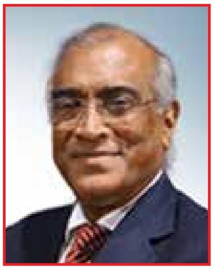
DIGITAL TRANSFORMATION - EMERGING DIMENSIONS OF RISKS AND AUDIT 4.0



CMA (Dr.) Paritosh Basu
Senior Professor
NMIMS School of Business Management
Mumbai
paritosh.basu@sbm.nmims.edu

Genesis of Accountability and Auditing

Desktop research of the author could trace conventional practices for documentation of movements in economic resources, reporting and exacting accountability from the in-charge of exchequer during the period of 1500 Before Common Era (BCE or BC). According to *Kautilya's Arthshastra*[1], this practice continued over centuries with progressively improved processes for recording and accountability of *rajashyas* (king's levies) and expenses to run the kingdom. The underlying objective of ensuring such accountability is essentially mitigation of various risks perceived by the kings of ancient era.

Pre-Vedic and Vedic literature, written by *Rishi* (Sage) Veda Vyas, sages of his clan and subsequent other literature, contain many references about audit. Mahajan and Mahajan[2] traced that in *Valmiki's Ramayana* there was a reference of auditing. Lord *Rama* asked his cousin brother *Bharata*, when the latter came to meet him during his exile, whether the income of his kingdom was more than expenditure or vice versa. In *Mahabharata* King *Dbarmaraj Judhistir* advised his younger brother *Nakula* to look after the army's accounts.

It seems that in that era independent record keeping by itself involved auditing, because the person responsible was a man of confidence like *Nakula* exacting accountability from persons in-charge of handling economic resources. Here again the drivers were anxieties driven by risks perception of a probability of the kingdom suffering from resource crisis or the army not being appropriately equipped and trained due to shortage or misappropriation of resources.

According to Wikipedia[3], *"By about the 4th century BC, the ancient Egyptians and Babylonians had auditing systems for checking movements in and out of storehouses, including oral "audit reports…"* LEE Teck-Heang and Azham Md. Ali[4] observed in their seminal paper on evolution of auditing *that. "The ancient checking activities found in Greece (around 350 B.C.) ..... The existence of such activities can be proven by Aristotle's quotation (as cited in McMickle, 1978, pp. 11-12).*

Similar kinds of checking activities were also found in the ancient Exchequer of England .... during the reign of Henry 1 (1100-1135) ... special audit officers were appointed to make sure that the state revenue and expenditure transactions were properly accounted for…."

One of the objectives of auditing is identification of risks followed by actions for mitigation. Processes for this have evolved over centuries in response to the perceived needs of investors for assurance about legitimate conduct and performance of individuals responsible for dealing with resources. Auditing continued to gain critical importance with accelerated industrialisation post World War - II. Lee and Azham[4] have quoted from papers of many research scholars observing that, *"… The aim of an audit has always been a dynamic rather than a static one. Brown (1962) asserts that the objective and techniques of auditing have changed during the four hundred years of recognizable existence of auditing to suit the changing needs and expectations of society."* Needs and expectations of society, investors, and business organisations from audit continued to metamorphose with impacts from mutated dimensions of political, economic, societal, technical, environmental, and legal (PESTEL) factors dynamically influencing business ecosystem.

Background and Objective

Human civilisation while evolving through centuries has witnessed three industrial revolutions, viz., mechanisation (1770), electrification (1870), Computerisation and Automation (1970) and expansion of horizon called Globalisation (1980). The present period is considered as the Industry 4.0 era which started from around year 2000. In the interregnum of about three and a half centuries mankind has experienced many regimentation changes. After World Wars the countries seem to have settled down to democracy in general.

The world had experienced dot.com bubble bursting in 1999-2000. Many believed that has heralded digital transformation (DT) powered by internet and innovative digitisation. The world had again endured worst ever global financial disaster during 2008 to 2010 due to subprime mortgage crisis in the USA. It is claimed that the birth of cryptocurrency is from the ashes of that crisis. Its cradle was provided by Blockchain technology. Having suffered such repeated man-made crises perceptions and scepticisms about efficacy, riskiness and success of digital technologies are still fresh in common people's mind.

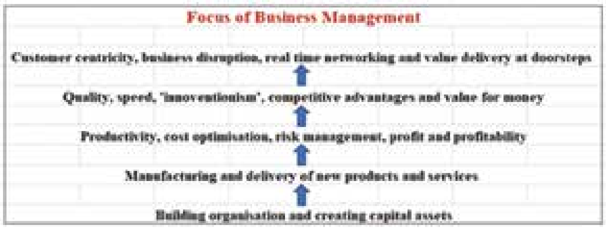
Advancements of digital technologies and 'innoventive' applications thereof at overwhelming speed are fearlessly yet beneficially disrupting corporates across industry sectors. Common people's way of living is being transformed through digital devices and soft aids. However, multipoint capturing of meta data and their unsafe storage are exposing peoples' core personal information to severe security and safety related risks. Their private digital spaces are also being invaded.

The newly added source of risks are employees working from home forced by Covid-19 Pandemic. On a positive note, the pandemic crises in waves are also the crucibles for building many more innovative digital solutions and multiplying success from existing applications. But cyber criminals are running their own industry by spawning malwares for hacking and extracting millions of dollars. Cyber warfare is also at the core of apprehensions of governments and commercial entities. The possibility of fighting the third world war at global cyber space are not being ruled out.

The author in his previous nineteen papers under this column has written about innovative applications of eight deep digital technologies, benefits being reaped, and startups working for building many more solutions. The objective of this article is to reflect on the risks that DTs are fraught with. It will examine how to approach identification and analyses of such risks through proactive and reactive auditing at different stages of planning, solution building, commercialisation, monitoring of systems, processes and deriving benefits for humanity.

Digital Transformation and Related Risks

The perception of this author as a student of finance gathered since 1967 through studies and research is that after the 2nd World War focus of business organisations have altered through decades in the following manner while horizon of conducting business activities kept on expanding:

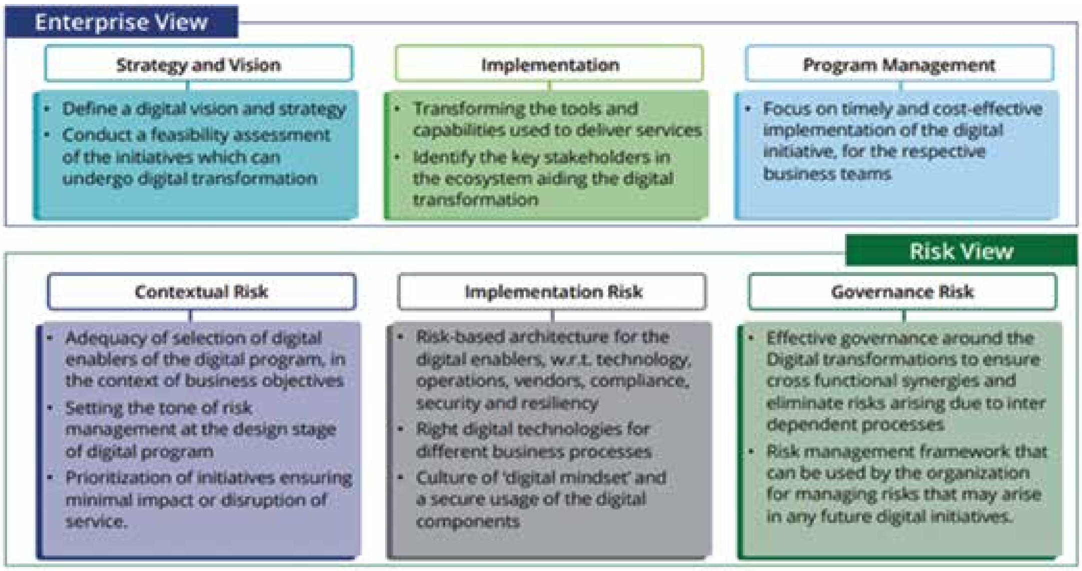

Focus of Business Management
Customer centricity, business disruption, real time networking and value delivery at doorsteps
Quality, speed, 'innoventionism', competitive advantages and value for money
Productivity, cost optimisation, risk management, profit and profitability
Manufacturing and delivery of new products and services
Building organisation and creating capital assets

The focal point of the present era of Industry 4.0 is at the top in which digital technologies are convincingly proving to be the most effective enabler of innovation. Business systems and processes are transforming at an overwhelming speed driven by the following major factors:

- Fast changing demographics, heightening consumer expectations and demands,
- Increasing urbanisation, deeper and speedy broadband, and logistical penetrations,
- Accelerated infiltration of smart devices and digital aids in the way common peoples' living life,
- Startupians challenging traditional operating systems by offering innoventive digital solutions with applications of IoTs, RPAs, deeper data analytics
- Growing propensity to adopt technological innovations to avoid being disrupted by first generation entrepreneurs.

Readers will agree that business risks are also equally going through multi-featured mutations triggered by the change of focus and technologies being adopted. Brian de Lemos[7] (2019) observed that *"Unfortunately, we've also seen what happens when these new technologies aren't managed properly: costly breaches or security incidents impacting reputation, trust, and the bottom line. It's critical to understand the factors that may introduce digital risks .... along with adoption. These risk challenges are not unique to any one industry…. What I hear from customers is the need for a consistent framework to assess their business risks. Additionally, security leaders want* *to buck the stereotype that they are "business inhibitors" and instead drive perception of being facilitators of their company's journey through vast disruption and change.*

All these, therefore, call for exploring and be informed about the dark side of DT before evaluating emerging risks, defining objectives of auditing of DT and designing processes for auditing. Deloitte in their risk advisory titled 'Managing Risks in Digital Transformation', 2018[6] advised that *"Digitalization means different things for different stakeholders. For an effective digital environment to meet the desired objective, it is critical to consider risk areas beyond traditional risk"*. They have captured the gamut of such new risks in the following visuals:



Enterprise View

Strategy and Vision
- Define a digital vision and strategy
- Conduct a feasibility assessment of the initiatives which can undergo digital transformation

Implementation
- Transforming the tools and capabilities used to deliver services
- Identify the key stakeholders in the ecosystem aiding the digital transformation

Program Management
- Focus on timely and cost-effective implementation of the digital initiative, for the respective business teams

Risk View

Contextual Risk
- Adequacy of selection of digital enablers of the digital program, in the context of business objectives
- Setting the tone of risk management at the design stage of digital program
- Prioritization of initiatives ensuring minimal impact or disruption of service.

Implementation Risk
- Risk-based architecture for the digital enablers, w.r.t. technology, operations, vendors, compliance, security and resiliency
- Right digital technologies for different business processes
- Culture of 'digital mindset' and a secure usage of the digital components

Governance Risk
- Effective governance around the Digital transformations to ensure cross functional synergies and eliminate risks arising due to inter dependent processes
- Risk management framework that can be used by the organization for managing risks that may arise in any future digital initiatives.

Source: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-managing-risk-in-digital-transformation-1-noexp.pdf

The above points are self-explanatory and easy to be assimilated for framing proactive and reactive audit plans and initiating mitigation measures. However, it will be worthwhile to appreciate the other dimensions of risks when a busines entity enlists DT at top of the CEO's agenda. If an entity plans for faster digital transformation with quantum leaps in operating proficiencies, customer centricity, new business and revenue models, the following risks threaten with dire consequences. This is because sub-optimal applications and inappropriate handling of digital technologies can lead to unprecedented security breaches, crisis of trust which can seriously damage reputation.

Syndromic Risks

Me Too Syndrome

Not all organisations need all sorts of DT in all segments of its business. The most common risk of cash burning without any tangible benefits occurs when digital technologies are adopted without relevant diagnostic studies befitting the specificities of a business entity and synergy analysis. Research findings suggest that random decisions driven by me too syndrome may slap adverse consequences even threatening an entity's very existence.

Sunflower Syndrome

One common perception is that plans for DT should be executed only when the going is good, and the entity is flushed with funds like blooming of sunflowers when the sun shines bright. Good going does not ensure sustainable growth and prosperity. Industry 4.0 is an era of disruption and 'destruption' (destructive disruption). Therefore, an entity need not wait for abundance to plan and adopt DT. At the same time profligacy may also negative returns. The decision for DT should absolutely be need based, else there would be possibilities of lagging at the wayside.

Shiny Object Syndrome

An entity should not adopt technologies, viz., RPA, Blockchain, AR & VR, FinTech and AI & ML because competitors or entities in other industry sectors are doing well by adopting one or more of those. The quest for finding a quick fix or a dropped from the sky solution for riding on the hype latest technology may prove to be perilous. Implementation of digital technology must be part of a larger vision for a company's sustainable journey, not an one-off activity.

Golden Goose Syndrome

Quite often entities end up with sub-optimal return from DT by expecting too much too soon. Power of digital technologies cannot be made to drive business at neck breaking speed like beating a horse to run fast. This may boomerang with law of diminishing return and may finally end up with tangible losses. The keynote of success depends on striking the right balance, ensuring flexibility and scalability.

Common Set of Risks from DT

i. ***Cyber militancy***

Cybercriminals and militants are equipping themselves with power of the same digital technologies that are being used by scientists to bring in inclusive smiles for humanity. Frequency of assaults with innovated digital weapons and stealthily manner of spawning malwares for extracting ransom are much more than before.

ii. ***Human resource***

Traditional manpower, unless made to learn, unlearn, and relearn can by itself be a source of risks. Balancing cost and reward calls for a combination of green horn digital technologists and retraining existing manpower having business insights. A structured framework for change management is a prerequisite for this.

iii. ***Flexibility and Scalability***

Initial success of digital transformation may not ensure scaling newer heights and/or adapting unforeseen/unprecedented changes in business ecosystem. Lack of flexibility and scope left for scalability in the blueprint for DT may pose as a source of risk. Such a risk can even cause derailing of an entity from the realms of its vision and mission.

iv. ***Cloud facility***

Despite all assurances from the cloud service providers, data security, safety and privacy risks cannot be ruled out. Proactive ethical hacking as a concurrent activity for monitoring such risks may be used as a deterrent for such risks.

v. ***Legal and regulatory compliance***

Compliance with legislated requirements should not be considered as the end of measures for risk mitigation. DT calls for remaining much ahead of one size fit all type of compliance requirements. This is because an entity has more insights about its business and technology specific vulnerabilities that may cause risks to sneak in.

vi. ***External Stakeholders***

Extending digitally transformed facilities to and integrating the same with those of external stakeholders, viz., vendors, customers, etc. are also sources of risks. Cyber criminals can infringe through the holes left unplugged at the stakeholders' end. Therefore, the same set of proactive risk mitigation measures with equal rigours should be insisted for implementation by those stakeholders.

vii. ***DT enabled SOPs***

DT would essentially necessitate reframing legacy operating practices for business operations with embedded measures for risk-enabled performance management. Such new SOPs, if are not in sync with solutions designed using digital tools, may be the fountain of self-generated risks with opened gateways for cyber criminals.

viii. ***Business Process Continuity Management (BPCM)***

DT entails voluminous storge of structured and unstructured data and analytics thereof. Experiences prompt that any type of hardware used for computerisation and data storage are susceptible to crashing and vulnerable to security risks. Business entities generally create facilities for disaster recovery and redressal (DRR) simultaneously with measures for business continuity. Therefore, BPCM and DRR can create potential risks unless redesigned and augmented with implementation of DT.

ix. ***Data privacy, safety, and security***

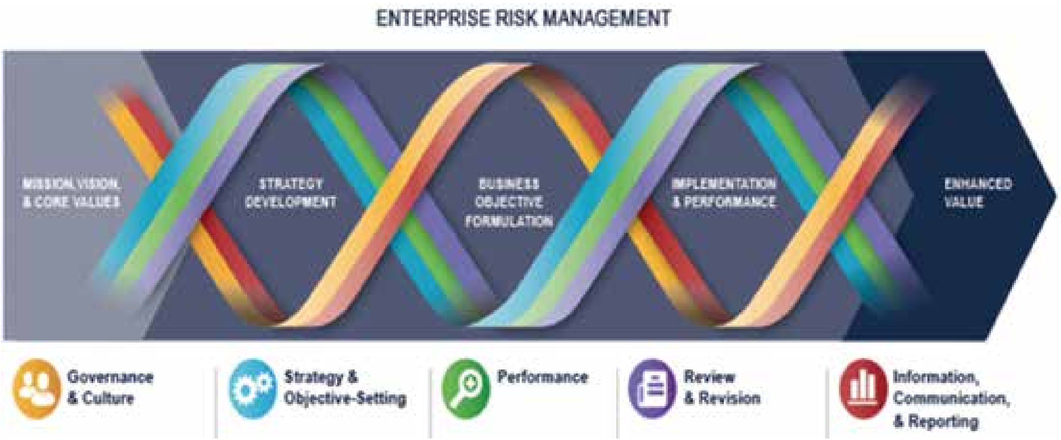
Last but not the least data is the most valuable strategic asset in present times, and key enabler of innovation. This is the new oil that drives business. Hacked out data can provide business insights/ secrets, key information of customers external stakeholders, etc. Therefore, such data is a source of potential risks because it is the most attractive asset to cybercriminals for extracting and abusing for monetary gains.

Digital Transformation and Audit

Readers by now might be sceptical and are thinking whether traditional post facto internal audits would still be effective in a digitally transformed operating environment! If not, what should be done about it? The author is not a professional auditor and hence will take resort to viewpoints of professional auditors and audit firms for bringing out the imperatives and recent developments. His research findings corroborate that such scepticism and anxiety are almost common across business entities.

Jim DeLoach, MD, USA, and a member of Protiviti's solution leadership team wrote in an article of August[8], 2020 that "*With digitization fuelling innovation and change, two questions arise: Is internal audit adjusting quickly enough to innovate and embrace underlying technologies, and should executive management and the board care?* The answer is in affirmative. The point that can be added to the views of Jim DeLoach is that every organisation should elevate and upscale responsibilities for in-house auditors to a digitally trained and equipped management audit team (MAT) with a differently designed approach befitting the need and specificities of the organisation.

The predominant objective for such elevation should be to ensure risks-enabled performance management. This function should no longer be treated as a post facto reviewer of what management has done and results thereof. Instead, it should participate as a proactive enabler for right decision making with responsibilities for continuous monitoring of the outcomes and suggest corrective actions. It would be useful to delve into 20 Principles[9] for enterprise risk management suggested by Committee of Sponsoring Organizations of the Treadway Commission (COSO, October 2018). This will inter alia help aligning the entire task with the vision, mission, and core values of the entity.


ENTERPRISE RISK MANAGEMENT
MISSION, VISION, & CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION & PERFORMANCE
ENHANCED VALUE
Governance & Culture
Strategy & Objective-Setting
Performance
Review & Revision
Information, Communication, & Reporting

Source: https://www.coso.org/Documents/COSO-WBCSD-ESGERM-Guidance-Full.pdf

Digital transformation is a journey and not a onetime exercise. Involvement of the MAT must be right from the beginning of this journey. For this purpose, an external expert group of consultants may be engaged for handholding and recommissioning the in-house team. But before that MAT must train their members to instil desired technical competencies and achieve a state of readiness for partnering with business and technology team members.

The statutory auditors' role should include the task of evaluating and attesting the process of governance and management audit functions as well as report on sufficiency and effectiveness of the newly framed/designed policies, SOPs, etc, in a digitally transformed environment. Members of MAT needs to also be effective in enhancing 'stragility' (ability to create agile strategies) and transforming into a multi-skilled technology enabled functional group. In the words of Jim DeLoach[8], this team *"..... must commit itself to elevate value proposition. .... Able to recognise emerging risks and changes to the organisation's risk profile quickly and efficiently enough .... To deliver stronger assurance and more valuable insights to the business efficiently, a next-generation function embraces a holistic approach focussing on competencies, qualities and components falling into three categories... Governance including strategic vision, Methodology and Enabling technology."*

In the context of proactive involvement of MAT in the journey with DT and a higher value proposition through assurance function, one can draw analogy from the following steps generally followed by business entities for implementing business expansion and/or diversification projects involving voluminous capital expenditure:

- ***Concept Study***: Environment scanning to bring out project idea as a broad investment proposition for DT.
- ***Pre-feasibility Study***: Further collection of data, analyses, and review to assess whether the concept study justifies a more informative study to be undertaken for aligning the DT project with vision, mission, and business model specific strategies.
- ***Technical and Financial Feasibility Study***: Establish technological, marketing, commercial and financial viabilities before investment decision is taken.
- ***Flexibility, Scalability and Sustainability Study***: Initial studies should contemplate probable changes in business ecosystem in predictable future that may necessitate ensuring flexibility and keeping scope for scaling up facilities with growth in business going forward. Sustainability in any case is an imperative to be kept in view at all stages.
- ***Detailed Project Report***: This would entail a complete report with analytical details of all aspects of the project including implementation schedule and systems for monitoring results and efficacy of risk management. This report is expected to include separate segments for the following:
  - Change Management: A white paper with well laid out plans for transition management from legacy to digitally transformed systems and processes.
  - Communication Strategy: Strategy for sharing the right information on a need-to-know basis at the right time with the right group of employees for creating the right impact and achieving a state of pervasive readiness. This would also help winning heart and garnering all-round support from all employees.
  - Training and Development: A detailed plan for training and upskilling existing manpower to make them future ready to successfully evolve and navigate through the process of executing DT and running the organisation with new capabilities. This should also include plan for talent acquisition with relevant knowledge and skillsets.

Involvement of the newly metamorphosed MAT right from conceptualisation stage would help:

- Developing a sense of shared ownership for their DT project right at the outset,
- Gathering more insights about the laid down policies and processes for conducting business with new systems and processes,
- Achieving consensus with all CXOs about future deliverables of MAT and the framework to be followed for auditing,
- Framing their own process for audit/review and

monitoring of results with applications of digitally enabled tools.

- Gaining abilities to proactively alerting management about challenges and upcoming risks that my disrupt and hinder progress, etc.

For this it would be logical to suggest, from the perspective of the principles of equity, that all the MAT members should also equally share all rewards and losses with all other functional team members.

Audit 4.0 - Smart Audit and Evidence Management

Organisations evolving with DT and riding through the trajectory of growth and prosperity, must plan for always working concurrent audit. In certain cases, if need be so, particularly for transactions processed through Blockchain platforms, online real time auditing systems may be introduced. It is not desirable to follow the traditional routine of periodical post facto audit because much damage might have been done in the intervening period. One must keep in mind that DT has accelerated the end-to-end processes of conducting business.

MAT must make efforts at regular intervals to anticipate, identify and appreciate nature, intensity and impacts of emerging risks and probable money value that could be exposed to risks in foreseeable future. This task of predictive analyses and profiling of business and technology related risks should be conducted at regular intervals with the objective of staying ahead of time. MAT should also organise brainstorming sessions at equal time intervals with leadership team members with the objective to frame audit plan and address those risks through appropriately articulated deliverables by assurance function.

The author could trace the following comment in an article titled 'Smart Audit: the digital transformation of audit' published in the Journal of European Court of Auditors, (February 2020)[10] - *"The world is changing at digital speed, but the accounting profession does not seem to notice it with arcane measures and old-fashioned assurance. The forthcoming data ecosystem (Cho, Vasarhelyi, and Zhang, 2019) will consist of a large chain of interlinked data sources and many constantly acting intelligent agents (Vasarhelyi and Hoitash, 2005) performing assurance tasks and drawing exceptions in some form of continuous audit (Vasarhelyi and Halper, 1991).*

When an organisation is evolving with DT, auditing also must adapt and transform with new realities. Jun Dai and Miklos Vasarhelyi[11] of Rutgers University in their paper on mentioned that *"Audit 4.0 will piggyback on technology promoted by Industry 4.0 to collect financial and non-financial information, and analyze, model, and visualize data for the purpose of providing effective, efficient, and real-time assurance. It is typically an overlay of Industry 4.0 business management processes and uses a similar infrastructure, but for assurance purposes."* They recommended auditors to master and use in auditing process digital tools offered by Sensors, computers embedded with Cyber-physical systems, IoTs linked to computers, RFID, GPS, and tools aided by AI and ML.

Aldo Dubacher, Mattig-Suter & Partner in his article on the subject[12] (Spring, 2020) wrote that, " ..... *digitalisation in auditing is not limited to electronic audit working papers. ..... the exchange of documents between audited companies and the audit firms is shifting to web-based data storage services. ....With the switch from paper to electronic working papers, powerful tools such as Excel-based analytical testing procedures will become essential. It is time to remove the critical attitude towards data analytics that is still widespread in the audit profession in the age of "big data*". Again tools for conducting audits should also be redesigned applying AI, ML and big data analytics.

Audit 4.0 and Ethical Hacking

Several research-based publications have pointed out with reference to facts that hackers with malicious objectives can penetrate any computing system howsoever strong and deep its fire walls and surveillance systems are. Cybercriminals have also infiltrated many a times data centres and cloud computing systems. The very recent two examples are alleged infiltration of computing and data storage systems of Maharashtra Industrial Development Corporation and Mobikwik, a digital wallet service providing Unicorn in India.

Cyber criminals are equally cerebral innovators, and create/sharpen weapons and strategize modus operandi with the power of AI and ML, etc. Therefore, testing hackability of any computing hardware, applications and data storage is a must before those are launched for commercial use and every time when those are modified and/or integrated with IT systems of external stakeholders.

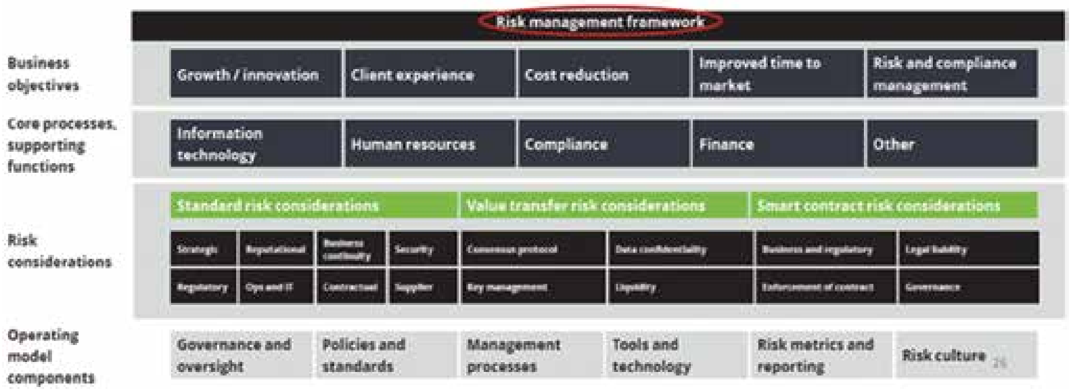
Ethical hacking is a legally permissioned assignment to penetrate any computing system, application, or data storage without being given any approved access. It comprises the task of anticipating and replicating strategies and actions of cybercriminals who may access with malicious objectives. This task also includes testing of penetrability into the system through the Apps in handheld devices of frontend customers.

The MAT of any organisation should, therefore, have a few such ethical hacking team members aka 'White Hats' who should proactively hack an entity's facilities for assessing vulnerabilities and suggest remedies for plugging apertures. The sole objective of such a group is to secure and improve in-house facilities and thus pre-empt attacks by cybercriminals. One time and recurring plans for friendly hacking should be done and approved by leadership team as a part of the main annual strategic plan for management audits. Utmost confidentiality must be maintained in all matters of ethical hacking and adverse findings must be addressed without losing any time what so ever.

Audit of Transactions through Blockchain Platforms

Blockchain, out of the eight deep digital technologies, can best be used for identity/credential management and conducting commercial transactions in a secured peer-to-peer network environment. The author has written about multifarious applications of Blockchain technology in his previous articles. Readers can access and study many those papers at the Knowledge Input section of the authors personal website https://www.innoventionians.com/ . In this article it would be worthwhile to examine new requirements for auditing. Deloitte in one of their publications titled 'Blockchain Risk Management'[13] mentioned the following about features of Blockchain Platforms:

Peer-to-peer framework offers the potential to transform current business processes by disintermediating central entities or processes, improving efficiencies, and creating an immutable audit trail of transactions. Blockchain technology and Smart Contracts embedded therein could alter the way organisations conduct business as many transactions are peer to peer in nature *"Blockchain technology will transform business models from a human-based trust model to an algorithm-based trust model, which might expose firms to risks that they have not encountered before. In order to respond to such risks, firms should consider establishing a robust risk management strategy, governance, and controls framework."* Deloitte has suggested the following risk management framework to be considered by auditors while framing their auditing strategies, plans and evidence management methodology.



Risk management framework

Business objectives: Growth / innovation | Client experience | Cost reduction | Improved time to market | Risk and compliance management

Core processes, supporting functions: Information technology | Human resources | Compliance | Finance | Other

Risk considerations:
Standard risk considerations: Strategic | Reputational | Business continuity | Security | Regulatory | Ops and IT | Contractual | Supplier
Value transfer risk considerations: Consensus protocol | Data confidentiality | Key management | Liquidity
Smart contract risk considerations: Business and regulatory | Legal liability | Enforcement of contract | Governance

Operating model components: Governance and oversight | Policies and standards | Management processes | Tools and technology | Risk metrics and reporting | Risk culture

Source:https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-blockchain-risk-management.pdf

The author is of the view that the MAT of every organisation can consider the above framework as the foundation for designing strategies and tools for auditing in a digitally transformed business environment with/without applications of Blockchain. It is accepted that there no standard way to validate blockchain-based business processes and the related control environment since Blockchain environments have unique architectures and lack standardization. Therefore, each business entity must design its customised control environment based on specificities of the platform designed by them. Traditional audit techniques may not be found effective for auditing transactions in Blockchain platforms. Audits for those should be planned and conducted on an online real time basis. There is a need for further research to ascertain whether tools have already been designed and applied for this purpose.

Conclusion

Digital transformation of business processes is helping commercial organisations to handle much larger volume of operations covering much wider horizon at an accelerated pace and achieving higher ROI. Needless to say, that complex, perilous and hitherto unknown risks are also being faced with far reaching impacts. Simultaneously with advancements of digital technologies and their more and more new applications the professionals engaged in rendering services for risk management, internal and statutory auditing are also evolving with new skill sets and experiential learning points.

In the above discourse the author has narrated how new systems, processes and audit tools are changing. Authorities for setting standards for both internal and statutory audits at global and country specific levels must be working for promulgating new versions of standards. Therefore, there seems to be no reason to believe that future does not hold many new promises for humanity to achieve inclusive smile. Readers must have appreciated the horizon, expanse, and enormity of the subject. A few pages of such an article are not enough to write about all its dimensions. The author would feel happy if ideas articulated in this paper, are found to be useful by readers for implementation at their respective organisations. MA

Bibliography and Webliography

1. *L. N. Rangarajan, "Kautilya - The Arthashastra", (India Penguin Random House India Pvt. Ltd.), 1992, pp 196 – 197, 245, 282.*
2. *Sanjeev Kumar Mahajan and Anupama Puri Mahajan, "Financial Administration in India", (India PHI Learning Private. Ltd.) pp 323-324.*
3. *https://en.wikipedia.org/wiki/History_of_accounting*
4. *LEE Teck-Heang and Azham Md. Ali, The evolution of auditing: An analysis of the historical development, Journal of Modern Accounting and Auditing, Dec. 2008, Vol.4, No.12 (Serial No.43) pp 1- 9.https://www.researchgate.net/publication/339251518_The_evolution_of_auditing_An_analysis_of_the_historical_development*
5. *https://www.researchgate.net/publication/339251518_The_evolution_of_auditing_An_analysis_of_the_historical_development*
6. *https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-managing-risk-in-digital-transformation-1-noexp.pdf*
7. *https://www.delltechnologies.com/en-us/perspectives/the-dark-side-of-digital-transformation-8-emerging-digital-risks/*
8. *https://www.corporatecomplianceinsights.com/getting-more-internal-audit-digital-age/*
9. *https://www.coso.org/Documents/COSO-WBCSD-ESGERM-Guidance-Full.pdf*
10. *https://medium.com/ecajournal/smart-audit-the-digital-transformation-of-audit-b283e1653bd4*
11. *http://raw.rutgers.edu/docs/wcars/38wcars/Presentations/Jun-Audit%204.0%20short.pdf*
12. *https://ggiforum.com/assurance/1946-how-digital-transformation-is-changing-audit-processes.html*
13. *https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-blockchain-risk-management.pdf*