MANAGING INFORMATION TECHNOLOGY RISKS IN BUSINESS

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 assaulted techno infra and salvage it within no time lost.

Keywords: Information Technology, Risks, Governance, Block chain, COBIT, Artificial Intelligence.

Author

Dr. Subhasish Roy Chowdhury
Adjunct Professor
Finance Department
Vivekanand Education Society Institute of Management Studies and Research
India.

Visiting Professor
Finance Department
Vijay Patil School of Management
D Y Patil University
India.

Risk is a probable possibility of loss, danger, injury or a probabilistic threat of any negative occurrence which is consequential to external or internal vulnerabilities. Such occurrences can be avoided with the help of taking preemptive actions.

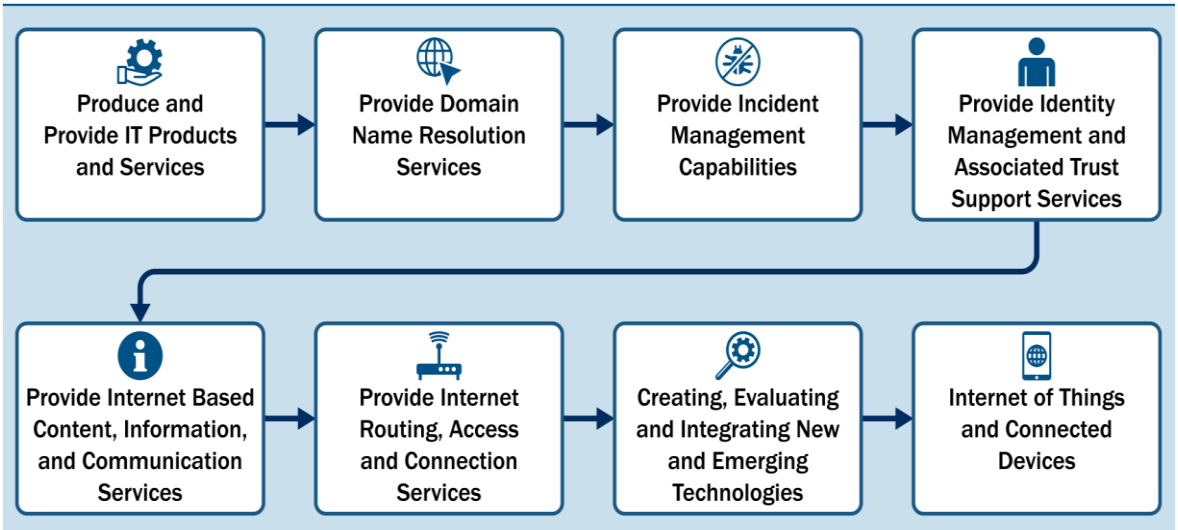
Risk is a probability of which any activity may have an outcome which may largely differ from the projected / expected results or returns. Occurrence of a risk may also lead to the probability of losing some or all of the expected outcome or results.

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 losses, liabilities, technological disruptions, strategical blunders or natural calamities. Therefore, any risk has a twofold aspect which are the probability or chances of a risk in an event happening or not happening which is termed as "Uncertainty" and the fatality of the result in case such an unwanted risk of an event happens which is termed as "Loss from risk".

I. 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.

II. CRITICAL FUNCTIONS IN AN INFORMATION TECHNOLOGY (IT) LIFE CYCLE

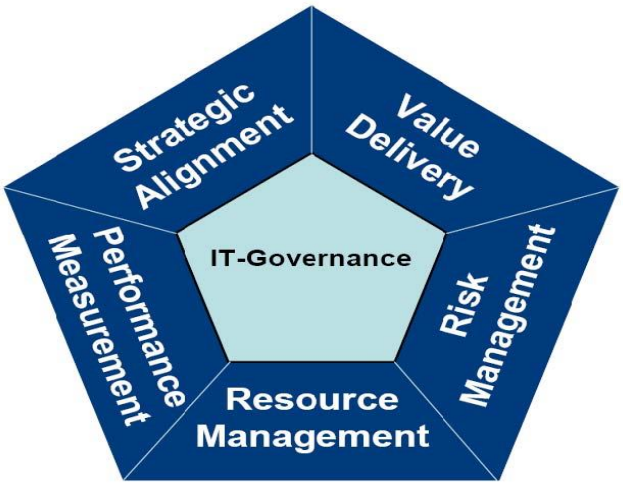


III. INFORMATION TECHNOLOGY (IT) GOVERNANCE AND RISK MANAGEMENT

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: -

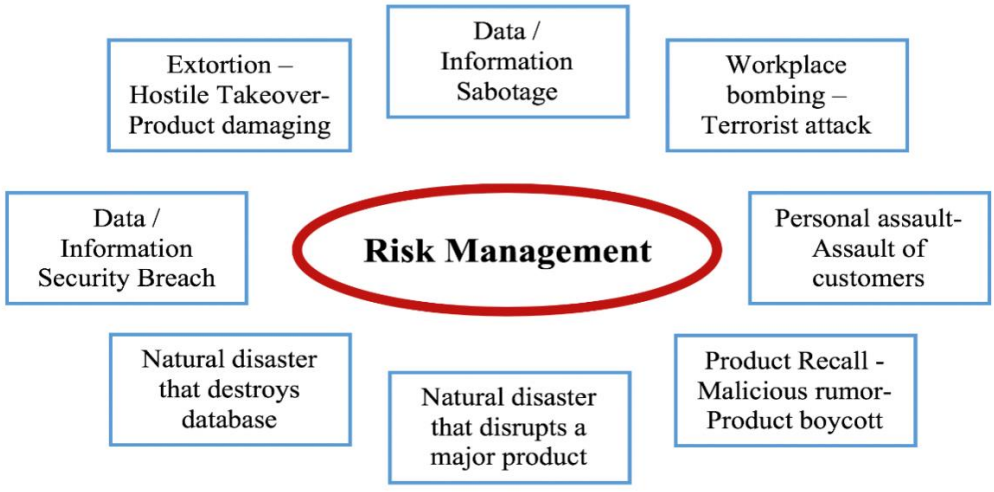
- Are there proper ways and means for the business to understand threadbare about how IT operates and how it can provide immense support and contribute towards operating a business cycle?
- What can an IT framework perform or not perform within a fixed time limit?
- Whether the IT organisational frame work is 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?
- Are IT spends adequately reviewed, monitored and controlled so that it doesn't shoot off the roof thereby eroding the business profits?
- Have the business been able to grasp a deep and clear understanding about the IT related risks and returns and whether such risks are properly managed to enhance the relative returns?

IT Governance Framework envelopes:



1. **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 minimizing the likely influence of technological business cataclysm through a technical or IT equipment failure or a cyber invasion of a simple power outage.

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



The most Generic IT Threats are: -

- hardware and software failures
- malware which are malevolent software formulated to disrupt any technological landscape or part of it
- viruses - the coded bugs which infiltrates into a technological platform to create an upheaval
- spam, scams, and phishing—most pestering links etc. which befools people by unknowingly sharing personal details or making fake investments, big or small. It may also include accidental opening of a virus infested email, inaccurate data processing or uncaring data handling / disposal

- natural calamities like floods, storms, and bush fires interrupting operations within or outside the business which strands the business functionality

The most Criminal IT Threats are: -

- ransomware stops users from accessing their files , data or any part of it until a ransom is paid
- hackers illegally invade into the computer system
- fraudulent alteration of data for illegal personal gains
- stealing log-in credentials to impersonate then user for fulfilling illegal advantages
- online cyber-attacks that prevent access to a website by authorized users
- physical break-ins or online intrusion leading to breach of security
- theft of data or sensitive information by dishonest employees

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: -

- Delinked from internet access
- Destroying key business documents like policies, SOPs , approvals etc.
- devastated business premises 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 measures, phishing, malware and how to protect the business from such threats
- Login / 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

Business Continuity Plan for a more polished, sophisticated and time-tested IT Risk Management are:

- Back-up plan / periodicity and strategy
- Faster data recovery policy and strategy from in-house and offsite data storages and data centers
- Resilient IT infrastructure should contain a spare capacity to faster replace any failures through mirrored central servers placed in multi locations
- Multi sourced power supply to auto connect in case a power source fails
- Associating with neighboring businesses 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

2. **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. Highly influenced by potential positive business environment, business leaders recently have taken their businesses beyond the comfort zones like remote offices, cloud, digital supply chain etc. followed by new risks every time whenever such a frame change in the business environment has been opted by business leaders. CISOs (Chief Information Security Officer) and the cyber team are exposed to extreme challenges of handling IT risks more meticulously to avoid any unforgettable business technology tragedies.

General principles of managing IT risks are: -

- **Risk Avoidance:** It's a process of eliminating business hazards, exposure to critical business complexities which can negatively impact upon business returns. It is a method of avoiding compromising events in its entirety. Business should be much careful in the process of avoiding risks so that it doesn't miss out on the business opportunities which provides good returns while avoiding associated risks. In other words, business should weigh between impact of risk and value of return and then decide whether the risk need to be thoroughly avoided or should be mitigated to a tolerable limit.

- **Risk Reduction:** It's a process of mitigating losses injecting specific strategy doses for risk reduction in terms of both likelihood of its occurrence and severity of its impact on the business. This may require revisiting the business strategies and plans and tweak or change them in a manner so that the impact and likelihood of a certain risk is mitigated enough.

- **Risk Sharing:** It's a process of dividing the risk between two or more co-operative business associates who agree to participate in the process of risk management, share some of the risks along with its outcome irrespective of whether it is negative or positive in order to provide solace to the business and get its operating cycle up and running without much fear or apprehension about the likelihood and impact of shared risks. This co-sharing strategy places both the parties to this model are enabled to shoulder joint responsibility of mitigating the risk with a more versatile and faster solutions.

- **Risk Retention:** Finally, this is the process of accepting the evil of the risk and progressing with the plan. It follows the essence of the saying 'grit your teeth, march full speed ahead, and hope for the best'. The risks are retained as it is felt that it cannot be zeroized else the business performance may succumb to such zeroization of risks. The return of retaining risks is deemed to be worthwhile and any blast happening out of such wilful retention of risks, if at all, becomes acceptable by the business.

3. **Inculcating Awareness about the Possible IT Risks:** 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 data loss.
   - 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 IT platforms and applications with cost effectivity and without any bottlenecks and silted architecture which may result into any major down time
   - Apprehending and understanding the probability of a business event that could trigger similar risk therefore, analyze its time value of exposure in case of its recurrence
   - 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.

IV. INTERTWINING RISK MANAGEMENT INTO BUSINESS SDLC (SYSTEM DEVELOPMENT LIFE CYCLE)

Effective risk management and SDLC should operate hand in hand. SDLC in the software industry is a mechanism to formulate, design and test high quality software which meets customer's expectations, stays within cost estimates and ensures job completion within pre-decided timeline. Risk management is an integral part of any SDLC phases as it eradicates any major lapses or inaccuracies that would put the SDLC into questions at the time of its implementation hence, it objectivises in preparing a hassle-free software which would enhance customer productivity and satisfaction. Risk analysis and mitigation need to happen at all the five stages of an effective SDLC viz.

1. '**Initiation':** need for an IT system is felt by the business along with defining and documenting the scope of developing the perceived IT infra, identifying allied risks and cyber security required,

2. **'Development and Acquisition':** decide upon designing/programming and constructing the IT infra in-house by a team having requisite core competence or outsource it to vendors / specialists wherein risks identified in the decision making process becomes a useful trade-off between architecture / design of the infra and the corresponding vulnerabilities,

3. **'Implementation':** configuring, enabling, testing , verifying and confirming the infra security measures as required for the modelled system environment before it is put to work,

4. **'Operation and Maintenance':** ensuring the continuity of system performance without any idle time even at the time when it undergoes various requirements about hardware / software modifications corresponding to changes in business needs and requirements. At this stage, it is imminent to have a periodic system re-authorisation and re-affiliation in times of changes made in the infra,

5. '**Disposal':** disposition of hardware / software like archiving, discarding, replacing, sanitising through a process of proper risk addressal system to ensure propriety and appropriateness of the process of disposition.

V. 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.

VI. APPLICATION OF BCT IN MANAGING IT RISKS

1. **Eliminates Human Intervention:** 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.

2. **Reduces Cost:** Cost for any third-party verification and validation of a transaction as it happens in case of a manual transaction is largely reduced.

3. **Decentralized Transparent Data Storage:** 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.

4. **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.

5. **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.

6. **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.

VII. 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 manoeuvre the expansion and performance growth of business technology needs. ISACA released COBIT 2.0 in 1998 which broadened application of the infra outside the audit community at large. 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.

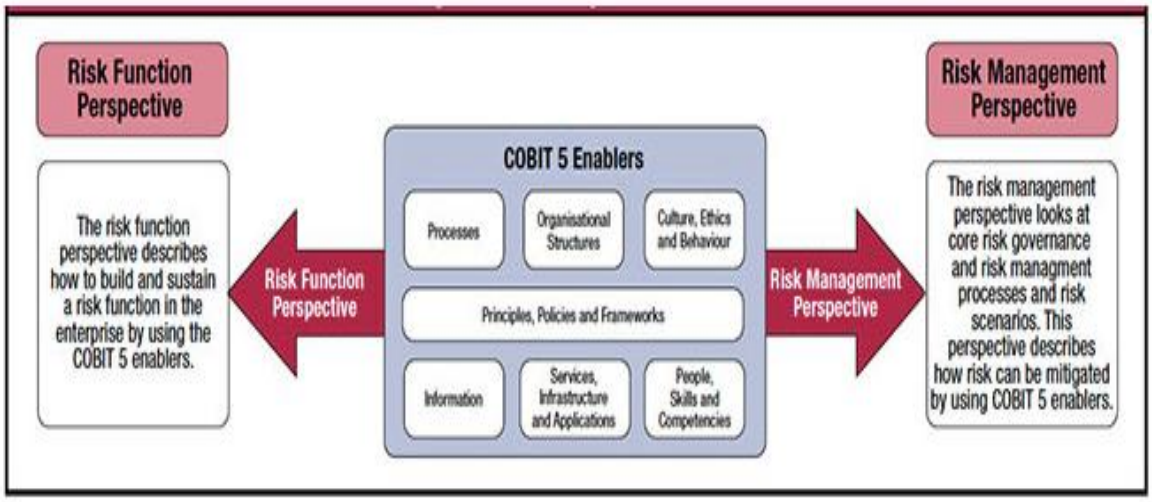
COBIT aims at providing a common language for IT professionals, business executives so that a mutual communication under the same wavelength wrt IT controls, goals, objectives and results can be drawn. Absence of a common language platform may lead to disparities of education about when, where, how and why such specific IT controls were created. Thus, COBIT is not a cheat sheet to follow but a dynamic tool to support technology-based business decision making process. The constituents of COBIT are: -

1. **Objectives:** Out of the 40-business management and governance objectives under COBIT 2019 model, IT managers need to think through deeply and prioritise or ignore these objectives based on the requirements of different business stakeholders.

2. **Domains:** COBIT objectives forms a delinkable chain where such objectives are mapped to specific business domains and processes like planning, architecting and monitoring so that Adequate fall backs are readily available for any vulnerabilities happening.

3. **Cascade Goals:** IT infra requirements should be connected with business goals in a manner that it facilitates achieving the business goals smoothly through enabling factors like skills, infrastructure, process descriptions etc. which should influence the IT landscape encouragingly.

4. **Design Factors:** Include contextual, strategic and tactical factors for defining the need of business and how they must be dealt with in a workable and well-governed IT framework so that it drives implementation of chosen technology such as cloud technology, agile technology, business process outsourcing etc.



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

VIII. 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.

1. **Deficient Transparency:** 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.

2. **Discriminatively Biased:** 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'.

3. **Privacy Intrusions:** 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.

4. **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.

5. **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.

6. **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.

IX. 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.

REFERENCES

[1] Gary Stoneburner, Alice Goguen, Alexis Feringa (July 2002) *Risk Management Guide for Information Technology Systems* Recommendations of the National Institute of Standards and Technology NIST Special Publication 800-30.

[2] Hamid Tohidi (Islamic Azad University, South Tehran Branch, Tehran, Iran – 2010) *The Role of Risk Management in IT systems of organizations*, www.sciencedirect.com , Procedia Computer Science 3 (2011) 881–887 , 1877-0509 , Published by Elsevier Ltd.

[3] Sikender Mohsienuddin Mohammad (June 2020) *Risk Management in Information Technology*, SSRN Electronic Journal

[4] Simplilearn (2021) *Top IT Risk Management Strategies and How to Apply Them*

[5] Jim Boehm, Peter Merrath, Thomas Poppensieker, Rolf Riemenschnitter, and Tobias Stähle (November 2018) *Cyber risk measurement and the holistic cybersecurity approach* (McKinsey & Company)

[6] Conrow, Edmund H (2004) "*Risk Management for Systems of Systems*." Systems and Software Technology Conference, Salt Lake City, UT.

[7] Thakurta, R. (2014). ' *Managing Software Projects Under Foreseen Uncertainty* ' Journal of Information Technology Management, 25(2), 40-52.

[8] Knut Haufe et al. (2016). ' *A process framework for information security management' International Journal of Information Systems and Project Management*, 27-47.

[9] L. Lema et al. (2015). '*ITIL in small to medium-sized enterprises software companies: towards an implementation sequence*' Journal of Software: Evolution and Process, vol. 27, no. 8, 528–538.

[10] Talet, A. N., Mat-Zin, R., & Houari, M. (2014). '*Risk Management and Information Technology Project*' International Journal of Digital Information and Wireless Communications, 4(1), 1-9.

[11] The Modernization of Corporate Governance: Blockchain as a solution? Anne Lafarre, 24-25 January, 2019 , Tilburg University
[12] The Potential Impact of Blockchains on Corporate Governance: A survey on Shareholders'' Rights in the Digital Era - Véronique Magnier & Patrick Barban , Intereulaweast, Vol. V (2) 2018
[13] Corporations on Blockchain: Opportunities & Challenges, Alexandra Andhov - Cornell International Law Journal Vol. 53
[14] Blockchain Technology for Corporate Governance and Shareholder Activism - Anne Lafarre & Christoph Van der Elst , Tilburg University - SSRN Electronic Journal · January 2018 , DOI: 10.2139/ssrn.3135209
[15] Corporate Governance and Blockchains - David Yermack - Review of Finance, 2017, 7–31
[16] OECD Corporate Governance Working Papers No. 21 – 'The Potential for Blockchain Technology in Corporate Governance - Vedat Akgiray- https://dx.doi.org/10.1787/ef4eba4c-en
[17] Fraud and Emerging Tech: Blockchain - Lucy Wang
[18] How Will Blockchain Change Corporate Governance? - Abdelkader Derbali1, Lamia Jamel, Yosra Mani, Raied Al Harbi - International Journal of Business and Risk Management, 2019, Vol. 2, No. 1, 16-18
[19] Blockchain-Enabled Corporate Governance and Regulation - Dulani Jayasuriya, Daluwathumullagamage, Alexandra Sims - International Journal of Financial Studies - 18 June 2020
[20] Corporate Governance and Blockchains - David Yermack - NYU Stern School of Business and National Bureau of Economic Research - November 28, 2016
[21] The Influence of Blockchain Technology on Fraud and Fake Protection - Youngju Yun-ODU Undergraduate Research Journal Volume 7, Special Issue: Interdisciplinary Cybersecurity Research
[22] Block chain Technology – Risk and Corporate Governance – Dr. Subhasish Roy Chowdhury - The Management Accountant (ISSN-0972-3528), November -2021, Vol.-56, Pg. 22 to 25

