Law, Governance & Compliance

Dr. Srinivas Josyula


ARE YOU SURE WE NEED GOVERNANCE?..
ABSOLUTELY BUT ONLY IF WE IMPLEMENT IT AT CONSIDERABLE COST...
CLEMENT

Agenda

- **Enterprise Governance**
- **Governance and Management**
- **IT Act/ NCIIPC**
- **MeitY - Frameworks / Standards Policies and Guidelines**
- **Compliance**

Enterprise Governance

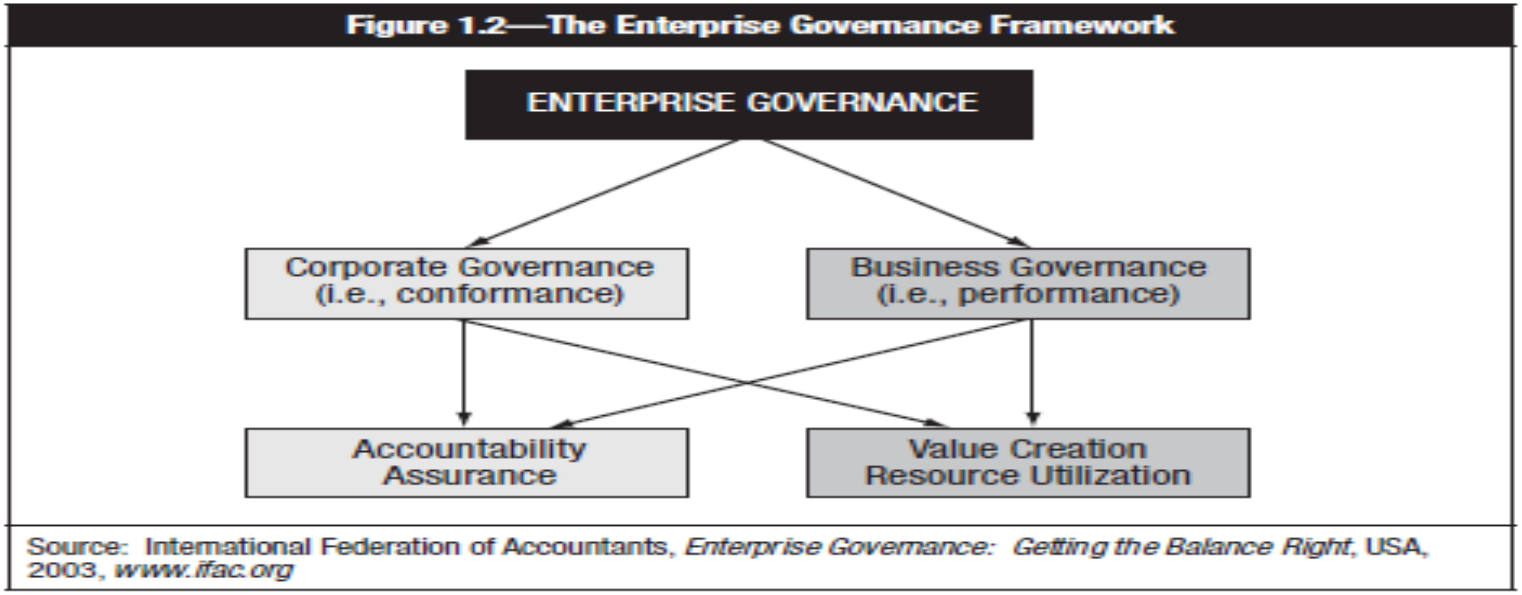
A set of responsibilities and practices exercised by the board and executive management with ***the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately,*** *and* ***verifying that the enterprise's resources are used responsibly.***

Conformance and Performance

International Federation of Accountants (IFAC) states that "**enterprise governance constitutes the accountability framework of the organization**" and identifies two dimensions namely :

1. Conformance and
2. Performance

They must be balanced



IT Governance

- IT governance is the responsibility of the Board of Directors and executive management. It is an integral part of enterprise governance and consists of the **leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives**

- IT governance is the organizational capacity exercised by the Board, executive management and IT management **to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT.**

Principles of Governance systems

- Provide Stakeholder value
- Holistic approach
- Dynamic process
- Governance distinct from Management
- Customised to enterprise needs
- End to End coverage

Governance and Management Compared

Governance

Evaluate, Direct, Monitor and Control an enterprise

Enable enterprises to create value for their stakeholders or promote the creation of value

Includes:

- Financial accountability and oversight
- Operational effectiveness
- Legal and regulatory compliance
- Adoption of fair labor practices
- Social responsibility
- Governance of IT investment, operations and control

Management

Focus on Planning, Building, Running and Monitoring

Ensure alignment with defined goals and objectives established by the governing body

Ensure enterprise strategic vision achievement as directed by governing body

- Create value for enterprise
- Optimal resources utilization

Governance of Key Assets, Including IT

The core focus of enterprise governance are these six asset types[4]:

1. Human Assets
2. Financial Assets
3. Physical Assets
4. Intellectual property (IP)
5. Information and IT Assets
6. Relationship Assets

Governance of key assets occurs through a large number of mechanisms , e.g., structures, processes, procedures and audits

4 Weill, Peter; Jeanne Ross: *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results,* Harvard Business School Press, USA, 2004

IT Governance - Views

- Board and Senior management view it as CTO/CIO/CISO business
- Business users think it is CTO/CIO/CISO responsibility
- IT is treated in a silo and not holistically
- Most organizations lack a comprehensive IT strategy, systemic approach, processes, change management, coordination and oversight

Whose Responsibility ?

- Board?
- Senior Management?
- Business ?
- IT/ Digital Technologies and Risk – CIO/ CTO ?
- Why should the Board/Senior management bother about IT/Security readiness?

ITGI : Approach and Desired Outcomes

According to ISACA's Information Technology Governance Institute (ITGI), *Governance includes* ***the accountabilities and methods undertaken by the board of directors and executive management*** **to provide:**

1. **Strategic alignment**
2. **Risk management**.
3. **Resource management**.
4. **Performance measurement**.
5. **Value delivery**

NACD - Governance : Board of Directors Essential Practices

National Association of Corporate Directors (NACD) suggests:

1. Place IT on the board's agenda.
2. Identify leaders, hold them accountable, and ensure support for them.
3. Ensure the effectiveness of the corporation's IT policy through review and approval.
4. Assign IT to a key committee and ensure adequate support for that committee

Benefits of IT Governance

1. *An increase in share value for organizations.*
2. *Increased predictability and reduced uncertainty of business operations by lowering IT -related risks to definable and acceptable levels.*
3. *Protection from the increasing potential for civil or legal liability as a result of information inaccuracy or the absence of due care.*
4. *Optimization of the allocation of limited security resources.*
5. *Assurance of effective IT policy and policy compliance.*
6. *A firm foundation for efficient and effective risk management, process improvement, and rapid incident response.*
7. *A level of assurance that critical decisions are not based on faulty information.*
8. *Accountability for safeguarding information during critical business activities, such as mergers and acquisitions, business process recovery, and regulatory response*

Industry Practices, Standards, and Frameworks

- Several frameworks provide standards for EGIT, including:
  - COBIT
  - International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000
  - Information Technology Infrastructure Library (ITIL®)
  - Open Information Security Management Maturity Model (O-ISM3)
  - ISO/IEC 38500:2015: Information technology—Governance of IT for the organization
  - ISO/IEC 20000
  - ISO 3100:2018: Risk management—Guidelines

IT Governance Objectives

- Evaluate the IT strategy for alignment with the organization's strategies and objectives.
- Evaluate the effectiveness of IT governance structure and IT organizational structure.
- Evaluate the organization's management of IT policies and practices.
- Evaluate the organization's IT policies and practices for compliance with regulatory and legal requirements.
- Evaluate IT resource and portfolio management for alignment with the organization's strategies and objectives.
- Evaluate the organization's risk management policies and practices.
- Evaluate IT management and monitoring of controls.

IT Governance Objectives

- Evaluate the monitoring and reporting of IT key performance indicators (KPIs).
- Evaluate whether IT supplier selection and contract management processes align with business requirements.
- Evaluate whether IT service management practices align with business requirements.
- Conduct periodic review of information systems and enterprise architecture.
- Evaluate data governance policies and practices.
- Evaluate the information security program to determine its effectiveness and alignment with the organization’s strategies and objectives.
- Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices.

Considerations

IT Governance

- IT Governance and IT Strategy
- IT-Related Frameworks
- IT Standards, Policies, and Procedures
- Organizational Structure
- Enterprise Architecture
- Enterprise Risk Management
- Maturity Models
- Laws, Regulations, and Industry Standards Affecting the Organization

IT Management

- IT Resource Management
- IT Service Provider Acquisition and Management
- IT Performance Monitoring and Reporting
- Quality Assurance and Quality Management of IT

Enterprise Governance of IT

- The purpose of EGIT is to direct IT endeavors to ensure that IT aligns with and supports the enterprise's objectives and its realization of promised benefits.
- Additionally, IT should enable the enterprise by exploiting opportunities and maximizing benefits.
- IT resources should be used responsibly, and IT-related risk should be managed appropriately.

Outcomes of Governance

IT resource management

- Focuses on maintaining an updated inventory of all IT resources and addresses the risk management process

Performance measurement

- Focuses on ensuring that all IT resources perform as expected to deliver value to the business and identify risk early on. This process is based on performance indicators that are optimized for value delivery and from which any deviation might lead to risk.

Compliance management

- Focuses on implementing processes that address legal and regulatory policy and contractual compliance requirements

EGIT Good Practices

1. Business managers and boards demanding a better return from IT investments.
2. Concern over the generally increasing level of IT expenditure
3. The need to meet regulatory requirements for IT controls in areas such as privacy and financial reporting and in specific sectors such as finance, pharmaceuticals and health care
4. The selection of service providers and the management of service outsourcing and acquisition
5. IT governance initiatives that include the adoption of control frameworks and good practices to help monitor and improve critical IT activities to increase business value and reduce business risk
6. The need to optimize costs by following, where possible, standardized rather than specially developed approaches
7. The growing maturity and the consequent acceptance of well-regarded frameworks
8. The need for enterprises to assess how they are performing against generally accepted standards and their peers

Framework & Standards

- A generally accepted, business-process oriented structure that establishes a common language and enables repeatable business processes

- A standard is a mandatory requirement, code of practice or specification approved by a recognized external standards organization.
- Professional standards refer to standards issued by professional organizations, such as ISO, ISACA, and related guidelines and techniques that assist in implementing and complying with other standards.

Policies

- Policies are the high-level statements of management intent, expectations and direction.
- Well-developed high-level policies in a mature organization can remain static for extended periods.
- Management should review all policies periodically.

IS Policy Components

The information security policy may comprise a set of policies, generally addressing the following concerns:

- **High-level information security policy** — Includes statements on confidentiality, integrity and availability
- **Data classification policy** — Provides classifications and levels of control at each classification
- **End-user computing policy** — Identifies the parameters and usage of desktop, mobile and other tools
- **Access control policy** — Describes methods for defining and granting access to users of various IT resources
- **Acceptable use policy (AUP)** — Controls the use of information system resources by defining how IT resources may be used by employees

Procedures

- The documented, defined steps in procedures aid in achieving policy objectives.

- Procedures documenting business and aligned IT processes and their embedded controls are formulated by process owners.

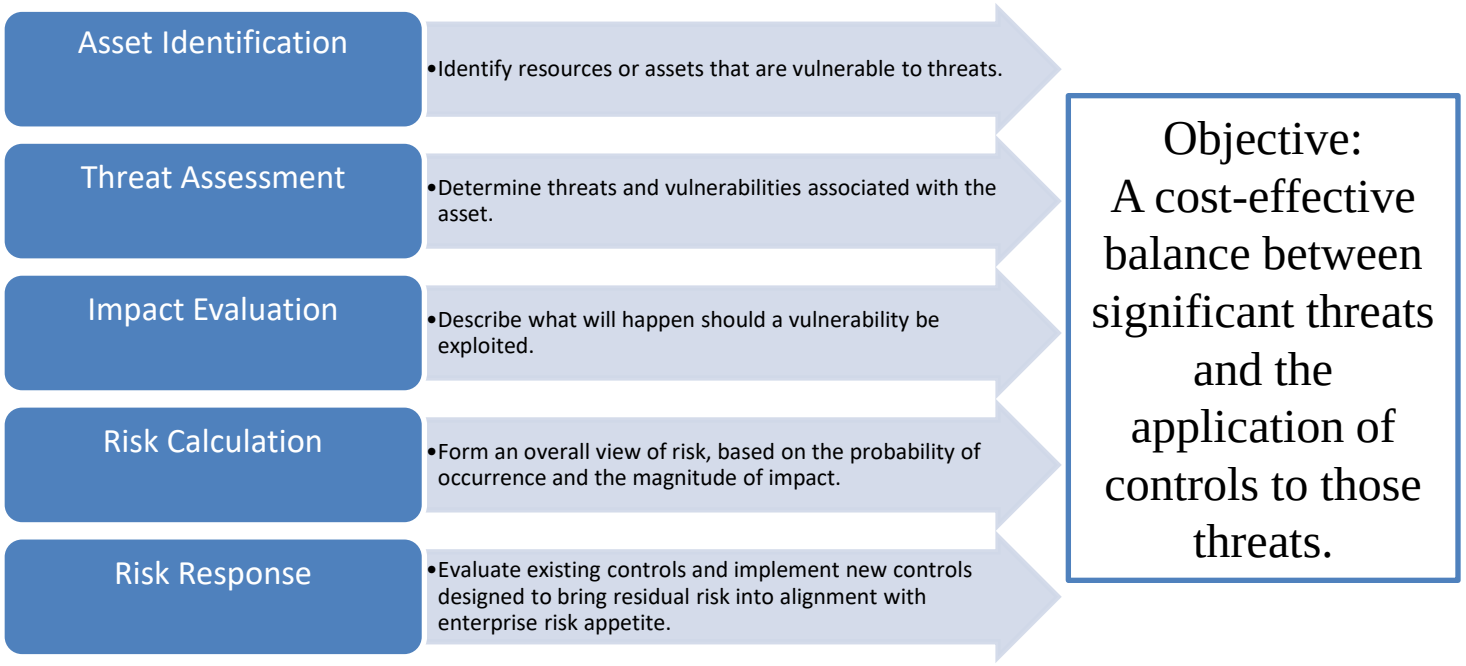
To be effective, procedures must:

- Be frequently reviewed and updated
- Be communicated to those affected by them

Guidelines

- Guidelines for executing procedures are also the responsibility of operations.
- Guidelines should contain information that will be helpful in executing the procedures. Including clarification of:
  - Policies and standards
  - Dependencies
  - Suggestions
  - Background information that may be useful
  - And tools that can be used

Enterprise Risk Management



Risk Response

Four possible options to risk are:

- Avoidance — elimination of the cause of the risk
- Mitigation — reduction of the probability of a risk's occurrence or of its impact
- Transfer — sharing of risk with partners, such as through insurance or joint ventures
- Acceptance — formal acknowledgment of the presence of risk with a commitment to monitor it

- Rejection of risk through choosing to ignore it, is not considered effective risk management. The presence of this risk response should be a red flag for the IS auditor.


Cyberlaw
information
internet
computer
software
rules
protection
access
technology
property
privacy
Legal
may
web
law
areas
licenses
bodies
aspects
intellectual

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

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.

Need…

All legal issues related to internet crime are dealt with through cyber laws. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great momentum.

Today:

- Almost all companies extensively depend upon their computers, networks and keep their valuable data in electronic form.
- Most people are using email, cell phones and use social media for communication
- Consumers are shopping online and increasingly using credit cards for shopping.
- Digital signatures and e-contracts are fast replacing conventional methods of transacting business.
- Almost all transactions in shares are in demat form.
- Government forms including income tax returns, company law forms etc. are now filled in electronic form.
- Cyber crime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc are becoming common.
- Even in "non-cyber crime" cases, important evidence is found in computers / cell phones e.g. in cases of divorce, murder, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency etc.

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

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.

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)*

Recognising Electronic Records and Electronic (Digital) Signatures [Sections 4 and 5]

- Recognizing electronic records is the basic pre-requisite of making.
- e- Business/ e- Governance initiatives successful.
- Authentication of electronic records by means of digital signatures.

Retention of Electronic Records (Section 7) & Audit of Documents in Electronic form (Section 7A)

The Act has created certain stringent conditions for retention of electronic records.

Under section 7 of the Act, onus is on the person(s) as well as on the Government to fulfill the **following conditions** for retention of electronic records:

(a) accessibility so as to be usable for a subsequent reference;
(b) retention in the format in which it was originally generated, sent or received or in a format, which can be demonstrated, to represent accurately the information originally generated, sent or received;
(c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record.

It is important to note that non-compliance of any aforesaid condition may render the ***electronic record inadmissible in the court of law*.**

For effective delivery of services electronically (EDS), ***proper accessibility, retention, origin, destination, date and time of despatch or receipt of electronic records is mandatory***.

Digital Signatures/PKI

Certifying Authorities (CA) has been granted a license to issue a digital signature certificate under Section 24 of the Indian IT-Act 2000.

Licensed CA's are :

1. NIC –
2. IDRBT
3. Safescricpt CA services, Sify Communications Ltd
4. (n) Code Solution Services
5. E-Mudhra
6. CDAC
7. NSDL
8. Capricorn

Civil liability

Section 43 : deals with Penalties, Compensation and Adjudication, which is a major significant step in the direction of combating data theft, claiming compensation, introduction of security practices etc.,

This Section addresses the civil offence of theft of data.

Earlier in the ITA -2000 the maximum damages under this head was Rs.1 crore, which (the ceiling) was since removed in the ITAA 2008.

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

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.

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.

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.

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.

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".

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.

Digital Forensics

- A major programme has been initiated on development of cyber forensics specifically cyber forensic tools, setting up of infrastructure for investigation and training of the users, particularly police and judicial officers in use of this tool to collect and analyze the digital evidence and present them in Court.

- Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) are involved in providing basic and advanced training of Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analyzing and presenting digital evidence.

- Cyber forensic training lab has been set up at Training Academy of Central Bureau of Investigation (CBI) to impart basic and advanced training in Cyber Forensics and Investigation of Cyber Crimes to Police Officers associated with CBI.

- In addition, Government has set up cyber forensic training and investigation labs in Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir.

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)

IT Act, 2000

Enabling Act

Facilitating Act

Regulatory Act

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**:

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

Policies and Guidelines

- Info-sec Policy
- Info-sec including Cyber Security policy
- Cloud Policy
- BYOD policies
- BCP, DC, DR and near-site policy
- Back up, restore, and archival policy
- Internet based Applications and Services policy

and many more

Issues to be considered

- Governance issues
- Technology issues
- Operational issues
- Implementation issues
- Integration issues
- Legal Issues

What is required is

- Risk Based Approach
- Assess, Understand, Categorise, Quantify and Mitigate

- First step is to look at Effective, Enforceable and Implementable Policies and Guidelines

Comprehensive Cyber Security Audit

- To ensure C,I and A of Information Systems and Resources
- To investigate possible security vulnerabilities and incidents in order to ensure conformance to the Bank's Security policies
- To ensure software systems designed and developed conforms to the Bank's software implementation policy
- To ensure changes made to any systems conforms to the Bank's change control and change management policy
- To ensure regular backup of data and business critical systems are taken and preserved
- To ensure restore of both data and full system is carried out on a regular basis so that data integrity is addressed and the Bank is prepared for any possible disaster
- To monitor user and system activity where appropriate
- To investigate security incidents as and when required

E- Gov Standards

Standards in e-Governance are a high priority activity, which will help ensure sharing of information and seamless interoperability of data across e-Governance applications. MEITY is promoting the usage of Open Standards to avoid any technology lock-ins. An Institutional Mechanism has been setup under NeGP to evolve/adopt Standards for e-Governance.

Some of the key priority areas of immediate concern that have been identified for standardization are:

- Policy on Open Standards
- Metadata & Data Standards
- Localisation and Language Technology Standards
- Information Security
- Technology Standards on Interoperability
- Biometrics
- Digital Signatures
- Enterprise Architecture
- Quality & Documentation

http://egovstandards.gov.in/

Open Data

- It is widely acknowledged that sharing of data and relevant information in public domain is a major step towards enhancing transparency and accountability in governance

- ***Open Data is Data that anyone can Access, Use or Share*** (UN) . It is published in accessible formats suited to researchers and statisticians.

- ***Open data is data that anyone can access, use and share.*** Governments, businesses and individuals can use open data to bring about social, economic and environmental benefits. (EU)
- Open data becomes usable when made available in a common, machine-readable format.
- Open data must be licensed. Its license must permit people to use the data in any way they want, including transforming, combining and sharing it with others, even commercially.

Open Data Policy of India

- **National Data Sharing and Accessibility Policy** (NDSAP) was published by Dept of Science and Technology in 2012 through a Gazette notification:
- Data collected or developed through public investments, when made publicly available and maintained over time, their potential value could be more realized.
- There has been an increasing demand by the community, that such data collected with the deployment of public funds should be made more readily available to all, for enablind rational debate, better decision making and use in meeting civil society needs
- Back ground : RTI Act and Sect 4(2) of the RTI Act reads:
- "**It shall be a constant endeavor of every public authority to take steps in accordance with the requirements of clause (b) of subsection (1) to provide as much information suo motu to the public at regular intervals through various means of communication, including internet, so that the public have minimum resort to the use of this Act to obtain information"**

Definitions

- Data , Data Archive, Data Generation, Data Set, Geo spatial Data, Information, Meta Data, Negative list , Restricted Data, Sensitive Data, Sharable data, Standards

(Note : * *Refer to Gazette notification*)

Principles

The principle on which data sharing and accessibility need to be based include:

1. **Openness**
2. **Flexibility**
3. **Transparency**
4. **Legal Conformity**
5. **Protection of Intellectual Property**
6. **Formal Responsibility**
7. **Professionalism**
8. **Standards**
9. **Interoperability**
10. **Quality**
11. **Security**
12. **Efficiency**
13. **Accountability**
14. **Sustainability and Privacy**

Applicability

1. NDSAP is designed so as to apply to all sharable non-sensitive data available in digital or analog formats but generated using public funds by various Ministries/ Departments/ Subordinate offices/organizations/ agencies of GoI

2. Designed to promote data sharing ane enable access to GOI owned data for national planning and development

3. NDSAP ***aims to provide platform for proactive and open access to the data generated through public funds.***

4. NDSAP applies to all data and information ***created, generated, collected and archived*** using public funds provided by GoI

NDSAP

Benefits:

1. Maximising Use
2. Avoiding duplication
3. Maximised Integration
4. Ownership Information
5. Better decision making
6. Equity of Access

Data Classification : Shareable data and Non sharable date (Negative list to be reviewed periodically

Types of Access:

1. Open Access
2. Registered Access
3. Restricted Access

* Monetization of Data

Technology for Sharing and Access : State of the art DWH and Data Archive with OLAP provides

NDSAP

Features of DWH:

1. User friendly interface
2. Dynamic/ Pull down menus
3. Search based reports
4. Secured Web access
5. Bulletin Board
6. Complete Meta data
7. Parametric and Dynamic report in exportable formst

IPR/ Ownership: Data ownership lies with the department. Legal framework of this policy will be aligned with various Acts and rules covering the data.

Pricing : Pricing of data, if any, would be decided by data owners as per govt policy

* Monetization of Data (for Registered and Restricted Access Data)

NDSAP Implementation

Policy Owner for NDSAP : - DST;

Standards and guidelines : MeitY

Implementation : NIC

Budgetary incentives for data owners for increasing open access to shareable date

Expenditure for data owners and data managers for analog to digital conversion, data refinement, data storage, quality upgradation etc, support for data management by GoI

OGD Platform India

- https://data.gov.in , is set up by NIC, in compliance with NDSAP of India
- Developed using Open Source Stack (Digital India initiative 6 : Information for All)
- Features of the plat form : user friendly interface with dynamic/ pull down menus, search based reports, secured web access, bulletin boards, based on Dublin core meta data standards and parametric & dynamic reports in exportable format.
- Platform has a rich mechanism for citizen engagement, citizens can express their need for specific data sets or apps, allows citizens to rate the quality of datasets, seek clarification or information from nodal officers of participating govt entities.
- Community Engagement encourages citizen participation with OGD
- Community Portal has been launched (https://community.data.gov.in) whch facilitates knowledge sharing, contribute through blogs , info-graphics, visualisation etc
- Awareness sessions: Trainings and state level workshops
- Citizens can directly write to CDO/ Data Controller and seek clarifications
- API's to query data sets
- Alert Services can be subscribed for catalogs
- Citizen Rating for resources (data sets/ apps) on Quality, Accesability and Usability

MeitY Policies (select)

1. Draft National Data governance framework policy , May 2022
2. Meghraj policy
3. “Policy on Adoption of Open Source Software for Government of India”
4. Email Policy
5. Policy on Use of IT Resources
6. NDSAP
7. Social media framework and policies
8. Notification dated, the 25th February, 2021 G.S.R. 139(E): the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

https://www.meity.gov.in/content/policies-0

MeitY Guidelines (select)

1. Guidelines for Indian Government websites

https://guidelines.india.gov.in/compliance-matrix/#1585239298471-fd39317c-8b66

1. Guidelines for procurement of cloud services
2. Application Form & Guidelines for submission of proposals for use of Aadhaar authentication under the Aadhaar Authentication for Good Governance Rules,2020
3. Guidelines for Strategic Control in Outsourced Projects, 2010
4. Application Development & Re-Engineering Guidelines for cloud-ready applications
5. Policy Guidelines for State Data Centre (SDC)
6. Guidelines for Strategic Control in Outsourced Projects
7. Guidelines for Setting up of Dedicated Project Teams

https://www.meity.gov.in/content/guidelines-0

TS Govt ITE&C Policies (select)

1. 2nd ICT Policy 2021-26
2. Telangana Open Data Policy
3. Telangana Data Analytics Policy
4. Telangana Data center policy
5. Telangana IoT policy
6. Telangana Cyber security policy
7. E- waste managementt policy

8. Social media framework and policies
9. Notification dated, the 25th February, 2021 G.S.R. 139(E): the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

https://it.telangana.gov.in/investor-info/it-policy/

Q&A