Regulatory Framework on AI, Cyber Security and Cyberspace

Lesson 5

KEY CONCEPTS

■ E-Governance ■ RBI Regulations ■ Artificial Intelligence ■ Cyber Security ■ Cyberspace ■ SEBI Regulations ■ International Principles

Learning Objectives

To understand:

- How to focus on major themes pertaining to artificial intelligence and cybersecurity-crime and its inter-relationship
- The responsibility and function of regulatory authority like SEBI and RBI governing the issues related to Artificial Intelligence and cyberspace
- To study international legal regime related to development of modern technology tools like AI to improve the existing position of digital security

Lesson Outline

E-GOVERNANCE IN INDIA

Meaning of e-Governance

E-Governance as the name suggest is made up of two words. "E" and "Governance". Hence to understand the concept of e-Governance, we shall first understand the meaning of Governance. Governance is the process of making and enforcing decisions within an organization or society.[1] It is the process of interactions through the laws, social norms, power (social and political) or language as structured in communication of an organized society over a social system (family, social group, formal or informal organization, a territory under a jurisdiction or across territories). It is usually done by the government of a state. Conceptually, governance can be defined as the rule of the rulers, typically within a given set of rules. One might conclude that governance is the process – by which authority is conferred on rulers, by which they make the rules, and by which those rules are enforced and modified. Hence with "e" in e-Governance which stands for 'electronic' - is basically associated with carrying out the functions and achieving the results of governance through the utilization of ICT (Information and Communications Technology).

However, this would require the government to change itself – its processes, its outlook, laws, rules and regulations and also its way of interacting with the citizens. It would also require capacity building within the government and creation of general awareness about e-Governance among the citizens.

The Council of Europe referred to e-Governance as:

- the use of electronic technologies in three areas of public action;
- relations between the public authorities and civil society the functioning of the public authorities at all stages of the democratic process (electronic democracy);
- the provision of public services (electronic public services).

In a broader sense, 'e-governance' is all about reform in governance facilitated with the inventive and resourceful use of ICT.

Evolution of E-Governance

Electronic Governance, popularly known as e-governance. E-Governance originated in India during the 1970s with a focus on in-house government applications in the areas of defence, economic monitoring, planning and deployment of ICT to manage data intensive functions related to elections, census, tax administration etc. It is a distinct dimension of New Public Management (NPM) which has gained considerable momentum since the early 1990s. The term 'e-Governance' is often used to describe the networking paradigm and its decentralizing and communicatory implications. E-governance as competing paradigms is the process of enabling governance experts using Information and Communication Technology (ICT) to make governance effective for citizens in terms of efficiency, transparency, and cost-effectiveness.

- The establishment of the Department of Electronics in 1970 was the first major step towards e-governance in India as it brought 'information' and its communication to focus.
- National Informatics Centre (NIC) established in 1977, launched the District Information System program to computerize all district offices in the country
- The main thrust for e-governance was provided by the launching of NICNET in 1987 – the national satellite-based computer network.

Demands of transparency, ethics, rightfulness, access to justice, eradication of corruption and other related issues along with welfare driven political leadership, other associated governments, capacity building needs

1. Compare: Bevir, Mark (2012). Governance: A very short introduction. Oxford, UK: Oxford University Press. ISBN 9780191646294

and perceived citizen expectations and all has contributed to adoption of e-government methods for good governance.

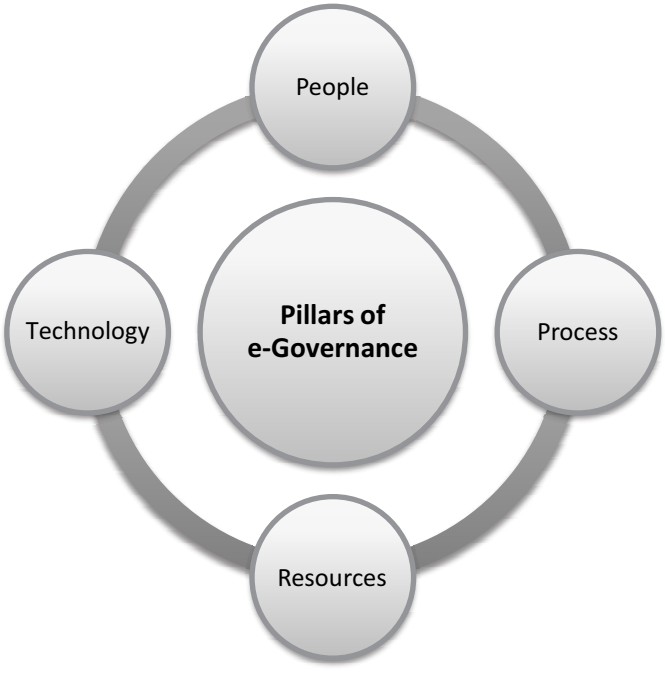
At a broader level, apart from delivering government services, e-governance includes integration of several stand-alone systems and services between ***Government-to-Citizens (G2C), Government-to-Business (G2B), and Government-to-Government (G2G)*** as well as back-office processes and interactions within entire government framework.

The overall objective of such e-governance is to enable the administration to provide services with affordable cost and optimum time to the end user (citizen).

Objectives

- Better service delivery to citizens.
- Ushering in transparency and accountability.
- Empowering people through information.
- Improve efficiency within Government i.e. between center-state or inter-states.
- Improve interface with business and industry.

Pillars of e-Governance



Types of Interaction in e-Governance

- G2G: Government to Government
- G2C: Government to Citizen
- G2B: Government to Business
- G2E: Government to Employee

Electronic governance or e-governance is adopted by countries across the world. In a fast-growing and demanding economy like India, e-governance has become essential. The rapid growth of digitalisation has led to many governments across the globe to introduce and incorporate technology into governmental processes. Electronic governance or e-governance can be defined as the usage of Information and Communication Technology (ICT) by the government to provide and facilitate government services, exchange of information, communication transactions and integration of various standalone systems and services.

In other words, it is the use of technology to perform government activities and achieve the objectives of governance. Through e-governance, government services are made available to citizens and businesses in a convenient, efficient and transparent manner. Examples of e-governance include Digital India initiative, National Portal of India, Prime Minister of India portal, Aadhaar, filing and payment of taxes online, digital land management systems, Common Entrance Test etc.

Types of interactions in e-Governance

e-Governance can take place in four major types of interactions, apart from the processes and interactions in the back-office, within the government framework:

Government to Government (G2G)

Information is exchanged within the government i.e., either, between the central government, state government and local governments or between different branches of the same government.

Government to Citizen (G2C)

The citizens have a platform through which they can interact with the government and get access to the variety of public services offered by the Government.

Government to Businesses (G2B)

The businesses are able to interact with the government seamlessly with respect to the services of the government offered to businesses.

Government to Employees (G2E)

The interaction between the government and its employees occurs in an efficient and speedy manner.

National E-governance Plan[2]

The National e-Governance Plan (NeGP) has been formulated by the Department of Electronics and Information Technology (DEITY) and Department of Administrative Reforms and Public Grievances (DARPG) in 2006.

The NeGP aims at improving delivery of Government services to citizens and businesses with the following vision: "Make all Government services accessible to the common man in his locality, through common service delivery outlets and ensure efficiency, transparency & reliability of such services at affordable costs to realise the basic needs of the common man." The National e-Governance Plan (NeGP), takes a holistic view of e-Governance initiatives across the country, integrating them into a collective vision, a shared cause. Around this idea, a massive countrywide infrastructure reaching down to the remotest of villages is evolving, and large-scale digitization of records is taking place to enable easy, reliable access over the internet. The ultimate objective is to bring public services closer home to citizens, as articulated in the Vision Statement of NeGP.

2. Reproduced from E-governance in India: Concept, Initiatives and Issues, Insignts on India, 2018

The Government approved the National e-Governance Plan (NeGP), comprising of 27 Mission Mode Projects and 8 components, on May 18, 2006. In the year 2011, 4 projects - Health, Education, PDS and Posts were introduced to make the list of 27 MMPs to 31Mission Mode Projects (MMPs). The Government has accorded approval to the vision, approach, strategy, key components, implementation methodology, and management structure for NeGP. However, the approval of NeGP does not constitute financial approval(s) for all the Mission Mode Projects (MMPs) and components under it. The existing or ongoing projects in the MMP category, being implemented by various Central Ministries, States, and State Departments would be suitably augmented and enhanced to align with the objectives of NeGP.

In order to promote e-Governance in a holistic manner, various policy initiatives and projects have been undertaken to develop core and support infrastructure. The major core infrastructure components are State Data Centres (SDCs), State Wide Area Networks (S.W.A.N), Common Services Centres (CSCs) and middleware gateways i.e National e-Governance Service Delivery Gateway (NSDG), State e-Governance Service Delivery Gateway (SSDG), and Mobile e-Governance Service Delivery Gateway (MSDG). The important support components include Core policies and guidelines on Security, HR, Citizen Engagement, Social Media as well as Standards related to Metadata, Interoperability, Enterprise Architecture, Information Security etc. New initiatives include a framework for authentication, viz.

e-Pramaan and G-I cloud, an initiative which will ensure benefits of cloud computing for e-Governance projects.

Central government initiatives as mission mode projects (MMP)

- ***e-office***

  The Government of India has recognized the need to modernize the Central Government offices through the introduction of Information and Communications Technology. e-Office is aimed at increasing the usage of work flow and rule-based file routing, quick search and retrieval of files and office orders, digital signatures for authentication, forms and reporting components.

- ***Immigration, Visa and Foreigner's Registration & Tracking (IVFRT)***

  India has emerged as a key tourist destination, besides being a major business and service hub. Immigration Check Post is the first point of contact that generates public and popular perception about the country, thus necessitating a state of the art system for prompt and user-friendly services.

- ***Unique Identification Number (UID)***

  The unique identification project was conceived as an initiative that would provide identification for each resident across the country and would be used primarily as the basis for efficient delivery of welfare services. It would also act as a tool for effective monitoring of various programs and schemes of the government.

- ***Pensions***

  The pensions MMP is primarily aimed at making the pension/ retirement related information, services and grievances handling mechanism accessible online to the needy pensioners, through a combination of interactive and non-interactive components, and thus, help bridge the gap between the pensioners and the government.

- ***Banking***

  The Banking MMP is yet another step towards improving operational efficiency and reducing the delays and efforts involved in handling and settling transactions. The MMP which is being implemented by the banking industry aims at streamlining various e-services initiatives undertaken by individual banks. Implementation is being done by the banks concerned, with the banking Department providing a broad framework and guidance.

- ***Posts***

  Modernization of Postal Services has been undertaken by the Department of Posts through computerization and networking of all post offices using a central server-based system, and setting up of computerized registration centers (CRCs).

State Mission Mode Projects

- ***e-Governance in Municipalities***

  It is a unique initiative of the Government of India conceptualized under the umbrella of the overall National e-Governance Plan (NeGP) and the Jawaharlal Nehru National Urban Renewal Mission (Jnnurm) aimed at improving operational efficiencies within Urban Local Bodies (ULBs).

- ***Crime and Criminal Tracking Network & Systems***

  Crime and Criminal Tracking Network & Systems (CCTNS) MMP aims at creating a comprehensive and integrated system for enhancing the efficiency and effective policing at all levels and especially at the Police Station level through adoption of principles of e-Governance, and creation of a nationwide networked infrastructure for evolution of IT-enabled state-of-the-art tracking system.

- ***Public Distribution System***

  Computerization of the PDS is envisaged as an end-to-end project covering key functional areas such as supply chain management including allocation and utilization reporting, storage and movement of food grains, grievance redressal and transparency portal, digitization of beneficiary database, Fair Price Shop automation, etc.

- ***Health***

  ICT for programme management has been undertaken by the Ministry of Health & Family Welfare in the Mother and Child Tracking System (MCTS) programme and the Ministry envisages a more comprehensive use of ICT including for Hospital Information Systems, supply chain management for drugs and vaccines, providing ICT tools to ASHA and ANM workers, programme management of National Rural Health Mission (NRHM), etc. through this MMP.

- **e-panchayat**

  The Panchayati Raj Institutions (PRIs) are saddled with the problems of inadequate physical and financial resources, technical capabilities and extremely limited computerization. As a result, the potential of PRIs as the preferred delivery channel for the schemes of State and Centre as well as for citizen services has not been fully realized. While some computerization efforts for PRIs have been made by NIC over the years, the e-Governance revolution sweeping the country has not touched the PRIs yet in significant measure. The Ministry of Panchayati Raj, Government of India has therefore decided to take up the computerization of PRIs on a mission mode basis.

- **e-District**

  e-District is one of the 31 Mission Mode Projects under National e Governance Plan (NeGP) with the DIT, GoI being the nodal ministry. This project aims at providing support to the basic administrative unit i.e. District Administration by undertaking backend computerization to enable electronic delivery of high volume citizen centric government services which would optimally leverage and utilize the three infrastructure pillars of State Wide Area Networks (SWAN), State Data Centers (SDC) and Common Service Centers (CSCs) to deliver services to the citizen at his doorsteps.

- **National Land Records Modernization Programme (NLRMP)**

  A Project for Computerization of Land Records (CLR) was launched in 1988-89 with the intention to remove the inherent flaws in the manual system of maintenance and updation of Land Records. In 1997-98, the scheme was extended to tehsils to start distribution of Records of Rights to landowners on demand. The focus of the entire operation has always been to employ state of the art information technology (IT) to galvanize and transform the existing land records system of the country.

Integrated Mission Mode Projects

- ***e-procurement***

  Ministry of Commerce & Industry (Department of Commerce) has been nominated as the Nodal Ministry for implementation of e-Government Procurement (e-GP) Mission Mode Projects (MMP). The vision of the e-Procurement MMP is "To create a national initiative to implement procurement reforms, through the use of electronic Government procurement, so as to make public procurement in all sectors more transparent and efficient".

- ***e-Courts***

  The e-Court Mission Mode Project (MMP) was conceptualized with a vision to transform the Indian judiciary by making use of technology. The project had been developed, following the report submitted by the e-Committee under Supreme Court on national policy & action plan on implementation of information communication tools in Indian judiciary. A clear objective – to re-engineer processes and enhance judicial productivity both qualitatively and quantitatively to make the justice delivery system affordable, accessible, cost effective, transparent and accountable.

- **e-Biz**

  The e-Biz Mission Mode Project, being executed by Department of Industrial Policy and Promotion (DIPP), Ministry of Commerce and Industry, Government of India, was conceptualized with the vision. Its vision is "To transform the business environment in the country by providing efficient, convenient, transparent and integrated electronic services to investors, industries and business throughout the business life cycle".

- **Common Services Centers**

  The CSCs would provide high quality and cost-effective video, voice and data content and services, in the areas of e-governance, education, health, telemedicine, entertainment as well as other private services. A highlight of the CSCs is that it will offer web-enabled e-governance services in rural areas, including application forms, certificates, and utility payments such as electricity, telephone and water bills.

Recent Initiatives

Some of the major recent initiatives under e-Governance includes the follows:

- Direct Cash Transfer
- Aadhar Enabled Payment System
- MyGov Citizen Portal
- E-Kranti Scheme
- Digital Cloud for every Indian
- Digital India Program.

Direct Cash Transfer

To facilitate disbursements of Government entitlements like NREGA, Social Security pension, Handicapped Old Age Pension etc. of any Central or State Government bodies, using Aadhaar and authentication thereof as supported by UIDAI.

Aadhar Enabled Payment System (AEPS)

AEPS is a bank led model which allows online interoperable financial inclusion transaction through the Business correspondent of any bank using the Aadhaar authentication. This has helped in financial inclusion. The four Aadhaar enabled basic types of banking transactions are as follows:-

- Balance Enquiry
- Cash Withdrawal
- Cash Deposit
- Aadhaar to Aadhaar Funds Transfer.

MyGov Citizen Portal

Prime Minister launched an online platform mygov.nic.in to engage citizens in the task of "good governance" (surajya) on 26th July 2014. MyGov is a technology-driven platform that would provide people with the opportunity to contribute towards good governance.

E-Kranti Scheme

This is project for linking the internet with remote villages in the country. This scheme will broaden the reach of internet services to the rural areas in the country. The fundamental features of this scheme will be making the records handy to the government with ease. It also includes Expansion of internet and commencement of IT-based jobs in rural areas. It will also boost the use of mobile phones and computers in rural areas. It will also expand the use of IT in agriculture and retail trade too.

Digital Cloud for every Indian

Certificates issued by the government - education, residential, medical records, birth certificates, etc. - are to be stored in individual 'digital lockers and a communication protocol established for government departments to access them without physically having to see the hard copy. The purpose of government is that copies of certificates issued by the government itself not to be carried around by people to government offices for various services.

Digital India Program

The advent of Information and Communication Technology (ICT) and related advances IT services have been one of the ground-breaking changes in the all-encompassing development of the world at large. India is not an exception to the progressive effect of ICT. This serves enormous benefits by way of building capacities and competencies of elevating developing economies like India. It creates a swift in connecting people, upgrades the technology base, eases out the realization of government schemes and design and also helps in effective institution of governance in the nation.

Digital Technologies along with the promotion of Cloud Computing and Mobile Applications have emerged as catalysts for rapid economic growth and citizen empowerment across the globe. Global statistics reveal that the number of users who access the internet on mobile devices has surpassed the users who access it on PCs. Digital technologies under the tagline of Smart Applications are intended to build smartly progressive and constructive existence for citizens. These technologies are increasingly used by the society in day-to-day life from personal communications, buying goods at retail stores, availing services at doorstep to availing the governance through government offices.

Seeing the potential of digitalization and its constructive impact supporting inclusive development of our country, Government of India has launched the "Digital India" campaign. The Digital India drive envisions transforming our nation and creating opportunities for all citizens by harnessing digital technologies.

One notable aspect of the Digital India program is that it is aimed at catching the imagination of the people and this is the reason that Digital India has attracted the attention of almost everyone, both within the country and abroad. This is potentially one of the schemes which can bring about transformational benefits and fundamentally alter almost every aspect of our national life including the way citizens interact with not just the government but with each other.

The vision of Digital India program is to empower every citizen with access to digital services, knowledge and information. It can be summarized that this is intending to develop a digitally empowered society and to digitally integrate the government departments and the citizens of India. It aims at ensuring that the government services are made available to people of India electronically. Digital India is a Programme to prepare India for a knowledge future.

Digital India- Meaning and Concepts

Digital India is an initiative undertaken by the Government of India to integrate the government departments and the people of India. It aims at ensuring that the government services are made available to citizens electronically by reducing paperwork, increasing transparency, and also to encourage transparency in the system for government services and facilities. The initiative also plans to connect rural areas with high-speed internet networks.

One of the major objectives of Digital India includes in providing high speed internet connectivity to 250,000 Gram Panchayats, improve inter-operability, and promote digital literacy.

Digital India is a campaign run by the government of India to make this country a digitally empowered country. The aim of launching this campaign is to provide Indian citizens electronic government services by reducing the paperwork. It is very effective and efficient technique which will save time and man power to a great extent. This initiative was started to connect people of rural areas with the high-speed internet networks to access any information needed.

Digital India movement is majorly emplacing on promoting e-governance and to transform India into digitally empowered society and knowledge economy. As per the expert views, Digital India movement is channelized in preparing India for the knowledge-based transformation and delivering good governance to citizens by synchronized and co-ordinated engagement with both Central Government and State Governments.

Aims and Objectives:

Digital India campaign has been implemented by the Government of India to ensure following aims and objectives:

- To ensure the broadband highways;
- To ensure the universal access to mobile phones;
- To facilitate people with high-speed internet;
- To bring e-Governance by reforming government through digitization;
- To bring e-Kranti through electronic delivery of services;
- To make available online information for all;
- To ensure more jobs under the IT specialization.

Key Areas:

With a view to enlarge the reach of government services to the remotest areas of our country, Digital India programme is objectifying on three key vision areas which includes 'Digital Empowerment; Development of Digital Infrastructure and Ease of accessibility of e-governance and digital services.'

1. **Digital Empowerment:** To avail the maximum gain of Digital India drive, it is must that the citizens of our nation should be aware about the facilities and the means to avail them to their fullest. Therefore, to ensure directed empowerment towards digitalization, government has introduced various schemes to achieve following aims like universal digital literacy, universally accessible digital resources, availability of digital resources and services in maximum Indian languages. Further, collaborative digital platforms are also established for participative governance wherein the citizens are not required to physically submit documents or certificates to the government and it can be done digitally.
2. **Digital Infrastructure:** No facility can be availed without a proper infrastructure, so it is with digital services. To set up an excellent Digital Infrastructure is one the major priority of the government to ensure reach of the utility to every citizen. To build the requisite digital infrastructure, government is initiating the following activities:
    - High speed internet shall be made available in all gram panchayats;
    - Cradle to grave digital identity;
    - Mobile and Bank account would enable participation in digital and financial space at individual level;
    - Easy access to common service centre within their locality;
    - Shareable private space on a public cloud; and
    - Safe and secure cyber space in the country.
3. **E-Governance & e-Services:** With a view to extend the reaping of e-governance and to ensure the availability of e-services on demand, effortlessly integrated services are established across departments or jurisdictions. The services of digital era are made available in real time from online & mobile platforms.

Apart from this, all citizens are receiving entitlements to be portable and available on the cloud. Digitally transformed services are provided for improving ease of doing business. Along with this, citizens are also encouraged in making financial transactions electronic & cashless. Best among all is the institution of Leveraging Geospatial Information Systems (GIS) for decision support systems & development.

Initiatives under Digital India

To emplace the key drivers of Digital India movement, the government has launched several initiatives like digital locker under the name "Digi Locker" which aims to minimize the usage of physical documents and enable sharing of e-documents across agencies. Another is 'MyGov.in' which is as an innovative platform to build a partnership between citizen and government. Swachh Bharat Mission (SBM) Mobile app has also been introduced and used by people and Government organizations for achieving the goals of Swachh Bharat Mission. Along with this, eSign framework is there which would allow citizens to digitally sign a document online using Aadhaar authentication.

E-Governance/Digital India: Snap Shot of Recent Government Initiatives[3]

The Ministry of Electronics and Information Technology (MeitY), Government of India launched the 'Digital India' programme with the vision to transform India into a digitally empowered society and knowledge-based economy by ensuring digital access, digital inclusion, digital empowerment and bridging the digital divide. In summary, our mission is to ensure that the digital technologies improve the life of every citizen; expand India's digital economy, create investment & employment opportunities and global digital technological capabilities in the country.

Digital India has dramatically reduced distance between Government and citizens significantly. Further, Digital India has also helped in delivery of substantial services directly to the beneficiary in a transparent and corruption free manner. India has become one of the pre-eminent nations of the world to use technology to transform the lives of citizens. Digital India is an umbrella programme that covers multiple projects of various Central Ministries/Departments and States/UTs. Some of the major initiatives related to public service delivery are as follows:

- **Common Services Centres** – CSCs are offering government and business services in digital mode in rural areas through Village Level Entrepreneurs (VLEs). Over 400 digital services are being offered by these CSCs. So far, 5.31 Lakh CSCs are functional (including urban & rural areas) across the country, out of which, 4.20 Lakh CSCs are functional at Gram Panchayat level.
- **Unified Mobile Application for New-age Governance (UMANG)** – for providing government services to citizen through mobile. More than 1,570 government services and over 22,000 bill payment services are made available at UMANG.
- **e-District Mission Mode Project (MMP)** – e-District project has been implemented at district and sub-district levels of all States/UTs, benefitting all citizens by delivering various e-Services such as Certificates (Birth, Caste, Death, Income and Local Resident), Pension (Old Age, Disability and Widow), Electoral, Consumer Court, Revenue Court, Land Record and services of various departments such as Commercial Tax, Agriculture, Labour, Employment Training & Skill Development etc. Presently 4,671 e-services have been launched in 709 districts across India.
- **DigiLocker** – It is facilitating paperless availability of public documents. Digital Locker has more than 11.7 crore users and more than 532 crore documents are made available through DigiLocker from 2,167 issuer organisations.
- Unified Payment Interface (UPI) is the leading digital payment platform. It is integrated with 330 banks and facilitated over 586 crore monthly transactions worth over Rs 10 lakh crore has been facilitated for the month of June, 2022.
- **CO-WIN** – It is an open platform for management of registration, appointment scheduling & managing vaccination certificates for Covid-19. More than 203 crore vaccination doses and 110 crore registrations have been facilitated by co-win.
- **MyGov** – It is a citizen engagement platform that is developed to facilitate participatory governance. More than 2.48 crore users are actively using MyGov.
- **MeriPehchaan** – National Single Sign-on platform called MeriPehchaan has been launched in July 2022 to facilitate / provide citizens ease of access to government portals.
- **MyScheme** – This platform has been launched in July 2022 to facilitate citizens to avail eligibility-based services.

3. This information was given by the Minister of State for Electronics & Information Technology, in a written reply to a question in Lok Sabha on August 03, 2022. Source – E-Governance, Press Information Bureau, Government of India.

- **Direct Benefit Transfers –** 315 Schemes across 53 Ministries are offering Aadhaar enabled direct benefit transfer to citizens. So far, Rs. 24.3 lakh crore has been disbursed through DBT platform.
- **Diksha** – Diksha is a national level educational platform that helps students and teachers to participate, contribute and leverage a common platform to achieve learning goals at scale for the country. As on 27th July 2022, 7,633 courses were available and more than 15 crore enrolments have been done.

Some of the major digital initiatives taken by the Government for welfare of farmers are as follows:

- **National Agriculture Market (e-NAM)** – Government of India has launched National Agriculture Market (e-NAM) Scheme with the objective of creating online transparent competitive bidding system to facilitate farmers with remunerative prices for their produce. More than 1.73 crore farmers & 2.26 lakh traders have been registered on e-NAM platform. Also, 1000 mandis of 18 States and 3 UTs have been integrated with e-NAM platform.
- **M-KISAN** – mKisan Portal (www.mkisan.gov.in) for sending advisories on various crop related matters to the registered farmers through SMSs. In mkisan more than 5.13 crore farmers are registered for receiving crop advisories through SMS. More than 2,462 crore mobile based advisories have been sent to farmers to assist them in their farming activities.
- **One Stop Window** – Farmers Portal (www.farmer.gov.in) for dissemination of information on various agricultural related matter including, seeds variety, Storage Godown, Pests and plant diseases, Best Agricultural Practices, Watershed, Mandi details etc.
- **Soil Health Card** – It provides soil related information to facilitate farmers in farming activities. More than 22 crore soil health cards have been printed and dispatched to farmers.
- Mobile based advisory system for agriculture & Horticulture (M4AGRI) – It is mobile based advisory system for agriculture and horticulture. It has been implemented in the North-East States namely Tripura, Mizoram, Manipur, Meghalaya, Sikkim, and Arunachal Pradesh.

The Government has taken following steps in direction of data governance for socio-economic development in the country. The brief details are as follows:

- **Open Government Data** – To facilitate data sharing and promote innovation over non-personal data, Open Government Data platform has been developed. More than 5.65 lakh datasets across 12,800+ catalogues are published. The platform has facilitated 93.5 lakh downloads.
- **API Setu** – To facilitate data exchange among the system, API Setu has been developed as a platform. The platform has more than 2100 APIs, and 1000+ user organisations.
- MeitY has prepared the draft National Data Governance Framework Policy which aims to realize the full potential of India's digital government vision, maximize the efficiency of data-led governance & public service delivery and to catalyze data-based research and innovation. Currently the draft policy is under finalization. MeitY released the Draft National Data Governance Framework Policy on 26th May 2022 for public consultation.

The Government has already taken necessary measures to tackle challenges with regard to data privacy and data security through administering the Information Technology (IT) Act, 2000 which has necessary provisions for data privacy and data security.

RBI REGULATIONS GOVERNING AI, CYBER SECURITY AND CYBERSPACE

The advent of information and communication technology has revolutionized all the sectors across the globe. Indian banking and financial sector are not an exception to the transformation that has happened with the advent of information technology. Of all the IT domains that are impacting this industry, Artificial Intelligence (AI) and Data Analytics are the most influential contenders. In the present banking scenario, these stand out to

be the solution to a plethora of problems – increasing competition, fraud and cyber security threats, regulatory compliances, improving efficiency of the revenue stream, etc. According to PwC's report titled 'Industry 4.0: Building the Digital Enterprise report'[4], nearly 39% of companies in India planned to invest 8% of their annual revenues in digital programmes by 2021. As the Indian government pushes for India to become a USD 5 trillion economy by 2024, it also wants India's digital economy to become USD 1 trillion by 2025.[5] With all these set-goals in digital India, the banking industry is playing vital role and preparing itself with major digital alterations in recent years. Most conventional banks are using modern technologies to streamline their operations.

Under this backdrop, regulators are taking lead in regulating the use of modern technologies including AI in the domain of banking industry.

RBI and Artificial Intelligence: Evolving Governance[6]

Machine Learning (ML) and Artificial Intelligence (AI) are already being used in supervisory procedures by RBI. It now intends to make sure that the Department of Supervision at the central bank may reap the rewards of advanced analytics. Additionally, they have plans to bring in outside consultants for this work. For supervisory tests, the department has been creating and utilizing linear and a few ML models. Urban Cooperative Banks (UCBs), Non-Bank Financial Businesses (NBFCs), payment banks, small financing banks, neighborhood banks, credit information firms, and a few more Indian financial organizations are all subject to the RBI's regulatory authority. Artificial Intelligence (AI) and Machine Learning (ML) driven tools for data analysis and information creation will be integral part of Reserve Bank's Medium-term Strategy Framework 'Utkarsh 2.0' for the period 2023-2025. The first strategy framework (Utkarsh 2022) covering the period 2019-2022 was launched in July 2019. It became a medium-term strategy document guiding the Bank's progress towards realisation of the identified milestones. Against the backdrop of a challenging global and domestic environment, Utkarsh 2.0 commences from 2023, when India assumes the G-20 Presidency, With India's G-20 presidency during the period of Utkarsh 2.0, it confers a unique opportunity to showcase our accomplishments in the realm of digital payments and strive towards broad basing of acceptance of the Indian Rupee in bilateral and multilateral trade. The Vision in Utkarsh 2.0 that will guide the Reserve Bank of India over the period 2023-25 include, 'Excellence in performance of its functions'; Strengthened trust of citizens and Institutions in the RBI; and Enhanced relevance and significance in national and global roles. In this age of data, the Bank plays the dual role of data collection as well as information dissemination. With this comes the responsibility of reliability of data collected to create meaningful and accurate information. Therefore, adoption of AI and ML driven tool for data analysis and information creation will be an integral part of Utkarsh 2.0. The RBI is looking to extensively use advanced analytics, artificial intelligence and machine learning to analyse its huge database and improve regulatory supervision over banks and NBFCs.

RBI Jurisdiction

- Banks, urban cooperative banks, Non-Bank Financial Businesses (NBFCs), payment banks, small financing banks, local area banks, credit information firms, and a few other Indian financial organizations are all subject to the RBI's regulatory authority.
- To safeguard the interests of depositors and maintain financial stability, it conducts supervision of these companies intending to evaluate their soundness, solvency, asset quality, governance structure, liquidity, and operational viability.

4. Available at https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf

5. Available https://meity.gov.in/ writereaddata/files/india_trillion-dollar_digital_opportunity.pdf

6. Reproduced from Cheguri Preethi (2022) India seeks to expand AI Regulatory Prospects – RBI comes to Rescue, Analytics India.

RBI intents to use AI and ML rigorously:

AI and ML technologies are utilized for real-time data reporting, efficient data management, and data distribution on the data gathering side. Monitoring supervised firm-specific risks, including liquidity risks, market risks, credit exposure and concentration risks, misconduct analysis, and product misspelling, is done through data analytics. RBI inter-alia is looking to investigate and profile data with a supervisory focus. Hence, RBI is adopting an active regulatory mechanism to improve the Reserve Bank's data-driven surveillance capabilities.

RBI Governing Cyber Security and Cyberspace:

The Reserve Bank of India (RBI), being the regulatory body of the Indian Banking System, circulates guidelines on various aspects. For the last few years, banks and other financial sectors have become the soft targets for cybercriminals. Attacks such as Ransomware, malware insertion, phishing emails, DDos thriving exponentially. Financial institutions are amongst the most highly targeted organizations for cyber security attacks. To address this, the Reserve Bank of India (RBI) has outlined a list of controls, known as the RBI Guidelines for Cyber Security Framework[7], for banks to achieve a minimum recommended baseline of cyber-attack resilience.

The "Cyber Security Framework in Banks" circular from RBI sets the guidelines for Banks in India for developing and implementing next-generation cyber defence capabilities. The framework would direct the execution of progressively more robust security measures based on the nature, scale and variety of bank digital product offering.

Source: https://valuementor.com/en-in/rbi-cyber-security-framework/

The RBI cyber security framework addresses three core areas:

a. Establish Cyber Security Baseline and Resilience;

b. Operate Cyber Security Operations Centre (C-SOC);

c. Cyber Security Incident Reporting (CSIR).

7. Available at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0

RBI Cyber Security Circular: Brief

Need for a Board approved Cyber-Security Policy

Banks were directed immediately put in place a cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk, duly approved by their Board. It may be ensured that the strategy deals with the following broad aspects:

1. **Cyber Security Policy to be distinct from the broader IT policy / IS Security Policy of a bank**

   In order to address the need for the entire bank to contribute to a cyber-safe environment, the Cyber Security Policy should be distinct and separate from the broader IT policy / IS Security policy so that it can highlight the risks from cyber threats and the measures to address / mitigate these risks.

   The size, systems, technological complexity, digital products, stakeholders and threat perception vary from bank to bank and hence it is important to identify the inherent risks and the controls in place to adopt appropriate cyber-security framework. While identifying and assessing the inherent risks, banks are required to reckon the technologies adopted, alignment with business and regulatory requirements, connections established, delivery channels, online / mobile products, technology services, organizational culture and internal & external threats. Depending on the level of inherent risks, the banks are required to identify their riskiness as low, moderate, high and very high or adopt any other similar categorisation. Riskiness of the business component also may be factored into while assessing the inherent risks. While evaluating the controls, Board oversight, policies, processes, cyber risk management architecture including experienced and qualified resources, training and culture, threat intelligence gathering arrangements, monitoring and analysing the threat intelligence received vis-à-vis the situation obtaining in banks, information sharing arrangements (among peer banks, with IDRBT/RBI/CERT-In), preventive, detective and corrective cyber security controls, vendor management and incident management & response are to be outlined.

2. **Arrangement for continuous surveillance**

   Testing for vulnerabilities at reasonable intervals of time is very important. The nature of cyber-attacks is such that they can occur at any time and in a manner that may not have been anticipated. Hence, it is mandated that a SOC (Security Operations Centre) be set up at the earliest, if not yet been done. It is also essential that this Centre ensures continuous surveillance and keeps itself regularly updated on the latest nature of emerging cyber threats.

3. **IT architecture should be conducive to security**

   The IT architecture should be designed in such a manner that it takes care of facilitating the security measures to be in place at all times. The same needs to be reviewed by the IT Sub Committee of the Board and upgraded, if required, as per their risk assessment in a phased manner. The risk cost/ potential cost trade off decisions which a bank may take should be recorded in writing to enable an appropriate supervisory assessment subsequently.

   An indicative, but not exhaustive, minimum baseline cyber security and resilience framework to be implemented by the banks (as given in Annex 1[8] of the circular).

   Banks should proactively initiate the process of setting up of and operationalizing a Security Operations Centre (SOC) to monitor and manage cyber risks in real time. (An indicative configuration of the SOC is given in Annex 2[9] the circular).

8. Available at https://rbidocs.rbi.org.in/rdocs/content/pdfs/CSFB020616_AN1.pdf

9. https://rbidocs.rbi.org.in/rdocs/content/pdfs/CSFB020616_AN2.pdf

4. Comprehensively address network and database security

Recent incidents have highlighted the need to thoroughly review network security in every bank. In addition, it has been observed that many times connections to networks/databases are allowed for a specified period of time to facilitate some business or operational requirement. However, the same do not get closed due to oversight making the network/database vulnerable to cyber-attacks. It is essential that unauthorized access to networks and databases is not allowed and wherever permitted, these are through well-defined processes which are invariably followed. Responsibility over such networks and databases should be clearly elucidated and should invariably rest with the officials of the bank.

5. Ensuring Protection of customer information

Banks depend on technology very heavily not only in their smooth functioning but also in providing cutting-edge digital products to their consumers and in the process collect various personal and sensitive information. Banks, as owners of such data, should take appropriate steps in preserving the Confidentiality, Integrity and Availability of the same, irrespective of whether the data is stored/in transit within themselves or with customers or with the third-party vendors; the confidentiality of such custodial information should not be compromised at any situation and to this end, suitable systems and processes across the data/information lifecycle need to be put in place by banks.

6. Cyber Crisis Management Plan

A Cyber Crisis Management Plan (CCMP) should be immediately evolved and should be a part of the overall Board approved strategy. Considering the fact that cyber-risk is different from many other risks, the traditional BCP/DR arrangements may not be adequate and hence needs to be revisited keeping in view the nuances of the cyber-risk. As you may be aware, in India, CERT-IN (Computer Emergency Response Team – India, a Government entity) has been taking important initiatives in strengthening cyber-security by providing proactive & reactive services as well as guidelines, threat intelligence and assessment of preparedness of various agencies across the sectors, including the financial sector. CERT-IN also have come out with National Cyber Crisis Management Plan and Cyber Security Assessment Framework. CERT-In/NCIIPC/RBI/IDRBT guidance may be referred to while formulating the CCMP.

CCMP should address the following four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment. Banks need to take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond / recover / contain the fall out. Banks are expected to be well prepared to face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks. Among other things, banks should take necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to, denial of Service, Distributed Denial of Services (DDoS), ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc.

7. Cyber security preparedness indicators

The adequacy of and adherence to cyber resilience framework should be assessed and measured through development of indicators to assess the level of risk/preparedness. These indicators should be used for comprehensive testing through independent compliance checks and audits carried out by qualified and competent professionals. The awareness among the stakeholders including employees may also form a part of this assessment.

8. Sharing of information on cyber-security incidents with RBI

It is observed that banks are hesitant to share cyber-incidents faced by them. However, the experience gained globally indicates that collaboration among entities in sharing the cyber-incidents and the best

practices would facilitate timely measures in containing cyber-risks. It is reiterated that banks need to report all unusual cyber-security incidents (whether they were successful or were attempts which did not fructify) to the Reserve Bank. Banks are also encouraged to actively participate in the activities of their CISOs' Forum coordinated by IDRBT and promptly report the incidents to Indian Banks – Center for Analysis of Risks and Threats (IB-CART) set up by IDRBT. Such collaborative efforts will help the banks in obtaining collective threat intelligence, timely alerts and adopting proactive cyber security measures.

9. Supervisory Reporting framework

It has been decided to collect both summary level information as well as details on information security incidents including cyber-incidents. Banks are required to report promptly the incidents, in the format given in Annex-3.[10]

10. Organizational arrangements

Banks should review the organisational arrangements so that the security concerns are appreciated, receive adequate attention and get escalated to appropriate levels in the hierarchy to enable quick action.

11. Cyber-security awareness among stakeholders / Top Management / Board

It should be realized that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This will require a high level of awareness among staff at all levels. Top Management and Board should also have a fair degree of awareness of the fine nuances of the threats and appropriate familiarisation may be organized. Banks should proactively promote, among their customers, vendors, service providers and other relevant stakeholders an understanding of the bank's cyber resilience objectives, and require and ensure appropriate action to support their synchronized implementation and testing. It is well recognized that stakeholders' (including customers, employees, partners and vendors) awareness about the potential impact of cyber-attacks helps in cyber-security preparedness of banks. Banks are required to take suitable steps in building this awareness. Concurrently, there is an urgent need to bring the Board of Directors and Top Management in banks up to speed on cyber-security related aspects, where necessary, and hence banks are advised to take immediate steps in this direction.

IMPLICATIONS OF RBI REQUIREMENTS

Security policy and procedures requirements:

1. Define and adopt a comprehensive Cyber Security Framework that includes: –
   - (i) The risks posed by cyber threats, as well as the actions to manage or reduce these risks, must be highlighted in a cyber-security strategy.
   - (ii) Banks must implement a cyber-security policy outlining a plan for combating cyber threats in light of the business's complexity and acceptable levels of risk.
   - (iii) The risk assessment approach may be used to identify major gaps in controls early on, and suitable corrective action can be recommended under the active supervision and monitoring of the IT Committee.
   - (iv) Put in place the measures specified in the Cyber Security Framework requirements.

10. Available at https://rbidocs.rbi.org.in/rdocs/content/pdfs/CSFB020616_AN3.pdf

2. Monitoring and surveillance of the Infrastructure:
   (i) Establish a cyber-security testing/assessment procedure on a regular basis to uncover vulnerabilities/security issues in the bank's infrastructure/applications.
   (ii) Establish a Cyber Security Operations Centre (C-SOC) for proactive monitoring with advanced technologies for detection, fast reaction, and data analytics.
   (iii) Ensure that C-SOC covers requirements defined in the guidelines.
3. Testing of the IT infrastructure and architecture audit:
   (i) Establish a cyber security testing/assessment program to identify vulnerabilities/ security flaws in Bank's infrastructure/applications on a periodic basis.
   (ii) Establish Cyber Security Operations Centre (C-SOC) for proactive monitoring using sophisticated tools for detection, quick response and backed by tools for data analytics.
   (iii) Ensure that C-SOC covers requirements defined in guidelines.
4. Setup network and database security:
   (i) Conduct a thorough evaluation of network (firewall rules, port opening/closing, etc.) and database (direct database access, back-end updates, etc.) security.
   (ii) Define and document processes for appropriate business or operational requirements to get access to networks and databases.
5. Securing Customer Information:
   (i) Bank is the owner of customer's personal and sensitive information collected by the Bank.
   (ii) Bank is responsible for securing customer information even when it is with the customer or with third party vendor.
6. Setting up Cyber Crisis Management Plan:
   (i) Create a Cyber Crisis Management Plan (CCMP) that addresses the following needs during a breach: Detection, Response, Recovery, and Containment.
   (ii) Examine the existing BCP/DR (Business Continuity Plan/Disaster Recovery) programme and ensure it is updated to satisfy the needs of modern cybersecurity.
   (iii) Establishing preventive, detective, and corrective measures to safeguard the bank against cyber-threats and to identify, respond to, contain, and recover from any cyber-intrusions as soon as possible.
7. Testing and assessment of the cyber security plan:
   (i) Define indicators to assess and measure adequacy of and adherence to cyber security/resilience framework.
   (ii) Use indicators for comprehensive testing through independent compliance checks and audits carried out by qualified and competent professionals.
8. Incident monitoring and management processes:
   (i) Improve incident monitoring and management systems for information security incidents and cyber security efforts.
   (ii) Process to be defined to report any abnormal cyber security incidents (whether successful or failed) to the Reserve Bank of India using the methodology outlined in the guidelines.

(iii) Update incident management policies and processes to cleanse and share cyber security issues

9. Setting up an Information Security team:

   Examine the information security organization structure, as well as the duties and responsibilities of the CISO, to verify that cyber security problems are effectively addressed inside the Bank.

10. Training and awareness:

    Hold cyber security awareness and training workshops for all important stakeholders, including the Board of Directors, top management, third-party vendors, customers, and employees.

Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices dated November 7, 2023[11]

The RBI came out with Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices on November 7, 2023 with an objective to tighten the governance framework for technology within banking segment. Earlier, the RBI had released the Master Direction on Outsourcing of IT Services released on June 23, 2022 to strengthen control framework for better management of outsourcing of technology services.

Who all will be impacted with these Regulations:

- Banks;
- Small Financial Banks and CICs
- NBFCs
- Service Provider, Fintech and Technology Enabler

The master direction will apply to all RBI regulated entities except local area banks and NBFC-core investment companies. It prescribes procedures and framework for strategic alignment, risk management, resource management, performance management and business continuity/ disaster recovery management. It also provides for periodic reviews of risks, IT and information security risk management framework, information security policy and cyber security policy.

The framework provides for the constitution of three major committees by the regulated entities — IT strategy committee of the board, IT steering committee and information security committee. The regulated entities are also required to designate a senior level executive having no direct reporting relationship with the head of IT Function as 'chief information security officer'. Further, the regulated entities have been recommended to conduct disaster recovery drills at least on a half-yearly basis for critical information and back up data in a secured manner as a business continuity measure.

These guidelines integrate consolidated and updated earlier instructions on IT Governance, Risk, Controls, Assurance Practices, and Business Continuity/Disaster Recovery Management separately released for Banks and NBFCs. **Newly released Master Direction shall come into effect from April 1, 2024**[12]

These guidelines are applicable to the following Regulated Entities (REs), unless explicitly exempted:

- Scheduled Commercial Banks (excluding Regional Rural Banks)
- Small Finance Banks
- Payments Banks

11. Reproduced from Charting the Course: Decoding RBI's Master Direction on IT Governance, Risk, Controls & Assurance Practices. The Digital Fifth. Available at https://thedigitalfifth.com/decoding-rbis-master-direction-on-it-governance/

12. Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices. Available at https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12562

- All Non-Banking Financial Companies (NBFCs) in Top, Upper, and Middle Layers as per Scale-Based Regulation (SBR)
- All India Financial Institutions (NHB, NABARD, EXIM Bank SIDBI, and NaBFID)
- Credit Information Companies

Companies excluded from the scope are:

- Local Area Banks
- NBFC – Core Investment Companies

Regulated Entities are required to establish a robust IT Governance Framework, including governance structure and processes essential to achieve the entity's business/strategic objectives. This framework should define the roles (including authority) and responsibilities of the Board of Directors (Board), Board level Committee, Local Management Committee (in the case of foreign banks operating as branches in India), and Senior Management. It must encompass adequate oversight mechanisms to ensure accountability and mitigate business risks.

RBI's Updated Master Direction: Navigating the Digital Landscape Safely

In response to the dynamic shifts in the financial sector, the Reserve Bank of India (RBI) has recently launched an updated Master Direction, reflecting the profound changes brought about by digital technologies. This article delves into the key drivers behind this strategic move and explores the thematic objectives set by the RBI to strengthen IT governance, risk management, and resilience in the banking sector.

- **Technology becoming central to Banking & Lending services:** Banks rely heavily on technology for daily operations, utilizing core banking systems, online platforms, and mobile applications. This technological dependence extends to risk management and automated decision-making, enhancing overall operational efficiency.
- **Shift in Operating Models of Banks:** The last decade has witnessed a monumental transformation in the financial sector, propelled by the advent of digital technologies. The surge in online services, coupled with competitive pressures and the need for operational efficiency, has paved the way for innovations in Mobility, AIML, APIs, and Cloud Computing. These technological integrations aim to enhance service delivery, elevate customer engagement, and fortify risk management strategies.
- **Rise of Banks-FinTech's Partnership:** Collaborations between traditional financial institutions and FinTech firms have become increasingly prevalent, ushering in a new era of opportunities and challenges. While these partnerships offer benefits, they also introduce complexities in managing IT systems, encompassing aspects such as data security, system integrations, interdependencies, regulatory compliance, vendor management, and shared responsibilities.
- **Increasing impetus on Digital Transformation:** The digital transformation wave underscores the importance of agile technologies, scalability, adaptability, and resilience across the financial spectrum. The ability to navigate these facets effectively is crucial for staying competitive and meeting evolving customer expectations.
- **Continued Cyber Threats:** With increased reliance on digital technologies comes an expanded attack surface for cyber threats. This has led to a surge in cybercrimes, including DDoS attacks, phishing attempts, data breaches, and ransomware attacks. Safeguarding against these threats is imperative for maintaining the integrity of financial systems.
- **Regulatory Monitoring:** The introduction of stringent regulations, such as the Digital Personal Data Protection Act, has heightened the need for financial institutions to ensure the security and compliance of their IT systems. This regulatory scrutiny has prompted the RBI to release updated guidelines, reinforcing the importance of robust IT governance and risk management.

Thematic Objectives of the New RBI Master Directions:

- **Elevating the Role of the Board and Top Management:** The RBI emphasizes the establishment of a Board-level IT strategy committee and an IT steering committee, underscoring the pivotal role of top management in mitigating IT risks.
- **Improving Delivery Capabilities and Excellence:** Encouraging best practices in software development, project management, and IT service management to enhance speed, efficiency, and quality in IT service delivery.
- **Sustaining the Technology Landscape:** Prioritizing regular technology updates, ongoing maintenance, and robust disaster recovery plans to ensure operational efficiency, system security, and business resilience.
- **Fortifying Risk Management:** Mandating regular IT risk reviews and comprehensive risk management frameworks, addressing infrastructure, security, cyber threats, and third party risks.
- **Boosting Security and Resilience:** Enforcing strict security controls, data encryption, regular cyber drills, and enhanced disaster recovery arrangements to fortify the overall security and resilience of IT systems.
- **Enhancing Monitoring & Supervision:** Calling for continuous auditing, regular vulnerability assessments, enhanced reporting on critical systems, and meticulous vendor risk management to bolster monitoring and supervision.

SEBI REGULATIONS GOVERNING AI, CYBER SECURITY AND CYBERSPACE

Established in 1988, the SEBI (Securities and Exchange Board of India) is the regulatory body for securities and commodity markets in India under the Ministry of Finance. It acts as an executive government entity with statutory powers thanks to the SEBI Act of January 1992. SEBI ensures that the needs of market intermediaries, investors, and issuers of securities are met, including safeguarding their data, customer data, and transactions.

As of April 2022, SEBI has six committee members that are required to oversee guidance for cybersecurity initiatives for the Indian market and advise SEBI to develop and maintain cybersecurity requirements following global industry standards. Amid increasing cybersecurity threats to the securities market, SEBI in year 2022 issued an advisory for stock exchanges, depositories and other regulated entities asking them to define roles and responsibilities of chief information security officer and other senior personnel. Also, it asked them to clearly specify the reporting and compliance requirements in the security policy. SEBI Regulated Entities (REs) have been advised to implement these cybersecurity practices as recommended by Financial Computer Security Incident Response Team (CSIRT-Fin). The REs have been asked to proactively monitor the cyberspace to identify phishing websites and report the same to CSIRT-Fin.Additionally, SEBI also communicates with other agencies like NCSC (National Cyber Coordination Center), DoT (Department of Telecommunications), and The Ministry of Electronics and Information Technology (MeitY).

Accordingly, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in e-mail, can establish an important pillar of defense. Given the sophistication and persistence of the threat with a high level of coordination among threat actors, it is important to recognise that many traditional approaches to risk management and governance that worked in the past may not be comprehensive or agile enough to address the rapid changes in the threat environment and the pace of technological change that is redefining public and private enterprise. SEBI implemented guidelines that apply to organizations within its scope — stock brokers, stock exchanges, AMCs (asset management companies), mutual funds, and depository participants, among others. The operating systems and applications should be updated with the latest patches on a regular basis. It further said that security audit or Vulnerability Assessment and Penetration Testing (VAPT) of the application should be conducted at regular basis. Penalties for SEBI non-

compliance, for example, violating disclosure regulations, are mandated with a fine of ₹ 20,000 per day until companies reach compliance.

Indian markets today generate over 550 crore daily order and trade messages in the equity and equity derivative segments. In order to keep pace with the demands and challenges of markets, the Securities and Exchange Board of India (SEBI) is investing in technology to improve its own productivity and speed of response to the market.

With advent of technologies such as machine learning and artificial intelligence, it is essential for a regulator like SEBI to leverage sophisticated algorithms, artificial intelligence and machine learning to address critical challenges for data analytics arising when processing vast amount of data, either structured or unstructured. Further, it is also imperative for it to have resilient infrastructure such as data centres and cloud facilities to safely and effectively manage this ever-increasing data. The regulator has developed a system based on Artificial Intelligence (AI) that scans various stock market shows and builds a database of recommendations made. This database will be a part of the big-data network SEBI is employing to conduct comprehensive surveillance for securities market offences, such as insider trading and front running.

The Securities and Exchange Board of India (SEBI) has asked all mutual funds companies in India to report Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered to investors (individuals and institutions) or used internally by it to facilitate investing and trading or for any other purpose. The move is aimed at conducting a survey for creating an inventory of the AI / ML landscape in the Indian financial markets to gain an in-depth understanding of the adoption of such technologies in the markets and to ensure preparedness for any AI / ML policies that may arise in the future.

As most AI / ML systems are black boxes and their behaviour cannot be easily quantified, it is imperative to ensure that any advertised financial benefit owing to these technologies in investor facing financial products offered by intermediaries should not constitute to misrepresentation.

The SEBI adopted the following key initiatives in recognition of the power of emerging technologies in the recent times in the interest of corporate governance:

- **Adoption of AI for surveillance**: The future of surveillance will entail sophisticated deployment of technology to detect more complex and evolving manipulation techniques by fraudsters. It is proposed that the use of AI for data analytics and pattern recognition will aid SEBI in better identifying abnormal or fraudulent behaviour in the market including front running and insider trading. Technology will be used to simulate human intelligence to further refine its alerts system.
- **Implementation of data lake at SEBI**: This is expected to be achieved through a data lake solution which can support open source analytical tools such as R, Python, etc. with interoperable features. During the year, SEBI completed its tendering process for implementation of the proposed Data Lake. The proposed Data Lake will have characteristics such as visualization, time series/machine learning analytical capabilities, ability to seek and search both structured/unstructured/semistructured data, self-serviced business intelligence capabilities, in memory processing of data etc. The implementation of Data Lake is now underway.
- **Setting up a new and modern data centre**: SEBI had implemented a large scale tier 3+ data center. The new data center is currently hosting SEBI's Private Cloud Infrastructure (SPCI). It is envisaged to consolidate infrastructure from other data centers in Mumbai to the new Data Center. The consolidation of all hardware will increase manageability of server side hardware and result in better turn-around times for service requests.
- **Setting up private cloud infrastructure to facilitate rapid scaling of all systems**: In 2020-21, SEBI implemented its private cloud infrastructure also known as 'SPCI'. It is proposed that new and upcoming projects will utilize the SPCI and in most cases no separate hardware procurements will be required.

Usage of commodity hardware will be encouraged where practicable. The SPCI is already hosting many applications such as Resource Person Portal, File Tracking System (IONS) and Data Lake.

- **Academic programmes**: The National Institute of Securities Markets (NISM) is involved in designing and offering academic programmes that focus on creating a cadre of professionals in securities markets. During the academic year 2020-21, NISM has conducted training programmes on various topics including artificial intelligence, cyber security, blockchain etc. A Post Graduate Certificate in Management (Data Science in Financial Markets) was also organised.
- **Policy initiatives**: With a view to analyse complex bank statements, call data records, internal protocol detail records, hash functions to ensure the sanctity of data, handling of IT digital devices and adoption of data analytics to identify the pattern of relationships for unearthing sophisticated connections while investigating complex cases, a new cell namely 'Connection Research and Analysis Cell' (CRAC) under Integrated Surveillance Department was created in December 2020. Further multiple subcommittees were formed for various projects such as Data Lake, Data Analytics, Private Cloud, Network Revamp, etc.

With a growing reliance on technology, the market infrastructure institutions (MIIs) have fully automated their operations and functions, from order entry to order matching to transaction confirmation, all the way to clearing and settlement of trades. However, according to SEBI, there have been instances of technical problems resulting in business disruption or service unavailability.

SEBI Cyber Security Guidelines, 2023 – Cyber Security and Cyber Resilience framework for Portfolio Managers[13]

Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity, and Availability (CIA) of the computer systems, networks, and databases (Confidentiality refers to limiting access of systems and information to authorized users, Integrity is the assurance that the information is reliable and accurate, and Availability refers to guarantee of reliable access to the systems and information by authorized users). The cyber security framework includes measures, tools, and processes that are intended to prevent cyber-attacks and improve cyber resilience. Cyber Resilience is an organization's ability to prepare and respond to a cyber-attack and to continue operations during, and recover from, a cyber-attack.

With rapid technological advancement in the securities market, there is a greater need for maintaining robust cyber security and to have a cyber resilience framework to protect the integrity of data and guard against breaches of privacy.

As part of the operational risk management, the Portfolio Managers need to have robust cyber security and cyber resilience framework in order to provide essential facilities and services and perform critical functions in the securities market as Portfolio Manager.

Based on feedback received from stakeholders, it has been decided that the guidelines annexed with this circular shall be effective from October 01, 2023.

In this context, Association of Portfolio Managers in India (APMI) shall also furnish activity wise implementation timelines and progress in implementation of provisions of this circular to SEBI on bi-monthly basis.

Portfolio Managers and APMI shall take necessary steps for implementing the circular, including putting the required processes and systems in place to ensure compliance with the provisions of this circular.

Accordingly, all Portfolio Managers with asset under management of INR 3000 crore or more, under discretionary

13. Reproduced from SEBI Circular on Cyber Security and Cyber Resilience framework for Portfolio Managers, March 29, 2023. Available at https://www.sebi.gov.in/legal/circulars/mar-2023/cyber-security-and-cyber-resilience-framework-for-portfolio-managers_69521.html

and non-discretionary portfolio management service taken together, as on the last date of the previous calendar month shall comply with the provisions of Cyber Security and Cyber Resilience as placed at below.

Governance

- As part of the operational risk management framework to manage risk to systems, networks, and databases from cyber-attacks and threats, Portfolio Managers should formulate comprehensive cyber security and cyber resilience policy document encompassing the framework mentioned hereunder. The policy document should be approved by the Board or equivalent body of the Portfolio Manager, and in case of deviations from the suggested framework, reasons for such deviations should also be provided in the policy document.
- The policy document should be reviewed by the Board or equivalent body of the Portfolio Manager at least once annually with the view to strengthen and improve its cyber security and cyber resilience framework.
- The cyber security and cyber resilience policy should include the following process to identify, assess, and manage cyber security risks associated with processes, information, networks, and systems;
  - (a) 'Identify' critical IT assets and risks associated with such assets,
  - (b) 'Protect' assets by deploying suitable controls, tools, and measures,
  - (c) 'Detect' incidents, anomalies, and attacks through appropriate monitoring tools/processes,
  - (d) 'Respond' by taking immediate steps after identification of the incident, anomaly, or attack,
  - (e) 'Recover' from incident through incident management, disaster recovery, and business continuity framework.
- The Cyber security policy should encompass the principles prescribed by the National Critical Information Infrastructure Protection Centre (NCIIPC) of the National Technical Research Organization (NTRO), Government of India, in the report titled 'Guidelines for Protection of National Critical Information Infrastructure' and subsequent revisions, if any, from time to time.
- Portfolio Managers should also incorporate best practices from standards such as ISO 27001, ISO 27002, COBIT 5, etc., or their subsequent revisions, if any, from time to time.
- Portfolio Managers should designate a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify and reduce cyber security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cyber security and resilience policy approved by the Board or equivalent body of Portfolio Manager.
- The Board or equivalent body of the Portfolio Manager shall constitute a Technology Committee comprising experts proficient in technology. This Technology Committee should on a half yearly basis review the implementation of the cyber security and cyber resilience policy approved by their Board or equivalent body, and such review should include a review of their current IT and cyber security and cyber resilience capabilities, set goals for a target level of cyber resilience, and establish a plan to improve and strengthen cyber security and cyber resilience. The review shall be placed before the Board or equivalent body of the Portfolio Manager for appropriate action.
- The Portfolio Managers should establish a reporting procedure to facilitate communication of unusual activities and events to CISO or to the senior management in a timely manner.
- The aforementioned committee and the senior management of the Portfolio Manager, including the CISO, should periodically review instances of cyberattacks, if any, domestically and globally, and take steps to strengthen cyber security and cyber resilience framework.

- Portfolio Managers should define the responsibilities of its employees, outsourced staff, and employees of vendors and other entities, who may have access to or use systems/networks of the Portfolio Managers, towards ensuring the goal of cyber security.

Identify

- Portfolio Manager shall identify and classify critical assets based on their sensitivity and criticality for business operations, services, and data management. The critical assets shall include business-critical systems, internet-facing applications/ systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/ communicating with critical systems either for operations or maintenance shall also be classified as critical assets. The Board or equivalent body of the Portfolio Manager shall approve the list of critical assets.
- To this end, Portfolio Manager shall maintain an up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows.
- Portfolio Managers should accordingly identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.
- Portfolio Managers should also encourage its third-party service providers, if any, such as Custodians, Brokers, Distributors, etc. to have similar standards of Information Security.

Protection

Access Controls

- No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities.
- Any access to Portfolio Manager's systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. Portfolio Manager should grant access to IT systems, applications, databases, and networks on a need-to-use basis and based on the principle of least privilege.
- Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.
- Portfolio Manager should implement strong password controls for users' access to systems, applications, networks and databases. Password controls should include a change of password upon first log-on, minimum password length and history, password complexity as well as maximum validity period. The user credential data should be stored using strong and latest hashing algorithms.
- Portfolio Managers should ensure that records of user access are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in encrypted form for a time period not less than two (2) years.
- Portfolio Managers should deploy additional controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users). Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallowing privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.

- Account access lock policies after failure attempts should be implemented for all accounts.
- Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the Portfolio Manager's critical systems, networks, and other computer resources, should be subject to stringent supervision, monitoring, and access restrictions.
- Two-factor authentication at log-in should be implemented for all users that connect using online/ internet facility.
- Portfolio Managers should formulate an Internet access policy to monitor and regulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc.
- Proper 'end of life' mechanism should be adopted to deactivate access privileges of users who are leaving the organization or whose access privileges have been withdrawn.

Physical Security

- Physical access to the critical systems should be restricted to minimum. Physical access of outsourced staff or visitors should be properly supervised by ensuring at the minimum that outsourced staff or visitors are accompanied at all times by authorized employees.
- Physical access to the critical systems should be revoked immediately if the same is no longer required.
- Portfolio Managers should ensure that the perimeter of the critical equipment rooms is physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate.

Network Security Management

- Portfolio Managers should establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices, and enterprise mobile devices within the IT environment. The Portfolio Manager should conduct regular enforcement checks to ensure that the baseline standards are applied uniformly. The checks should be done at least once in a year.
- Portfolio Managers should install network security devices, such as firewalls as well as intrusion detection and prevention systems, to protect their IT infrastructure from security exposures originating from internal and external sources.
- Anti-virus software should be installed on servers and other computer systems. Updation of anti-virus definition files and automatic anti-virus scanning should be done on a regular basis.

Security of Data

- Data-in motion and Data-at-rest should be in encrypted form by using strong encryption methods such as Advanced Encryption Standard (AES), RSA, SHA2, etc.
- Portfolio Managers should implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.
- The information security policy should also cover use of devices such as mobile phone, faxes, photocopiers, scanners, etc. that can be used for capturing and transmission of data.
- Portfolio Managers should allow only authorized data storage devices through appropriate validation processes.

Hardening of Hardware and Software

- Only a hardened and vetted hardware / software should be deployed by the Portfolio Managers. During the hardening process, Portfolio Managers should inter-alia ensure that default passwords are replaced with strong passwords and all unnecessary services are removed or disabled in equipments/ software.
- All open ports which are not in use or can potentially be used for exploitation of data should be blocked. Other open ports should be monitored and appropriate measures should be taken to secure the ports.

Application Security and Testing

- Portfolio Managers should ensure that regression testing is undertaken before new or modified system is implemented. The scope of tests should cover business logic, security controls and system performance under various stressload scenarios and recovery conditions.
- Patch Management
- Portfolio Managers should establish and ensure that the patch management procedures include the identification, categorization and prioritization of security patches. An implementation timeframe for each category of security patches should be established to implement security patches in a timely manner.
- Portfolio Managers should perform rigorous testing of security patches before deployment into the production environment so as to ensure that the application of patches do not impact other systems.
- Disposal of systems and storage devices
- Portfolio Managers should frame suitable policy for disposals of the storage media and systems. The data / information on such devices and systems should be removed by using methods viz. wiping / cleaning / overwrite, degauss and physical destruction, as applicable.

Vulnerability Assessment and Penetration Testing (VAPT)

- Portfolio Managers shall carry out periodic VAPT, inter-alia, including critical assets and infrastructure components like servers, networking systems, security devices, load balancers, other IT systems pertaining to the activities done as Portfolio Manager, etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.
- Portfolio Managers shall conduct VAPT at least once in a financial year. However, for the Portfolio Managers, whose systems have been identified as “protected system” by National Critical Information Infrastructure Protection Centre (NCIIPC) under the Information Technology (IT) Act, 2000, VAPT shall be conducted at least twice in a financial year.
- Further, all Portfolio Managers shall engage only Indian Computer Emergency Response Team (CERT-In) empanelled organizations for conducting VAPT.
- The final report on said VAPT shall be submitted to SEBI after approval from Technology Committee of respective Portfolio Manager, within 1 month of completion of VAPT activity.
- Any gaps or vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to SEBI within 3 months post the submission of final VAPT report.
- In addition, Portfolio Managers shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system which is a critical system or part of an existing critical system.

Monitoring and Detection

- Portfolio Managers should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices should also be monitored for anomalies.
- Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks, Portfolio Managers should implement suitable mechanism to monitor capacity utilization of its critical systems and networks.
- Suitable alerts should be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual online transactions.

Response and Recovery

- Alerts generated from monitoring and detection systems should be suitably investigated, including impact and forensic analysis of such alerts, in order to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect and eradicate the incident.
- The response and recovery plan of the Portfolio Manager should aim at the timely restoration of systems affected by incidents of cyber-attacks or breaches. Portfolio Managers should have Recovery Time Objective (RTO) and Recovery Point Objective (RPO) not more than 4 hours and 30 minutes, respectively
- The response plan should define responsibilities and actions to be performed by its employees and support or outsourced staff in the event of cyber-attacks or breach of cyber security mechanism.
- Any incident of loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.
- Portfolio Managers should also conduct suitable periodic drills to test the adequacy and effectiveness of response and recovery plan.

Sharing of information

- All cyber-attacks, threats, cyber-incidents, and breaches experienced by Portfolio Managers shall be reported to SEBI within 6 hours of noticing/ detecting such incidents or being brought to their notice about such incidents. The incident shall also be reported to CERT-In in accordance with the guidelines/ directions issued by CERT-In from time to time. Additionally, the Portfolio Manager, whose systems have been identified as “protected system” by NCIIPC, shall also report the incident to NCIIPC. The quarterly reports containing information on cyber-attacks, threats, cyber-incidents, and breaches experienced by Portfolio Manager and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs/ vulnerabilities/ threats that may be useful for other Portfolio Managers shall be submitted to SEBI within 15 days from the quarter ended June, September, December and March of every year. The above information/ reports shall be shared through the dedicated e-mail ids: vapt_reports@sebi.gov.in and cybersecurity_pms@sebi.gov.in
- Such details as are felt useful for sharing with other Portfolio Managers in masked and anonymous manner shall be shared using mechanism to be specified by SEBI from time to time.

Training

Portfolio Managers should conduct periodic training programs to enhance awareness level among the employees and outsourced staff, vendors, etc. on IT / Cyber security policy and standards. Special focus should be given to build awareness levels and skills of staff from non-technical disciplines.

The training program should be reviewed and updated to ensure that the contents of the program remain current and relevant.

Periodic Audit

Portfolio Managers shall arrange to have its systems audited on an annual basis by an independent CISA / CISM qualified or CERT-IN empanelled auditor to check compliance with the above areas and shall submit the report to SEBI along with the comments of the Board or equivalent body of Portfolio Manager within three months of the end of the financial year.

Vendors or Service Providers

Portfolio Managers have outsourced many of their critical activities to different agencies / vendors / service providers. The responsibility, accountability and ownership of those outsourced activities lies primarily with Portfolio Manager.

Therefore, Portfolio Manager have to come out with appropriate monitoring mechanism through clearly defined framework to ensure that all the requirements as specified in this circular is complied with. The periodic report submitted to SEBI should highlight the critical activities handled by the agencies and to certify the above requirement is complied.

INTERNATIONAL PRINCIPLES GOVERNING AI, CYBER SECURITY AND CYBERSPACE: AN OVERVIEW[14]

With few exceptions (most notably, the Budapest Convention on Cybercrime and the not-yet-in-force African Union Convention on Cyber Security and Personal Data Protection), international law does not have tailor-made rules for regulating cyberspace. Moreover, the technology is both novel and dynamic. Thus, for several years, there were open questions about whether existing international law applied to cyberspace at all. Today, most states and several international organizations, including -

- UN General Assembly's First Committee on Disarmament and International Security,
- G20,
- European Union,
- ASEAN, and
- Organization of American States (OAS).

Have affirmed that existing international law applies to the use of Information and Communication Technologies (ICTs) by states. As such, the current discourse centers not on whether international law applies, but rather how it does so.

Major Issues:

Issues surrounding international law's application to cyberspace may be broken into five discrete categories: (i) silence; (ii) existential disagreements; (iii) interpretative challenges; (iv) attribution; and (v) accountability.

14 . Students to note that arena of international principals governing AI, Cyber Security and Cyberspace is quite wide. Hence in this chapter, we are highlighting major bodies guiding the unfirm practice and principles governing/guiding AI, Cyber Security and Cyberspace

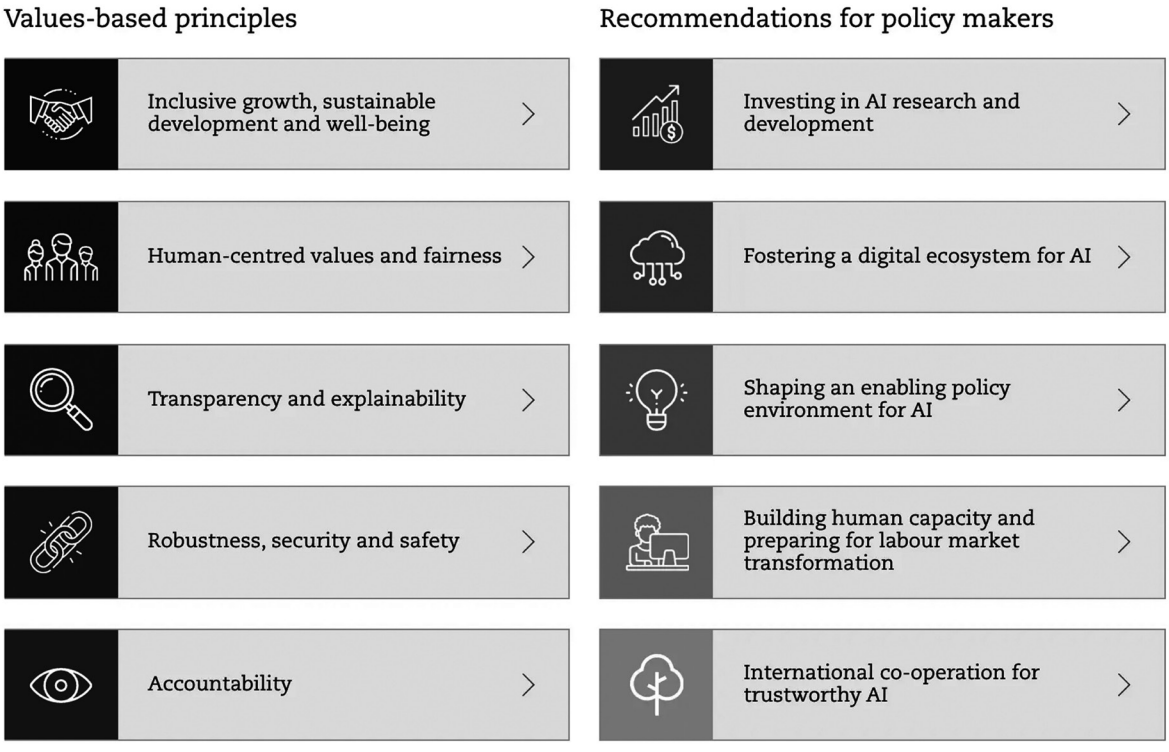
OECD AI Principles: Overview[15]

Artificial intelligence (AI) is transforming every aspect of our lives. It influences how we work and play. It promises to help solve global challenges like climate change and access to quality medical care. Yet AI also brings real challenges for governments and citizens alike. As it permeates economies and societies, what sort of policy and institutional frameworks should guide AI design and use, and how can we ensure that it benefits society as a whole? The OECD supports governments by measuring and analysing the economic and social impacts of AI technologies and applications, and engaging with all stakeholders to identify good practices for public policy. The OECD AI Policy Observatory (OECD.AI) combines resources from across the OECD and its partners from all stakeholder groups. It facilitates dialogue and provides multidisciplinary, evidence-based policy analysis and data on AI's areas of impact. It is a unique source of real-time information, analysis and dialogue designed to shape and share AI policies across the globe.

Its country dashboards allow you to browse and compare hundreds of AI policy initiatives in over 60 countries and territories. The Observatory also hosts the AI Wonk blog, a space where the OECD Network of Experts on AI and guest contributors share their experiences and research.

The OECD Principles on Artificial Intelligence promote AI that is innovative and trustworthy and that respects human rights and democratic values. They were adopted in May 2019 by OECD member countries when they approved the OECD Council Recommendation on Artificial Intelligence.

The OECD AI Principles are the first such principles signed up to by Governments. They include concrete recommendations for public policy and strategy, and their general scope ensures they can be applied to AI developments around the world.



Source: https://oecd.ai/en/ai-principles

15. https://oecd.ai/en/ai-principles

Other Applicable Regulatory Framework[16]

In addition to RBI and SEBI which regulates the banking and securities aspects of Indian economy, there are other regulatory bodies also – which aims to enforce cybersecurity regulations in other sectors of Indian economy. These are the main regulating bodies that ensure laws and standards are upheld by all Indian organizations.

1. Computer Emergency Response Team (CERT-In)

Made official in 2004, the Computer Emergency Response Team (CERT-In) is the national nodal agency for collecting, analyzing, forecasting, and disseminating non-critical cybersecurity incidents.

In addition to cybersecurity incident reporting and notifying, the CERT-In cybersecurity directive helps with issuing guidelines for Indian organizations guidelines as well, offering the best information security practices for managing and preventing cybersecurity incidents.

The Jurisdiction of Information Technology Rules, 2013 is responsible for mandating all Indian data centers, service providers, and their intermediates. All intermediaries are required to report any cybersecurity incidents to CERT-In.

CERT-In acts as the primary task force that:

- Analyzes cyber threats, vulnerabilities, and warning information;
- Responds to cybersecurity incidents and data breaches;
- Coordinates suitable incident response to cyber-attacks and conducts forensics for incident handling;
- Identify, define, and take suitable measures to mitigate cyber risks;
- Recommend best practices, guidelines, and precautions to organizations for cyber incident management so that they can respond effectively.

CERT-In roles and functions were later clarified in an additional amendment under Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules (IT Rules, 2013).

CERT-In Newest 6-Hour Data Breach Reporting Deadline

The newest regulations by CERT-In address cybersecurity reporting, mandating all Indian companies, service providers, intermediaries, data centers, and businesses to report identified cybersecurity incidents and data breaches within a 6-hour deadline.

However, many Indian organizations disapproved of the impossible requirement, stating that the short reporting window is insufficient to respond to cybersecurity incidents with a detailed report.

Despite the backlash, affected organizations that fail to follow these regulations face up to one-year imprisonment, significant penalties, and non-compliance fines if they fail to report cybersecurity incidents to CERT-In.

2. National Critical Information Infrastructure Protection Center (NCIIPC)

The National Critical Information Infrastructure Protection Center (NCIIPC) was established on January 16, 2014, by the Indian government, under Section 70A of the IT Act, 2000 (amended 2008).

Based in New Delhi, the NCIIPC was appointed as the national nodal agency in terms of Critical Information Infrastructure Protection. Additionally, the NCIIPC is regarded as a unit of the National

16. Reproduced from Kyle Chin (2023) Top Cyber Security Regulations in India, UpGuard. Available at https://www.upguard.com

Technical Research Organization (NTRO) and therefore comes under the Prime Minister's Office (PMO).

The Indian Parliament divides cybersecurity into two segments: "Non-Critical Infrastructure (NCI)," which CERT-In is responsible for, and "Critical Information Infrastructure (CII)," which NCIIPIC is responsible for. CII is defined by the Indian Parliament as "facilities, systems or functions whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation."

NCIIPC is required to monitor and report national-level threats to critical information infrastructure. The critical sectors include:

- Power and energy
- Banking, financial services, and insurance
- Telecommunication and information
- Transportation
- Government
- Strategic and public enterprises

NCIIPC successfully implemented several guidelines for policy guidance, knowledge sharing, and cybersecurity awareness for organizations to conduct preemptive measures of these important sectors, especially in power and energy. The guidelines represent the first means for regulating such sectors and requiring "mandatory compliance by all responsible entities."

Additionally, the Indian government approved the Revamped Distribution Sector Scheme in August 2021. The main goal of this regulation is to improve the operations of DISCOMs (distribution companies) by enhancing the cyber infrastructure with AI-based solutions. This will ultimately aid organizations and companies in meeting the framework's goals.

3. Cyber Regulations Appellate Tribunal (CRAT)

Under the IT Act, 2000, Section 62, the Central Government of India created the Cyber Regulations Appellate Tribunal (CRAT) as a chief governing body and authority for fact-finding, receiving cyber evidence, and examining witnesses.

While CRAT doesn't have as much jurisdiction for cybersecurity notification as CERT-In, the government also serves to respond to and act on related cybersecurity incidents and breaches.

According to the Civil Court and Code of Civil Procedure, 1908, CRAT has the power to:

- Receive evidence on affidavits;
- Ensure that all electronic and cyber evidence and records are presented for court;
- Enforce, summon, and issue regular commissions for examining witnesses, documents, and people under oath;
- Review final decisions of the court to resolve incidents and cases;
- Approve, dismiss, or declare the defaulter's applications as ex-parte.

4. Insurance Regulatory and Development Authority (IRDAI)

The insurance sector of India is regulated by IRDAI, which issues information security guidelines for insurers and addresses the importance of maintaining data integrity and confidentiality.

With this new Information and Cyber Security for Insurers Guidelines, the IRDAI:

- Mandates insurance companies to have a CISO (chief information security officer);
- Puts together an information security committee;
- Creates plans for managing cyber crises;
- Creates and implements cybersecurity assurance programs;
- Implements proper methods for protecting data;
- Maintains risk identification and risk mitigation processes.

The insurance sector of India mainly focuses on areas of higher risk, including ransomware attacks, transaction frauds, data leaks, and risks of violating intellectual property rights. According to a report by Sophos, 68% of Indian organizations were affected by ransomware and resorted to paying ransom to recover their data.

On October 9, 2022, IRDAI introduced an improved cybersecurity framework focused on the insurers' main security concerns. It aims to encourage insurance firms to establish and maintain a robust risk assessment plan, improve mitigation methods of internal and external threats, prevent ransomware attacks and other types of fraud, and implement a strong and robust business continuity.

Depending on the seriousness of the violation, insurers and businesses may be penalized upward of ₹1 lakh (₹100,000). If insurers fail to protect data they may be fined up to ₹5 crores per affected person. The IRDAI Guidelines for Information and Cyber Security for Insurers apply to all insurers regulated by Insurance Regulatory.

5. Telecom Regulatory Authority of India (TRAI) & Department of Telecommunications (DoT)

The Telecom Regulatory Authority of India, along with the DoT (Department of Telecommunication), have tightened regulations for user data privacy and how it's used.

TRAI is a regulatory body, and DoT is a separate executive department of the Ministry of Communications in India. Although TRAI has been granted more regulatory powers, both works together to govern and regulate telephone operators and service providers.

On June 16, 2018, TRAI released recommendations for telecom providers on "Privacy, Security and Ownership of the Data in the Telecom Sector." In the newest guidelines, TRAI addresses newer responsibilities governing consumer data because most digital transactions in India are done via cell phones.

TRAI addresses data protection with the following objectives:

- Define and understand the scope of "Personal data, Ownership, and Control of Data," namely, the data of users of the telecom service providers;
- Understand and identify the "Rights and Responsibilities of Data Controllers";
- Assess and identify the efficiency of how data is protected and which data protection measures are currently in place in the telecommunications sector;
- Identify and address critical issues regarding data protection;
- Collect and control user data of TISP (traffic information service providers) services.

The DoT has collaborated with the Indian IT ministry to impose layered data consent rules that safeguard

personal data processing. This gives users the freedom to decide whether or not they will consent to the usage of their personal data and the right to withdraw consent at any time.

The new rules state that organizations and companies will only have to collect the necessary user details and that the data may be retained only for as long as required. Additionally, Indian telecommunications service providers comply with common standards like ISO 27000, 3GPP and 3GPP2, and ISO/IEC 15408.

LESSON ROUND-UP

- E-Governance as the name suggest is made up of two words. “E” and “Governance”.
- Demands of transparency, ethics, rightfulness, access to justice, eradication of corruption and other related issues along with welfare driven political leadership, other associated governments, capacity building needs and perceived citizen expectations and all has contributed to adoption of e-government methods for good governance.
- The National e-Governance Plan (NeGP) has been formulated by the Department of Electronics and Information Technology (DEITY) and Department of Administrative Reforms and Public Grievances (DARPG) in 2006.
- These technologies are increasingly used by the society in day-to-day life from personal communications, buying goods at retail stores, availing services at doorstep to availing the governance through government offices.
- Seeing the potential of digitalization and its constructive impact supporting inclusive development of our country, Government of India has launched the “Digital India” campaign. The Digital India drive envisions transforming our nation and creating opportunities for all citizens by harnessing digital technologies.
- The advent of information and communication technology has revolutionized all the sectors across the globe. Indian banking and financial sector are not an exception to the transformation that has happened with the advent of information technology.
- Of all the IT domains that are impacting this industry, Artificial Intelligence (AI) and Data Analytics are the most influential contenders.
- Machine Learning (ML) and Artificial Intelligence (AI) are already being used in supervisory procedures by RBI. It now intends to make sure that the Department of Supervision at the central bank may reap the rewards of advanced analytics.
- Additionally, they have plans to bring in outside consultants for this work. For supervisory tests, the department has been creating and utilizing linear and a few ML models. Urban cooperative banks (UCBs), non-bank financial businesses (NBFCs), payment banks, small financing banks, neighborhood banks, credit information firms, and a few more Indian financial organizations are all subject to the RBI’s regulatory authority.
- The RBI came out with Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices on November 7, 2023 with an objective to tighten the governance framework for technology within banking segment.
- Earlier, the RBI had released the Master Direction on Outsourcing of IT Services released on June 23, 2022 to strengthen control framework for better management of outsourcing of technology services.

- These guidelines integrate consolidated and updated earlier instructions on IT Governance, Risk, Controls, Assurance Practices, and Business Continuity/Disaster Recovery Management separately released for Banks and NBFCs.
- Newly released Master Direction shall come into effect from April 1, 2024
- Governance structure and processes essential to achieve the entity's business/strategic objectives.
- This framework should define the roles (including authority) and responsibilities of the Board of Directors (Board), Board level Committee, Local Management Committee (in the case of foreign banks operating as branches in India), and Senior Management. It must encompass adequate oversight mechanisms to ensure accountability and mitigate business risks.
- As of April 2022, SEBI has six committee members that are required to oversee guidance for cybersecurity initiatives for the Indian market and advise SEBI to develop and maintain cybersecurity requirements following global industry standards.
- Additionally, SEBI also communicates with other agencies like CERT-In, NCSC (National Cyber Coordination Center), DoT (Department of Telecommunications), and The Ministry of Electronics and Information Technology (MeitY).
- SEBI implemented guidelines that apply to organizations within its scope — stock brokers, stock exchanges, AMCs (asset management companies), mutual funds, and depository participants, among others.
- With rapid technological advancement in the securities market, there is a greater need for maintaining robust cyber security and to have a cyber resilience framework to protect the integrity of data and guard against breaches of privacy.
- As part of the operational risk management, the Portfolio Managers need to have robust cyber security and cyber resilience framework in order to provide essential facilities and services and perform critical functions in the securities market as Portfolio Manager.
- Accordingly, all Portfolio Managers with asset under management of INR 3000 crore or more, under discretionary and non-discretionary portfolio management service taken together, as on the last date of the previous calendar month shall comply with the provisions of Cyber Security and Cyber Resilience, which has been put to effect from October 01, 2023.
- Thus, for several years, there were open questions about whether existing international law applied to cyberspace at all. Today, most states and several international organizations governs AI, cyber security and cyberspace.

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation.)

1. Briefly explain the concept of e-governance and types of e-governance.
2. Write a short note on RBI Circular on Cyber Security and its present-day impact on Banking Industry.
3. Write a brief note on compliance required to be followed as per SEBI Cyber Security Guidelines, 2023 – Cyber Security and Cyber Resilience framework for Portfolio Managers.

4. Write short note on any two of the following:
    - Vulnerability Assessment and Penetration Testing (VAPT)
    - Data Incident Reporting
    - RBI Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (November 7, 2023).

LIST OF FURTHER READINGS

- Nisha Dewani and Others (2022) Handbook of Research on Cyber Law, Data Protection and Privacy
- RBI Guidelines for Cyber Security, Deloitte Report, July 2016
- RBI Cyber Security Framework in India, Value Mentor, 2020
- RBI Circular on Cyber Security, PwC
- Walters and Novak (2021) Cyber Security, Artificial Intelligence, Data Protection and Law, Spinger.

LIST OF OTHER REFERENCES

- CSC 2.0 – Aims to cover 2.5 Lakhs of Gram Panchayats for Maximising delivery of e-Services to the citizens, The Digital India Campaign, Ministry of Electronics and Information Technology, Government of India;
- Digital India – Power to Empower, Ministry of Electronics and Information Technology, Government of India;
- Digital India – Unlocking the Trillion Dollar Opportunity (2016), A Report by Deloitte in association with ASSOCHAM India;
- Deepak J.S. (2015), Digital India-The Way Forward, MyGov Blog, Government of India;
- Ghosh Shyamal (2015), Digital India-Way Forward, Broadband India Forum, The Broadcast and Cable Set, India;
- Sengupta Deb Deep (2015), Digital Transformation-An Only Way Forward, December 2, 2015, The Live Mint;
- Teletalk 2016 – Digital India: The Way Forward, (2016), MITSOT, MIT School of Telecom Management's Blog.