, and encourage a single EU market for AI

Affected Stakeholders

- The AI Act has set out clear definitions for the different actors involved in AI like providers, deployers, importers, distributors, and product manufacturers.

- All parties involved in the development, usage, import, distribution, or manufacturing of AI systems will be held accountable.

- AI Act also applies to providers and deployers of AI systems located outside of the EU, if output produced by the system is intended to be used in the EU.

Penalties for Non-Compliance

- The penalties for non-compliance with the AI Act are significant and can have a severe impact on the provider’s or deployer's business.

- They range from €7.5 million to €35 million or 1% to 7% of the global annual turnover, depending on the severity of the infringement.

New Cyber Risks & their respective policies, controls and compliance

New Cyber Risks

- Data Loss
- Ransomware
- Cloud Risks
- PII Breaches
- Critical Infrastructure Threats
- CIA Threats

Data Loss

Data loss refers to the destruction, deletion, corruption, or inaccessibility of data. It can occur due to various reasons, including human error, system failures, malware, or malicious attacks.

Data loss can have severe consequences for individuals and organizations, like financial losses to reputational damage, operational disruptions, Legal Ramifications and Loss of competitive advantages .

Data Loss Control & Policies

- Data Retention Policy
- Backups and check
- Data Loss Prevention Software
- Information Right Management Software
- Security Awareness Training
- Strong Access Controls
- Regular Security Audits
- BC/DR test

Ransomware

Ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyber attackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files.

Difficult-to-trace digital currencies such as paysafecard or Bitcoin and other cryptocurrencies are commonly used for the ransoms, making tracing and prosecuting the perpetrators difficult.

Ransomware Control & Policies

- Security Awareness Training
- Cyber Security Policy
- Data Retention Policy
- Backups and check
- IPS & Firewall on the Network
- Antivirus and Antimalware on the user’s system

Cloud Risks

Cloud risks refer to the various threats and challenges associated with using cloud computing services, primarily focused on security and compliance.

These risks can be broadly categorized into data breaches, data loss, insider threats, misconfigurations, compliance issues, account hijacking, denial of service (DoS) attacks, API threats, Lack of Visibility.

Cloud Risk Control & Policies

- Cloud Migration understanding
- Service Level Agreement (SLA)
- Cyber Security Policy
- Data Retention Policy
- Backups and check
- Encryption of data before sending to cloud
- Cryptographic erasure
- Security Awareness Training

PII Breaches

PII, or Personally Identifiable Information, risks encompass a range of potential harms stemming from the unauthorized access, use, or disclosure of sensitive personal data.

These risks include identity theft, financial loss, reputational damage, and legal repercussions for both individuals and organizations.

Breaches often result from inadequate security measures, cyberattacks, or even internal negligence.

PII Breaches Control & Policies

- Cyber Security Policy
- PII Sensitization by Awareness Training
- Data Backups and check
- Encryption of data for Data at Rest and Data in Transit
- Background checks of both employees of Data fiduciary and Data Processor.

Critical Infrastructure Threats

Critical infrastructure refers to the essential physical and virtual systems, assets, and networks that are vital for the functioning of a society, economy, and public health and safety.

These systems, often interconnected, are considered critical because their failure or disruption could have a debilitating impact on national security, economic stability, and public well-being.

Example of Critical infrastructure includes Energy, Transportation, Communication, Financial Services, Railways, Aviation, Water Supply

Critical Infrastructure Threats

Critical infrastructure faces a wide range of threats, including cyberattacks, natural disasters, and physical attacks, all of which can have severe consequences for public safety, national security, and the economy.

These threats are particularly concerning because critical infrastructure systems are interconnected and often rely on legacy systems, making them vulnerable to cascading failures and widespread disruptions.

Critical Infrastructure Control & Policies

- IT & OT Cyber Security Policy
- User Awareness Training
- Data Backups and check
- IPS & Firewall on the Network
- Antivirus and Antimalware on the user’s system

CIA Threats

The CIA Triad in information security refers to Confidentiality, Integrity, and Availability.

Confidentiality is protecting information from unauthorized access.

Integrity is ensuring data remains accurate and trustworthy. This means preventing unauthorized modification or corruption of data.

Availability is making sure data and systems are accessible to authorized users when needed.

CIA Threats

Confidentiality threats includes unauthorized access, weak encryption, insider threats, and social engineering attacks.

Integrity threats includes data corruption, unauthorized modification, errors in processing, and malware infections.

Availability threats includes System failures, power outages, network issues, natural disasters, and cyberattacks like DDoS.

CIA Control & Policies

- Cyber Security Policy
- User Awareness Training
- Data Backups and check
- Strong Encryption like AES, RSA
- Strong Hashing algorithm like SHA 256
- IPS & Firewall on the Network
- Antivirus and Antimalware on the user’s system
- BC/DR

Risk Control Matrix

Risk Control Matrix

- A risk control matrix is a structured tool for identifying, assessing, and managing risks within an organization’s processes or operations.

- It serves as a comprehensive framework that maps risks to corresponding controls, ensuring that all potential vulnerabilities are addressed effectively.

Creating Risk Control Matrix

Creating a risk control matrix involves a structured process that ensures all potential risks are identified, assessed, and mitigated effectively. Follow these steps to prepare a comprehensive risk control matrix:

- Define the scope and objectives
- Identify key risks
- Set control objectives
- Define control activities
- Assign risk owners
- Evaluate risk severity and control effectiveness
- Document and organize the matrix
- Review and update regularly

Risk Control Matrix

Risk Description	Control Objective	Control Activities	Risk Owner	Risk Severity	Control Effectiveness
Unauthorised Access	Prevent Data Breaches	Implemented RBAC	IT Security Manager	Medium	Effective
IT System Downtime	Ensure minimal downtime	Update recovery plan	IT Operation Manager	High	Effective
Inadequate employee training	Minimize operational errors	Develop training program	HR Head	Medium	Moderately Effective
Phishing cyber security breach	Reducing phishing Risk	Conduct phishing training	IT Security Manager	High	Effective

Utility of Risk Control Matrix

- Enhanced risk identification and mitigation – A risk control matrix provides a systematic approach to identifying and addressing risks in organizational processes.

- Streamlined decision-making – With a clear and concise overview of risks and controls, the risk control matrix empowers decision-makers to prioritize risk mitigation efforts while ensuring that resources are allocated efficiently to address the most critical risks.

- Ongoing risk monitoring and adaptability –Regular matrix updates enable organizations to adapt to emerging risks and shifting business priorities, ensuring risk management efforts remain relevant and effective over time.

Audit tools & Techniques

Auditing Essentials

- Auditing is essential not only for providing financial assurance but also for addressing the growing demands from stakeholders, regulators, and management for real-time insights and predictive capabilities.

- Today’s stakeholders expect more than periodic financial compliance—they are looking for continuous monitoring and rapid detection of potential risks, fraud, or errors.

- The modern business environment demands agility and foresight, both of which advanced auditing practices can provide.

Auditee Requirements

- Auditing moves beyond simple compliance and becomes a strategic asset, helping companies navigate complex business landscapes with greater confidence and foresight.

- This shift is particularly important for organizations managing large volumes of transactions online/offline across borders and in various regulatory environments.

1.6 Auditing of the Information System and Auditing around the Information System

Head	Auditing of the Information System	Auditing Around the Information System
Scope	Involves a detailed review of the entire IT infrastructure, including controls, processes, and configurations.	Focuses primarily on the outputs generated by the IT systems, verifying their accuracy and reliability.
Focus	Emphasizes evaluating and improving IT controls and security measures.	Concentrates on the accuracy of financial and operational data produced by the IT systems.
Techniques	Utilizes control testing, vulnerability assessments, and configuration reviews.	Employs substantive testing, analytical procedures, and reconciliations.
Advantages	Provides a comprehensive understanding of IT controls and enhances overall security.	More efficient and focuses on ensuring the reliability of decision making data.
Limitations	Resource-intensive and complex, requiring specialized knowledge.	Limited in scope, potentially overlooking system vulnerabilities and control deficiencies.
Application	Suitable for organizations with complex IT environments and a high reliance on IT systems for critical operations	Appropriate for organizations seeking assurance on the accuracy of financial and operational data without delving deeply into IT infrastructure.

Need of Auditing tools

- The emergence of sophisticated technologies has revolutionized auditing, enabling the field to move from traditional, manual processes to data-intensive and technology-driven approaches. Advanced auditing techniques allow auditors to analyze large datasets with unprecedented accuracy, detect anomalies faster, and conduct audits more efficiently.

- By incorporating data-driven insights into audits, auditors can proactively identify emerging risks, provide recommendations to enhance operational efficiencies, and contribute to organizational resilience.

Auditing tools & Techniques

Data Analytics in Auditing:

- Data analytics has become one of the most powerful tools in modern auditing, transforming how auditors handle vast amounts of data.

- Data analytics, however, enables auditors to evaluate entire datasets, identifying patterns, trends, and outliers across large volumes of transactions.

- This holistic approach enhances the accuracy of audits by reducing the likelihood of undetected errors or irregularities.

Auditing tools & Techniques

Artificial Intelligence (AI) and Machine Learning (ML):

- AI and ML have added a new dimension to the field of auditing, enabling auditors to perform complex tasks more efficiently and accurately.

- AI and ML are particularly effective in areas such as fraud detection, risk assessment, and process automation. These technologies can analyze unstructured data, learn from patterns over time, and enhance decision-making in the audit process.

Auditing tools & Techniques

Blockchain Technology:

- Blockchain technology is reshaping the way transactions are recorded, verified, and audited. As a decentralized, tamper-resistant ledger, blockchain provides a high level of security and transparency, allowing auditors to verify transactions with minimal need for third-party verification.

- In an audit context, blockchain offers several advantages, particularly for industries where data integrity and transaction validation are critical.

Auditing tools & Techniques

Continuous Auditing:

- Continuous auditing represents a shift from periodic audits to real-time, ongoing audit activities that provide more timely insights and enable proactive risk management.

- With continuous auditing, auditors can monitor transactions, financial statements, and operational metrics on an ongoing basis, identifying issues and potential risks as they arise. This approach enhances the relevance of audits in fast-paced business environments, where waiting for periodic audits may delay the detection of critical issues. Continuous auditing relies heavily on automation and real-time data integration.

Crafting Audit Checklist for different Audits using Generative AI

Generative AI :

- Is a type of artificial intelligence that creates new content, such as text, images, audio, and video, by learning from existing data. It does this by training models on large datasets and then using those models to generate novel outputs that resemble the data it was trained on.

- In essence, generative AI learns from examples and then uses that knowledge to create something new, similar to how a human artist might learn from studying existing art and then create their own unique pieces.

Crafting Audit Checklist for different Audits using Generative AI

- Automate account reconciliation
- Maintain compréhensive digital audit trails
- Establishment and enforce consistent Financial polices
- Implement AI power error detection
- Fraud detection and prevention
- Prioritize data security and privacy
- Maintain accurate and up-to-date financial records
- Conduct periodic self-audits
- Foster open communication with auditors
- Stay current on regulatory changes

Firewall Configuration

Logical/Technical Risks

- Logical risks refer to vulnerabilities and threats related to the logical components of an information system, including access control mechanisms, authentication processes, software vulnerabilities, and logical pathways that data follows within a system.

- These risks arise from improper configurations, weak policies, or flawed software, open internet, malicious codes, potentially leading to data breaches, improper segregation of duties, and operational disruptions.

Firewalls

- A firewall is a critical security device that monitors and controls incoming and outgoing traffic based on predefined security rules. Packet-filtering firewalls analyze data packets based on IP and port, while stateful inspection firewalls keep track of active sessions to decide packet permissions.

- Application firewalls focus on specific application data, and Next-Generation Firewalls (NGFWs) integrate advanced features like deep packet inspection and threat intelligence.

Firewall Configuration

- Change Default Setting, like password, name of the router etc.
- Update Firmware
- Enable Logging & Monitoring
- IP Addressing
- Defining Rules (Access Controll List)
- Enable Services (VPN, Proxy, or DHCP)
- Thorough Testing
- Regular Monitoring

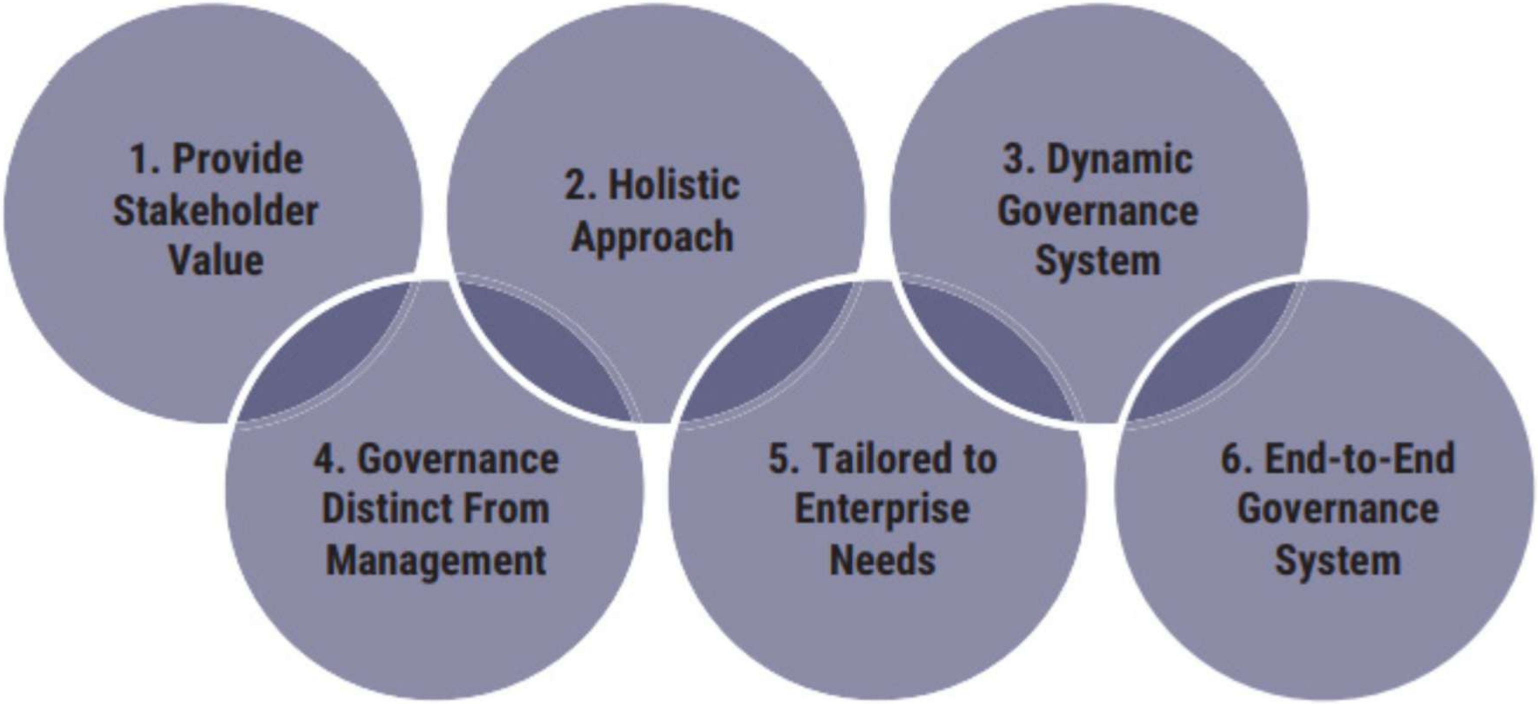
COBIT 2019

COBIT 2019

- Control Objectives for Information and Related Technologies (COBIT) version 2019 defines the design factors that should be considered by the enterprise to build a best fit governance system and addresses governance issues by grouping relevant governance components into governance and management objectives that can be managed to the required capability levels.

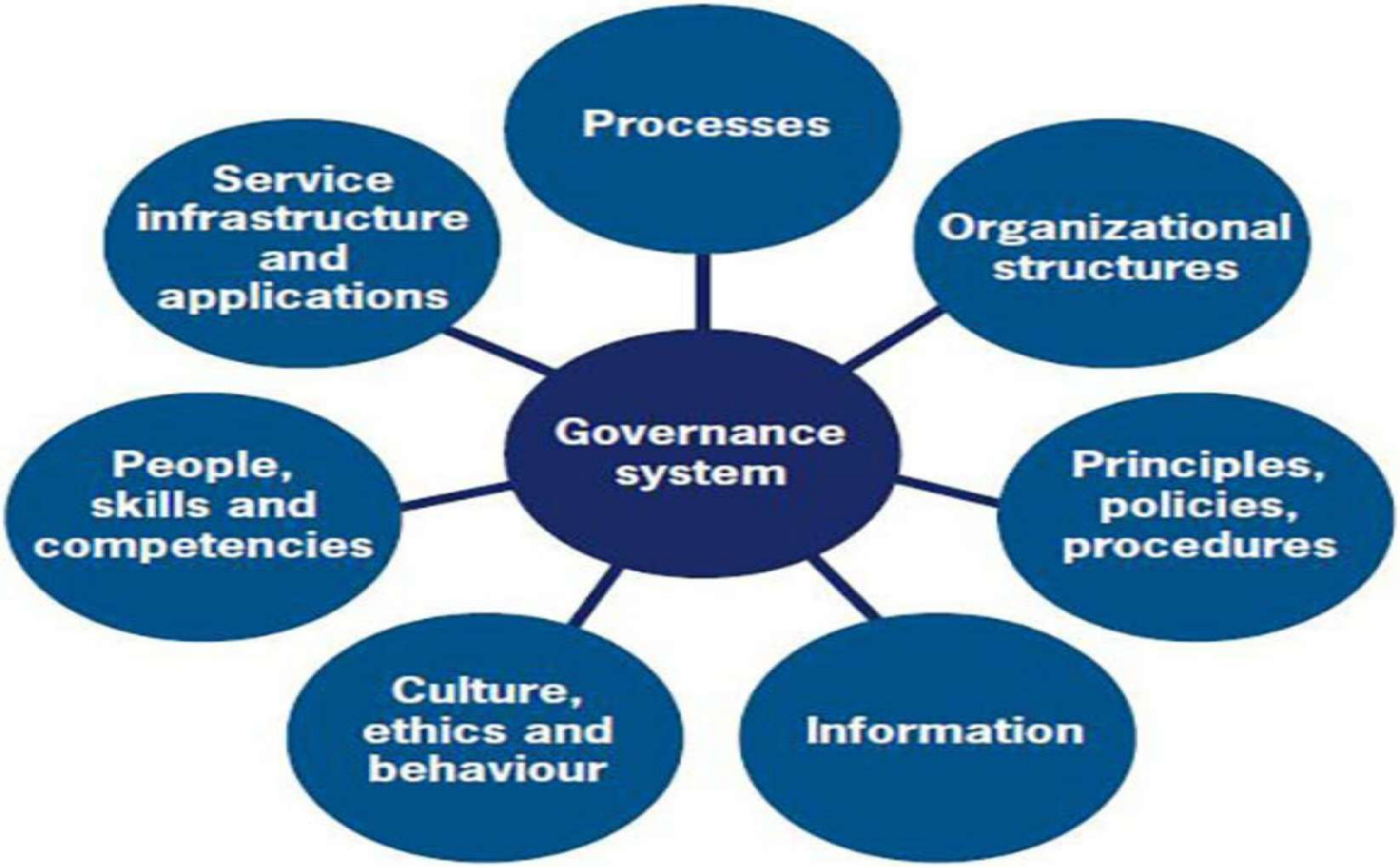
- COBIT helps organizations meet business challenges in regulatory compliance, and risk management and align their strategy with regulatory objectives.

Six Principles of COBIT 2019



1. Provide Stakeholder Value
2. Holistic Approach
3. Dynamic Governance System
4. Governance Distinct From Management
5. Tailored to Enterprise Needs
6. End-to-End Governance System

Components of COBIT 2019


Processes
Service infrastructure and applications
Organizational structures
Governance system
People, skills and competencies
Principles, policies, procedures
Culture, ethics and behaviour
Information

GDPR

GDPR

- The General Data Protection Regulation (GDPR) is a comprehensive data protection law enacted by the European Union (EU) that came into effect on May 25, 2018.

- It is designed to protect the privacy and personal data of individuals within the EU, setting a high standard for data protection globally.

- GDPR applies to all organizations that process the personal data of EU citizens, regardless of where the organization is based, making it one of the most far-reaching data protection laws in the world.

Key Provisions of GDPR

1. Scope and Applicability

- *Global Reach*: GDPR applies not only to organizations within the EU but also to non-EU organizations that offer goods or services to, or monitor the behavior of, EU data subjects.

- *Personal Data:* GDPR defines personal data broadly to include any information that can identify an individual, directly or indirectly, such as names, addresses, email IDs, IP addresses, and biometric data.

Key Provisions of GDPR

2. Data Subject Rights

- *Right to Access:* Individuals have the right to access their personal data held by an organization and understand how it is being used.

- *Right to Erasure (Right to be Forgotten):* Individuals can request the deletion of their personal data under certain conditions, such as when the data is no longer necessary for the purposes for which it was collected.

- *Right to Data Portability:* GDPR allows individuals to obtain and reuse their personal data across different services.

Key Provisions of GDPR

2. Data Subject Rights

- *Right to Object:* Individuals can object to the processing of their personal data for specific purposes, such as direct marketing.

3. Data Protection Principles

- *Lawfulness, Fairness, and Transparency*: Organizations must process personal data lawfully, fairly, and transparently.

- *Purpose Limitation*: Data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

Key Provisions of GDPR

3. Data Protection Principles

- *Data Minimization:* Only data that is necessary for the specified purpose should be collected.

- *Accuracy:* Personal data must be accurate and kept up to date*.*

- *Storage Limitation: Personal data should not be kept longer than necessary.*

Key Provisions of GDPR

3. Data Protection Principles

- *Integrity and Confidentiality:* Personal data must be processed securely to protect against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

4. Data Breach Notifications

- Obligation to Report: Organizations must report data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to individuals' rights and freedoms.

Key Provisions of GDPR

5. Penalties

- *Significant Fines:* Non-compliance with GDPR can result in hefty fines—up to €20 million or 4% of the organization’s global annual turnover, whichever is higher.

Relevence of GDPR in India

1. Impact on Indian Business

- *Global Operation*
- *Competitive advantage*

2. Influence on Indian Data Protection Laws

- Shaping Domestic Legislation
- Harmonization with Global Standards

Relevance of GDPR in India

3. Competitive Challenges

- *Operational Challenges*
- *Data Sovereignty and Localization*

New Generation Cyber Frauds

New Generation Cyber Frauds

- *FinTech Frauds*
- *Digital Arrest*
- *SIM cloning*
- *Organization Cyber Frauds*
- *Online Frauds*

Cyber Frauds Detection & Controls

- *Strong Organizational Policies*
- *Strong Organizational Guidelines*
- *User / Employee Trainings*
- *Regular & Continuous Monitoring*
- *Regular Audit*
- *Awareness*

Cyber Frauds Detection & Controls

- *Use of AI Tools for Analysis & Analytics*
- *Regular updates and patching of mobiles and computer devices*
- *Beware of Phishing and spear Phishing attacks*
- *Beware of Social Engineering Attacks*
- *Refer to the Guidelines of RBI and relevant banks*

Business Continuity Planning

Business Continuity Planning

- *Incident:* An incident, in the context of information system continuity, refers to any event or occurrence that disrupts normal operations, threatens the confidentiality, integrity, or availability of information assets, or potentially impacts the organization’s ability to conduct business. Incidents can range from minor technical issues to major security breaches.

- An incident is typically characterized by its potential to cause harm, financial loss, reputational damage, or regulatory non-compliance.

Business Continuity Planning

- *Disaster:* A disaster is a sudden, catastrophic event that causes significant disruption, damage, or loss to an organization or community. Disasters can be natural, such as earthquakes, floods, or hurricanes, or man-made, such as cyber-attacks, industrial accidents, or terrorist activities.

- Effective disaster management involves preparedness, immediate response, and recovery efforts to minimize impact, protect lives and assets, and ensure a swift return to normal operations.

Business Continuity Planning

- *Incident Response (IR) Plan:* An IR Plan is a set of procedures and guidelines designed to detect, respond to, and recover from security incidents or breaches. The IR Plan aims to manage and mitigate the impact of incidents, ensuring a swift and effective response.

- It includes steps for identifying incidents, containing and eradicating threats, recovering affected systems, and learning from the incident to prevent future occurrences.

Business Continuity Planning

- *Business Continuity Plan (BCP):* A Business Continuity Plan (BCP) is a strategic framework designed to ensure that an organization can continue operating during and after a disruption. It outlines procedures and instructions an organization must follow in the face of disaster, covering business processes, assets, human resources, and business partners.

- The BCP aims to minimize downtime and maintain essential functions, ensuring that critical operations can continue with minimal impact and that recovery is swift and efficient.

Business Continuity Planning

- *Business Continuity Management (BCM):* Business Continuity Management (BCM) is a holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause. It provides a framework for building organizational resilience and the capability for an effective response.

- BCM involves planning and preparation to ensure the continuity of critical business functions during and after a crisis, disaster, or any disruptive event, emphasizing risk management, recovery strategies, and ongoing management.

Business Continuity Planning

- *Business Impact Analysis (BIA):* Business Impact Analysis (BIA) is a systematic process to identify and evaluate the potential effects of disruptions to critical business operations. It helps determine the essential functions of an organization, the resources required to maintain them, and the potential financial and operational impacts of an interruption.

- The BIA informs the development of recovery strategies and prioritizes recovery efforts to minimize downtime and ensure business continuity.

Business Continuity Planning

- *Recovery Time Objective (RTO):* RTO defines the maximum acceptable time for restoring a system or process after a disruption, i.e. it is user's tolerance to downtime. It represents how quickly an organization must recover to maintain business continuity after an unfavorable incident.

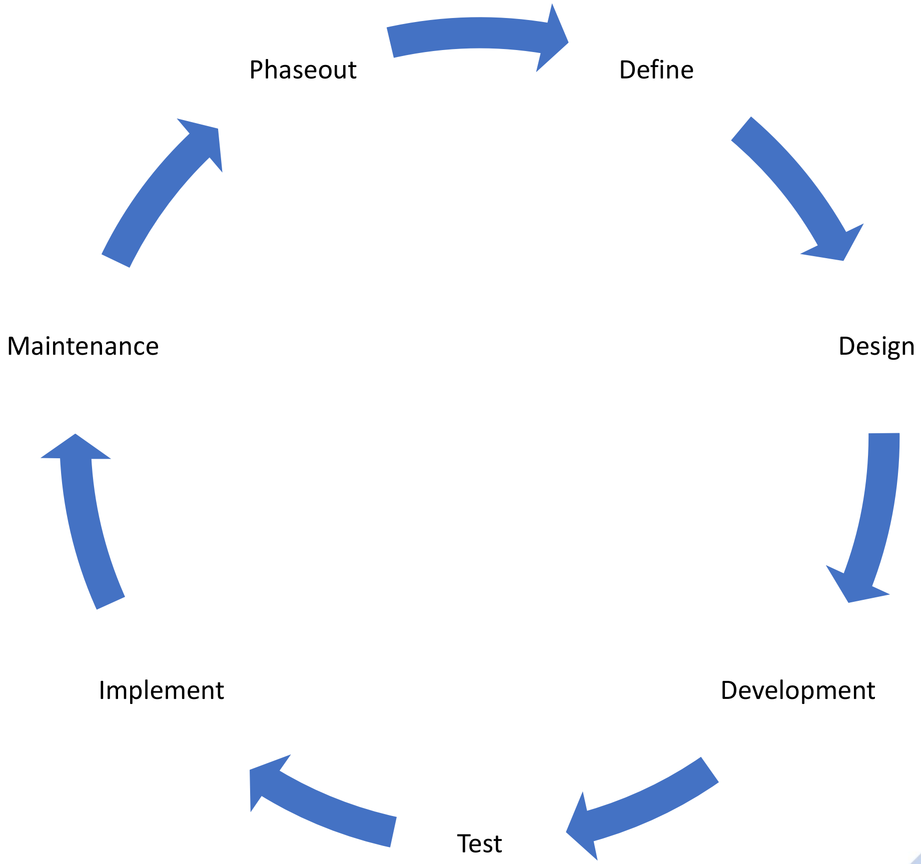
- *Recovery Point Objective (RPO):* RPO defines the maximum acceptable amount of data loss measured in time, following a disruptive event. It represents the point in time to which systems and data must be recovered to resume normal operations. In practical terms, RPO answers the question: "How much data can the organization afford to lose?" For example, an RPO of 4 hours means the system should be restored to a state no older than 4 hours before the disruption occurred.

Business Continuity Planning Testing

- *Plan Review*
- *Walkthrough Test*
- *Tabletop Exercise*
- *Simulation Test*
- *Parallel Test*
- *Full Interruption Test*

Automation of MSME (SDLC)

Software Development Life Cycle



Phaseout

Define

Maintenance

Design

Implement

Development

Test

SDLC

- *Define:* This phase involves defining requirement and gathering information related to software and security requirements from the stakeholders, such as customers, end-users, and business analysts.

- *Designing:* In this phase, the software design is created, which includes the overall architecture of the software, data structures, and interfaces. It has two steps:

  1. High-level design (HLD): It gives the architecture of software products.
  2. Low-level design (LLD): It describes how each and every feature in the product should work and every component.

SDLC

- *Development:* This is the actual coding or implementation phase, where the software is built according to the design specifications.

- *Testing:* The software is thoroughly tested to identify and fix any bugs or defects. This includes unit testing, integration testing, system testing, and user acceptance testing.

- *Implementation:* The tested software is released and implemented to the production environment, making it available to users.

SDLC

- *Maintenance:* After implementation, the software is monitored, maintained, and updated to address any issues, add new features, or adapt to changing user needs. .

- *Phase out:* The software is phased out when software is formally decommissioned and replaced by a newer system or technology. The phase-out phase is a critical part of the SDLC, ensuring a smooth transition from an old system to a new one and minimizing disruption to business operations.

Cloud Service Provider – SLA & Cloud Audit

CSP – Service Level Agreement

- *SLA:* In cloud computing, a Service Level Agreement (SLA) is crucial for defining the terms and conditions of the service provided by a cloud provider to a customer.

- It ensures accountability, sets clear expectations for performance and availability, and outlines consequences for non-compliance.

- Essentially, an SLA acts as a contract, outlining the responsibilities of both the provider and the customer, and protecting the customer's interests in case of service disruptions or failures.

CSP – Service Level Agreement

1. *Defining Service Expectations:*

    - *Performance Metrics*
    - *Availability*
    - *Security*
    - *Support*

2. Accountability and Consequences:

- *Liabilities*
- *Remedies*
- *Monitoring & Reporting*

CSP – Service Level Agreement

3. *Building Trust & Confidence:*

    - *Transparency*
    - *Risk Mitigation*
    - *Long -Term Relationships*

4. *Customization & Flexibilities:*

    - *Tailored Agreement*
    - *Specific Needs*

CSP – Audit

- *A cloud audit is a systematic assessment of a cloud computing environment to evaluate its security, performance, and compliance with relevant regulations and standards.*

- *It's typically conducted by an independent third-party auditor or sometimes by internal IT professionals.*

- *The goal is to identify vulnerabilities, inefficiencies, and areas for improvement in the cloud environment.*

CSP – Audit

- *Assessment of Controls*
- *Focus Areas*
- *Verification of Compliance*
- *Risk Identification*
- *Shared Responsibility*

THANK YOU