Information Technology Risk and its Management

Dr. Subhasish Roy Chowdhury

Abstract

New incidents of cyber-attacks often come up in the news where an organisation's technological security infra web is compromised leading to loss and malafide use of confidential data. With the proliferation of such incidents at a high rate, it is pertinent and much wiser to assess the risk and volatility which exist in the domain of information technology, constantly and uninterruptedly with the help of a robust 'Information Technology Risk Management Framework'. Such a framework should possess enough intelligence to spot and predict the risks proactively and apply 'firewalls' to resist such risk from attacking the techno infra as well as apply adequate and faster healer to the already assalted techno infra and salvage it within no time lost.

==

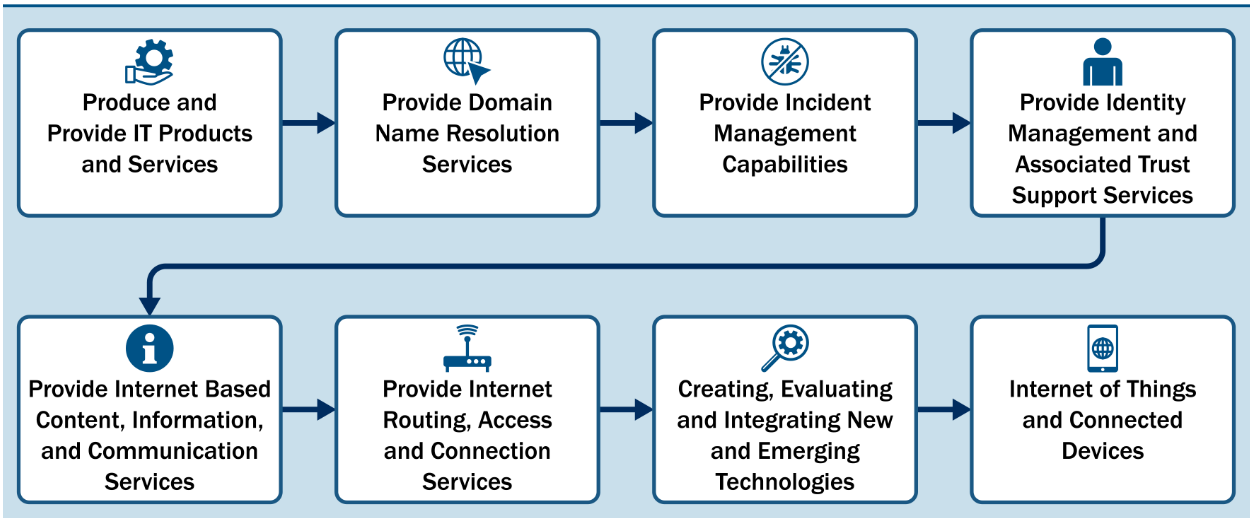
Risk is a probable possibility of loss, danger or injury. It is a probability or threat of damage, injury, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action. Risk is defined in financial terms as the probability that an outcome or actual gains will vary from an expected outcome or return. Risk may lead to the immense possibility of losing some or all of an expected outcome or return.

Managing risk is a well-articulated and designed mechanism of identifying, assessing and controlling any threat or menace to any life, business or asset / earnings. Risks usually stems out from a variety of known as well as unknown and unpredictable sources and uncertainties causing unbearable liabilities, technology issues, strategic management errors, accidents and natural disasters. So, there are two aspects to any risk: Uncertainty: An event may or may not happen Loss: An event has unwanted consequences or losses.

Corporate Governance – Conceptual Framework

Corporate Governance is much more than corporate management which includes fair, efficient and transparent administrative and management capabilities to achieve certain set and defined goals and objectives. It structures, operates and controls a corporate identity for achieving long term strategic goals with a satisfactory output for shareholders, creditors, employees, customers, suppliers / vendors and complying with legal and regulatory requirements and applications and also meeting local and environment community upliftment needs. Today in the age of globalisation, free flow and exchange of goods and services, capital and intellectual capabilities across the globe between different countries is an essential traffic system. Expansion and restructuring of corporate organisations are leading more to the exploration of vast potential resources and opportunities available across the globe. Thus, with the speedy expansion of global economy, Corporate Governance has evolved as a dependable system by which a corporate organisation can be directed and controlled towards achieving strategic goals and objectives of owners , safeguarding interest of employees , undertaking social responsibilities towards environment and community , maintaining very cordial relationship with customers and entire supply chain and complying with applicable legal and regulatory framework of the country of operations.

Critical functions in an Information Technology (IT) life cycle


Produce and Provide IT Products and Services
Provide Domain Name Resolution Services
Provide Incident Management Capabilities
Provide Identity Management and Associated Trust Support Services
Provide Internet Based Content, Information, and Communication Services
Provide Internet Routing, Access and Connection Services
Creating, Evaluating and Integrating New and Emerging Technologies
Internet of Things and Connected Devices

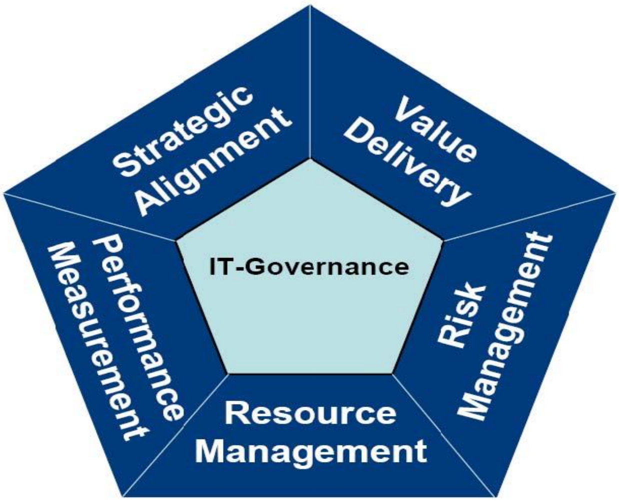
Information Technology (IT) Governance and Risk Management

Information Technology encompasses the most basic components like networks, devices, infrastructure, software and its applications, data and information including its storage and protection, human resources like developers, users, support staffs and other individuals involved in the operation and use of technology and lastly, processes – manual or automated. Business Technology risk relates with deployment of and reliance on technological automation of business processes. Any threat or invasion to the business data, critical systems / processes with regard to its use, ownership, operation, involvement, influence and adoption with the organisation can pose a potential damage of business health and value. The immediate potential questions which triggers the impetus of thoughts in the arena of IT Risk management are: -

- Are there proper ways and means for the business to understand threadbare about how IT operates and how it can provide immense support and contribute towards operating a business cycle?

- What can an IT framework perform or not perform within a certain time frame?
- Is the IT organisational frame work facing dramatic changes in post COVID times with major inception of Artificial Intelligence, Machine Learnings, ChatGPT, Claude etc. invading into the forte of business organisation big time?
- Is there adequate view or control over IT spending, or are IT costs perceived to be too high?
- Is there good understanding of IT related risk? Are IT related risks properly managed?

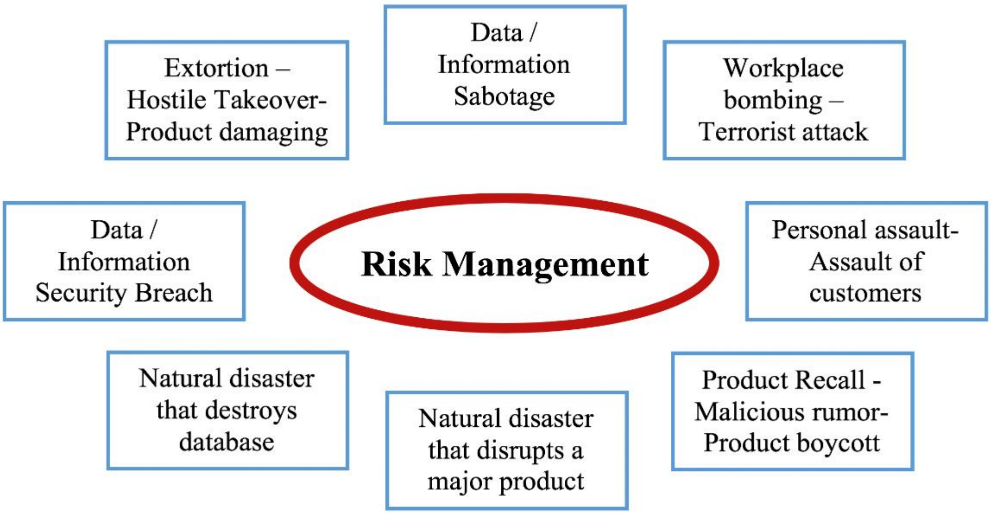
IT Governance Framework envelopes:



Information Technology Risks Areas

Business Continuity Plan (BCP) forms an impairable part of managing IT risks in a business. Adequate business planning through Proactive Risk Management (PRM) and Disaster Recovery Plan (DRP) can aid in minimising the potential impact of technological disaster in a business – be it a technical / equipment failure, a cyber-attack or a simple power outage.

The broad invaders into Information Technology areas as picturized below: -


Extortion – Hostile Takeover- Product damaging
Data / Information Sabotage
Workplace bombing – Terrorist attack
Data / Information Security Breach
Risk Management
Personal assault- Assault of customers
Natural disaster that destroys database
Natural disaster that disrupts a major product
Product Recall - Malicious rumor- Product boycott

The most generic IT threats are: -

- hardware and software failures
- malware—malicious software designed to disrupt computer operation
- viruses—codes that can spread from 1 computer to another, disrupting computer operations
- spam, scams, and phishing—unsolicited contact that fool people into giving personal details or buying fake goods
- human error—accidentally opening an email containing viruses, incorrect data processing, or careless data disposal
- natural disasters—floods, storms, and bush fires may interrupt service within the business or to external suppliers

The most criminal IT threats are: -

- ransomware—software that prevents the user from accessing their files or any part of the computer system until a ransom is paid
- hackers—people who illegally break into computer systems
- fraud—using a computer to alter data for illegal benefit
- password theft—stealing log-in credentials to impersonate you for illegal gain
- denial-of-service—online attacks that prevent website access for authorised users
- security breaches—physical break-ins as well as online intrusion
- staff dishonesty—theft of data or sensitive information, such as customer details.

Worst case scenarios which eventually lead to disruptive IT risks in a business

Some of the worst-case incidents which eventually lead to a disastrous IT risk and disruption in a company are: -

- Lost power supply - having no access to internet
- Key company documents have been destroyed
- Business premises have been totally damaged thus, leading to loss of data through disruption of data server and cyber connectivities
- Staff with extreme knowledge about IT quits the company – there has been no process of perfectly substitutable succession planning of such key/critical expert brain
- Company's sensitive data can be accessed through external devices by downloading company software – there is no process of autoblocking ingress or egress of data into and from the company's data server

- Unawareness in staffs about cyber security, phishing, malware and how to prevent such threats
- Login and password sharing by staffs specially the high end executives of the company
- Absence of duty / responsibility segregation and two-factor authorization process in the company's software

Bare minimal measures which may need to include in the organization's business continuity plan wrt IT Risk Management are:

- a backup and data recovery strategy, including off-site storage
- development of a resilient IT infrastructure with spare capacity in case of failure – i.e. mirrored central server computers sited in different locations
- elimination of single points of failure, such as a single power supply
- secondary manual systems to use until the ability to restore IT services is ensured
- agreeing with another business to use each other's premises in the event of a disaster
- arranging to use third-party IT services and accommodation until the restoration happens
- authority mapping and delegation along with responsibility segregation process

General Principles of Managing Information Technology Risks

An organisation deflects as much risks as practical and possible through a matured IT risk management framework by deploying significant resources in that direction as in today's business, IT has become an organ of the business body which if fails will horrifyingly result into a multi organ failure of the business.

Any organisation aiming at zeroising risks may miss out on potential business growth and profit earning opportunities hence, it is the smartest possible way of handling such risks in business which can curb disasters and simultaneously enhance business health in terms of growth of both top and bottom lines. Driven by events no one could have foreseen, leaders in recent years have pushed their companies and themselves beyond their comfort zones i.e. out of the office to remote workplaces, into the cloud, along chains of supply that are almost completely digital. And with each new venture has come new cyber risks. CISOs and cyber teams are rising to the challenge. C-suites are joining forces with them, recognising that their bold moves have increased their organisations' cyber risk exposure.

The general principles of managing IT risks are: -

- Risk Avoidance: The organization deflects as many risks as is practical and possible, focusing significant resources to that end. Unfortunately, most rewards require some risk, so an organization practicing avoidance may miss many opportunities for growth and profit
- Risk Reduction: Risk reduction is a mitigation strategy, where the organization changes certain aspects of a project plan, altering the process, or possibly reducing the scope.
- Risk Sharing: The organization spreads the risk's impact among other departments or project members. Companies could even share the risk with an outside business partner or vendor.
- Risk Retention: Finally, we come to the "grit your teeth, march full speed ahead, and hope for the best" approach. This strategy involves accepting the risk as a necessary evil and proceeding with the plan. The reward is deemed worthy of the risk, and if anything blows up, so be it.

Developing awareness about the possible IT risks within the premises of the organisation

Considering the utmost significance of IT in today's business environment, the jet speed at which the developments are happening in the IT front worldwide has its own pros and cons. On one hand, the rapid IT knowledge domain developments happening regularly is helping the business to boost itself up at a much higher pace wrt decision making, implementing decisions and monitoring impacts of such decisions. On the other hand, it also catastrophe the business environment through occurrence of cyber-attacks, crimes and other technological holocausts.

In view of the threats it is of much necessary to develop awareness about the threats by establishing an IT risk management template, roping therein all the possible treats which the business may be prone to hence, explicitly define the expectations from a robust and efficient IT risk management framework through developing sound awareness within the organisation which include: -

- Well-articulated Business Disaster Recovery Plan (BDRP) which can be followed as a guideline to ensure faster recovery of data in the event of potential loss of data
- Deploying stringent security measures through password policy, data confidentiality and access policy, data center management policy, intrusion into business software through external devices like pen drive, external hard disks etc.

- Developing awareness sessions about different types of Cybercrimes or cyber Terrorism which the business may be prone to so that employees working in the organisation are pre-aware and trained to act with appropriate safeguards in case of such events take place suddenly in order to stop it at its root itself.
- Staying prepared for hardware / software malfunctions where lost data cannot be recovered in which case regular data backup is a mandatory process which will help in salvaging the situation
- Preparedness to manage scalability issues in case of migration to new major applications in a cost-effective manner without any bottlenecks and silted architecture without any major down time
- Understand the probability of an event that could trigger similar risk and analyze how it relates to the time value of the exposure, if such risk occurs again. At this stage, the threat of the attack should also be understood completely
- Evaluation of risk management logistics to be reviewed within legitimate periodicity so that no scope of a system breakdown is left open which may lead to painful suffering for the business operations.

Block Chain Technology (BCT) in managing Information Technology Risks

BCT is a revolutionary decentralized autonomous organization (DAO) built on the pedestal of cryptography and information technology in contrast to the old modus operandi of record keeping issues by forging more trust, accuracy, transparency and less cost. In 2008, a group of individuals under the stewardship of Satoshi Nakamato ideated the theory of Blockchain (BC) in a paper 'Bitcoin: A Peer-to-Peer Electronic Cash System' without any trusted third party coming in-between. 'Ethereum' – a new technology with new functionalities was born aiding in better use of tokens and implementation of 'Smart Contracts'.

- BCT is an open (anyone with an internet connection can join the chain) , distributed (many can enter into transactions without a centralized intermediary – no authority can either allow or deny access to the chain - the chain is a composite of computers across the world connected to each other on the network directly or indirectly via an overarching software protocol) , decentralized (no single party can control / influence the chain – it is governed by a set of rules which no party forming part of the chain can violate it or deviate from it) and global ledger/ database (transparent data storage capability however, a limited capacity and an expensive archive) .

- As a BC envelope and connects a large and unlimited number of computers across the globe, each computer in the chain is termed as 'Node' having same copy of the database. The BC database has 2 key elements viz. (a) Record – which is information, data, contract, money or almost anything else, (b) Block – a bundle of records linked to other blocks, creating a chain.
- When a record with a transaction is created in the chain, the nodes synchronize between themselves along the entire chain and checks those transactions to ensure its validity subsequent to which, the record/transaction is linked to the block post its threadbare auto validation.
- Each block auto creates its own unique finger print known as cryptographic 'Hash' through a mathematical 'guess game' known as the 'Proof Of Work' and connects with the hash of its immediately preceding block in the chain with a time stamp which is non-tamperable after being added and helps in data tracking and information security.
- Hash takes the digital information and generates a unique string containing letters / numbers which is then uniquely associated with the block's transactions. The Hash code changes whenever the block is edited in any way thus making it extremely difficult for information on the BC to be changed without getting noticed across the chain.
- After a Node finds a valid Hash for the BC, it broadcasts the solution to the rest of the network which enables other Nodes to cross verify that the resulting Hash meet the protocol requirements. If the consensus protocol between the Nodes proves that the Hash is valid only then the block is added to the chain over writing the preceding block – a new BC is formed.

<u>Application of BCT in managing IT Risks</u>

- **<u>Eliminates human intervention:</u>** Transactions being approved by all nodes on the BC eliminates human intervention and resultant manual errors. Single node computational error would only be made on single copy of BC, repetition of it by at least 51% of the nodes can only multiply the error which is a near impossibility in BC.
- **<u>Reduces cost:</u>** Cost for any third-party verification and validation of a transaction as it happens in case of a manual transaction is largely reduced.
- **<u>Decentralized transparent data storage:</u>** BC information isn't centrally stored and controlled single handed hence, has less susceptibility of tampering / hacking the database as it has a universal visibility across the chain.

- **Time efficient:** BC is operational 24x7 in contrast to any other organisation like a bank, corporate etc. Like in case of a cheque deposited in bank can be completed in a BC instantly with utmost accuracy.
- **Secrecy of user information:** BC user nodes can't access identifying information about a user making a transaction without knowing unique code 'Public hence, the personal information of the user initiating any transaction will remain unrevealed to any other user in the chain.
- **Secured transaction:** A BC transaction is authenticated / validated by thousands of nodes only after which, the transaction is added to the BC block with a unique hash attached to it as a distinctive identifier.

COBIT (Control Objectives for Information and Related Technology)

COBIT – an IT management framework developed by ISACA (Information Systems Audit and Control Association, USA) containing a design of a set of IT control objectives to better navigate the growth of business IT environments. ISACA released COBIT 2.0 in 1998 which enlarged the framework to apply outside the auditing community. COBIT 3.0 was developed in 2000 to bring about more deeper IT management and information governance techniques. COBIT 4.0 was developed in 2005 followed by refreshed COBIT 4.1 in 2007 to induce more stricter governance over information and technological communication and wider risk management and information governance landscape.

The significance of COBIT is to provide a common language for IT professionals, business executives and compliance auditors to have a mutual communication over the same wavelength regarding IT controls, goals, objectives and results. Without a common language platform, a business under audit runs the risk of having to educate the individual auditors about when, where, how and why specific IT controls were created.

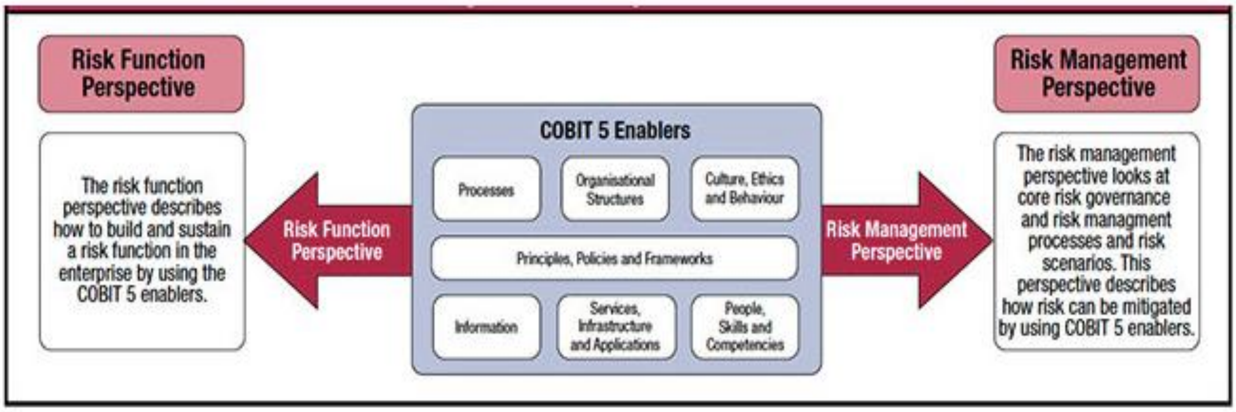
The current version of COBIT is not a cheat sheet but a generic tool to support business decision making with technology. The constituents of COBIT are: -

Objectives: COBIT 2019 have 40 business management and governance objectives which the IT managers need to prioritise or ignore these objectives based on the requirements of different stakeholders.

Domains: COBIT objectives are mapped and clubbed into specific domains which in turn is mapped to different business processes like planning, building and monitoring.

<u>**Cascade goals:**</u> This defines the connectivity between needs and business goals which need to be achieved through enabling components like IT skills, infrastructure, process descriptions and structures which influence IT landscape.

<u>**Design factors:**</u> Such factors include contextual, strategic and tactical factors which help in defining the need of business and how they must be addressed in a workable and well-governed IT framework. These factors drive implementation of chosen technology such as cloud technology, agile technology, business process outsourcing etc.


Risk Function Perspective
The risk function perspective describes how to build and sustain a risk function in the enterprise by using the COBIT 5 enablers.
Risk Function Perspective
COBIT 5 Enablers
Processes
Organisational Structures
Culture, Ethics and Behaviour
Principles, Policies and Frameworks
Information
Services, Infrastructure and Applications
People, Skills and Competencies
Risk Management Perspective
Risk Management Perspective
The risk management perspective looks at core risk governance and risk managment processes and risk scenarios. This perspective describes how risk can be mitigated by using COBIT 5 enablers.

Source: ISACA, *COBIT 5 for Risk*, USA, 2013. Reprinted with permission.

Artificial Intelligence (AI) - Information Technology Risks

In today's very fast changing world of activities, AI/ML/DL plays a very significant role in order to bring in minute precision in an activity with minimum resources and time deployment and maximising the quality of results obtained to its fullest potential.

- <u>**Deficient Transparency:**</u> Opaque AI /ML and DL models can become complex to understand and interpret about the results of its action on the global life. The opacity may also make the decision-making cycle and processes very obscure and incomprehensible. Such ambiguities about decisions taken by an AI may lead to distrust and unputdownable resistance to adopt the technology by the mass.
- <u>**Discriminatively biased:**</u> AI whether advertently or inadvertently perpetuates or amplifies social biases while functioning on algorithmic designs of data which may be used for mass training and development. This may in turn loose out in ensuring all fairness to its application to the diverse mass resulting into a massive pushback resulting into wastage of deployed resources in terms of '3Ms Management' i.e. 'Man-Money-Material'.
- <u>**Privacy intrusions:**</u> Food for any AI is 'Big Data' on which it works and demonstrates its charismatic results. These substantially voluminous data sets are personal in nature hence, if such data sets are not guarded well from the view point of data privacy and

protection, the safety, security and confidentiality of the data remains open to all possible usages having a malafide and deceiving intentions which may even to ransacking the originating source of such data.

- **Ethical Dilemmas:** AI Researchers and developers should focus more into morals and ethics while building an AI instead of staying in a quandary or impasse about ensuring ethical behaviour of an AI tool. The moot ethical driver in making of any AI should be of use to societal benefits where the concept of ethics plays a pivotal role.
- **Existential Risks:** Artificial General Intelligence which surpasses human intelligence raises a long-term concern over humanity which can lead to potential catastrophic consequences with regard to human values and priorities. AI research vigilantes need to engage very actively in setting up safety, governance guidelines so that the model serves the society to the best interest of humanity and doesn't become a paramount existential threat.
- **Overreliance on AI:** Over dependability on AI may lead to a phenomenon of loss of human creativity, critical thinking, skills and intuition which may disrupt human cognitive abilities. Also, automation through AI has the potential of leading to loss of employment across various industries, mostly of low / mid skilled employees, though the emerging technologies will create jobs as well for technologically knowledgeable candidatures. Ai can also create economic inequality by disproportionately benefiting wealthy individuals and corporations.

Final thoughts

Information Technology is perpetuating regularly into more and more developmental modes along with emerging new technologies where the potential multiplicity of risk factors cannot be thoroughly obliviated as the technology lies at the plinth and root of large decision-making processes. Therefore, it is quintessential and significant enough to have a live security infrastructure at the backdrop which will stay activated 24x7 to identify any risk factor which creeps into the technology landscape to devastate it before it is arrested and adequately redressed though the process of 'Likelihood-Impact' analysis of the invading risks. Also, it is eminently required to simultaneously address and risks which are indirectly related with the technological developments happening around the globe so that humanity at large stay safe and sound and do not face any eventual holocaust in human life cycle.