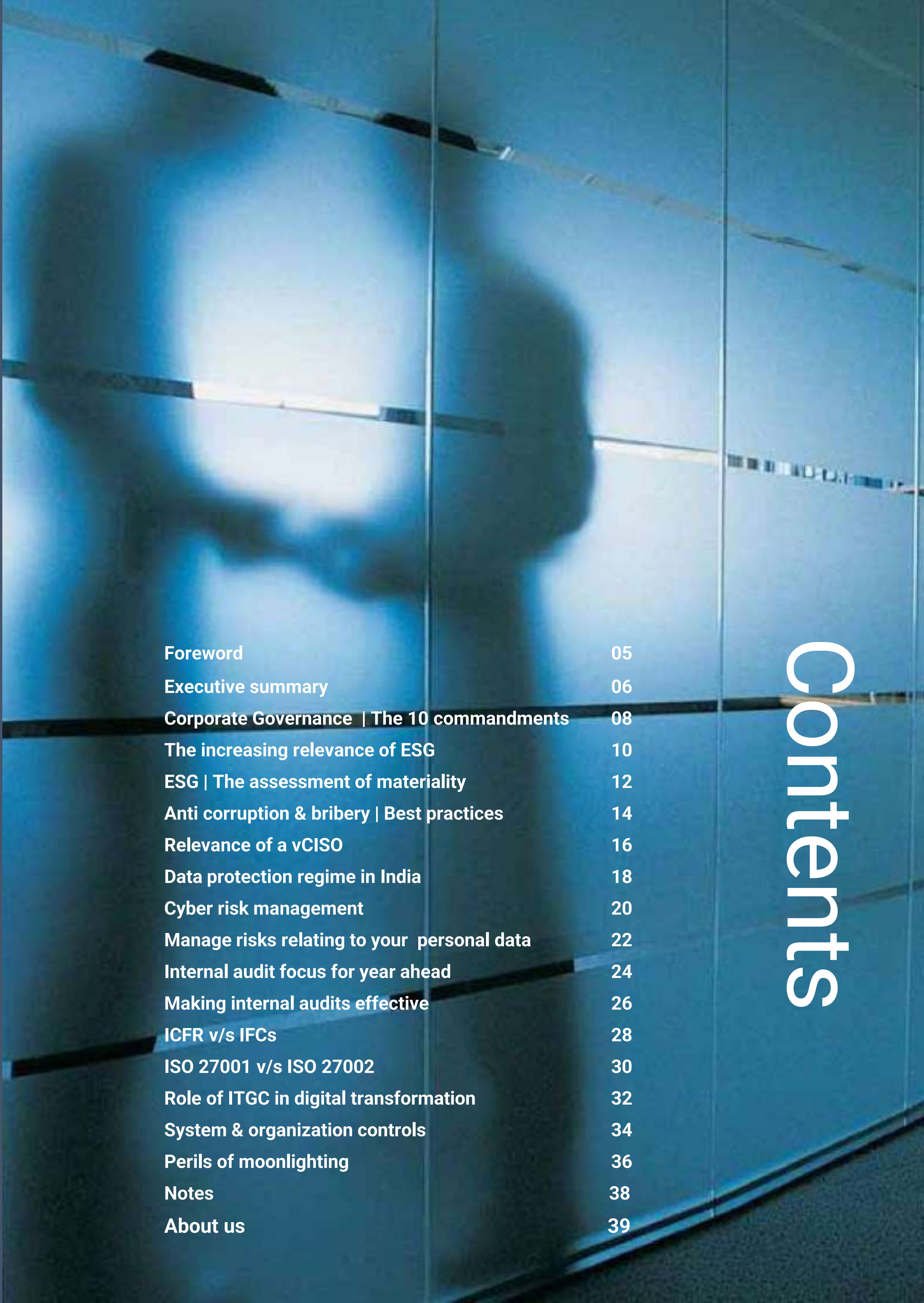
MGC
GLOBAL RISK ADVISORY LLP

2024 | Staying ahead

A compendium of 15 thought leaderships

Disclaimer

The information contained in this publication is of a general nature and is not intended to address the circumstances of any particular individual or entity. The document has been prepared with the help of various sources believed to be reliable, but no representation or warranty is made to its accuracy, completeness or correctness. The facts stated in this publication are based on data currently available and can change when this data gets updated. The information contained in this publication is of a general nature and is in no way meant to be a substitute for professional advice. Whilst due care has been taken in the preparation of this publication and information contained herein, MGC Global Risk Advisory LLP ('MGC Global' or 'our firm') takes no ownership of or endorses any findings or views expressed herein or accepts any liability whatsoever, for any direct or consequential loss howsoever arising from any use of this publication or its contents or otherwise arising in connection herewith.



Contents

“

In this book, you will find a collection of essays from some of the most innovative and forward-thinking minds in the risk advisory industry. These thought leaders have come together to share their insights and ideas on the future of our field. They offer a unique perspective on the challenges and opportunities that lie ahead; and provide valuable guidance on how to navigate this rapidly changing landscape.

I have worked with this talented group of professionals from MGC Global Risk Advisory as the Chairman of the firm’s board and would like to compliment them on this unique publication.

I am confident that their contributions will inspire and inform readers for years to come.

Arvind Chopra
Chief Risk and Assurance Officer
Essar Oil (UK) Limited

FOREWORD

Excellence in the specialized field of risk advisory services is our passion and we have been sharing our knowledge and experience with not only regulatory authorities at various forums but also on a regular basis with our clients and stakeholders.

In the ever-evolving landscape of corporate intricacies, the pursuit of knowledge is both an enduring beacon and a dynamic necessity. As we stand on the cusp of this transformational moment, we are delighted to present to you this compendium of thought-provoking articles, which we had published during the course of the past year. These relate to issues and topics that were pertinent not only at the time that the same were published but also continue to hold importance in the current times and the times ahead.

We realize that in the rapidly changing dynamics of business, staying ahead requires more than just agility; it demands the selfless sharing of knowledge with regularity. The compilation you hold in your hands today is a testament to the commitment of MGC Global to share, inspire, and foster a deeper understanding of the critical issues shaping our corporate world.

From the nuanced realms of data privacy and risk management to the compelling imperatives of ESG and governance matters, the articles within these pages offer a panoramic view of the challenges and opportunities that define our times. It is our belief that this compendium will serve not only as a valuable reference guide but also as a source of inspiration for corporate leaders navigating the complexities of the current and emerging business landscape.

In the spirit of collective growth, we recognize the paramount importance of sharing best practices. This is more than just a collection of words; it is a conduit for the exchange of ideas, experiences and insights. By bringing together these diverse perspectives, we hope to contribute to a richer dialogue that propels us toward innovative solutions and enduring success.

As you delve into the pages of this compilation, may you find not only answers to pressing questions but also the motivation to question further, to challenge the status quo and to embark on your own journey of continuous learning. Together, let us embrace the compendium of thought leaderships contained herein and chart a course towards a future where informed decision-making becomes the hallmark of corporate excellence.

We are grateful to our clients for their insights and specific perspectives that have not only provided us with invaluable feedback but have also served as a guiding light in aligning our services to address their requirements. Your words have resonated deeply within our team, inspiring us to continuously strive for excellence. These have been incorporated in specific sections of this compendium that relate to the areas of services provided by our firm.

Monish G Chatrath
Managing Partner

MGC
GLOBAL RISK ADVISORY LLP

Executive summary

The board of directors and CxO level officers are gearing up to address four critical questions for the year ahead:

1. How to anticipate market trends *(business, economic, political, competitive, environmental)* by realistic planning, sound market intelligence and management tools.
2. How to seek effective assurance over the effectiveness of the policies, procedures, risk management and governance frameworks in their organizations.
3. How to define the drivers of growth and the critical success factors, while proactively identifying and mitigating risks relating to fraud and data breach.
4. How to align their respective functions and their daily activities in line with the organization's strategy, while complying with all applicable laws and regulations.

As organizations with growth ambitions gear up to face the challenges that lie ahead, we have highlighted specific positive trends that MGC Global has witnessed with several of our clients.

Firstly, an increasing number of companies are aspiring to be fully compliant with the legislative framework. The Digital Personal Data Protection Act 2023 and the Business Responsibility and Sustainability Report are the latest amongst these.

Secondly, several organizations are overcoming their reticence to open up about their principal risks and are enhancing the ambit of their risk management frameworks across the length and breadth of their operations and enabling functions.

Thirdly, Indian corporations are facing pressure to implement healthier governance procedures due to the ongoing deregulation, disintermediation, institutionalization and globalization. Importantly, the corporate governance structure and competitive strategy of your organization is closely linked regardless of the model you choose to use.

However, nothing is flawless. Organizations must be mindful of how they demonstrate compliance and identify the underlying causes of any shortcomings even as they strive for complete and comprehensive compliance. This places a strong emphasis on their audit and finance operations as well as important facets of their moral, ethical and compliance standards

An organization that practices good governance, adheres firmly to ethical standards throughout its entire value chain and in all of its interactions with a diverse range of stakeholders, including workers, clients, suppliers, regulators, and shareholders *(including minority shareholders)*. A wholehearted embrace of specific checks and processes is required to accomplish this. In order to maintain economic prosperity in the future, boards and management must ensure that trust and integrity are given the recognition they deserve

The first chapter of this book highlights and deliberates on 10 key imperatives of a good governance framework. This covers the role of an independent body *(or nomination committee, as applicable*), right sizing the board of directors and board level committees, internal audits, risk management, stakeholder relationship management, whistle blowing, anti corruption & bribery practices & information systems.

Related to governance and driven by united demand and an active stance from stakeholders such as employees, investors, customers, regulators and societal considerations; is the philosophy that social, environmental and governance ('ESG') issues should be of equal concern as profits and this aspect is increasingly being expected to embed itself in corporate consciousness, in India and across the globe.

This book contains two specific chapters covering the relevance of ESG and deployment of the concept of materiality in ESG assessments and reporting.

Raising the thresholds on materiality would translate into insufficient information with costs to undertake such an assessment outweighing benefits to the market. This can result in adverse perceptions on the ability of an organization to provide complete, transparent, comparable & reliable information. On the other hand, low thresholds for materiality can result in extensive & potentially excessive reporting and enhance pressures on organizations in such assessments, while placing an overwhelming burden of information on stakeholders.

ESG on the whole promotes the well-being of all employees *(including those in their value chains and elements such as diversity)* and facilitates inclusive growth in an economy.

Security is one of the most intricate and rapidly area of information technology and a critical concern for companies. Threats to data security are gaining in terms of their severity in the midst of a volatile security landscape and emerging regulations. **This book has three specific chapters covering information security - the role of a virtual CISO, the data protection regime in India and cyber risk assessment with best practices**.

In addition, we have addressed the confusion between **ISO 27001 and ISO 27002 - the former is the main standard for certifying an organization, while the latter is the supporting standard with guidelines on the implementation of security controls**.

With over 50 billion devices expected to be connected to the internet by 2030, the development of a strategy for digital transformation is no longer considered to be a holy grail, rather this has become a practical necessity. **One of our thought leaderships examines the concept of ITGCs with emphasis on assessment, institutionalization and ongoing monitoring of their effectiveness in the context of digital transformation**.

We have also included a specific thought leadership that examines **the dichotomy between internal financial controls ('IFC')s and internal controls over financial reporting ('ICFC')**.

The underlying presumption of outsourcing is that the service company, or service provider *(the service organization*) will be able to build a robust internal control framework. System and organization control attestations are gaining prominence due to the ability of this attestation to enable service organizations meet their customer's requirements in the context of the afore-stated risk considerations. With increasing number of the user organizations requesting for SOC attestations, **we have examined the technical considerations for determination on the type of SOC attestation your organization may require.** And finally, we round up with the **impending issue of moonlighting** where our experts share best practices for mitigation.

Corporate Governance

The 10 commandments

The potential for corporate governance to enhance investor confidence makes a periodic, systematic and objective assessment of an organization's framework for governance an imperative.

This is an opportune time for organizations to reassess your organization's commitment towards corporate governance and align the same with its vision, objectives & long-term strategy.

Areas for improvement may be identified with reference to best practices and organizations should remain in continuous lookout for these, while they review their own practices. It is organizations who vigilantly and diligently monitor the effectiveness of their governance frameworks *(with emphasis on strengths & weaknesses)* that will go far - they will lead the way for others to follow.

In a recent discussion, which has generated substantial interest, our Managing Partner - Monish Gaurav Chatrath has reiterated MGC Global's commitment to our clients in assessing and enhancing their systems, controls, policies, procedures and risk management frameworks, to boost their stakeholder confidence and optimize value creation.

In this thought leadership we have examined **10 key commandments related to good governance.**

1 | Enhance the role of an independent body *(or nomination committee, as applicable)*
Develop a clear charter and assess the effectiveness of the functioning of the board of directors and sub-board level committees at regular intervals.

2 | Right size the board of directors and board level committees
Emphasize on experience, diversity & independence - quality versus quantity is the key.

3 | Segregate the roles of Chairman and CEO *(where the two positions exist)*
To enhance monitoring oversight & objectivity.

4 | Make enterprise-wide risk management an ongoing activity
Integrate risk management with your strategy formulation & implementation and develop a risk-driven internal audit charter for your business.

5 | Benchmark your internal audit function
Focus on aspects such as budget, resources, structure and extent of outsourcing/co-sourcing.

6 | Institutionalize an independent body to assess the level of executive pay and benefits
Ensure that these are consistent with performance *(both the company and individual)* and the business strategy.

7 | Instill an effective whistle-blower policy framework
One that is applicable for all stakeholders and not limited to employees. Further, ensure that whistle blowing is heard at the highest levels to enable meaningful corrective action. A direct reporting of the ombudsmen to the audit committee or the board can go a long way in this regard.

8 | Make ongoing stakeholder engagement a priority
The reasons why unlisted companies should also concern themselves with corporate governance, particularly when it comes to management of relationships with its stakeholders, are equally, if not more compelling as those for listed companies.

The bottom line is that all companies need to be transparent in their communication with stakeholders.

9 | Develop robust & reliable Internal Management Reporting ('IMR') systems
Financial statements, while useful for annual planning, often favor consistency, transparency and simplicity over the economic reality of the moment. To ensure that management decisions are fully in line with both ground reality and economic reality, develop effective IMR systems with common characteristics such as accuracy to the most reasonable degree, timeliness, alignment with organizational complexity and detailing to a level that facilitates actionable business decisions.

10 | Enhance monitoring oversight
In monitoring your accounting and financial reporting processes and systems of internal control, the board of directors or the audit committee *(where formed)* should:

- Hold their meetings without restrictions or time constraints *(at least quarterly)*;
- Schedule these meetings well in advance to coincide with the completion of each quarter's financial statements and prior to finalizing the company's quarterly earnings releases;
- Distribute written materials for review sufficiently in advance of the meeting; &
- Meet separately with each of the key players involved in the financial reporting process *(members of management, the internal audit department and the independent auditors)* to review internal controls, the fullness and accuracy of the organization's financial statements, the financial reporting process and other appropriate matters.

Key takeaways
The potential for corporate governance to enhance investor confidence makes a periodic, systematic and objective assessment of an organization's framework for governance an imperative. This is an opportune time for organizations to reassess their commitment towards corporate governance and align the same with their vision, objectives & long-term strategy.

> "
>
> I am glad to see this thought-provoking publication on important issues currently confronting both the private and public sector organizations. In various positions that I have held in the Indian Administrative Service and the United Nations, I have witnessed the sustainable impact that honesty and ethics can make on corporate governance provided one has the determination and courage of conviction.
>
> Reading the 10 commandments of corporate governance, that have been articulated and analyzed so precisely in MGC Global's compendium, I believe that these serve as excellent guiding principles that need to be adopted to enhance the value and ability of any organization whether private or public, in fulfilling its corporate social responsibility.
>
> Ravi Sawhney (IAS Retd.).
> Former Principal Officer, United Nations
> Economic and Social Commission for Asia
> & the Pacific

The increasing relevance of ESG

A revolutionary movement that addresses corporate governance, risk management, corporate social responsibility ('CSR'), sustainability, environmental conservation; promotes the well-being of all employees *(including those in their value chains and elements such as diversity)* and facilitates inclusive growth in an economy; Environmental, Social, and Governance is on course to become the mainstream during the course of this decade.

Driven by united demand and an active stance from stakeholders such as employees, investors, customers, regulators and societal considerations; the philosophy that moves beyond profits to making social, environmental and governance as issues of concern, is embedding itself in corporate consciousness, in India and across the globe.

What is the status of its implementation?
ESG can be viewed as an advancement of CSR, the voluntary guidelines for which were published by the Government of India in 2009 and subsequently refined under the National Voluntary Guidelines on Social, Environmental and Economic Responsibilities of Business in 2011.

These eventually gained legislative standing in India with CSR becoming a mandatory requirement through the provisions of Section 135 of the Companies Act 2013.

The last decade has seen some radical changes in the manner in which CSR has been managed in India and also across the globe. India was one of first countries to enforce a law to enhance the level of CSR and the United Nations followed suit in 2017 by developing a CSR structure for companies to follow with their business objectives. CSR picked up steam after 2013 in India and while many may believe that ESG is still in its stage of infancy, the same has been gaining considerable traction in India, in terms of appreciation of merits and adoption in principle, specially post the COVID pandemic.

Is ESG is here to stay?
In a world that has witnessed strong resurgence from a widespread epidemic and uncertainty, the corporate environment has changed considerably. Stakeholders are increasingly demanding accountability, transparency and responsibility, with risk management and corporate governance becoming two key buzz words.

ESG provides a structure that enables stakeholders to assess the effectiveness of their risk management frameworks on parameters that go beyond the world of finance to environmental, social and governance factors. As part of good governance, ESG also seeks to evaluate an organization’s policies and actions in combating corruption.

It also places emphasis on non-financial factors that are being used as metrics for guiding investment decisions, while displacing a sole focus on financial returns. It is in the interests and protection of all stakeholders of organizations that the concept of ESG gains widespread adoption.

What is the relevance/importance of ESG for companies?
Corporate sustainability is not a new movement. However, unlike the 1990s, this is currently not restricted to the reduction of the environmental impact. ESG holds merit on social grounds as the same seeks to enhance inclusive growth, which inextricably, is an integral component of any economy’s quest for development.

While CSR brought under its ambit specific sections of the society that had been relatively neglected from the mainstream of development, ESG is more measurable, both in qualitative and quantitative terms; and has a broader process and impact, by integrating social, environmental and human development concerns in the entire value chain of corporate business.

What are the challenges that companies face during the implementation of ESG? Is there a proper framework yet, or can it be expected soon?
Limited awareness, inadequate resources to integrate ESG considerations into business practices,

varying data and emerging regulations with guidelines are some challenges being faced by organizations today. In this context, it is fair to acknowledge the ongoing measures to set out disclosure requirements for ESG such as the National Voluntary Guidelines on Social, Environmental and Economic Responsibilities of Business, the Formulation of Business Responsibility Reports by the SEBI followed by a more comprehensive integrated mechanism for Business Responsibility and Sustainability Reporting ('BRSR').

The BRSR seeks disclosures from listed entities on their performance against the nine principles of the National Guidelines on Responsible Business Conduct.

Key takeaways

Will true comparability of ESG norms and practices be attainable in the short term, or will we see harmony emerge from discord? Time will tell.

However, regulators, standard setters, practitioners and stakeholders will need to work closely together if realization of the true value is to be derived from the impact of ESG.

> "
>
> Combatting corruption requires more than rules; it demands a collective dedication to ethical behavior and a steadfast refusal to compromise on principles. The true cost of bribery isn't just financial; it erodes trust, tarnishes reputations, and corrodes the foundation of a fair and just society. And in the end, transparency defeats corruption; integrity fuels trust.
>
> Congratulations to MGC Global on this useful compilation, with the level of focus given to topics such as these that impact businesses today.
>
> Balaji Venkatachalam, Vice Chairman and Chief Financial Officer, Indecomm Global Services

ESG | The assessment of materiality

ESG assessments & reporting are gaining prominence in addressing the requirements of a varied set of stakeholders, such as investors, shareholders, institutions, regulators and customers.

These require the identification & prioritization of the most relevant & impactful factors; and a systematic assessment of measures that protect the environment & people, address climate change and strengthen human rights.

With various frameworks already in place and others in development *(please refer to an indicative list of existing and evolving frameworks in the ensuing section)* the choice and usage of the pertinent standards for ESG assessments and reporting have gained complexity.

Existing frameworks
Such as those set out by the Sustainability Accounting Standards Board ('SASB') the United Nations on business & human rights, the Climate Disclosure Standards Board, IFRS sustainability disclosures, the Global Reporting Initiative ('GRI']) the Carbon Disclosure Project and the Financial stability board's task force on climate-related financial disclosures.

Evolving frameworks
Such as those being developed by the US Securities and Exchange Commission, the European Financial Reporting Advisory Group and the International Sustainability Standards Board.

Defining materiality
The GRI has defined "material" as those ESG topics that may reasonably be considered important for:

- Reflecting the organization's economic, environmental, or social impact; &
- Substantively influencing the assessments and decisions of stakeholders.

These include climate change, diversity & inclusion, human rights, supply chain management, risk management, business continuity & corporate governance.

The 2-dimensional model
The first dimension of the materiality assessment should focus on financial aspects and an analysis of the broader issues. The financial assessment should entail an exclusive focus on ESG risks that could have an impact on an organization's financial value.

The second element *(double materiality assessment*) should seek to address ESG issues from both a financial impact and the impact of an organization's activities on the environment and society at large.

The 6-factor framework
The ensuing key tasks *(developed in-house by our firm with reference to best practices & globally accepted standards/frameworks)* are used for undertaking a materiality assessment.

Define the scope
Determine the scope of the assessment, with reference to specific stakeholders & after considering areas, sectors, or operations that need evaluation. Consider the nature of business, industry & expectations from stakeholders. Identify the framework/s being used by the organization's competitors and narrow the assessment further to the direct competitors.

Using the same framework will facilitate benchmarking for the organization's investors, customers, employees & other stakeholders, who may have varying information on requirements on ESG initiatives.

Go beyond the specific regulatory requirements for other factors as different countries and jurisdictions may have varying legal constructs governing corporate disclosure, as well as different legal liability profiles.

Assess internal data & policies
Review internal data and existing policies, procedures & reports related to ESG issues. The objective should be to identify areas where the organization has already taken action or has policies in place.

External benchmarking
Use the information relating to the organization *(gathered from internal & publicly available sources)* & conduct additional research to

benchmark against industry peers, best practices & relevant ESG frameworks, standards or guidelines *(e.g., GRI or SASB)* to identify commonly recognized ESG topics that are pertinent to the organization and locations being covered.

Prioritize ESG topics
Analyze the information gathered from stakeholder engagement, internal data & external benchmarking to identify the most significant ESG topics for the organization. In doing so, consider the frequency and severity of potential impact, stakeholder concerns, regulatory requirements & industry trends.

For the environment, these could include carbon emissions, climate change vulnerability, energy conservation, water stress, waste management *(including electronic wastages)*, land usage & clean tech opportunities in green buildings, and renewable energy among others.

For social, these could include labor management, privacy & data security, human capital development, health & safety, supply chain labor, consumer financial protection, responsible investment, community relations, access to finance, access to health care, human rights & working conditions in the supply chain and inclusion & diversity.

For governance, these could include the tone at the top, ownership & control, management of the board, executive compensation, code of conduct & business ethics, risk management, transparency in accounting and tax to name a few.

Materiality matrix & diagnostics
Create a materiality matrix or heat map to visualize the identified ESG topics based on their significance to both the organization and its stakeholders. Plot the issues on the matrix based on their impact and level of stakeholder concern.

Validate and refine
Validate the identified ESG topics by seeking feedback from the relevant stakeholders. The matrix so developed should be refined *(if necessary)* based on their input.

> "
>
> A systematic ESG materiality assessment enables an effective prioritization of initiatives relating to your ESG strategy and enhances alignment across your organization. Your goals, targets and consequently key performance indicators emanate from the same.
>
> Surender Sharma,
> ESG Leader & Associate Partner
> MGC Global Risk Advisory

Anti corruption & bribery

Best practices

The world order is changing with the dynamics of the post COVID era exerting a relatively unprecedented set of pressures on businesses across the globe.

The impending threats of geo-political conflicts, intricacies of socio-economic balancing, adoption of cutting-edge information technology to enhance competitiveness, evolving regulations, data protection, fears of deceleration of global growth [triggered by an uncertainty of a widely anticipated recession in the United States of America ('US')] and evolution of hybrid models are some of these.

During this time, the scope of white-collar crime has expanded significantly to encompass bribery & corruption, embezzlement, forgery, insider trading, money laundering, racketeering, larceny, diversion of funds, counterfeiting and cyber-crimes.

Research has revealed that amongst these, bribery & corruption alone are costing the world over US$ 5 trillion annually, which translates into ~4% of the global gross domestic product and is as high as 25% of the procurement costs in specific economies.

Our forensic experts believe that notwithstanding their severity; bribery & corruption should not be viewed from a narrow prism, as the same **(a)** are a consequence of; **(b)** lead to; and **(c)** coexist with various forms of financial crimes such as money laundering *(to disguise corrupt payments).*

Main bribery & corruption risks
Corruption activities encompass a wide range of unethical and illegal practices, such as bribery to officials and executives and misappropriation or theft of funds or assets, which may be committed in collusion by employees, management and third parties.

The inherent characteristic of bribery and corruption is "deceptiveness", with implications of each act of bribery or corruption, not only undermining the trust in political & economic institutions but also scarring the organization and individuals concerned, sometimes permanently for life. The other main risks in this context, which include specific internal and external risks *(including jurisdictional, transaction and business risks)* are the following**.**

- Derailing economic and social development;
- Promoting unfair trade practices.
- Discouraging investments;
- Convictions, fines & imprisonment;
- Significant legal & professional fees;
- Overvalued organizations;
- Stock market volatility;
- Collateral defaults; &
- Intrusive & costly post-transaction investigations**.**

Mitigation measures
A holistic and collaborative approach between governments, organizations and individuals with strong anti-corruption laws, transparent governance structures, accountable institutions and active enforcement efforts pave the way to combat bribery and corruption risks. Additionally, promoting ethical behavior, fostering a culture of integrity and encouraging transparency within organizations and societies are imperatives to address and prevent corruption.

While countries like US and the United Kingdom ('UK') have implemented stringent anti-fraud and anti-corruption frameworks along with penalties for wrongdoers, emerging markets like India are also making significant progress in developing unique and effective approaches to identify and prevent such risks, while aligning themselves with global standards.

In this context the Prevention of Corruption Act that prohibits public officials from accepting bribes, the "know your customer" regulations, intensified scrutiny of suspicious transactions, enhancement of the legislative frameworks to address non-performing assets in the banking and financial services sector and promotion of digitization of large-scale public procurement are some significant measures taken by the Indian government to curb corruption.

Enhancement of measures to promote competition, to address the fear of retaliation and institutionalization of legislations on the lines of US's Foreign Corrupt

Practices Act and UK's Bribery Act are some additional aspects that can be considered by governments across the globe as best mitigating practices.

Organizations should reassess their internal financial controls to address fraud risks, enhance their whistle blower frameworks, revisit their code of ethical business conduct, closely monitor their compliance frameworks *(by potentially automating and developing workflows & reporting dashboards)* and policies *(with emphasis on money laundering policies)*, undertake third party due diligences *(vendors, customers & employees)* and implement comprehensive fraud risk assessments. In doing so, organizations should identify all regions and locations in which they operate and conduct preliminary country specific risk assessment/s.

In this context, the latest "Corruption Perceptions Index" published by Transparency International can also be used as a good reference point.

Inherent in fraud risks is an element that can at best be controlled by frameworks and practices, but only expelled by individual conduct, which requires top level commitment *(the "tone from the top")*. The culture of ethical and moral conduct should permeate across levels, influencing individuals to shun malpractices at the workplace and not fall prey to temptations of making quick money by accepting and giving bribes. However, this has been and remains the hardest part of the nut to crack.

Key takeaways

Every organization faces the inherent challenge of striking a delicate balance between profitability and growth on one hand and upholding their values and ethics on the other. Procedures to prevent bribery and corruption should be proportionate to the risks that an organization faces and their varying levels of complexity.

"

Organizations should consider an independent vertical to focus on fraud detection & mitigation, with resources that have relatively unique skill sets that combine expertise in auditing & investigations with proficiency in data analysis tools & techniques; and softer aspects that entail natural curiosity, detail orientation, effective communication and interpersonal skills. These would facilitate the timely identification of trends, anomalies, seemingly innocuous documentation & other potential fraud indicators; and effective communication of the same.

Robin Banerjee
Chairman,
Nucleon Research Pvt Ltd

.

Relevance of a vCISO

Security is one of the most intricate and rapidly evolving areas of information technology and a critical concern for companies and this is not sector agnostic. Organizations are facing challenges in adapting to the ever-changing security landscape and regulations, and threats to data security are gaining in terms of their severity in the midst of a volatile security landscape and emerging regulations. With the rise of security incidents and data breaches, organizations are seeing the merit of having a Chief Information Security Officer ('CISO') who is given the overall responsible for their IT strategy, information security and for educating the management team on risks.

Clearly and evidently, the impact of the role of a CISO is being heightened in the current scenario, however relatively few organizations have invested in a dedicated professional to mitigate their information security risks. There are sceptics who will raise the big question - Why would you need a virtual CISO ('vCISO') when you could just engage a CISO on a long-term contract? The response varies and is not necessarily the same for all organizations.

To begin with, highly regarded, full-time CISOs are in high demand, and it may not to an easy task to hire them, keep them on board and continuously work towards inspiring them to stay on in an organization on a long- term basis.

MGC Global had conducted a survey to gauge the compelling factors that drive organizations to hire vCISOs. The results of the survey are set below and are in 4 parts:

Part 1 | Limited IT budgets
Nearly 66% of the respondents saw the merit of a vCISO due to limited IT security budgets.

These respondents were largely from small and medium-sized businesses who face budgetary constraints that come in the way of hiring a full time CISO. Respondents from larger organizations have indicated that v CISOs were hied by way of a stop gap arrangement between CISO hires in the event of a vacancy.

While analyzing the responses we have seen that several organizations who are venturing into unfamiliar territory, look to a vCISO to bring diversified experience in the development and attainment of the security mission and objectives that is tied to a framework that mitigates organization specific information security risks.

Consequently, a vCISO is viewed by organizations as a smart and prudent way of realizing their information security objectives without the deployment of a full-fledged information security team on their payroll.

Part 2 | Leveraging on best practices
26% of the respondents were of the view that a vCISO can facilitate the identification while providing unbiased insights on their cybersecurity requirements that include the following:

- Evaluating the cyber security program's current state and identifying and prioritizing their requirements.
- Assessing the organization's maturity level and posture in combating cyber security risks.
- Aligning the cybersecurity program to the organizational mission that encompasses the security framework.
- Developing realistic strategic plans and effectively monitoring their execution.

- Mentoring junior team members vis a vis best practices that address vulnerabilities within the system.
- Implementing sustainable security controls to minimize cybersecurity risks across the entire organization.
- Monitoring the overall cybersecurity effectiveness and health of the system.

Part 3 | Specific information security requirements
6% of the respondents believe that a vCISO is best suited to address pertinent information security requirements, for which the organization may not have the internal means. These include:

- Assessment and alignment of the IT security architecture and policies maintaining compliance and security control standards within industry regulations *(including PCI, DSS & HIPAA).*

- Facilitating ISO 27001 compliances.
- Undertaking vendor risk assessments.
- Developing and testing disaster recovery and business continuity plans.
- Assessing risks and providing on going risk metrics for review and decision making.

Part 4 | Continuity in role
The remaining 2% believe that a vCISO provides stability to the information security function.

Key takeaways:
The net take away is that organizations can secure their businesses without excessive expenditures by investing in bringing on board a vCISO.

Securing your organization does not necessarily require hiring large IT teams or major financial investments. A sound and secure IT risk and security framework can display success by having IT manage risks rather than risks managing IT.

"

What was once a relatively unknown position has become a necessity for many businesses across all industries. As more of us continue to work remotely, the necessity of a strong enterprise-level cybersecurity infrastructure becomes more and more prevalent.

Krish Anand
Executive Vice President & Chief Information Officer
Encora Group

Data protection regime in India

The Digital Data Protection Act ('DPDP' or 'the Act') was put in to affect by both houses of the Indian Parliament on August 11, 2023 and is applicable to Indian residents and businesses that collect the data of Indian residents as well as to non-citizens living in India whose data processing "in connection with any activity related to offering of goods or services" happens outside India.

The imperatives of the far-reaching affects of the Act are getting clearer, with several organizations well on course to transition their policies to comply with the DPDP. Yet some challenges in putting their policies into practice remain to be overcome.

MGC Global was one of the first advisory services firm to publish a thought leadership that delved on these challenges by identifying 6 main areas with clarity on the way forward.

Purpose limitation
Data fiduciaries need to specify the purpose of processing and describe the personal data involved in such processing. Personal data can only be processed to the extent that it achieves the stated purpose. This effectively means that personal data can only be used for the purposes for which it was collected.

Consequently, organizations that use personal data for a variety of reasons, need to proactively, systematically and comprehensively identify the purposes for processing in advance of seeking consent.

Obtaining explicit consent
"Consent" is the cornerstone for privacy protection and individual autonomy. The DPDP requires explicit consent from data principals before processing their personal data.

India is a remarkably diverse nation, and consequently, effective consent requires more than legal and regulatory controls. This can be challenging to implement, especially for organizations that collect personal data from a large number of individuals. In this context, the role of the consent manager in digitally enabling consent, possibly through an interoperable technology framework, needs to be defined with clarity and adequate training.

Data minimization
The principle of data minimization requires personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. This can be challenging for organizations that collect large amounts of personal data.

Organizations should define the purpose of the data as explicitly as possible and implement methodologies of data collection minimization by designing and implementing processes that require the least personal data or that only require anonymized data. This will help in determining what data is relevant and adequate for the intended use and avoid collecting excessive or irrelevant data. The data retention policies and practices should specify how long data will be stored, and when and how it will be deleted or erased which would in turn reduce the storage costs and security risks associated with keeping data longer than necessary.

Data security
Organizations can be fined up to ₹250 crores *(~US$ 30 million)* for non-compliance with the DPDP. Consequently, security measures need to be engineered in a manner that the same are commensurate with the nature, size, complexity and volume of data and the personal data at risk to unauthorized access, use, or disclosure.

These include implementing technical and organizational security measures, such as encryption, anonymization, access control and awareness for employees through training sessions.

Right to access and erasure
Data principals have the right to access their personal data and to have the same completed, modified and erased.

This can be challenging for organizations that need to retain personal data for legal or compliance purposes and in this context segregation of personal data for potential legal and compliance purposes is important.

Cross-border transfer of personal data
Cross-border data transfers can increase the risk of cyber-attacks and data breaches, especially if the data is being transferred through third-party providers or cloud services.

Countries across the globe have varying regulations on data protection, making it challenging to ensure compliance when transferring data across borders.

The DPDP imposes restrictions on the cross-border transfer of personal data. This can be challenging for organizations that have offices or customers in multiple countries.

Organizations should understand the data they process and identify the types of data transferred across borders.

This would enhance the identification of risks associated with cross-border data transfers and implement appropriate security measures.

Key takeaways
The DPDP will impact the Indian economy and society at large in a significant manner. Organizations will now have to invest in data security measures, which in turn will require consulting firms to gear up in terms of innovation & collaboration with IT solution providers in order to provide a comprehensive range of solutions to their clients. The rest of the world will look at India with increased consumer confidence in our digital economy.

The Act shall equip individuals in exercising increased control over their personal data, which combined with enhanced privacy awareness, will provide a greater sense of security among individuals.

> "
>
> While the Act has been notified from August 11, 2023, the rules are not notified as yet. The views being taken by some organizations and practioners is that since the DPDP rules are not in effect as yet, the DPDP Act is also not mandatory for implementation as yet – notably, we do not agree with this position, as the DPDP Act is already in force.
>
> Research & compliance team, MGC Global Risk Advisory

Cyber risk management

If you believe that a password that comprises eight characters *(with a combination of digits, uppercase, lowercase & special characters)* is completely secure, then you will be surprised to know that the same can be cracked in less than eight hours. Add just two additional characters to this password and the time taken to crack the same can grow to over two years.

With the consequences of password breaches being significant, several organizations have assigned the highest risk profile to password protection while developing their IT strategy.

To apprise you of the potential adversity of not protecting your data we have highlighted the main forms of password attacks along with best practices to mitigate the same.

Brute force attack
A brute force attack is a hacking technique in which an attacker systematically attempts all possible combinations of passwords or encryption keys until the correct one is found.

The mitigating measures include the following:

- Implement strong passwords *(unguessable passwords)*, keep them private, log out of portals when these are not in use, keep your computer locked, change the passwords regularly, while using a secure password manager to generate & store them;
- Encourage account lockouts and timeouts;
- Use CAPTCHA and rate limiting features; &
- Induct regular software updates and patches.

Dictionary attack
A dictionary attack is a type of cyber-attack that relies on systematically trying a list of pre-existing words, phrases, or commonly used passwords *(known as a "dictionary")* to gain unauthorized access to user accounts or encrypted data.

The mitigating measures include the following

- Use password complexity strength testers;
- Deploy multi-factor authentication frameworks;
- Blacklist passwords *(not using compromised/weak passwords strengthens the security posture by preventing attackers from uncovering a user's domain password & getting past the initial password login into the active directory domain); &*
- Encourage regular password updates *(where the frequency of change should be dependent on what the password is used for, how often the account is accessed & the strength of the password).*

Rainbow table attack
A rainbow table attack is a precomputed hash-based attack that is used to crack password hashes. This exploits the vulnerability of unsalted password-hashing algorithms by using a precomputed table of password-hash pairs known as a rainbow table.

The mitigating measures include the following:

- Use strong password hashing algorithms.
- Implement strong passwords *(do refer to the mitigating measure stated for brute force attack).*
- Deploy multi-factor authentication frameworks.

- Encourage regular password updates *(please refer to this mitigating measure stated for dictionary attack*).

Social engineering attack
This is a form of cyber-attack in which an attacker manipulates individuals through psychological techniques to trick them into revealing their passwords or other sensitive information.

The mitigating measures include the following:

- Develop a security awareness training calendar & implement the same;
- Deploy multi-factor authentication frameworks;
- Be alert for suspicious links & attachments;
- Do not open the same;
- Data for potential legal and compliance purposes is important; &

- Implement a process with the turnaround time for reporting incidents *(based on their severity)* & responding to such an attack.

Credential stuffing attack
This is a type of cyber attack in which an attacker uses automated scripts or tools to launch a large-scale login attempt, using compromised or a leaked username and password combination.

The mitigating measures include the following:

- Educate users through e-mails and training;
- Deploy multi-factor authentication frameworks;
- Monitor credentials *(which entails identifying, validating & and defining users with their access privileges); &*
- Institutionalize a process for analysis of traffic *(this should address activities for intercepting & examining messages in order to deduce information from)*.

Key takeaways
While the measures stated in this thought leadership may not address all forms of password attacks, your password protection policy should seek to strike an effective balance between security, relevance, usability and practicality.

In some cases, the choice of security controls is determined by the applicable standard(s) - for instance, specific applications need to be compliant with the **Payment Card Industry Data Security Standard** *(what is referred to as "PCI DSS")* and the types of controls that need to be implemented for the same is predetermined.

Your security policy should define the guidelines adequately for securing your gateway, while keeping the same updated for emerging risks. This policy should be developed after considering the nature and volume of data at risk, and there are specific standards that provide guidelines for developing the same *(such as NIST SP 800-63 & ISO 27001 & ISO 27002).*

Finally, your information *(or data)* is your castle and your password is its key. You must protect your castle.

Manage risks relating to your personal data

The digital curtain that was tailored with a belief that personal data was the proprietary secret of organizations has been pulled back, allowing for data subjects to gain more control over their personal information.

Countries across the globe have developed regulations that are based on the principle that personal data is an asset owned by people and held in trust by businesses, rather than as a resource that can be freely collected.

As a consequence of the foregoing, management of risks relating to personal and sensitive information has become an imperative in every business setting and the days of managing data without classifying the same on their sensitivity levels, may well soon be over.

We see specific main considerations that are driving this change, all of which are not only inextricably intertwined, but are inevitably also setting the tone for effective cyber risk assessments and consequent privacy programs. The main considerations in this context are to maintain privacy, prevent identity theft, comply with regulations, preserve trust and ensure the smooth functioning of a business.

Classification of data on the basis of sensitivity levels is an essential factor while developing safeguards to secure sensitive data. This is considered to be an effective organizing principle for the data economy and as the first step, one can look at the following 3 broad buckets for the same:

Restricted
This is the most sensitive data with the highest severity in the event of a compromise. Access to the same should be on a need-to-know basis only.

Confidential or private
This is moderately sensitive data with a relatively lower level of severity, if compromised. Access to such information should be internal to the organization or department that owns the data.

Public
This is non-sensitive data that would cause little or no risk to the organization, if accessed. Access to the same is generally loosely, or not controlled.

The difference between personal data and personally identifiable information ('PII') is tricky to outline, especially after considering various regulations, authorities and procedures *(as listed below)* that address the same:

- General Data Protection Regulation ('GDPR');
- Health Insurance and Portability Act, 1996 ('HIPAA');
- The Graham-Leach-Bailey Act (‘GLBA’);
- Securities Exchange Act of 1934 ('SEC Act');
- Children’s Online Privacy Protection Act;
- Federal Trade Commission;
- US Department of Labor; &
- National Institute of Standards and Technology ('NIST’).

GDPR
The definition of personal data set out in GDPR is relatively wider than most privacy regulations across the globe. PII is a term that is primarily used in the United States of America, while the European Union equivalent of the same is in Article 4 of GDPR, which defines personal data as "any information relating to an identified or identifiable natural person.“

GDPR has gone a step further than the PII while specifying that personal information could include the following types of sensitive personal data and built additional safeguards for the same:

- Racial or ethnic origin.
- Political opinions.
- Religion.
- Trade union membership.
- Health.

The SEC Act
The SEC Act aims to monitor and prevent illegal insider trading by preventing those who hold material nonpublic information ('MNPI') from using it to their advantage in the trading of stock or other securities - or sharing it with others who may use it to their advantage.

Information about an organization that has not been made public but may have an impact on the share price is referred to as MNPI.

It is also illegal for those who possess material nonpublic knowledge to use it for stock trading.

Sharing this information with anyone who utilizes the same for financial gains from the stock market, particularly if those decisions can impact the financial well-being of an organization, is considered illegal and is a civil and criminal offense that is punishable with prison time and fines.

The GLBA

The GLBA contains rules regarding the privacy of non-public personal information ('NPI') that is collected by financial institutions and defines the same as “personally identifiable financial information, provided by a consumer to a financial institution, resulting from any transaction with the consumer or any service performed for the consumer, or otherwise obtained by the financial institution”.

GLBA deals with safeguarding and privacy of NPI.

The "Safeguards Rule" requires financial institutions to store & protect sensitive customer information and ensure its secure transmission, as well as maintain programs and implement audit procedures that prevent unauthorized access and improper disclosure.

Like GDPR and the California Consumer Privacy Act, GLBA also protects the privacy of consumer NPI by giving consumers the ability to prevent disclosure of their personal data to third parties via the “opt-out” right.

Our inhouse specialists have identified best practices for securing your sensitive data/information:

- Use a complete security platform that can also protect your privacy | A security software should include a firewall that prevents unwanted/ malicious traffic from entering the network.
- Protect your files | Many antivirus solutions include "File Lock", which is a file encryption feature that lets the user lock important files in secure digital vaults on their device.
- Use a virtual private network ('VPN') that enables protection | The VPN should encrypt internet connection to keep online activity private on any network, including public networks.
- Lookout for phishing attacks | Using browser protections alert users in the event they come across suspicious links and downloads that can steal PII or otherwise expose their organizations to attacks. These can provide protection against various threats such as malware, trojans, phishing, identity threats and other cyber-attacks.

Key takeaways:

While the measures stated above are essential, there is no substitute for a systematic cybersecurity risk assessment to enable organizations identify, control, and mitigate cyber risks. In this context, NIST has developed guidance for establishing a cybersecurity framework and the same can also provide a base for the development of an effective cyber risk management & privacy program.

Internal audit focus for year ahead

Requirements for greater transparency, accountability and sustainability are increasing by the day. And they certainly look like they are here to stay.

Developing an effective internal audit plan for the upcoming period in this complex and relatively unprecedented landscape of risks will not be easy, Yet your internal audit function needs to be agile and proactive, while addressing the current and emerging set of risks through the prism of a wide ambit of stakeholders' and doing so proactively and comprehensively.

A survey undertaken by MGC Global showed that while there are several imperatives before the audit committees in the context of the internal audit strategy for their respective organizations, there are three main and common issues that need to be addressed. This thought leadership is analyzing the same.

Management of privacy & cyber security risks

The current and emerging set of regulations relating to data protection have pushed the internal audit function into the world of cybersecurity.

Consequently, it was not surprising to find 58% of our respondents rating management of privacy and cyber security risks as the most important area of focus for their internal audit plans for 2023.

While cyber fraud has been in existence from the time of the internet boom, intensity of its current and emerging nature has led to the wide adoption and strengthening of cyber laws - from a mere 12 countries with relevant legislations in 2000 to 156 countries that have currently opted for cyber protection laws and codes.

Several organizations are finding it extremely challenging to disentangle a growing number of legislative, regulator, and internal requirements to demonstrate compliance.

The Information Technology Act of 2000, as amended by the Information Technology Act, 2008 and read with the Information Technology *(Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)* Rules 2011, currently regulates electronic commerce, criminalizes digital and internet crime and establishes a strict data protection and privacy regime for Indian and foreign companies operating in India.

While the right to privacy was deemed a basic right under the umbrella of life and liberty in Article 21 of our Constitution by India's Supreme Court in a landmark decision issued in 2017, a new data protection regulation *(the DPDP),* modeled on the lines of the General Data Protection Regulation *(albeit with specific variations)* was adopted in India during 2023.

In light of the foregoing and with the expectation of enhancement of privacy regulations in 2023, your internal audit function needs to stay informed of these changes and develop a better understanding of potential privacy risks, so it can be more actively involved in identifying appropriate controls to mitigate those risks.

It must also be understood that while internal auditors are not expected to be cyber security and data protection experts, they must be aware of the applicable data protection and privacy regulations and take into consideration the adequacy of internal controls and procedures for identifying cyber cybersecurity risks and incidents as part of the design and effectiveness of an organization's disclosure controls, data security policies, plans and procedures. Consequently, you may consider having your internal audit charter incorporate your organization's risk exposure to cyber-attacks and also determine the extent to which your current security framework has been able to ring-fence your exposure to data leakage.

Management of fraud risks

Predicting the volatility of events that have taken place over the last 4 years was next to impossible - a global pandemic, political polarization, extreme weather conditions, market volatility; and finally, looming fears of yet another pandemic-like situation and another recession. Unequivocally, no account can accurately state which curveballs lie ahead, however, if there is one element of certainty then this relates to demands from stakeholders for greater transparency, accountability and sustainability from businesses in the period ahead.

This brings a sharp focus on the development of an effective internal audit charter for the upcoming financial year - one that can proactively and comprehensively integrate the management of critical fraud risks in delivery. The Institute of Internal Auditors ('IIA') has, in its International Standards for the professional practice of internal auditing, addressed the internal auditor's role in detecting, preventing and monitoring fraud risks and addressing those risks in audits and investigations.

By way of reference, these include the following:

- **IIA's Standard 1200 on Proficiency and Due Professional Care 1210.A2 |** This standard requires internal auditors to have sufficient knowledge to evaluate the risk of fraud and the manner in which the fraud prevention program is managed by an organization.
  IIA's Standard 2120 on Risk Management 2120.A2 | This standard sets out the expectation from the internal audit team in evaluating the potential for occurrence of fraud and the effectiveness of the organization's fraud risk management framework.
- **IIA Standard 2210 on Engagement Objectives 2210.A2 |** This standard calls for the internal auditor to consider the probability of significant errors, fraud noncompliance, and other exposures when developing the engagement objectives.

  With nearly one-third of the respondents to our poll highlighting the importance of managing fraud risks as part of internal audits, it becomes pertinent to bring to the fore the role & expectations from internal auditors.

The IIA has also specified that the internal audit function should not be viewed as an expert, whose primary responsibility is detecting and investigating fraud. We appreciate the practicality of setting this expectation and believe that the internal auditor must be vigilant in terms of sighting signs and possibilities of fraud or fraud risks, which can be taken up for separate investigations by experts if deemed necessary.

With the management and the boards being held responsible for fraud detection, prevention, and reporting, they need to establish clear expectations from the internal audit function and consider supplementing their skills with those of a forensic specialist, as may be required.

Management of environmental, social and governance ('ESG') risks

Despite being a fast-emerging area for board-level attention, only 11% of the respondents rated management of ESG risks as the top priority in the internal audit agenda for their organizations.

While internal audits may not have directly played a part in ESG efforts or reporting, they can serve as a strong line of defence in evaluating an organization's readiness to comply with the existing and emerging ESG reporting guidelines across the globe.

Regulators in many jurisdictions have also increased their focus on ESG risks with initiatives related to climate change, executive pay, diversity and inclusion, working conditions, human trafficking, and product content, among others. These jurisdictions have mandated greater disclosure of sustainability practices and risks, and several major stock exchanges are instituting similar requirements.

ESG considerations can be factored into internal audit approaches in several ways. Standalone reviews can help to highlight policies, controls, and responsibilities with respect to ESG strategies and tactics at specific points of time. More focused ESG reviews can provide a deeper dive into specific ESG areas, such as where stakeholders have heightened concerns or where risk appetite may be low. Internal audits can also adopt an integrated approach, incorporating assessment of ESG risk areas into broader audit plans to provide a pulse check on the business.

This approach can help highlight the extent to which ESG-related activities are being identified, considered, and documented throughout the business. Given their broad purview across the enterprise, internal auditors are well placed to assess an organization's ESG risk from multiple perspectives and help connect the dots.

> "
>
> It is heartening to see a compilation of such pertinent topics, which have been well researched and articulated. I am glad to see the articles covering internal audits, which are an essential part of any organization's risk management and governance frameworks. The management needs assurance of the authenticity of the financial records and the efficiency of the operations of the firm. An internal audit helps establish both. It plays a strong role in giving management assurance over the inherent controls over the implementation of strategy, management of risks and compliance with policies, procedures and the statutory legislation. Developing an internal audit strategy is akin to building a sturdy bridge and organizations should focus on agility and relevance in their internal audit functions, while fostering a culture of innovation, flexibility, engagement, and talent development.
>
> Mukesh Gupta, Director on the Board & Convenor of Audit Committee, India Exposition Mart Limited

Making internal audits effective

The three layers of defense that have come to be recognized as imperatives for corporate governance structures are:

First layer
Process owners, who manage risks associated with day-to-day operational activities, while being accountable for the implementation of controls.

Second layer
Management & specific functions *(such as compliance, risk management, and legal)*, that set standards and provide oversight in the form of frameworks, policies, tools and techniques to support risk and compliance management.

Third layer
The function that provides an objective and independent assurance, while assessing the operation of the first-and second layers, with a reporting to the board/audit committee ('AC').

This brings us to our survey, which related to approaches that contribute in making the internal audits *(as the third layer)* most effective. The results of our survey have revealed three significant best practices.

Risk driven internal audit charter
A majority of the respondents (52%) have assigned the greatest importance to the development and polarization of a risk universe and making this the fulcrum of their strategy to make internal audits effective.

A well-prepared risk driven internal audit charter **(a)** depicts the nature, frequency, extent, manner and type of tests; **(b)** is based on polarization of the risks *(i.e. where risks are rated in terms of their relative importance to the business on parameters of likelihood and impact)*; and **(c)** is in alignment with the risk appetite and tolerance of an organization.

This should be viewed as the blueprint relating to the operation of an internal audit function and one which seeks to ensure that the management is provided ongoing assurance on the effectiveness of measures to mitigate their strategic, financial, operational and compliance risks.

The life cycle of the internal audit charter should therefore not be retrofitted to a year and can potentially extend to longer periods. The internal audit function needs to address the state of the current practices and controls to combat these risks, while considering the nature, size and complexity of the business and planned growth, so that the results of such assessments can enable the senior management team to make well-informed decisions. In the current and emerging business environment, the value from internal audits can be optimized by identifying and polarizing risks at an early stage *(i.e at the time of planning, before fieldwork)*, rather than doing a post-event analysis of the same.

The Reserve Bank of India ('RBI') has mandated the conduct of risk based internal audits in Scheduled Commercial Banks (except regional rural banks) through its notification CO.PP.BC.10/11.01.005/2002-03 dated December 27, 2002 and has issued a detailed guidance note for the same.

The previous notification from the RBI in this context that was issued on January 07, 2021, had outlined additional best practices to be followed by a bank's internal audit team such as authority, stature, independence of the internal audit function along with aspects relating to competence, staff rotation and reporting lines.

Direct reporting to the board/AC
Over 1/4th of the respondents of our survey have attributed maximum weightage to the reporting relationship, in making internal audits effective. Clearly, to be an effective third layer of defense, the internal audit function should be independent and capable of providing objective assurance on a wide range of activities, through a systematic approach to evaluate and improve the effectiveness of the risk management framework, controls and governance processes. The structural separation of the internal audit function from the management facilitates greater objectivity when its direct reporting is to the board/AC.

The manner of this reporting relationship should provide the basis for a coherent flow of communication that merits importance and facilitates direct feedback from the board/AC.

What brings the role of the board/AC come to the forefront is independence and objectivity from the internal audit function, which require direct reporting to and guidance from the board/AC. In turn, it is essential that the board/AC facilitates suitable independence and stature with visible support from the senior management and other stakeholders.

As best practices, the board/AC should approve the internal audit charter with the internal audit budget and resource plan. They should receive ongoing communication from the chief audit executive/internal audit head on the internal audit's performance to assess its progress with reference to the pre-approved plan. They should make appropriate inquiries of the management to establish facts and address limitations as a consequence of the scope or resources.

Usage of data analytic tools

With over 1/5th of our respondents rating data analytic tools as a necessity for enhancing the effectiveness of internal audits, the clear message is that the usage of data analytic tools are gaining prominence.

Analytic-driven recommendations support effective decision-making through the usage of software and programs that collect and analyze data related to areas of audit - information regarding the business, its customer and its competition. This helps internal auditors in understanding trends and uncovering patterns of decision making and transactions, with agility and soundness.

Intelligence generated from data analytic tools help in improving processes that otherwise would require the involvement of data scientists or technology experts. For example, an internal audit team might use data analytics to review employment data such as onboarding logs to ascertain presence of any anomalies, the results of which could then be shared with other departments, such as payroll/Human Resources, finance and compliance, to see if the observations are in sync.

Key take aways

The question that invariably comes up for discussions is whether the internal auditor must be rotated every five years as is the case that has been specified for statutory auditors in section 139 (2) of the Companies Act .

As long as objectivity of the internal audit function is maintained, there are changes in team composition for a constant provision of fresh perspectives with industry insights and the involvement of senior resources, this is not a practical necessity, neither a legal requirement. What is most important is for the internal audit function to be independence from the responsibilities of management, which is critical to its objectivity, authority and credibility.

The internal auditors must have unfettered access to people, resources and data, which are required to undertake their mandate, with freedom from bias or interference in the planning and delivery of their services.

ICFR v/s IFCs

They have been around for over 22 years, however, there remains some degree of confusion between the terms internal financial controls ('IFC')s and internal financial controls over reporting '(ICFR'); with the two being used interchangeably. This thought leadership examines the dichotomy.

Genesis | The Sarbanes-Oxley Act ('SOX')
Assessments of ICFR for the effectiveness of their design and operation, gained prominence with SOX in 2022. Following accounting scandals at significant organizations (such as Enron, Tyco International and WorldCom), Section 404 of SOX introduced the requirement for public companies in the US to establish and report on their ICFR.

Companies listed in the US need to include their own assessment of the effectiveness of their internal controls *(management assertion),* as well as have their auditor attest on the management assertion, in their annual reports. Publicly listed companies in the US also need to document, test and maintain their internal controls and procedures on an ongoing basis.

Equally significant is the personal accountability of signing officers on disclosure controls and procedures, which through Section 302 of SOX requires the principal executive and financial officers of a company *(typically the CEO and CFO)* to personally attest that the published financial information is accurate and reliable. These officers need to make their attestations within the quarterly 10-Q and annual 10-K reports that are filed with the SEC.

Control assessments in India
With the advent of SOX in the US, India also established new corporate governance norms under Clause 49 of Listing Agreement, which first came into effect from December 31, 2005 and have been mandatory for all listed companies ever since. However, Clause 49 made the requirement for IFCs broader to encompass ICFR, in addition to other controls.

The second area where the requirements for assessing IFCs in India has deviated from SOX is in terms of its coverage. While SOX is applicable at a consolidated financial statement level and requires only material subsidiaries to be covered, the listing regulations in India *(as amended from time to time)* and specific provisions of the Companies Act 2013 ('the Companies Act') require the assessment of IFCs and ICFR to be undertaken at a stand-alone entity level.

IFC v/s ICFR
IFC has been defined under explanation to Section 134(5)(e) of the Companies Act as policies and procedures adopted by a company for ensuring the orderly and efficient conduct of its business, including adherence to the company's policies, safeguarding of its assets, prevention and detection of frauds and errors, in addition to the accuracy and completeness of the accounting records and the timely preparation of reliable financial information. This is where the concept of controls assessment moves beyond ICFR to include internal controls relating to operations, compliances and fraud prevention.

ICFR has been defined in the guidance note issued by the Institute of Chartered Accountants of India in September 2015 and this definition is consistent with Auditing Standard 5 on "Audit of Internal Control Over Financial Reporting that Is Integrated with An Audit of Financial Statements" issued by the Public Company Accounting Oversight Board, US. According to this definition, ICFR refers to a process which is implemented by those charged with governance and management to provide reasonable assurance that a mechanism of internal control is in place to achieve the following main objectives:

- Preparation of financial statements as per the applicable financial reporting framework.
- Authorized transactions & events reported in the financial statements as per the established protocols.
- Prevention, timely detection and amendment of any unauthorized use of assets.

Applicability in India
IFC and ICFR are applicable to all companies except for those specifically exempted by the Ministry of Corporate Affairs. IFCs and ICFR are applicable without any terms and conditions for listed companies and public unlisted companies. ICFR is applicable to private companies, whose turnover is greater than 500 million or outstanding loan & borrowings from the bank are greater than 250 million.

The provisions in the Companies Act that draw specific references to IFCs and ICFR with the roles of the respective stakeholders are covered below.

- Responsibilities of the statutory auditor | Section 143(3)(i) of the Companies Act requires statutory auditors to report on the adequacy & operating effectiveness of a company's ICFR only and not their IFCs. Prior to this, the scope of reporting on IFC was provided under the Companies (Auditor's Report). Order, 2015, which was limited to the adequacy of controls over purchase of inventory and fixed assets & sale of goods & services
- Responsibilities of the board of directors ('BoD') | Section 134(5) of the Companies Act requires the BoD of listed entities to provide a confirmation that they have laid down the IFCs and that such IFCs are adequate and operating effectively. However, Rule 8(5) of Companies (Accounts) Rules 2014 (which applies to all companies) requires the BoD's report to address the adequacy of ICFR only.
- Responsibilities of the AC | Section 177 of the Companies Act, which relates to companies that have an AC, requires this committee to evaluate the IFCs and the risk management systems and to call upon the statutory auditors to comment on the ICFR.
- Section 177 of the Companies Act, which relates to companies that have an AC, requires this committee to evaluate the IFCs and the risk management systems and to call upon the statutory auditors to comment on the ICFR.

Key take aways
The management should assess the scope of coverage of their assessment of IFC or ICFR *(as the case may be)* on quantitative and qualitative aspects, after considering the company's size, complexity, global reach and risk profile.

The statutory auditor should make an independent attestation of a company's ICFR; which is possible when it has no role in enabling or assisting the management in forming their assertion over the design and operation of the same.

Companies that choose to undertake this exercise objectively will unlock value from this assessment, reduce fraud risk, avoid financial reporting surprises and facilitate sustained business performance over the long term

ISO 27001 v/s ISO 27002

ISO 27001 is the leading international standard on information security and has been published by the International Organization for Standardization ('ISO') in partnership with the International Electrotechnical Commission ('IEC'). Both ISO and IEC are globally recognized organizations that develop international standards.

ISO 27001 compared with ISO 27002
There is often some degree of confusion between ISO 27001 and ISO 27002 - the former is the main standard against which one can certify their organization, while the latter is the supporting standard that provides guidelines on the implementation of security controls. The most important difference is that ISO 27002 is not mandatory for ISO 27001 certification and organizations cannot get certified against ISO 27002.

Evolution of ISO 27001 & ISO 27002

- The introductory version of ISO 27001 titled, 'BS 7799-2' was published back in 1999 and has gone through several changes since.
- ISO 27002 titled, 'BS 7799-1' was first published in 1995.
- February 2022 saw the ISO 27002:2022 revision, published with the new structure of 93 controls and the same structure of controls was adopted by ISO 27001:2022.

Effective dates
The 'Transition requirements for ISO/IEC 27001:2022' from the International Accreditation Forum states that for companies that are already certified against ISO 27001:2013, the transition to ISO 27001:2022 needs to be completed by October 31, 2025. While accreditation bodies needed to certify companies against ISO 27001:2022 latest by October 31, 2023, several of them had commenced doing so with the new revision way before.

An overview of the changes
Set below are the main changes that we have seen in ISO 27001:2022, when compared with ISO 27001:2013.

- Clause 4.4 relating to the information security management system | The new clause requires processes and “their interactions” to be identified, which is similar to ISO 9001. The design interactions can be presented through diagrams and flow charts.
- Clause 6.2 relating to information security objectives | The new clause requires the information security objectives to be documented and available for all stakeholders.
- Clause 6.3 relating to planning of changes | The new clause requires all changes to have their plans documented.
- Clause 8.1 relating to operational planning and control | The new clause requires organizations to define a criteria for operational processes. This criteria can be a broad term, which could address a security requirement and/or a business requirement and/or a customer request.
- Clause 9 relating to performance evaluation | The new clause requires methods to evaluate and monitor controls that produce comparable results for the organization to assess trends.
- Clause 9.2 relating to internal audits | The new clause requires internal assessments to cover all organizational requirements, which should go beyond ISO 27001. This seeks to ensure a broader attempt to have a comprehensive management system.
- Organizational and physical controls | While no existing controls were deleted, new controls have been introduced and several controls were merged, reducing the overall number of controls.
- Security controls contained in Annexure A | These have decreased from 114 to 93. The security controls are now divided into 4 sections instead of the previous 14. Furthermore, this change represents a tangible attempt to make the standard more concise and simpler to implement. The overlaps and repetitions have been eliminated to create five major security attributes that make them easier to group.

A summary of the changes

35 controls remain unchanged, 23 have been renamed and 57 controls have been merged to form 24 controls.

Depicted below is an overview are the 11 newly added controls.

- Clause 5.23 | Information security for use of cloud services.
- Clause 5.30 | ICT readiness for business continuity.
- Clause 5.7 | Threat intelligence
- Clause 7.4 | Physical security monitoring
- Clause 8.1 | Data masking.
- Clause 8.9 | Configuration management
- Clause 8.10 | Information deletion.
- Clause 8.12 | Data leakage prevention.
- Clause 8.16 | Monitoring activities.
- Clause 8.23 | Web filtering.
- Clause 8.28 | Secure coding.

Next steps

You could follow these steps to update your compliance processes in alignment with the new ISO 27001:2022 requirements and gain certification:

- Develop a sound foundation by defining the rules and methodology for your risk assessment.
- List all assets, with related threats, vulnerabilities and risks.
- Choose the right tool for risk assessment.
- Polarize the risks.
- Develop the treatment plan.
- Align your statement of applicability to align with the updated Annexure A of ISO 27001:2022.
- Review and update documentation, including policies and procedures, to meet the new control requirements.
- Get audited against the new ISO 27001:2022 standard revision.

> "
>
> An ISO certification helps companies with business credibility, safety and quality of the products. It can improve the efficiency of the products or the services that a company provides. When companies find it difficult to differentiate their products in the market and face increased market rates, getting an ISO certification can be helpful in solving these problems and sustaining in the market.
>
> Kirti Kumar Salunke
> Leader, IT Risk Advisory
> MGC Global Risk Advisory

Role of ITGC in digital transformation

The nature and extent of our reliance on technology to manage business operations has been transforming over the years; and the epidemic had only hastened this digital revolution.

With over 50 billion devices expected to be connected to the internet by 2030, the development of a strategy for digital transformation is no longer considered to be a holy grail, rather this has become a practical necessity. Consequently, the role of an effective risk management framework *(entailing risk avoidance, risk reduction, risk transfer, and risk retention*) in accomplishing critical objectives for digital transformation has come to the fore.

The institutionalization and assessment of ITGCs are one set of creditable measures to gain assurance on the effectiveness of your digital risk program. This thought leadership examines the concept of ITGCs with emphasis on the assessment, institutionalization and ongoing monitoring of their effectiveness in the context of digital transformation.

Further, we also discuss the utility of ITGCs in enhancing cybersecurity and data integrity, both of which are cornerstones that will only grow in significance in your ongoing digital transformation journey.

What are ITGCs
ITGCs govern how an organization uses technology and safeguard the data it owns. For instance, ITGCs describe how a business deploys technology throughout an organization and how it applies access and security controls for its IT systems.

If you are a publicly traded corporation in the United States of America, then you need to comply with the Sarbanes-Oxley Act, which requires your management to assert and your auditors to form their attestation over the management's assertion on the effectiveness of the design and operation of the corporation's ICFR.

If you are working for specific companies in *India (i.e. those with revenues in excess of INR 50 Crores or those that have aggregate borrowings from banks or financial institutions or any corporate at any point of time during the financial year in excess of INR 25 Crores)*, then similar requirements for a management assertion and your auditor's attestation on this assertion applies to you.

ITGCs are one of the three components of ICFR with entity level and process level controls being the other two.

Role of ITGC in digital transformation
ITGCs encompass a governance framework; access controls; change management controls & data management measures; and also seek to ensure integrity of processing with a monitoring framework.

The relevance of these components to digital transformation is summarized in the ensuing bullets.

- Governance framework | This constitutes the development & alignment of the IT strategy with objectives for digital transformation, risk assessment, policies, procedures, organogram, roles & responsibilities and cover service delivery points *(*including primary applications such as ERP systems and others influencing *digitization)* and the underlying infrastructure. The criterion for ITGC assessments needs to manifest itself on the ability of the IT system to not only meet the current requirements of the business but to also enable the organization to run more efficiently as it progresses in its digital transformation journey.
- Access controls | These include physical, logical & cyber security controls, which relate to data that is collected, processed, stored, retrieved and destroyed at various stages of digital transformation. Such data needs to be protected from unauthorized access and usage. Digital transformation can expose businesses to new risks like those related to compliance, cybersecurity, and data privacy.

  These risks need to be identified, evaluated and mitigated while testing the effectiveness of the design and operation of ITGCs.

With the ongoing evolution and refinements of data protection & privacy laws across the globe, organizations need to have adequate measures in place for compliance.

- Change management | Without successful change management, no digital transformation initiative will meet its objectives. Change management refers to the processes, tools & techniques that are required to manage people in order to achieve a set of established business outcomes. Digital transformation often involves the development and deployment of new software. This software must be tested thoroughly to ensure that it is reliable and secure. While integrating these efforts into digital transformation initiatives from kickoff through to launch may not guarantee 100% success; however, these will inevitably stack the odds in your favor.
- Data management | This includes backup, disaster recovery & business continuity. An important element of ITGC testing is the identification and elimination of bottlenecks and inefficiencies in the IT infrastructure and processes. Being future-ready and responsive to market changes instead of taking reactive measures to unexpected business contingencies is the dividing line between success & failure.
- Processing integrity | Adequacy, accuracy, completeness, timeliness, reliability and authorization are essential elements that set up the framework of processing integrity. Measures to ensure that data is processed in a way that is consistent with the business objectives and goals for financial reporting are imperative for the success of digital transformation initiatives.
- Monitoring controls | Digital transformation is invariably a long-term journey, which sets the platform for organizations to gain business value by exploring and embracing new technologies. However, the lifecycle of digital transformation is filled with challenges that emanate from internal and external factors. The establishment of a monitoring function and key performance metrics for the IT steering committee to track activity and progress in alignment with the IT strategy are key monitoring controls that are also included in ITGC.

Key take aways

When developing a plan for testing ITGC controls, a risk-based approach should be adopted.   The compliance framework that can be used as a reference should include IT-based risks and potential controls relating to financial reporting. The COSO framework for internal controls is one example and the COBIT framework specifically for IT controls is another. This allows the CISO *(or the IT auditor or your internal auditor)* to conduct a risk assessment & identify weaknesses in your ITGCs.

System & organization controls

Drive trust with transparency

The fundamental assumption at the core of outsourcing is that the service provider *(the service organization*) will be able to build a robust internal control framework.

In doing so, the user organization *(the organization that outsources activities)* needs to gain comfort that the data, processes, inputs and outputs at the service provider's location are effectively handled and the service organization is able to mitigate risks relating to financial reporting, security, availability, confidentiality, processing integrity, privacy of their customer's data, cyber security & supply chain.

System and organization control ('SOC') attestations *(formerly known as SAS 70 or SSAE 16 attestations)* are gaining prominence due to the ability of this attestation to enable service organizations meet their customer's requirements in the context of the afore-stated risk considerations.

In addition, regulations in the US and across the globe, require organizations to implement and maintain effective data security and privacy controls. SOC compliance *(specially SOC 2 and SOC for cyber security*) can help organizations meet these requirements.

Why get a SOC attestation

Initially designed specifically for technology and cloud computing organizations, SOC attestations have become a gold standard for demonstrating a service organization's ability to address a relatively wide ambit of risks pertinent to the user entity. With increasing number of the user organizations requesting for SOC attestations, you run the risk of losing out on business opportunities if your organization does not have the relevant SOC attestation in place.

Having worked with several service organizations across the globe, we are publishing this thought leadership to enable you understand pertinent considerations and intricacies, so that you can determine an appropriate scope, nature & type of attestation that will enable your organization meet the objectives for which you are seeking a SOC attestation.

You will in the process save costs and your time.

Deciding on the type of SOC attestation

A SOC 1 attestation enables helps a service organization examine and report on its internal controls relevant to its customers' financial statements. This is typically undertaken for organizations that process or impact financial transactions for their clients, such as payroll processors, data centers, or financial application providers.

A SOC 2 audit examines and reports on a service organization's internal controls relevant to one or more of 5 Trust Services Criteria ('TSC')s, which are (i) security; (ii) availability; (iii) confidentiality; (iv) processing integrity; and (v) privacy of their customer's data.

The objective of a SOC 2 report is to enable the clients and stakeholders of the user organization effectively manage their risks related to one or more of the 5 TSCs. The SOC 2 report applies to a broader range of service organizations, including cloud services, data storage, or other IT services, where data security and system performance are vital.

A Type 1 attestation provides a report of procedures / controls that are in place at a point of time *(example - at September 30, 2023)*, while a Type 2 report covers the period that corresponds to the operation of the controls *(example - 9 months ended September 30, 2023).*

As a service organization, you will first need to decide on the nature of the SOC attestation *(i.e., SOC 1, SOC 2, SOC 3, SOC for cyber security or SOC for supply chain)*. The second aspect that you would need to address is the type and period of the SOC 2 report *(i.e., Type I or Type II)* to meet your objectives. You can then proceed to assess your current standing vis a vis the compliance requirements for the relevant SOC attestation and get a detailed readiness report with a road map for compliance.

"I wanted to express my heartfelt gratitude for your support and active engagement in the successful completion of our SOC2 Type II certification. Your timely actions and invaluable insights have played a pivotal role in not only obtaining this crucial certification but also enhancing the value we bring to our client engagements."

"Here is a sincere appreciation for the exceptional work you and your team have contributed to the successful completion of the SOC project. Your dedication, expertise, and attention to detail have undoubtedly played a pivotal role in its success."

"Thank you for your committed efforts."

Once you have closed the identified compliance gaps in the readiness assessment, you are set to hire a PCAOB registered CPA firm for your SOC audit/attestation. Set out in the ensuing table is an overview of the key differences between various SOC attestations.

> "
>
> To succeed in SOC attestations, you need to understand the different types of SOC reports & the trust service principles that apply to your organization, prepare your environment & documentation to meet the criteria of the selected principles and communicate with your clients and stakeholders about the scope & results of the SOC attestation.
>
> Sarthak Taneja
> Leader, SOC Advisory, MGC Global Risk Advisory

Nature of report	Users	Purpose	Coverage
SOC 1	• User entity's controllers' office. • User entity's auditors.	Audits of financial statements.	Internal controls relevant to the customers' financial statements.
SOC 2	• Internal management. • Regulators.	• GRC programs. • Oversight. • Due diligence.	TSCs.
SOC 3	General public.	Marketing.	TSCs.
SOC for cyber security	• Senior management. • Board of directors. • Analysts. • Investors. • Business partners.	To provide intended users with information about an entity's cyber security risk management program for making informed decisions.	Enterprise-wide cybersecurity risk management program
SOC for supply chain	• Senior management. • Board of directors. • Analysts. • Investors. • Business partners	To enable management assess risks arising from business relationships with their supplier and distribution networks.	Enables an entity that produces, manufactures, or distributes products to have a supply chain assurance report.

Perils of moonlighting

The contentious issue of moonlighting continues to gain prominence, albeit with a clear polarization of views across India today.

While some of these have been expressed with conflicting perspectives on various media platforms, others are influencing changes in corporate policies and their code of ethical business conduct. This divergence of views is further accentuated by the rise of the gig economy, which our experts believe is growing at a CAGR of 17% in India.

Elsewhere across the globe *(especially in the US)*, the increasing share of independent workers in the employment pie, has sparked the interesting debate on whether moonlighting is the future of the gig economy.

As we look closely at the narrative to explore whether companies are truly defining their position on moonlighting, we find that not all organizations have established a clear stand on what is acceptable, and aligned their operating models, policies & processes with their moonlighting risk mitigation strategy.

Overview of a case study

On undertaking a recent forensic engagement covering a sample of 100 employees for one of our clients, our team had identified and established as many as 29 instances of moonlighting.

These ranged from dual & simultaneous employment to active directorships in unlisted entities, intra-day trading in shares and employees running separate businesses in the names of their family members.

Risks & implications

Some of the inherent risks of moonlighting relate to conflicts of interest, compromise of data confidentiality & privacy norms, misusage and theft of intellectual property and ownership issues *(especially if the second job is related to or is in competition with the primary one).*

Implications emanating from risks such as these manifest themselves in workforce inefficiencies, drop in productivity, legal issues *(with contract violations & data breaches)*, loss of business and erosion of brand equity.

Inevitably and evidently, these risks would vary in severity across roles *(after considering the nature, complexity and type of industry)* with some levels of commonalities in practices across levels.

The ethical consideration

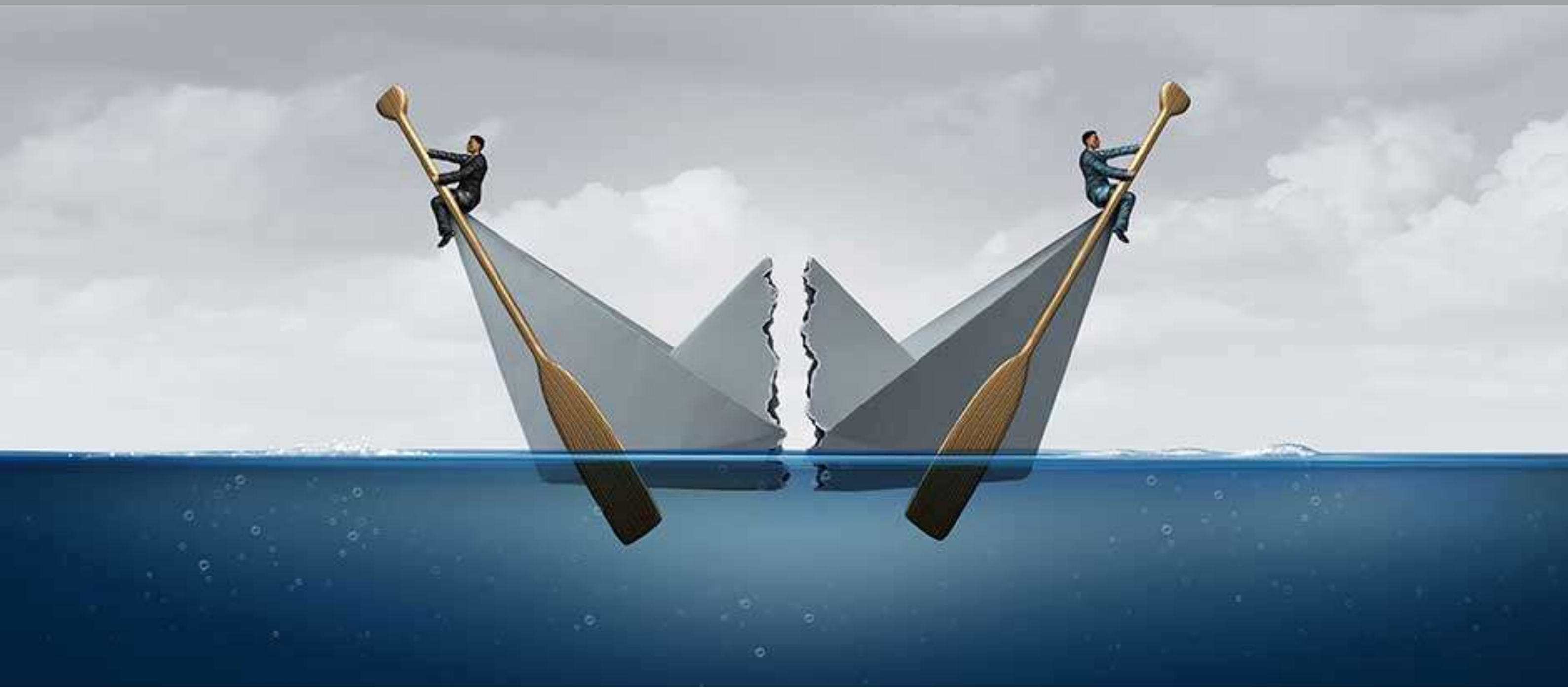
If organizations believe that workforce activity relating to other organizations that take place outside or even within their office hours do not impact their productivity or pose conflicts with their contractual obligations, then establishing a moonlighting policy that sets out specific considerations for such engagement is an imperative.

In the absence of the foregoing and with no overarching law against moonlighting, our experts believe that moonlighting would be unethical when this is undertaken in secrecy and/or when the same conflicts with or undermines an employer's interests.

Key takeaways:

With this balanced advocacy, we also recommend revisiting the corporate governance framework with an emphasis on safeguards against the perils of moonlighting.

Our guidelines are based on principles and pragmatism and the same also entail undertaking a role-based moonlighting risk assessment - this is a critical aspect that we are bringing under the radar of the enterprise-wide risk management strategies of our clients.



> “
>
> Sometimes there could be thin dividing lines between a professional's passion and employment. In all situations, moonlighting should be conducted as per the employer's policy, in the absence of which, with transparency and disclosure. The moral conscience driving the nature and extent of such activities should be avoidance of conflicts and, or adverse impact of workforce productivity. It is always best to disclose and check rather than assume that the completed moonlighting activity is acceptable in your organization.
>
> Vinit Ajit Teredesai
> Chief Financial Officer
> LTIMindtree Ltd.

Notes

About us

About MGC Global Risk Advisory

Recognized as one of the '10 most promising risk advisory services firms' in 2017, as the 'Company of the Year' in 2018 &, 2019 *(both in the category of risk advisory services)*, one of the 'Top Exceptional Companies to Work For' in 2020, amongst the 'Top 25 Customer Centric Companies' in 2020, 'The Consultant of the year' in 2021 *(in the category of risk advisory services)*, 'Top Exceptional Leaders in Risk Advisory Services' in 2023 and 'Best place to work' in 2024; MGC Global is an independent member firm of Allinial Global.

MGC Global provides services in the areas of enterprise-wide risk management, forensic, internal audits, control assessments *(SOC, IFCR & SOX)*, process re-engineering, governance frameworks, privacy & data protection *(including GDPR & DPDP)*, IT risk advisory, GDPR, VAPT, ISO readiness, cyber security, vCISO, accounting advisory, forensic, ESG & CSR services.

Our firm has the capabilities to service its clients through its offices in Bengaluru, Mumbai, NCR; and has service arrangements with associate firms in all major cities in India.

About Allinial Global

Allinial Global *(formerly PKF North America)* is currently the world's second-largest member-based association.

With collective revenues to the tune of approximately US$ 5 billion, Allinial Global has dedicated itself to the success of independent accounting and consulting firms since its founding in 1969.

It currently has 261 member firms in over 105 countries, who have over 28,000 professional staff and over 6,000 partners operating from nearly 700 offices across the globe.

Allinial Global provides its member firms with a broad array of resources and support that benefit both its member firms and their clients in the key impact areas of learning & development, human resources, international outreach, technical support, knowledge-sharing through its specialized communities of practice, information technology and practice management.

.