www.pwc.in

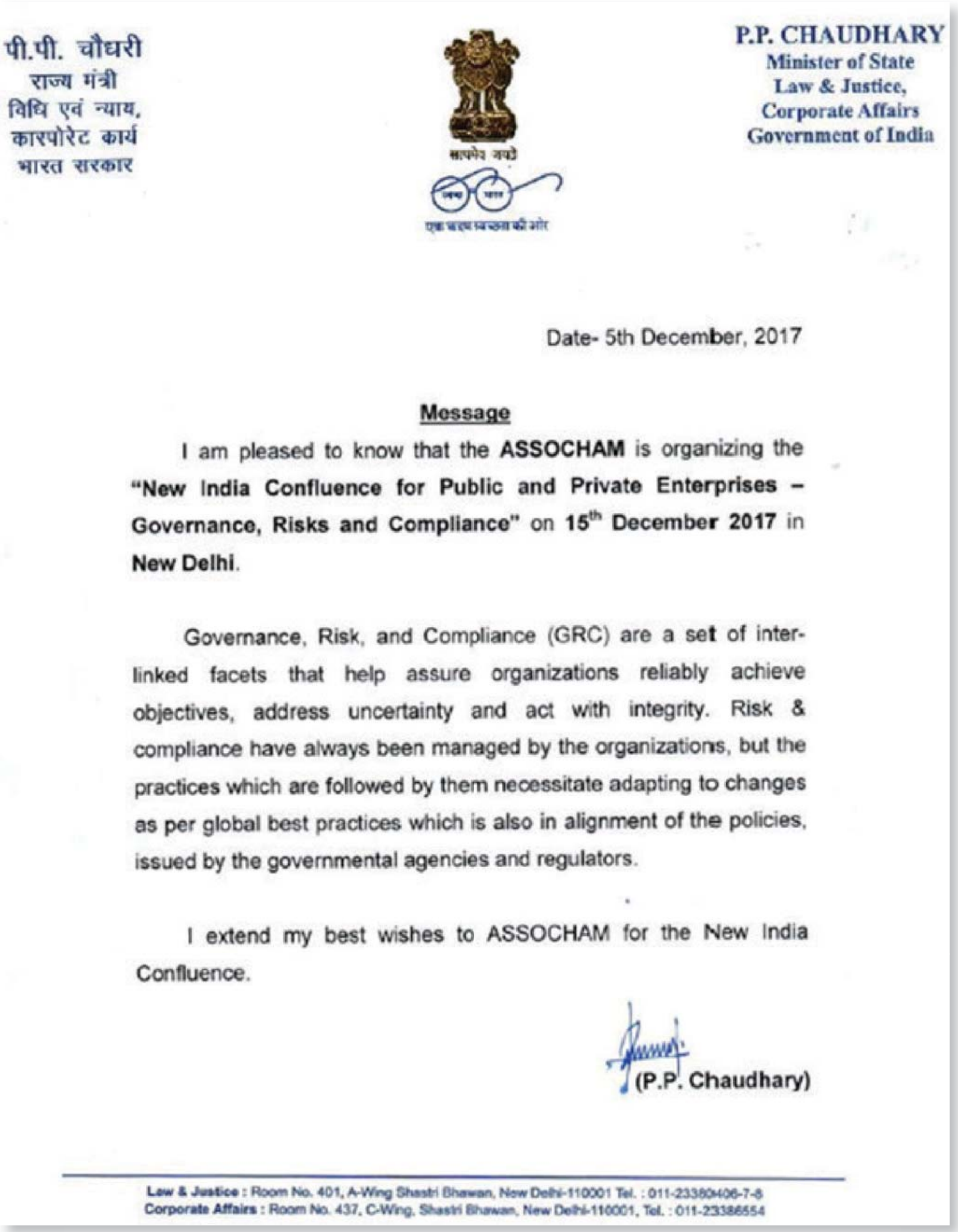
Enabling business performance through a well-defined GRC programme

December 2017

ASSOCHAM INDIA

pwc

Table of contents



पी.पी. चौधरी
राज्य मंत्री
विधि एवं न्याय,
कारपोरेट कार्य
भारत सरकार

सत्यमेव जयते

स्वच्छ भारत
एक कदम स्वच्छता की ओर

P.P. CHAUDHARY
Minister of State
Law & Justice,
Corporate Affairs
Government of India

Date- 5th December, 2017

Message

I am pleased to know that the **ASSOCHAM** is organizing the **"New India Confluence for Public and Private Enterprises – Governance, Risks and Compliance"** on **15th December 2017** in **New Delhi**.

Governance, Risk, and Compliance (GRC) are a set of inter-linked facets that help assure organizations reliably achieve objectives, address uncertainty and act with integrity. Risk & compliance have always been managed by the organizations, but the practices which are followed by them necessitate adapting to changes as per global best practices which is also in alignment of the policies, issued by the governmental agencies and regulators.

I extend my best wishes to ASSOCHAM for the New India Confluence.

(P.P. Chaudhary)

Law & Justice : Room No. 401, A-Wing Shastri Bhawan, New Delhi-110001 Tel. : 011-23380406-7-8
Corporate Affairs : Room No. 437, C-Wing, Shastri Bhawan, New Delhi-110001, Tel. : 011-23386554

Message from PwC

Neeraj Gupta
Leader
Risk Assurance Services

Harpreet Singh
Partner
Risk Assurance Services

We are living in a very volatile environment. Many events which were earlier thought unlikely, distant or isolated—climate change, energy supply volatility, technology advancements and negative interest rates, to name a few—have manifested and changed the course of business for many organisations. Company executives and boards have to be agile to respond to these challenges. Not only do they have to manage this volatility but also meet the investor expectations around growth. Moreover, there is heightened scrutiny from the regulators.

In India, we have seen regulatory developments such as the enactment of the Companies Act, 2013, which have significantly enhanced the focus on good governance. There are statutory obligations now which require the boards to build effective systems and processes to manage risks and also ensure compliance with the laws of the land. Boards are required to make affirmative statements regarding operating effectiveness of some of these processes in their annual reports.

Given this complex environment, companies need to build adequate safeguards in the form of robust processes around governance, risk and Compliance (GRC). Traditionally, we have seen that these programmes are run in silos and hence companies are not necessarily able to derive the desired benefits. There is a need to take a holistic and integrated view of these programmes. A fully optimised and integrated GRC framework that employs tactics and tools such as continuous risk assessment and predictive analytics can alert stakeholders to potential risk related issues in a timely manner.

Our knowledge paper focuses on some of the challenges which companies face while building these programmes and how those can be addressed. We have shared some of the leading industry practices related to governance, risk and compliance programmes. Relevant data points from the various surveys which we conduct have also been included in this knowledge paper. We have also covered the concept of an integrated GRC programme and how using the same, companies can build robust defence mechanisms to safeguard stakeholder value.

From the President, ASSOCHAM

The corporate sector in India is characterised by multidirectional flows of various resources, including people, ideas, products, services, and capital. A complex web of interconnections among them is bringing new opportunities and options to companies. Also, there are the specific as well as common factors that impact the future growth path of public sector and private sector companies. Hence, an update and exposure on corporate governance, risk management practices, and regulatory compliance requirements is essential for people, particularly those at the helm of organisations, which in turn helps their respective organisations to favourably transform adversities by escalating the unwanted and latent export or import of risk factors.

I believe that the **'New India Confluence for Public and Private Enterprises – Governance, Risk and Compliance'**, being organised by ASSOCHAM, is highly significant and timely. The confluence can be seen as an opportunity for stakeholders to participate and discuss all such relevant issues and advancements happening in the context of policies, processes, and programmes under GRC.

I am pleased to acknowledge the joint efforts of the **ASSOCHAM** team and **PwC India** in bringing out this knowledge report. I am confident that this knowledge report will be useful to board members, KMPs, and other stakeholders of public and private companies to contribute and partner towards the progress of New India.

I wish the knowledge report reaches far and wide in the country and all the participants of the confluence great success.

Thank you,

Sincerely,

Sandeep Jajodia
President
ASSOCHAM

December 2017
New Delhi

From the Secretary General, ASSOCHAM

Greetings from ASSOCHAM!

It's worth measuring beyond numbers the contribution of the vital cog of the Indian economy—that is, the public and private sector—in fostering the multidimensional and sustainable growth of the country. The benchmarks set by the corporates by radically shifting gears on policies, processes, and programmes have become indispensable for the economy and emerged as a torchbearer for others within the sector. However, several of the economic and non-economic, domestic and global odds and complexities need to be addressed towards the commitment of public and private enterprises to the nation and the contribution to the New India Vision of Prime Minister Narendra Modi.

In view of the above and to discuss the primacy of corporate governance, approaches to transform next-generation risks into opportunities, drive exceptional business performance and stay ahead by effectively allaying the regulatory compliance requirements under the changing dynamics among corporates, ASSOCHAM is organising the 'New India Confluence for Public and Private Enterprises – Governance, Risk and Compliance' in December 2017 in New Delhi.

I wish to acknowledge the contribution made by the expert team of **PwC India** along with the **Department of Corporate Affairs and PSU's Affairs** of **ASSOCHAM** for their untiring efforts in preparing an extensively in-depth comprehensive study.

I am sure this study will give rich insights and adequate knowledge to all the stakeholders on GRC issues.

I wish the participants and stakeholders of the confluence a great success.

With best wishes,

D. S. Rawat
Secretary General
ASSOCHAM

December 2017
New Delhi

Foreword

Patrons & Friends,

At the outset and to set the tone; as rightly said by James Joseph, former US ambassador to South Africa "Business must harness the power of ethics which is assuming a new level of importance and power".

Governance, Risk Management and Compliance (GRC) are three related facets that helps an organization reliably achieve its objectives, addresses uncertainty, inculcate & acts with integrity and attains utmost compliance level. Governance is the combination of processes established and executed by the Board that are reflected in the organization's structure and how it is managed and led toward achieving goals. Risk management is predicting and managing risks that could hinder the organization from reliably achieving its objectives under uncertainty. Compliance refers to adhering with the mandated boundaries (laws and regulations) and voluntary boundaries (company's policies, procedures, etc).

Implementing a comprehensive and innovative GRC program enables organizations to address multiple factors such as profits optimization, process standardization, mapping regulatory & statutory compliance landscape and its adherence, integrate risk and compliance functions, etc that are essential in managing and controlling enterprise risk. The downside of having a less than adequate program is potentially severe reputational and financial harm.

One of the misconceptions is that GRC – is a new requirement. It has been and always will be important. The problem is that organizations may not do it so well because they view it as, three silos of activities and not as an integrated business requirement, a part of the organization's DNA. Just like the core issues with cyber security are not mainly related to technology but rather people, the same holds for GRC. People need to be governed by principles, generated and lived from the top down, informing everyone as to what is expected when the policies, processes and controls apply and moreover when do not seem to apply.

The three areas of GRC create a triangle, which includes strategy, processes and people and technology. The last two are particularly important in the ongoing times of business disruptions. For example, on the technology side, Industry 4.0 and Artificial Intelligence (AI) offer fascinating opportunities, but also present new risks. Today, people and technologies change processes and strategies. The model does not mean that GRC is responsible for these four areas, but GRC has to interact with their respective owners.

With a view to make Indian private and public enterprises more conducive and robust, the ASSOCHAM is organising **New India Confluence for Public and Private Enterprises on Governance, Risk and Compliance** on December 15, 2017 in New Delhi, India.

ASSOCHAM along with PwC as Knowledge Partner, have come up with this knowledge report that attempts to give rich and useful insights about the subject.

I acknowledge Ms. Preeti Malhotra, our Chairperson for ASSOCHAM National Council for Corporate Affairs & CSR for her leadership, Mr. D.S. Rawat for his encouragement and dedicated efforts made by the ASSOCHAM team for organising the event on the subject.

I sincerely hope that with the galaxy of eminent speakers and judicious topics, the participants would get deeper and rich insight about GRC during the deliberations.

With Best Wishes,

Vijay Sachdeva
Co-Chairperson, ASSOCHAM National Council for Corporate Affairs & CSR

Introduction

In today's operating landscape, businesses are burdened daily by the demands of rapid market shifts, political and environmental change, rapid technological advances, complex third-party relationships, and heightened regulatory scrutiny. The inability to keep pace with this multidirectional change has put many organisations on a defensive risk footing. Driven by the need to comply with business and regulatory requirements and protect themselves and their stakeholders from value erosion, organisations have built their governance, risk management, and compliance (GRC) activities on a practically ad hoc basis, each focused solely on protecting the business from a specific risk or addressing a specific risk/ compliance responsibility.

The result is often an unintentional separation of these companies' GRC activities, with each function working hard to fulfil its mandate but operating in the vacuum of its own silo, cut off from natural cross-functional alliances and lacking real alignment with the business's strategy and objectives. This lack of coordination and enterprise-wide focus can lead to gaps and inefficiencies in business risk coverage, lack of insight into the interconnections between risks, lack of confidence by key internal and external stakeholders, inadequate support to the board for its oversight of enterprise risk management, audit fatigue across the business from duplicative monitoring and testing, and excessive GRC costs.

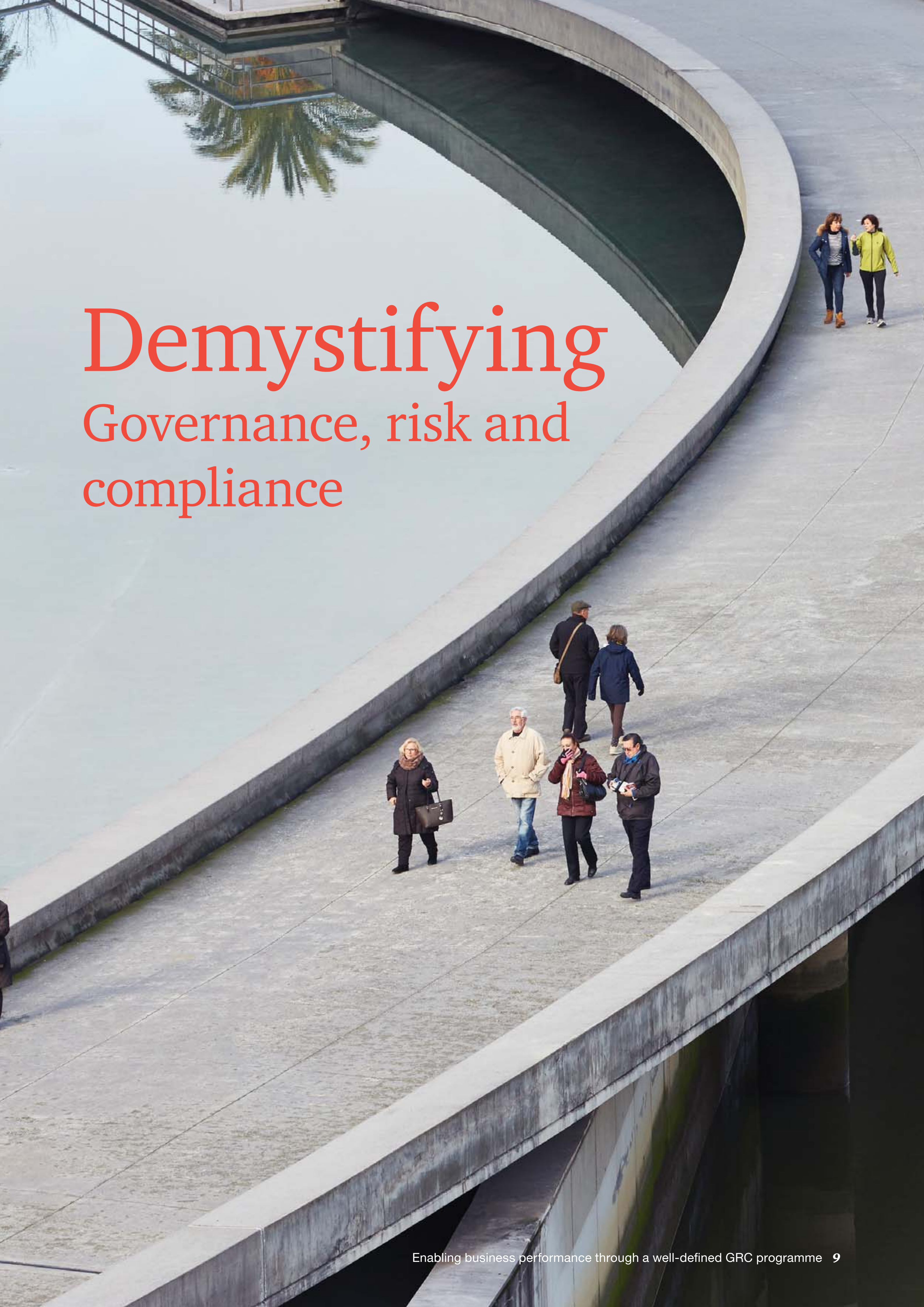
In a world that increasingly expects vital data to flow instantly wherever it's needed, corporations may view GRC as onerous, a set of expensive corks that act as stoppers against value loss and keep the company in compliance, but do little to create value and move the enterprise forward. Ironically, this attitude is particularly prevalent in the more heavily regulated industries, where an excessive focus on traditional compliance activities has prevented GRC leaders from focusing more of their time on enabling strategic and operational value because of the demands of new and evolving risks and regulations.

The complexity of today's business environment demands that GRC assumes a new role, upping its value protection and compliance game and also becoming a direct enabler of business performance. Instead of functioning in silos, the disparate strands of GRC must be brought together into a coordinated, collaborative system whose people, processes, and technologies are integrated and synthesised for greater effectiveness and efficiency. Instead of being the unfriendly face of 'no', GRC must become a positive, proactive force that pushes companies forward by providing a holistic view of risks, responsibilities and opportunities. Instead of being a back-office watchdog, the GRC programme must become a fully integrated part of the business, injecting a risk and compliance mindset into day-to-day activities across functions and aligning culture, people, and systems with management's strategic priorities, financial and operational imperatives, and business performance drivers.

In the subsequent sections, we have outlined how a company can run an effective GRC programme by focusing not only on value protection but also on value enhancement.

Demystifying

Governance, risk and compliance



Governance – the changing landscape

Evolution of governance – the journey so far

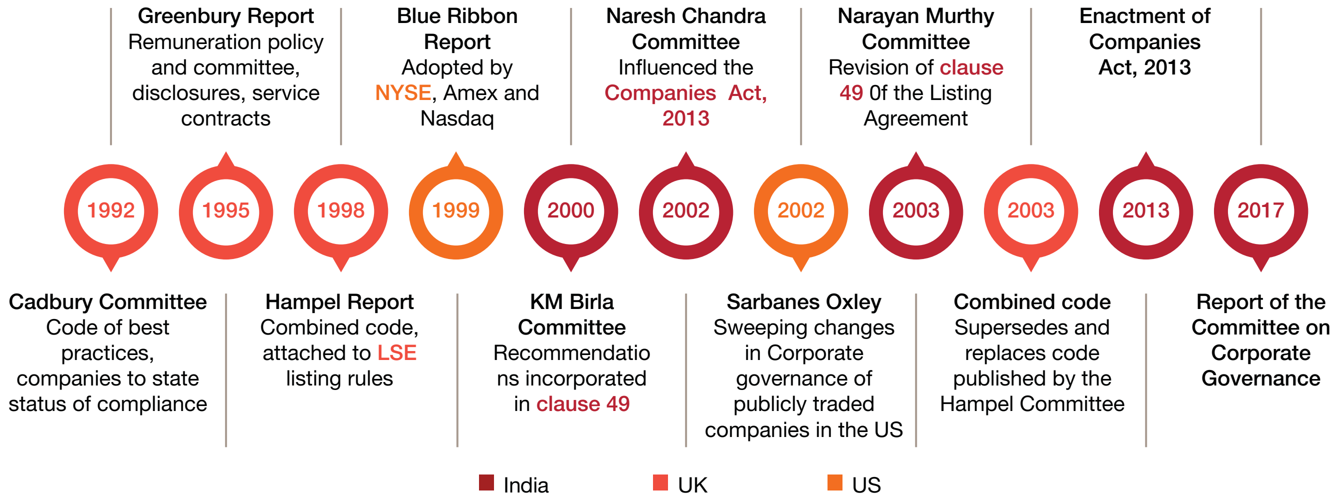
Most of the large corporate groups in India were family-owned and businesses were run by the family members who held the key managerial positions and took all the important business decisions. Although with the development of the capital markets in India, many of those large corporate groups got listed on stock exchanges, traditional governance practices were being followed.

Due to the involvement of public funds, a need for greater accountability of companies to their shareholders was felt. As a result, in 1992, the securities market regulator Securities and Exchange Board of India (SEBI) was formed and various corporate governance reforms were initiated in India.

In 1999, SEBI constituted a committee on corporate governance under the chairmanship of Shri Kumar Mangalam Birla. Considering the recommendations made in the committee report issued in 2000, the Stock Exchange Listing Agreement was amended by inserting a new clause—i.e. clause 49—which became a mandatory governance code for listed companies. Clause 49 introduced significant provisions related to governance for listed companies in India.

Clause 49 facilitated a transformation of governance culture in corporate India, driven by several conscious promoters, independent directors and professional management. Listed companies were required to open up their boards for 'outsiders', i.e. independent directors. There was also a sharp focus on financial reporting and a variety of other disclosures to stock exchanges. The disclosures in the annual report became far more elaborate.

The journey of the development of the concept of a corporate governance framework around the globe and in India is depicted below.



1992 **Cadbury Committee** Code of best practices, companies to state status of compliance

1995 **Greenbury Report** Remuneration policy and committee, disclosures, service contracts

1998 **Hampel Report** Combined code, attached to LSE listing rules

1999 **Blue Ribbon Report** Adopted by NYSE, Amex and Nasdaq

2000 **KM Birla Committee** Recommendations incorporated in clause 49

2002 **Naresh Chandra Committee** Influenced the Companies Act, 2013

2002 **Sarbanes Oxley** Sweeping changes in Corporate governance of publicly traded companies in the US

2003 **Narayan Murthy Committee** Revision of clause 49 0f the Listing Agreement

2003 **Combined code** Supersedes and replaces code published by the Hampel Committee

2013 **Enactment of Companies Act, 2013**

2017 **Report of the Committee on Corporate Governance**

🟥 India 🟥 UK 🟧 US

A significant regulatory change in India happened in the year 2013 with the enactment of a new Companies Act. The Companies Act, 2013, has significantly raised the bar on governance and board accountability.

Some of the key areas which have been impacted relate to board structure and functioning, disclosure and reporting requirements, controls framework, responsibilities of auditors, related party transactions, CSR, etc.

Recently, in order to enhance the standards of corporate governance of listed companies in India, SEBI had formed a committee under the chairmanship of Mr. Uday Kotak. The committee's report suggests certain changes with respect to independent directors, promoters, management and auditors. The intent is to bring greater accountability and transparency in the way companies operate in India.

The key changes/improvements suggested by the committee report are as follows:

- Independent directors: Confirmation in the corporate governance report that the board has been responsible for the business and overall affairs of the listed company; increase in minimum number of independent directors (50% whether the chairman is executive or non-executive); increased presence of independent directors in the nomination and remuneration committee, etc.
- Promoters: Separation of the roles of chairperson and MD/CEO; greater transparency through increase sharing of information with controlling promoters/shareholders and nominee directors; enhanced approval requirements related to the remuneration of promoter directors, mandatory appointment of lead independent director in case of non-independent chairperson; gender diversity; increase in minimum strength of board; approval by minority shareholders for royalty payments, etc.
- Management: Enhanced governance over subsidiaries – incorporated both in India and overseas; formal induction and training programmes for independent directors; disclosure requirements of skill required and availability in the annual report, etc.
- Accounting and audit related: Mandatory quantification by management of the impact of audit qualifications; auditor's right to obtain independent expert opinion; IFC reporting requirements extended to foreign operations; enhanced disclosures for related party transactions, etc.

While the finalisation of the recommendations from the above report and its implementation is yet to be seen, it is almost certain that these will further enhance the governance standards on the companies in India.

Implementing key changes to meet governance expectations

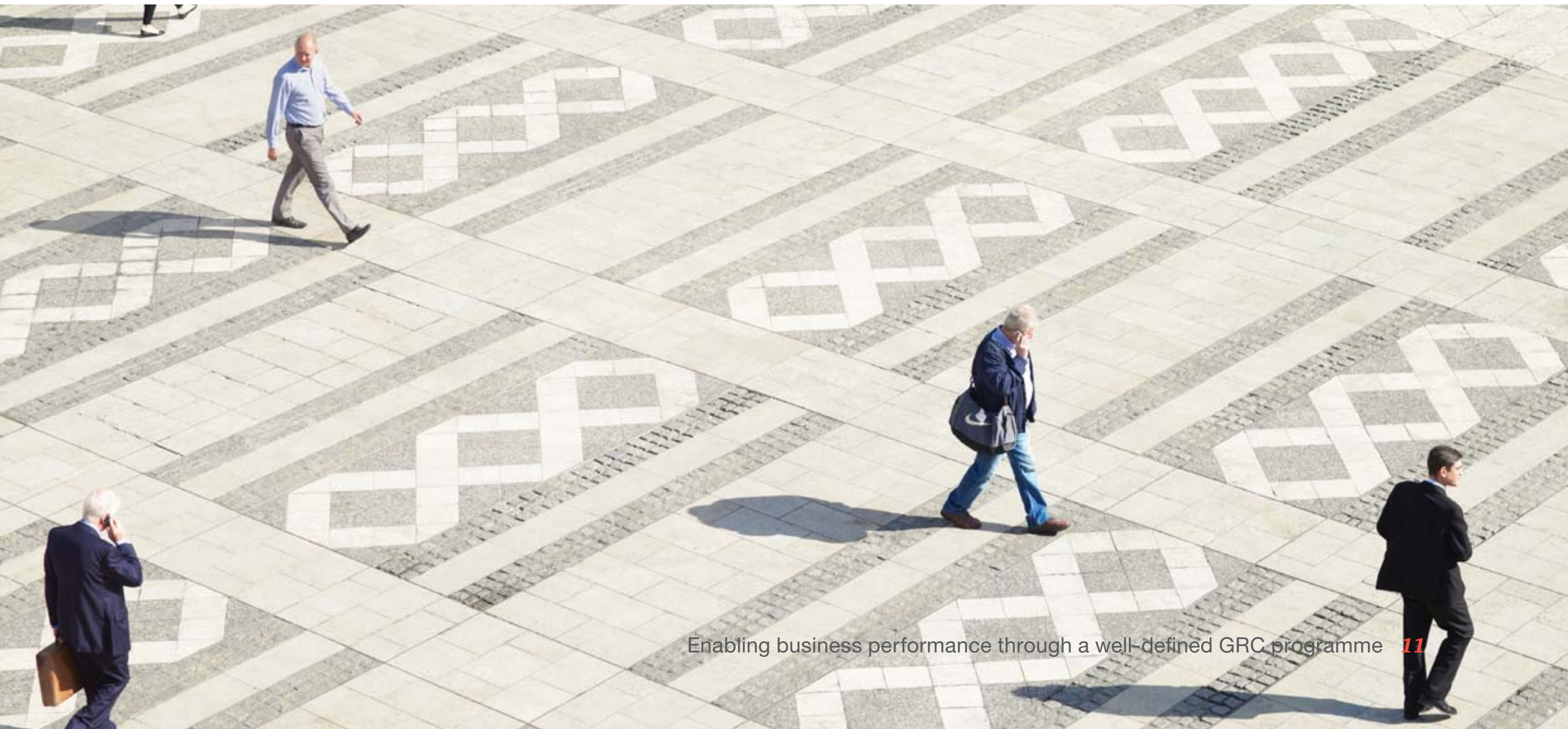
Against the backdrop of regulatory requirements, companies, especially listed companies, are faced with great expectations from investors and the public. Perhaps, now more than ever, public companies are being asked to take the lead in addressing some of society's most difficult problems. From seeking action on climate change to advancing diversity, stakeholder expectations are increasing and many companies are responding.

Under enhanced regulatory regime, the organisations need to focus on the following key aspects with regard to the governance:

- **Board composition and diversity**

  In a rapidly changing business climate, a high-performing board requires agile directors who can grasp concepts quickly. Directors need to be fiercely independent thinkers who consciously avoid groupthink and are able to challenge management—while still contributing to a productive and collegial boardroom environment. A strong board includes directors with different backgrounds, and individuals who understand how the company's strategy is impacted by emerging economic and technological trends.

  In assessing their composition, boards and their governance committees need to think critically about what skills and attributes the board currently has, and how they tie to the oversight of the company. As companies' strategies change and their business models evolve, it is imperative that board composition be evaluated regularly to ensure that the right mix of skills are present to meet the company's current needs. Many boards conduct a gap analysis that compares current director attributes with those that it has identified as critical to effective oversight. They can then choose to fill any gaps by recruiting new directors with such attributes or by consulting external advisors.



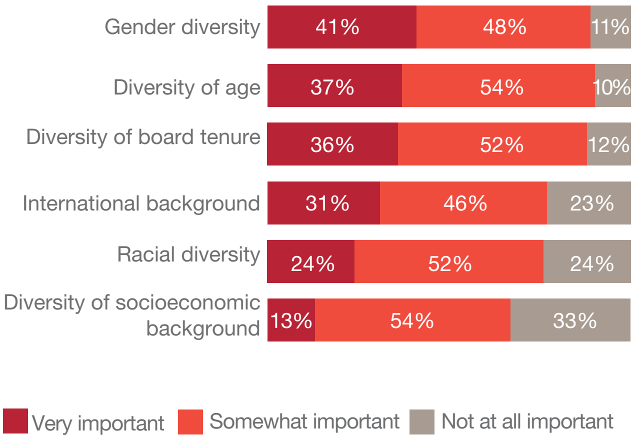
Some companies use a matrix in their disclosures to graphically display to investors the particular attributes of each director nominee.

Leading practices adopted by companies globally suggest that while considering board composition, due consideration is given to various competencies/ aspects—financial expertise, risk management expertise, industry expertise, international expertise, cyber security expertise.

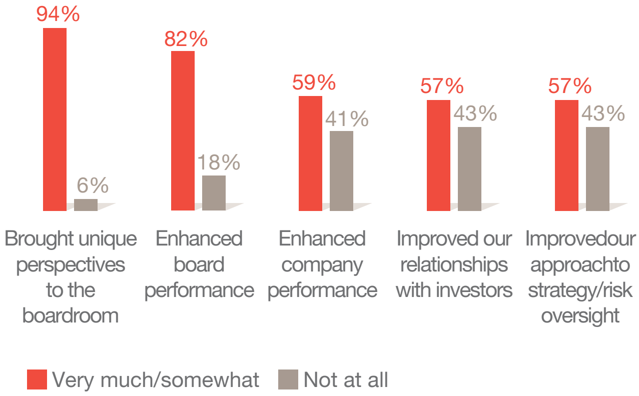
Further, diversity is a key element of any discussion of board composition. Diversity includes not only gender, race, and ethnicity, but also diversity of skills, backgrounds, personalities, opinions, and experiences. Gender is the factor most commonly viewed by directors as very important to achieving diversity of thought in the boardroom. The Annual Director Survey conducted by PwC US in 2017, clearly indicates that the director group strongly believe board diversity brings in significant value by way of bringing in a unique perspective in the boardroom and enhancing the board's and company's performance.

Directors' views with regard to diversity and its value as per the Annual Director Survey are depicted below:

What brings diversity of thought?



The impact of board diversity



Some of the other key leading practices that are followed with regard to board composition and refreshments are:

- Acting on the results of board assessments: Board assessments greatly help in determining the appropriate board composition. This is discussed in our next point on board performance evaluation.
- Taking a strategic approach to director succession planning: Director succession planning is essential to promoting board refreshment. In board succession planning, it's important to think about the current state of the board, the tenure of current members and the company's future needs. Boards should identify possible director candidates based upon anticipated turnover and director retirements.
- Broadening the pool of candidates: Often, boards recruit directors by soliciting recommendations from other sitting directors, which can be a small pool. Forward-looking boards expand the universe of potential qualified candidates by looking outside of the C-suite, considering investor recommendations, and by looking for candidates outside the corporate world—those retired from the military, academia, and large non-profits. This will provide a broader pool of individuals with more diverse backgrounds who can be great board contributors.

- **Board performance evaluation**

  Board assessments can be useful tools to promote board refreshment—when used right. In our view, boards that view the process as one of continuous improvement, rather than as an annual compliance exercise, will obtain faster and better results. Having a robust board assessment process can offer insights into how the board is functioning and how individual directors are performing. The board can use this process to identify directors that may be underperforming or whose skills may no longer match what the company needs.

  Effective board leadership can also make a real difference, but only if the board chair or lead director is willing to have difficult discussions, including providing honest individual director feedback. A periodic independent perspective can help as well.

  The most effective boards we see are also disciplined about identifying action items coming out of their assessments, and holding themselves accountable for those actions. They take concrete steps, often integrating assessment results into their director succession plan.

  Giving stakeholders a clear picture of what the board's process is and why directors think it works demonstrates a strong commitment to ongoing board refreshment. In fact, some of the boards believe that conducting the board performance evaluation through a defined performance and competency matrix and publishing the results in their annual reports or sharing with investors will boost the confidence of the investors and shareholders on the board.

- **Alignment of board and the CEO/management**

  The job of steering a company's strategy is split between management and the board. While management largely designs the strategy and is responsible for its execution, the board contributes to strategy formation, oversees its implementation and provides ongoing monitoring.

  The relationship between the CEO and the board is extremely important. For sustained organisational success, it is essential that the relationships between the CEO, the executive team, the chair, and the board are of high quality. Some of the aspects which can enable foster a successful board and CEO relationship are as follows:

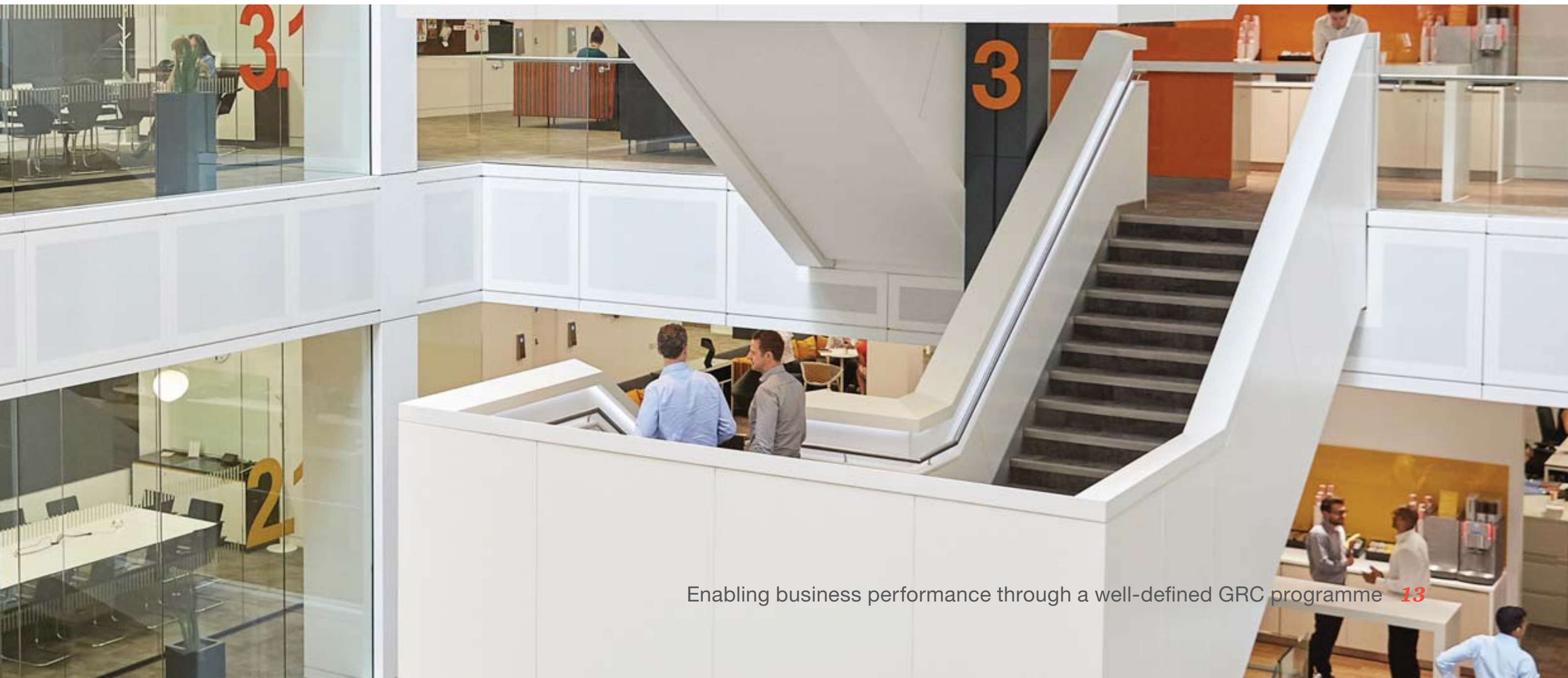
  - Each should have clear understanding of its role through a defined responsibility statement and a board charter.
  - Alignment of board and executive management on strategic direction: It is critical for the board, the CEO and the executive team to have regular discussions on strategy—not just an annual strategic meet.
  - The CEO and the executive team must have adequate delegation or authority from the board to enable them to operationalise the strategic direction.
  - Regular performance review of the CEO by the board.
  - Board evaluation, as mentioned earlier, is also very important as it conveys their seriousness about continuous improvement. Use of external facilitators to evaluate board performance will show greater transparency, leadership and accountability.

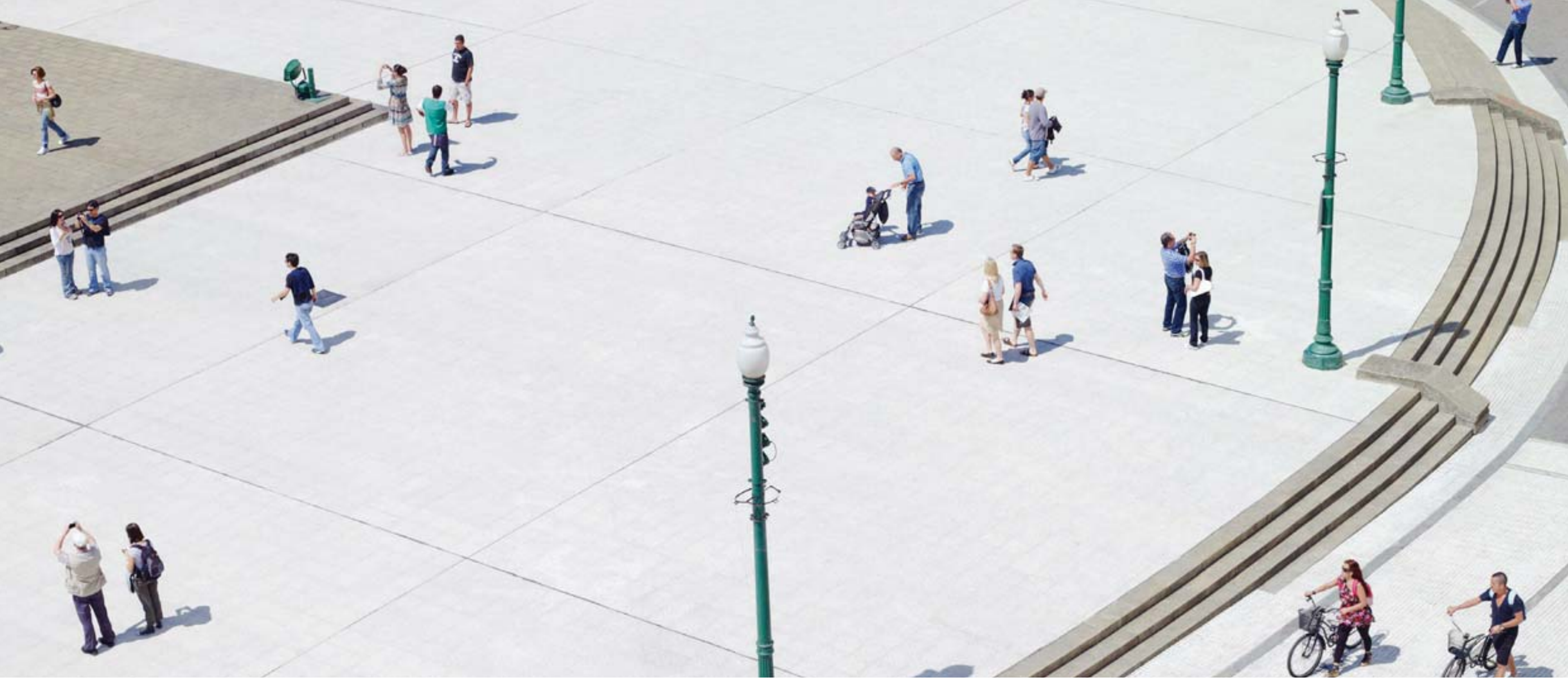
  Based on the above, it's clear that for a successful board-management relationship, clear roles, goals and performance expectations are imperative. However, for sustained success, even more critical are the leadership and behavioural expectations between the chair and the CEO.

- **Building a strong control environment**

  As a result of the enhanced governance requirements, boards need to lay down the foundation for a robust internal control framework within the organisation. These should cover the following key aspects:

  - Processes, procedures and policies
  - Delegation of authority
  - Risk management policy framework
  - Legal compliance management framework
  - Cyber security framework
  - Enterprise risk management framework





These frameworks and systems cannot work in silos. They need to be integrated and embedded in the DNA of organisation.

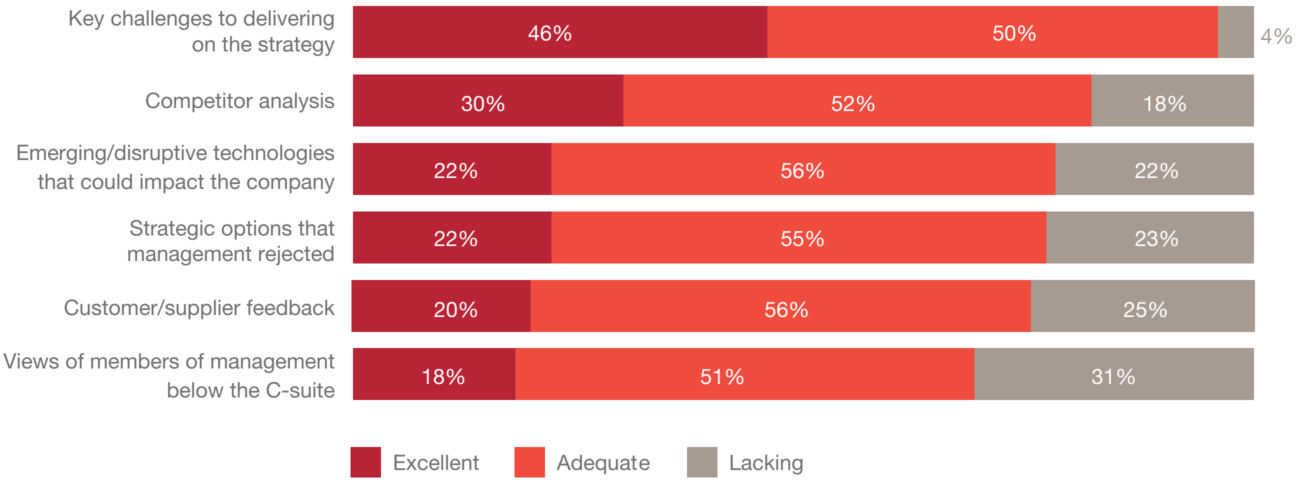
Further, a strong oversight mechanism needs to be in place to ensure that such frameworks and processes operating effectively. In the last few years, the board and management, globally, are driving such oversight through the use of technology enablers. These technology tools provide boards with the required insight and analytics for their review and decision making.

- **Oversight and reporting**

  It's fundamental for an organisation to develop a robust oversight mechanism. Reporting to the board is extremely critical. The board needs to be provided with appropriate information at the right time for them to review, challenge and take strategic decisions for the company.

  As per the Annual Director Survey conducted by PwC US in 2017, while the board believes that management is mostly effective in providing the appropriate information to evaluate the company's proposed strategy, there are key areas in which the information flow may be a problem. A concerning number of directors say the information they receive is 'lacking' in the areas of emerging/disruptive technologies, strategic options that management rejected, customer/supplier feedback and views of management below the C-suite.

How good is the information the board gets on strategy?



Governance sets the tone of the organisation. It creates the overarching framework within the organisation according to which company will operate. Hence, a strong governance structure is fundamental for any organisation to sustain and grow in the long term.

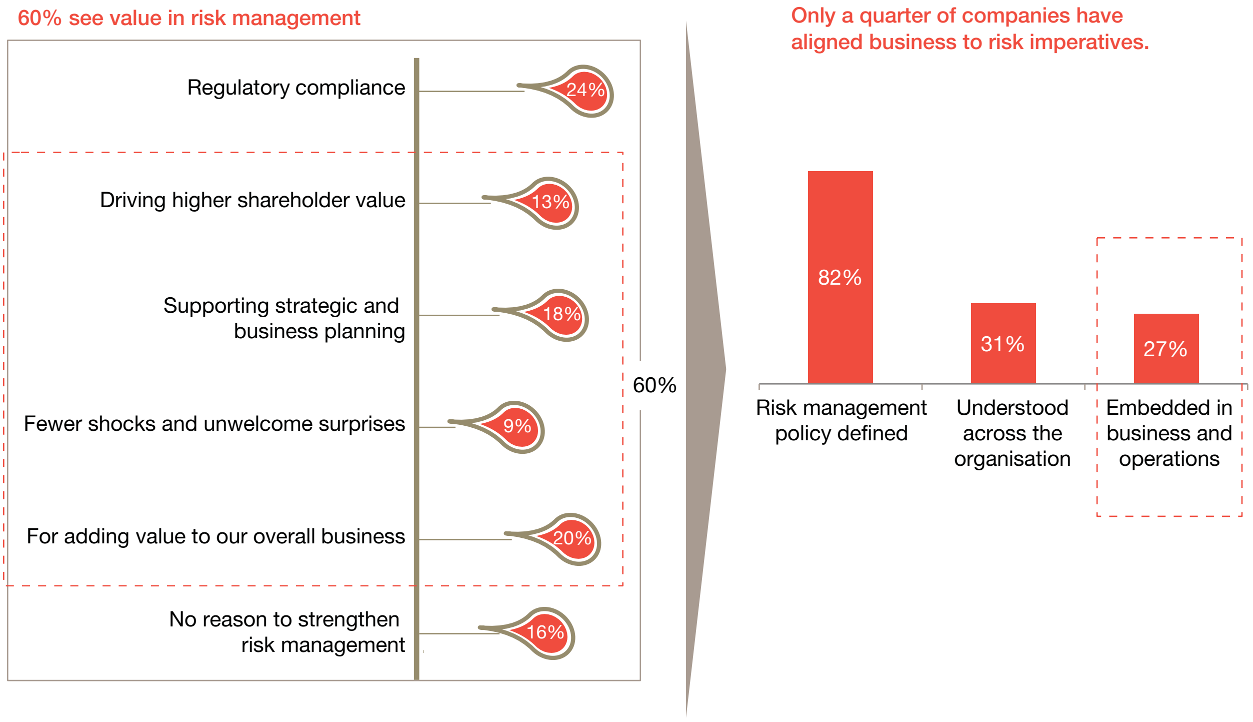
The key pillars supporting the overall governance framework are risk management and compliance management. Robust risk and compliance management frameworks are imperative to drive governance within an organisation.

Current state of risk management: Why do risk management programmes fail to deliver value?

The concept of risk management is neither new nor novel in the business context. Businesses have been managing their risk exposures since time immemorial, albeit in an ad hoc fashion. Hence, the need for risk management is well established, but a formal regulatory structure for the same was accorded through clause 49 of the Listing Agreement by SEBI in India. This was a landmark initiative in the risk management space; however, it was limited to listed companies. This made it mandatory for listed companies to lay down procedures to inform board members about the risk assessment and minimisation procedures. Further, it also laid the requirements for a certain set of listed companies to constitute a board sub-committee as a risk management committee for specific oversight in risks. With the introduction of the Companies Act, 2013, the onus of risk management has been laid squarely on the board of directors. The requirements reflect the prevalent global sentiment that the board and management need to set the right tone at the top for effective and strategic risk management.

While there has been significant traction in the adoption of risk management in India, organisations have found it challenging to derive true value from the programme. In one of the studies conducted by PwC on risk management, 60% of C-suite executives acknowledged that they see value in a risk management programme; however, only a few could realise the said value. This can be attributed to a compliance-driven mindset and failure of organisations to effectively align risk management with business.

Although most organisations in India see value in enterprise risk management, only a few have realised its benefits.


60% see value in risk management

Only a quarter of companies have aligned business to risk imperatives.

Source: PwC's Risk Management Survey – India at a glance

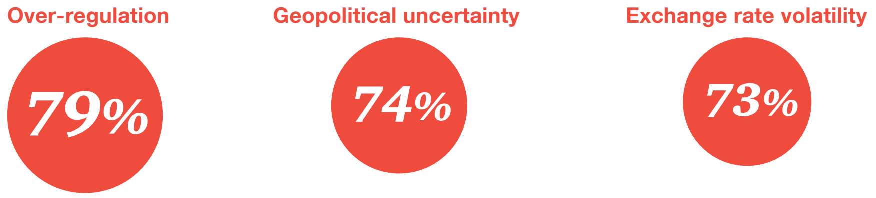
Changing risk landscape – an era of complexity and risks

The ever-increasing and stringent mandate around risk management is a reflection of the times we are living in. In the past several years, many large-scale events that were once thought unlikely, distant, or isolated—climate change, food security, energy supply volatility, overhaul of technology, and a global liquidity crisis, to name a few—have manifested and changed the course of business for many organisations. As the business environment changes, a host of opportunities arise constantly. With them, however, new 'emerging' risks appear. The global macroeconomic environment remains challenging, and the global operating models have added a mixture of efficiency and complexity to virtually every business today. Technology continues to connect us faster and with more ease, but maintaining volumes of data and keeping levels of consistency has become harder. Consumers are better informed and more demanding. And competitors, both new and old, are looking for ways to expand their market share at a time when growth remains low. In this context, it is no surprise that risk management is increasingly finding its due place in boardrooms.

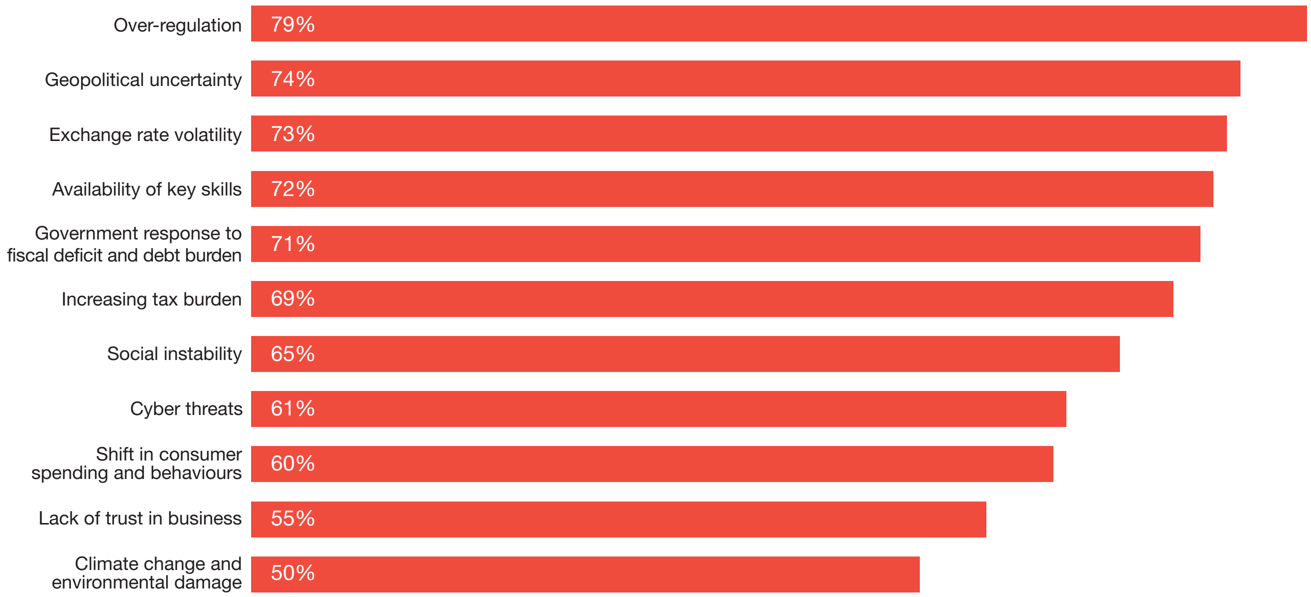
Today's CEOs face a business environment that's becoming increasingly complicated to read and adapt to. Accordingly, as per PwC's Annual Global CEO Survey, the level of worry around areas such as regulations, national debt, availability of skill sets, geopolitical uncertainty and taxes has increased.

Based on PwC's Annual Global CEO Survey, the key concerns of CEOs can be well understood below:

Top-three threats



Key threats

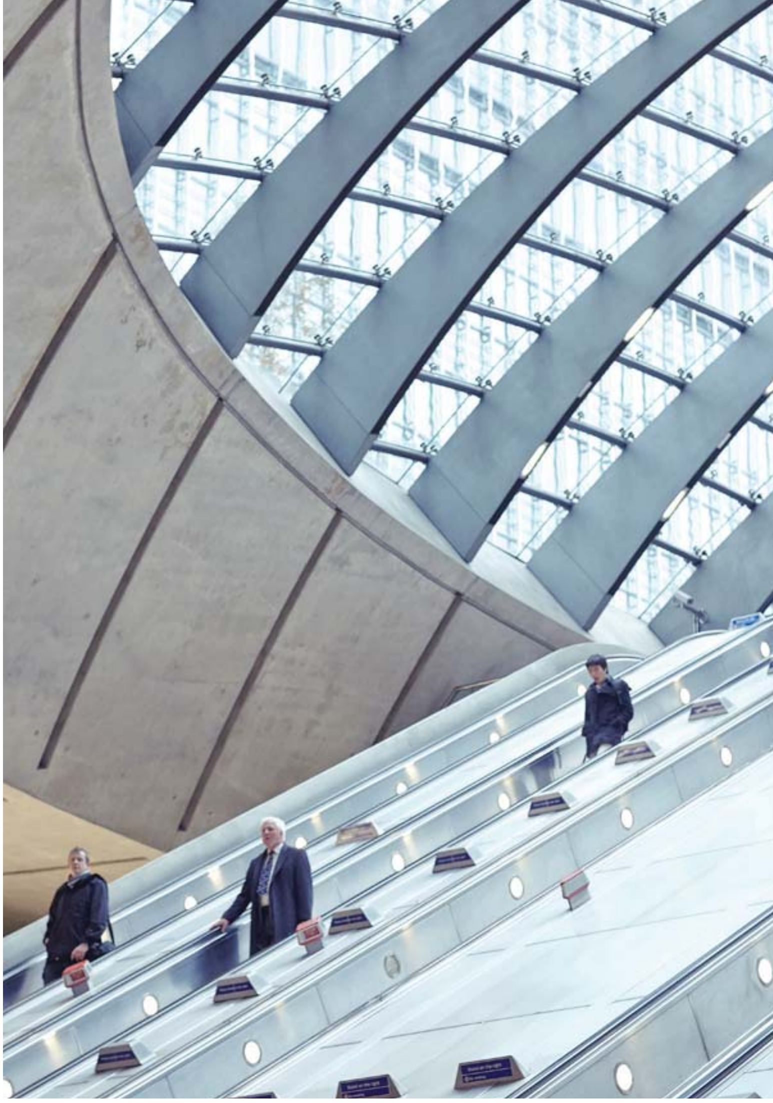


Source: PWC 19th Annual Global CEO Survey - Redefining business success in a changing world CEO Survey

One of the common emerging concerns, based on the results of PwC's Annual Global CEO Survey, is cyber security. Across sectors, all the respondents indicated that they expect cyber security and data privacy breaches to cause significantly more disruption in the years ahead. Cybercrime and data privacy risks now have the potential to affect every aspect of company's operations, and that threat becomes only greater as industries expand their interfaces with the internet and other emergent technologies. As per the survey, while 62% expect cyber risk to cause disruption in the next three years, only 9% have high or very high cyber risk maturity. Further, cyber security is one of the areas where respondents' claims of response effectiveness indicated the greatest improvements over past survey results. This suggests that even though companies are feeling more confident in their capabilities, they remain on purely defensive footing against cyber risk and have not adopted leading practices yet.

Indian CEOs are no outliers and are equally worried about the state of risks and opportunities in their business landscape. Most of the Indian CEOs (around 80%) believe that over the next five years, technological advances will transform wider stakeholder expectations. A majority of the respondents also expect demographic shifts and changes in global economic power to have a similar impact.

In the last couple of decades, India has enjoyed services-led growth and has been relatively insulated from technological change in a number of industries. The last few years have seen waves of technology-led disruption in areas as diverse as taxi services and retail. Further, India's IT industry is seriously trying to come to grips with the technological developments related to robotic process automation (RPA), artificial intelligence, machine learning, etc., which are at our doorstep. The incumbent CEOs have thus rightly elevated the threat posed by speed of technological change.



What makes Indian CEOs sceptical about their growth plans?

67%
Geopolitical uncertainty

58%
High and volatile energy costs

55%
Cyberthreat

Key risk trends:

- Anti-globalisation
- Neo-nationalism
- Fluctuating oil prices/ Paris Agreement
- Cyber sabotage
- Digital disruption

68%
of Indian CEOs are concerned that their readiness to respond to a crisis or risk event can impact their growth prospects.

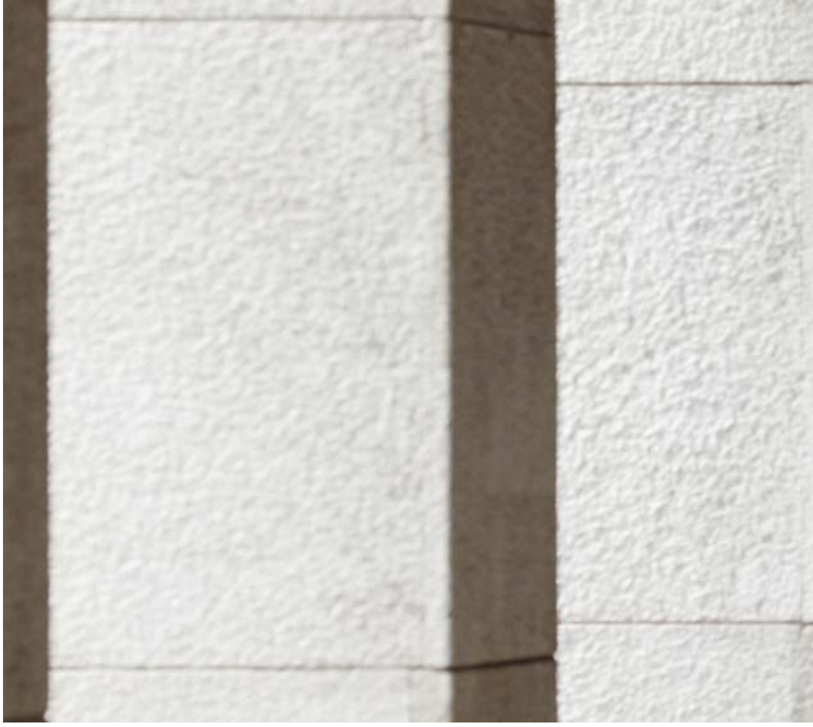
69%
of Indian CEOs think that business should do more to measure the impact of key risks.

93%
of Indian CEOs are already making changes to the way they define and manage risks.

Source: PwC's 19th Annual Global CEO Survey: The view from India

CEOs understand that despite the tremendous challenges they face in managing their business today, they also need to look ahead and build a business that's ready for the more complex global marketplace of the future. CEOs are seeking to better measure the impact and value of innovation and key risks for stakeholders. Companies are addressing these by ensuring better insight into business processes and measuring a broader range of defining variables.

Deriving value for a risk management programme



Faced with the new challenge of today's complex business risk environment, companies are seeing the tide shift once again. Today, a collaborative approach to risk management, with risk accountability sitting squarely in the first line of defence, can be the key to greater organisational resiliency and growth. That means an engaged first line that makes risk decisions in alignment with strategy. Further, it implies a proactive second line that influences decision making through effective challenge and timely consultation and collaboration. And it means a diligent, independent third line focused on its core missions of protecting the organisation and delivering value.

Senior management and business units

First line:
Decision makers anticipate business risks, embed risk management in strategic planning and tactical execution, and assign the right risks to be managed in right places.

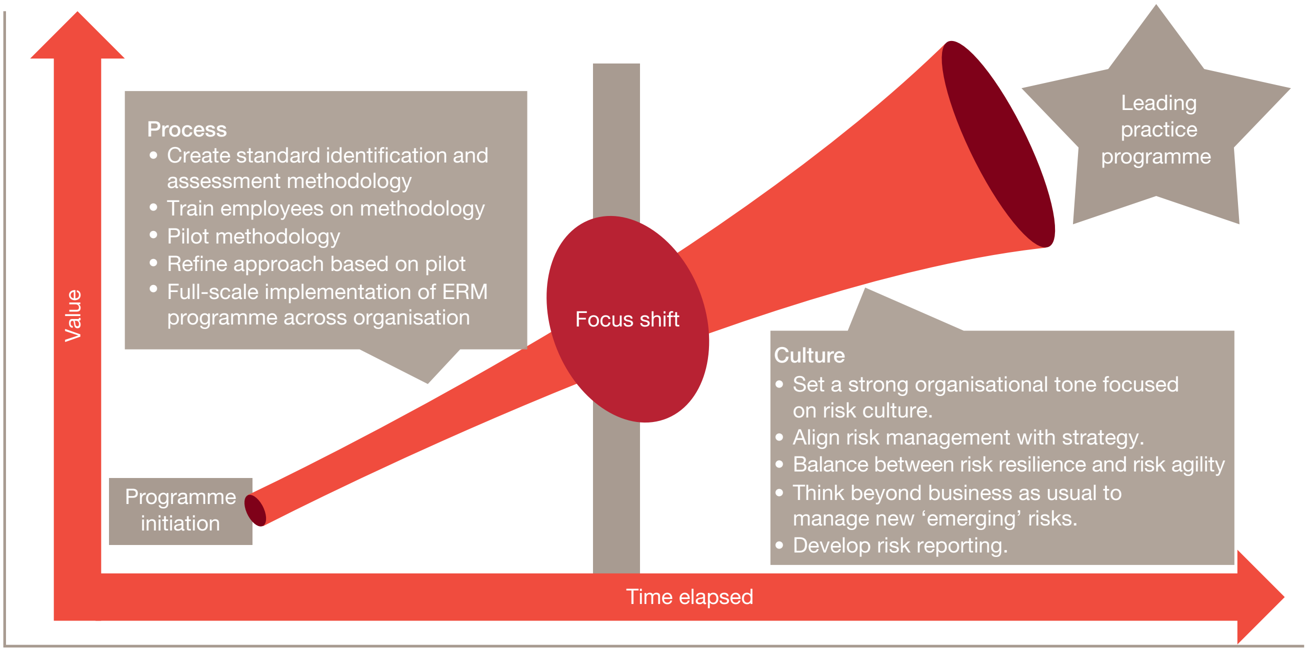
Risk and compliance functions

Second line:
Risk and function work collaboratively with the first line, providing checks and balances to optimise the risk management process.

Internal audit

Third line:
Internal audit provides objective test controls and provides independent assurance, assessing the first and second line risk activities.

Shifting risk management activities to the first line of defence is only one part of moving towards a more proactive, strategically aligned risk management programme. Value creation requires a shift from a process-driven approach to a risk culture centric approach to risk management.



Process
- Create standard identification and assessment methodology
- Train employees on methodology
- Pilot methodology
- Refine approach based on pilot
- Full-scale implementation of ERM programme across organisation

Culture
- Set a strong organisational tone focused on risk culture.
- Align risk management with strategy.
- Balance between risk resilience and risk agility
- Think beyond business as usual to manage new 'emerging' risks.
- Develop risk reporting.

Some of the key aspects that can enable this shift from a process-centric approach to a value-driven culture are as follows:

1. **Set a strong organisational tone focussed on risk culture**

   The CEO and the board should model this tone, which should permeate the organisation and be continually monitored and measured for effectiveness. Organisations need to review and assess their current risk culture to drive the transformation into a risk-aware culture. Stakeholders need to understand that risks are not to be avoided but to be proactively identified, understood and responded to in alignment with the organisation's business strategy. Most importantly, risk transparency and communication should be worked upon to enhance the risk culture of the organisation. Some of the initiatives in this direction could be:

   - CEOs should ensure performance management and incentives are aligned with risk culture goals.
   - Leadership communications should foster clear and consistent messaging.
   - Risk should be incorporated into routine conversations and decision making.

2. **Align risk management with strategy**

   A risk appetite statement, effected by top management, sets the tone for balanced risk-taking across the organisation. The decision makers, thus, have a clear understanding of how much risk is acceptable in their pursuit of objectives, both organisational and unit wise (division, function). Also, risk appetite is a prerequisite for objective setting in an organisation as organisations should consider the risks involved in attaining strategic goals and their appetite for such risks.

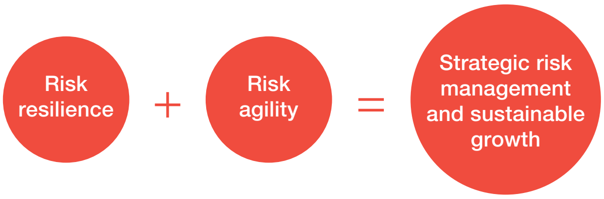
   Although defining and integrating the risk appetite at management level is the first step, it is not enough. Risk appetite must be communicated across the organisation and to all decision makers in a language that helps the relevant stakeholder imbibe it as part of their decision-making process and take an aggregate view of risks. Besides, the risk-monitoring mechanism should ensure that all decisions across the organisation are consistent with the risk appetite statement.

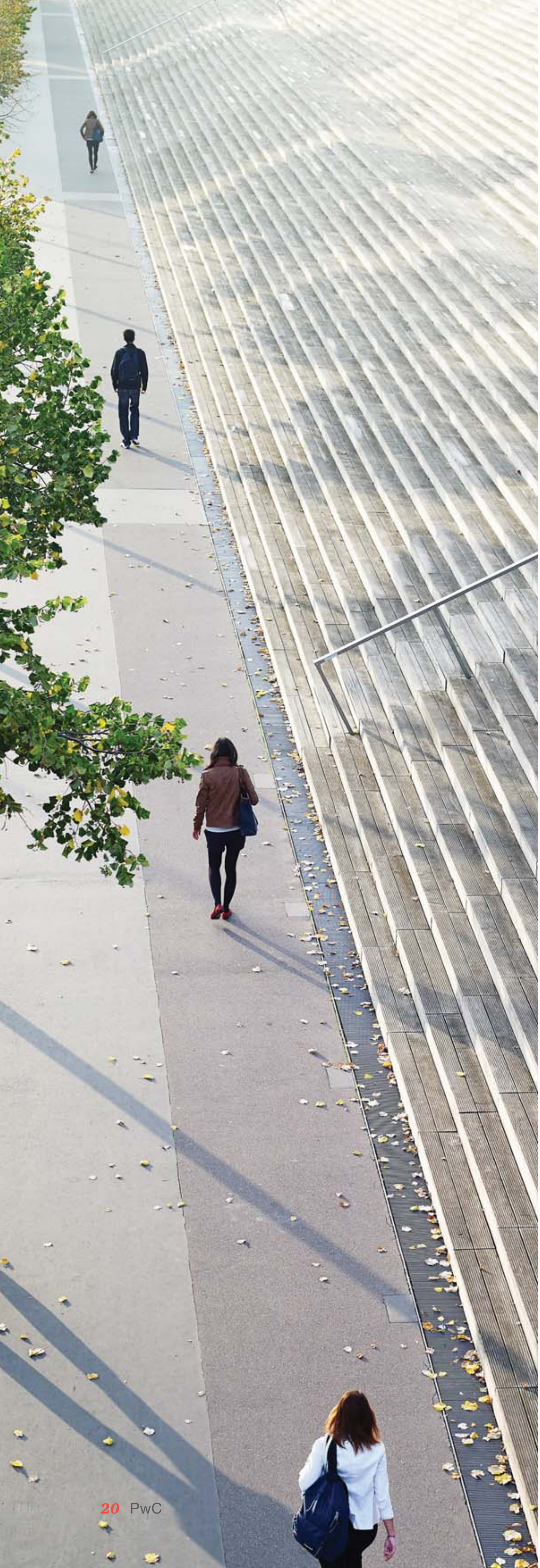
3. **Balance between risk resilience and risk agility**

   The company needs to strike the appropriate balance between risk agility and risk resilience. The companies that use their risk management activities to play both sides are more likely to see sustainable growth and better performance patterns because they are balanced between moving the business forward and keeping the business in check.

   Risk agility: The ability to alter and adapt risk management infrastructure to respond quickly to changing markets, customer preferences or market dynamics

   Risk resilience: The ability to withstand business disruption by relying on solid processes, controls and risk management tools and techniques, including a well-defined corporate culture and powerful brand





4. **Thinking beyond business-as-usual to manage new 'emerging' risks**

   Management should institutionalise mechanisms to proactively identify sources of emerging risks through an early warning system and establish a response strategy in line with the nature of risk. Based on the nature of emerging risk, the strategy could be either an 'anticipate and respond' framework or an 'absorb and rebound' framework.

   At times, the emerging risks provide ample indication of their imminence and can be anticipated, provided adequate early warning systems are in place, thereby allowing organisations to prepare a response strategy in line with the 'anticipate and respond' framework. In another scenario, where an early warning system is not mature enough or where current risk indicators fail to identify the emerging risks, the organisation must develop resilience to absorb the shock and act in order to rebound back to business as usual.

5. **Develop risk reporting**

   The risk reporting should enable executive management and board to effectively execute their risk oversight responsibilities. It is imperative that the right information is available with the management/board to evaluate the risks vis-à-vis business objectives. Thus, it is very important for the line functions or risk management team to effectively collate and report information related to risks.

   Such reporting can be efficiently and effectively managed through use of technology enablers. The technology enablers can assist management in collating the results of risk assessment, scenario analysis and reporting in a meaningful manner. On top of it, companies can engage in data analytics and simulations, etc.

   Considering some of the above key practices/ elements above, companies can evaluate their risk management programs and take it to the next level. This can help them achieve their desired business benefits under a risk managed or assessed scenario.

Compliance: Navigating legal and regulatory complexity

In today's world, market innovation has created enormous opportunity for organisations to serve customers, solve problems and achieve growth in new ways. Of course, with this potential, comes both uncertainty and risk. Even a seemingly simple regulatory change can have significant ripple effects across systems, operations, and many other areas of a company's business. Additionally, companies are expanding into new and emerging markets, where regulation is in its early stage or subject to rapid change. The advent of extra-territorial laws are adding an additional dimension to the complexity of compliance.

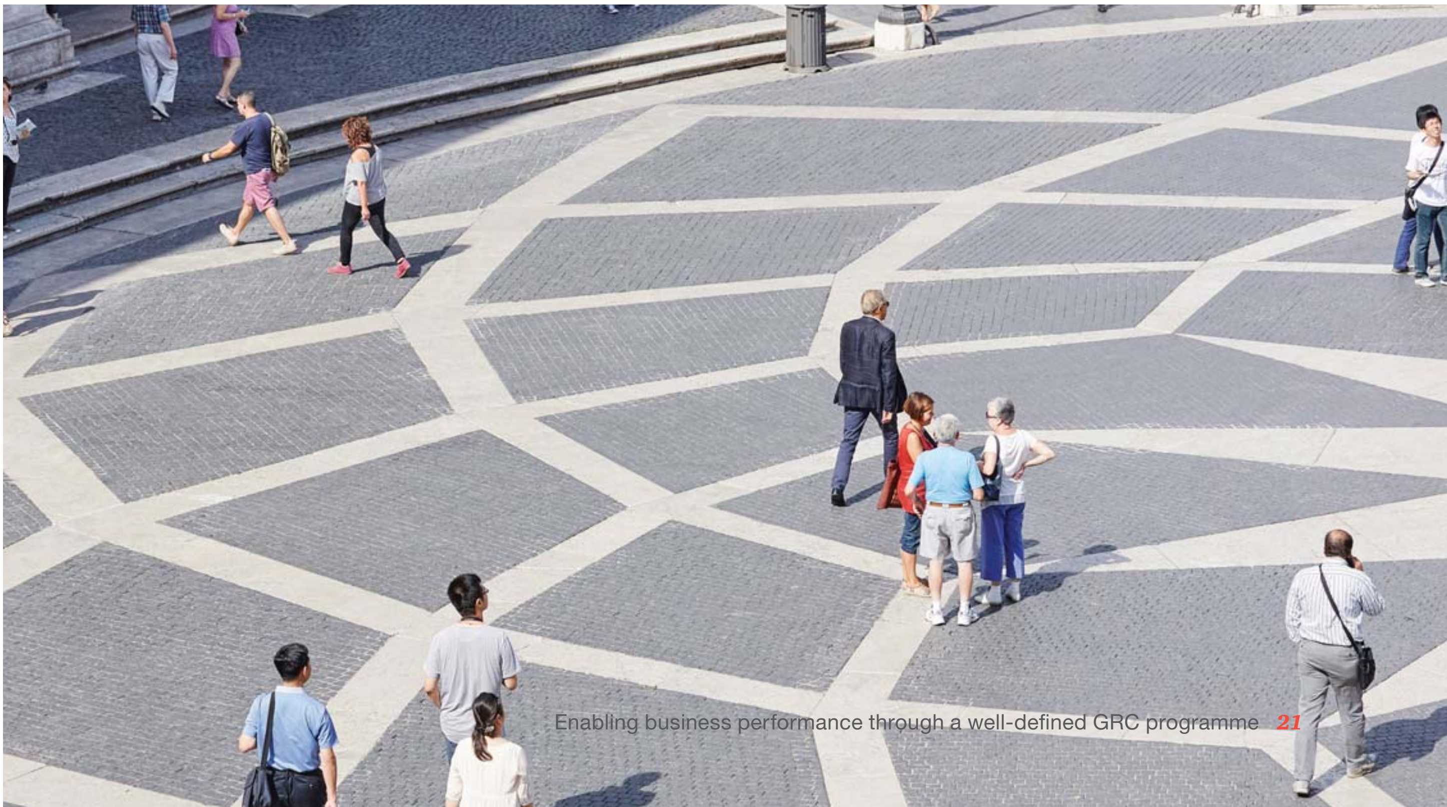
As an example, the advent of the General Data Protection Regulation (GDPR) in the EU has created challenges for corporations to navigate through the data privacy maze. Globally companies have been penalised heavily due to non-compliance of FCPA and UK Anti-Bribery laws which has extra –territorial impact. Heavily regulated financial sector have been busy in adopting Foreign Account Tax Compliance Act (FATCA). Globally as well in India, heightened scrutiny from regulators and challenges of an ever-evolving legal universe has compelled companies, to focus on regulatory and business compliance.

Complexities in India

The Indian federal structure is complex and so are the onerous laws. There are central, state and local/municipal laws which are applicable to every organisation. On top of it, there are industry-specific laws which co-exist with rules defined by regulators. In the normal course of business, where business expansion and growth is at the top of the agenda, compliance takes a back seat in several cases. However, given the stringent government scanner, it is imperative for Indian companies to put strong systems in place to ensure compliance with laws and regulations. A lax compliance approach exposes a company to a lot of risks, not only in terms of regulatory misses, but also business risks. It exhibits a poor corporate governance strategy and risk management plan.

The Companies Act, 2013, places great onus on the boards to devise proper systems to ensure compliance with the provisions of all applicable laws and to confirm in the board's report that such systems are adequate and operating effectively. Additionally, the boards of listed companies are required to periodically review compliance reports pertaining to all laws applicable to their company, as well as steps taken by the listed entity to rectify instances of non-compliances.

The Companies Act requires the company secretary to report to the board about compliances applicable to the company. Additionally, for listed companies, it is mandatory to appoint a company secretary as the compliance officer.



Key challenges in managing compliance complexities

There are multiple challenges faced by companies to manage the complexities of the compliance landscape. Some of the key challenges are:

- Business strategy is often developed without a full picture of potential compliance risks.
- It's challenging to see through the maze of rules, regulations and obligations to not only comply, but to drive advantage.
- Roles and responsibilities are not clearly defined, resulting in compliance misses.
- Regulators are not able to keep up with the changes driven by technology. Hence, laws are not evolving to address current requirements.

Strengthening the compliance function

To overcome the challenges faced by the business to manage compliance complexities and to manage the demands of ever-changing market dynamics and unforeseen regulations, leading organisations are striving to strengthen the compliance function.

We suggest the following eight evolutionary steps to strengthen the compliance function:

1. Define the compliance function's scope of responsibility, establish a governance structure, a compliance team, and a compliance committee

Which areas will the function own? Which areas will be owned by other groups but be closely monitored by the compliance function? And in which areas will the compliance function have limited involvement? These aspects should be defined upfront.

The establishment of an effective governance structure for compliance includes:

- Securing the committed involvement of senior management in compliance program development
- Appointing a compliance leader to coordinate and oversee the program on a day-to-day basis—and specifying that leader's responsibilities
- Securing budget, resources, and staff for the function
- Assembling a compliance committee to advise the compliance leader, approve compliance initiatives, and assist with the implementation and ongoing operation of the compliance programme
- Establishing initial and baseline protocols for reporting relevant compliance management information to senior management and the board.

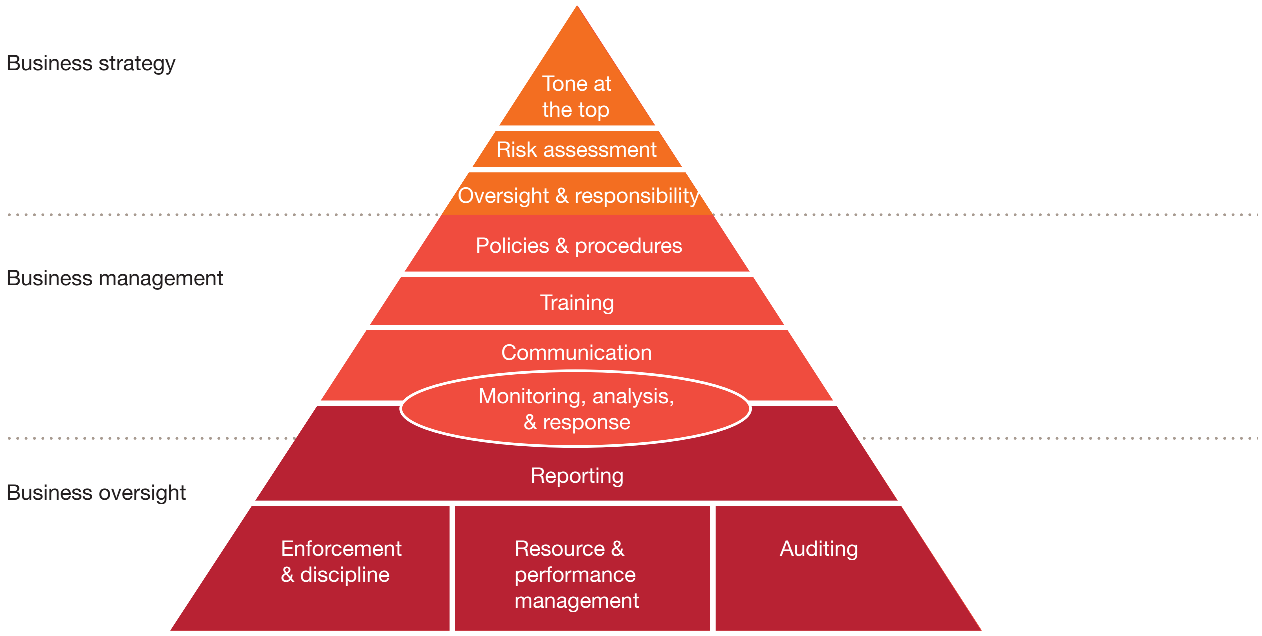
In 6th State of Compliance Study conducted by PwC, we found

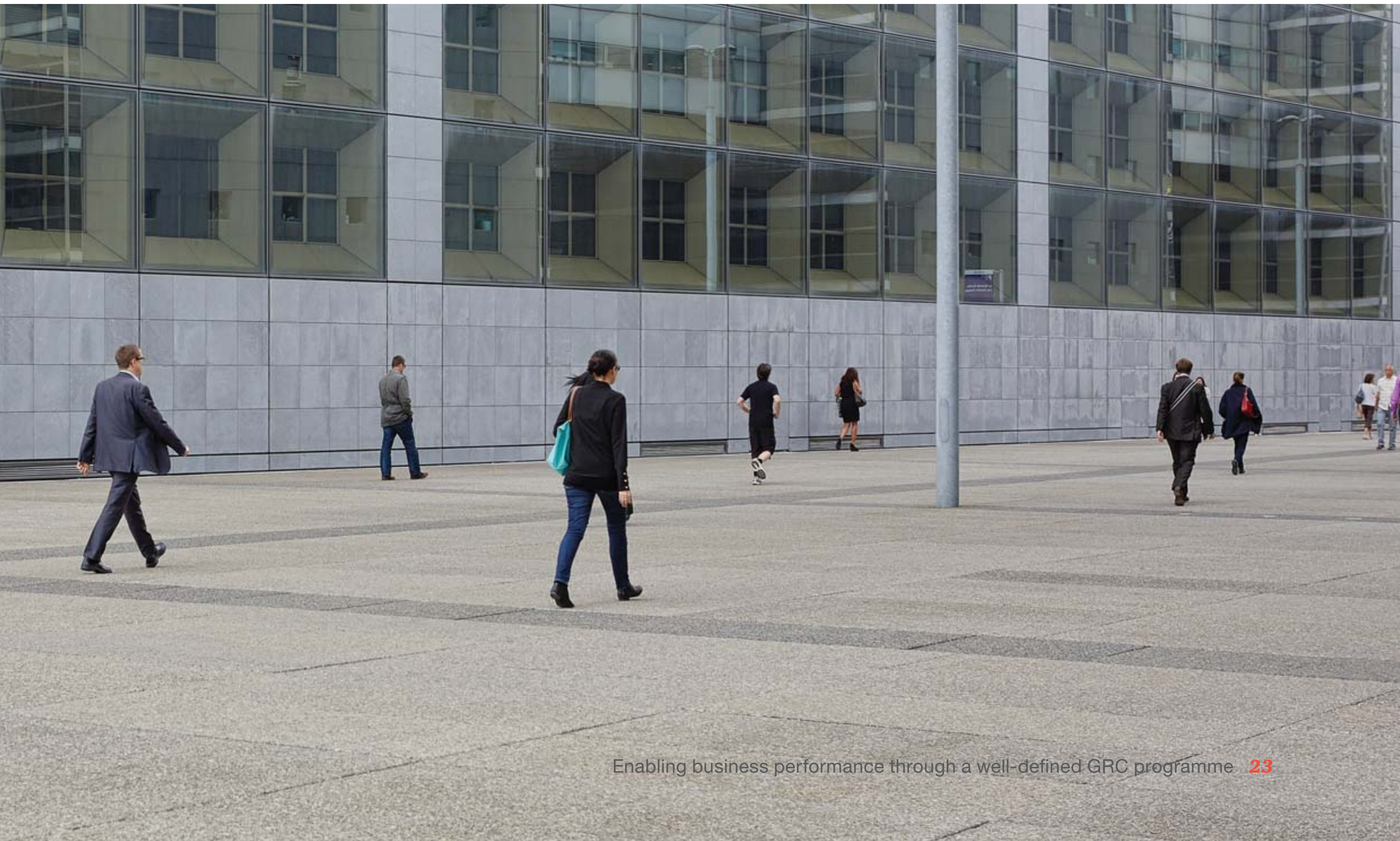
> ***(98%) indicated that senior leadership is, at the very least, committed to compliance and ethics. But a majority of respondents (55%) indicated senior leadership either provides only ad hoc oversight of the compliance and ethics program or delegates most oversight activities.***

2. Create an effective compliance framework

Once the company considers ethics and compliance an integral part of its business, the company should define the framework it will use for compliance management. An organization-wide framework fosters consistency, leads to ease of reporting, and results in improved program documentation irrespective of who in the organization owns a particular compliance risk.

PwC has built an Compliance Effectiveness Framework which recognises the following elements:





3. Assess corporate compliance obligations, identify compliance owners, and focus on critical risks

By way of a compliance risk assessment, companies identify the universe of compliance requirements and ethical risks they are exposed to, they determine which organisational functions are currently accountable for management of those risks, they prioritize efforts based on perceived risks to the business, and they gauge resource allocations based on assigned risk ratings.

As per our PwC's 6th State of Compliance Study,

> *While the audit committee oversees most compliance and ethics programs (65%), it is somewhat surprising that 20% of respondents indicated that their Boards of Directors have formed a separate, stand-alone compliance/ ethics committee to provide oversight of the compliance and ethics program.*

The new function may initially conduct a limited compliance risk assessment to (1) identify overlaps, duplications, and gaps in current compliance risk management and (2) pinpoint compliance risks within the company's culture and among the company's mission-critical areas, where failure could be catastrophic for the enterprise's reputation and long-term success. At a later stage, the compliance function might conduct a more-comprehensive compliance risk assessment for a deeper understanding and a more extensive analysis of how the organization manages compliance risks. Such a comprehensive assessment can serve as a step toward the creation of a sustainable enterprise-wide compliance risk management programme.

4. Create policies and procedures for major risks and requirements

The compliance function should work with both management and the business units to draft policies, procedures, and guidelines that facilitate compliance with applicable laws and regulations. Such policies should be clear and unambiguous. They should project the expectations of the company's top ranks. And they should reflect actual expected behaviour. Vital core policies and procedures to create and communicate during the compliance function's first year include a corporate code of conduct, anti-bribery and anticorruption policies, prevention of sexual harassment policy, insider trading policy, related party policy, whistle-blower policy, risk management policies, etc. Later, the function can expand its policy focus to second-tier issues and to handling new regulatory developments and the compliance risks that come with new business products, services, and trends.

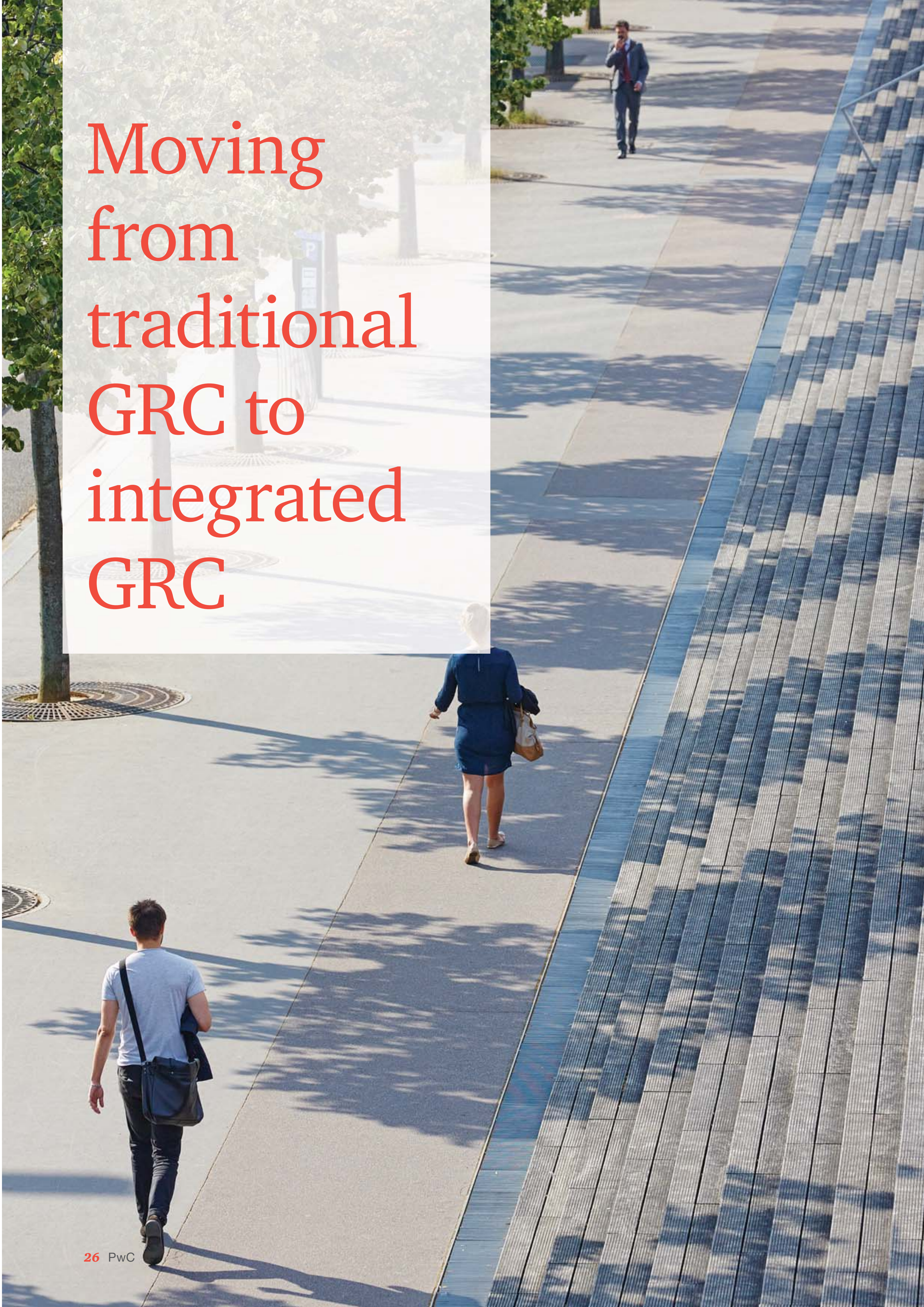
5. Launch initial compliance communications and training

The Compliance function spreads the compliance message and conducts training to disseminate knowledge covering regulatory requirements, ethical expectations, and corporate compliance policies and procedures across the business. The biggest challenge involves building awareness that the compliance program exists and is there to help employees do their jobs in ethical and lawful ways. Training should focus on core areas as set forth in the code of conduct. Over time, the programme should align to the company's risks and encompass both (1) broad training that mainstreams new compliance policies across the business or that educates new hires on company policies and (2) targeted training relevant to specific roles. Social media channels—especially internal channels—are ideal for communicating compliance topics to employees.

6. Establish an oversight and monitoring mechanism

In order to monitor the success of the compliance function, companies should establish an oversight and monitoring mechanism at the senior management level. This will enable them to monitor the effectiveness of controls, thereby determining how well compliance functions are operating.

Moving from traditional GRC to integrated GRC



Governance + risk + compliance = Integrated GRC

In the previous sections, we have explained the three components of the GRC (i.e. governance, risk and compliance) focusing on the key imperatives for each of those. We have observed that due to the multitude of regulatory and compliance requirements, the approach of GRC practitioners has largely been restricted to a reactionary approach—merely trying to stay abreast with the plethora of regulatory and compliance demands. Hence, it is not surprising that governance, risk and compliance have restricted themselves to their own cocoons by adopting a silo-based approach. We believe that companies would fail to realise value if these programmes are run in a disintegrated manner. Organisations need to develop a culture wherein holistic approach to GRC can lead to increased synergy, less redundancy and more value. Such an approach, geared towards generating maximum value and reducing cost of compliance, is termed as integrated GRC.

Integrated GRC corrects the deficiencies of traditional GRC at every level. It allows for independence of individual components of GRC while ensuring synergy and minimising redundancy.

Benefits of integrated GRC over traditional GRC

Significant benefits can be achieved by aligning and integrating GRC suite of activities within an organisation. It leads to improvement in quality and availability of information, reduces breaches, increases efficiencies and most importantly, and generates value for management by providing holistic oversight with increased assurance over GRC activities. Further, it leads to clearly defined roles and responsibilities, fixed accountabilities and transparency through effective reporting and monitoring.

The key benefits are summarised below:

Traditional GRC		Integrated GRC
Lack of synergy - lack of common underlying language	→	Enables synergy - common underlying language
Duplication in efforts - increased redundancy	→	Removes redundancy - common platform improves efficiency
Inadequate management oversight	→	Common platform - enables holistic oversight
Gaps/redundancies in coverage due to lack of visibility	→	Ensures holistic coverage on account of holistic visibility
Resource under/over-utilisation	→	Optional utilisation of resources

Further, an integrated GRC enables consistency in data treatment, evaluation methodologies and taxonomy. Ultimately, to summarise it all, integrated GRC facilitates optimum allocation of resources and assets, thereby resulting in increased business performance.

How to achieve desired integration?

While the challenge of integration can be attributed to multiple factors such as organisational structure, regulatory complexities and leadership attitude, the underlying root cause in all major cases is, more often than not, cultural boundaries within the organisation. As per the OCEG Survey, the following are some of the key challenges in creating an integrated GRC approach:

- Inability to narrow down on GRC champions
- Lack of organisation wide interdepartmental coordination
- Lack of strategy for integrated GRC
- Inability to measure ROI of integrated GRC and showcase relative value vis-à-vis the traditional approach
- Complex regulatory environment

The complexity of today's business environment demands that the disparate strands of GRC must be brought together into a coordinated, collaborative system whose people, processes, and technologies are integrated and synthesised for greater effectiveness and efficiency. Instead of being the dour face of 'no', GRC must become a positive, proactive force that pushes companies forward by providing a holistic view of risks, responsibilities, and opportunities.

Integrating governance, risk and compliance is a journey, a process of breaking down walls and opening up the lines of communication, coordination, and collaboration between the organisation's various risk and compliance groups and activities. It's about establishing clear ownership of risk and compliance in the business, driving efficiency and effectiveness, and providing the business with better data and improved reporting of leading risk indicators.

The journey to integrated GRC needs to start with a compelling story—a value proposition which can't be refuted. This value proposition can be in the form of a business case clearly outlining the benefits in terms of value generated and decreased cost of compliance. Setting up a management sub-committee in the form of a GRC committee can be a good starting point. This committee can share the charter of the vision and guide the overall change management process.

Once there is a buy-in from management and employees, a number of specific strategies can be adopted to align the organisation with the path of integration and optimisation.

- ### Build continuous communication

  Establish mechanisms to promote continuous communication between the company's various GRC activities. Having periodic updates is not enough to achieve this. It is imperative that organisations open up a communication portal, in theory, which enables dynamic sharing of information between facets of GRC.

- ### Share annual plans and testing schedules

  To promote coordination, reduce duplicative efforts, and foster broader understanding of review scope, timing, and direction, the various GRC activities should share their annual plans and testing schedules with one another and with internal audit.

- ### Perform joint risk assessments

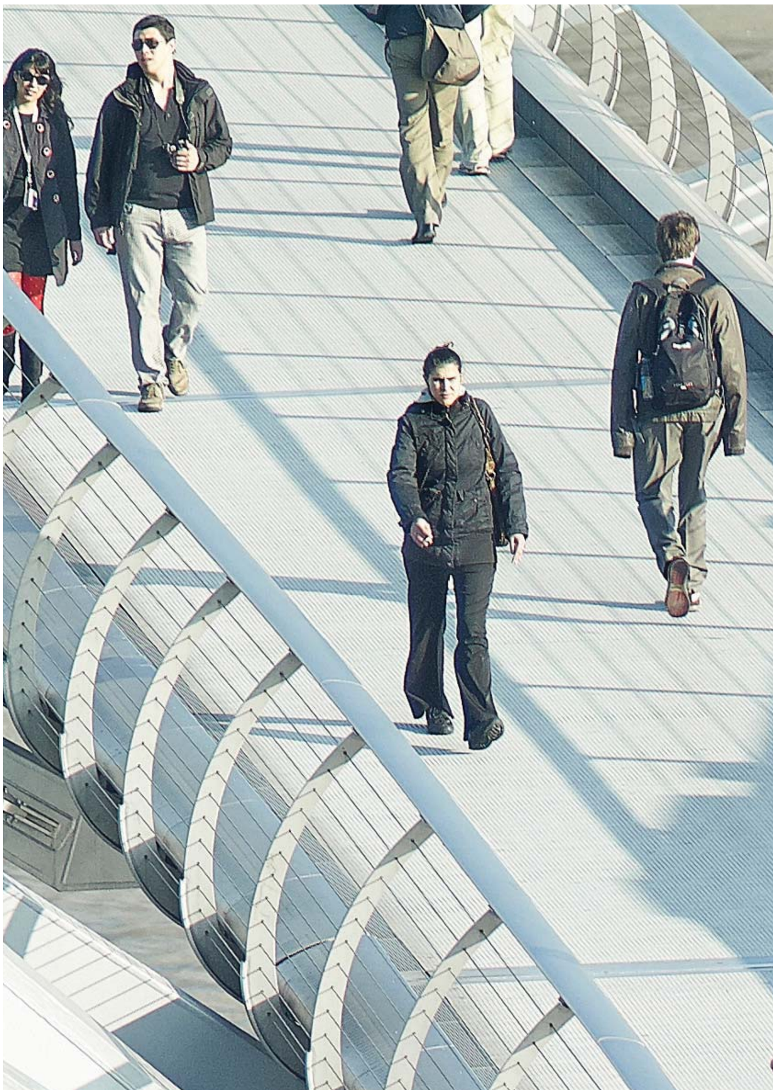
  Collaboration on risk assessments reduces the burden on resources within the individual GRC activities and across the enterprise while simultaneously amplifying the scope and usability of results.

- ### Share key issues and findings

  Sharing the key issues and findings of audits/reviews with risk functions that did not participate in those reviews allows those functions to leverage that intelligence and avoid duplicative efforts.

- ### Coordinate follow-up activities

  GRC activities quite often require follow-up on identified issues. When GRC is not coordinated, activities across different functions will often identify similar issues and conduct separate follow-up processes with the business—a clear instance of duplicative efforts that can be solved through coordination.



- **Share resources and training programmes**

  A company may be structured in such a way that its risk management group is significantly bigger than its compliance function. In such cases, a sensible integration approach is for the compliance function to leverage risk management resources as needed, and for the two groups to share strategies around training programmes.

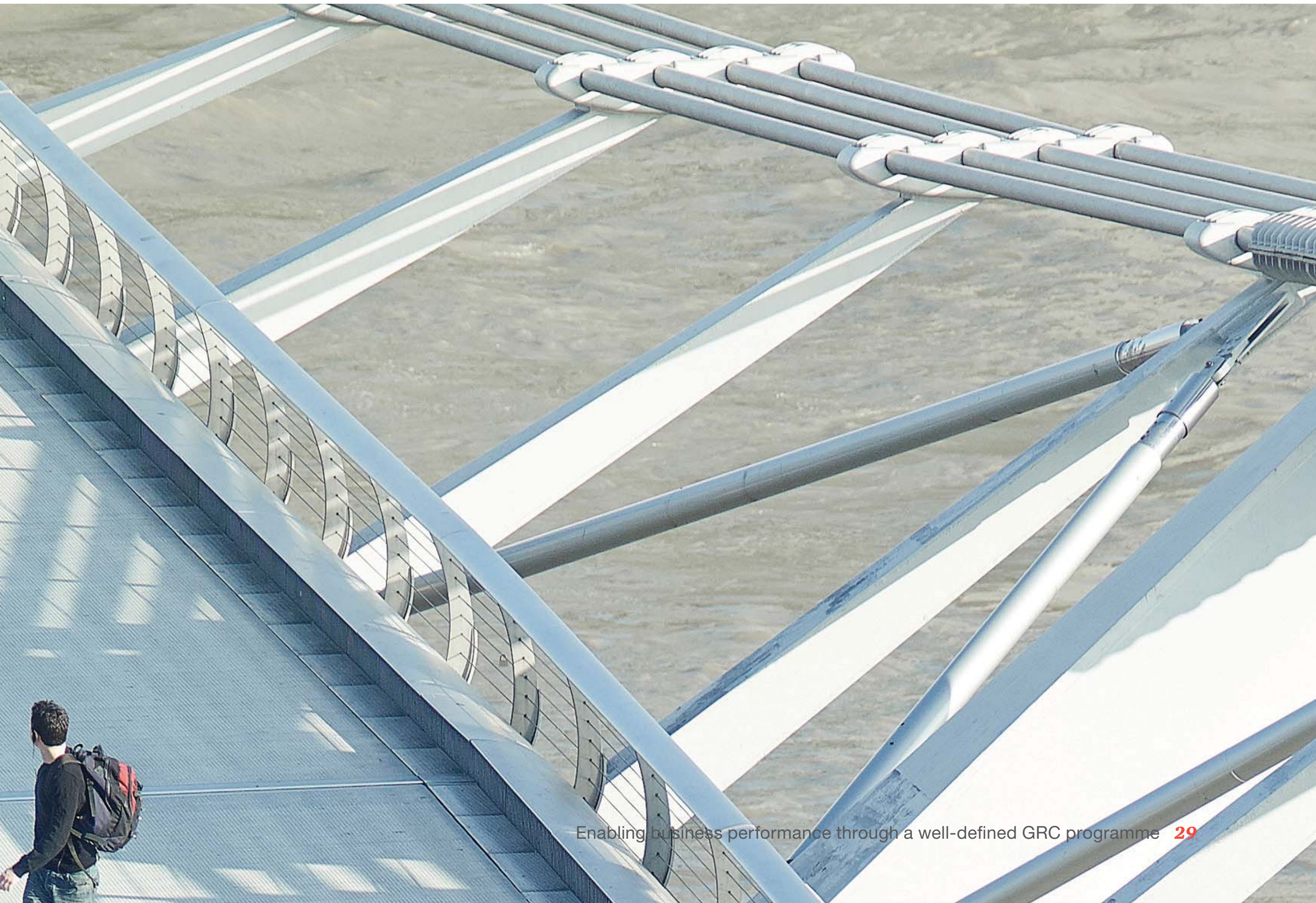
- **Plan joint risk assurance mapping**

  As an element of long-term planning, a company's risk functions can collaborate on risk assurance mapping to build a shared understanding of where key risks reside throughout the organisation, and which group or groups will monitor which risks. The more coordination you bring to bear on risk mapping, the more quickly you'll uncover gaps and redundancies and build a more effective and efficient overall risk management programme.

- **Leveraging technology for GRC integration**

  Integrating governance, risk and compliance is often time consuming. Technology has a significant role to play in addressing this challenge and embedding GRC in the DNA of the organisation. GRC technology helps businesses effectively and efficiently manage their risk and compliance activities by automating processes and accelerating the benefits of a well-defined GRC programme. As of now, there are a multitude of GRC solutions available which can be leveraged by organisations. In selecting the right technology partner, organisations should ensure that it enables risk and compliance management, vendor risk management, IT risk policy, etc., while ensuring visibility and transparency.

To achieve integration, responsibility for GRC must cut across the enterprise. The board and management must establish the appropriate culture for the effort, facilitating the processes and setting the approach and tone at the top regarding GRC's importance. Optimisation of GRC activities will never happen if management doesn't hold up its end and embrace the idea that GRC is an interconnected process across risk management's lines of defence, from top to bottom. At the same time, a company won't achieve GRC optimisation until the processes become embedded in the culture, the mission and day-to-day functioning of the enterprise. GRC may be the functional responsibility of the chief risk officer or the chief compliance officer, but it becomes operationalised only when it is inextricably embedded within the business.



About ASSOCHAM

THE KNOWLEDGE ARCHITECT OF CORPORATE INDIA

The Associated Chambers of Commerce and Industry of India (ASSOCHAM), India's premier apex chamber covers a membership of over 4 lakh companies and professionals across the country. ASSOCHAM is one of the oldest Chambers of Commerce which started in 1920. ASSOCHAM is known as the "knowledge chamber" for its ability to gather and disseminate knowledge. Its vision is to empower industry with knowledge so that they become strong and powerful global competitors with world class management, technology and quality standards.

ASSOCHAM is also a "pillar of democracy" as it reflects diverse views and sometimes opposing ideas in industry group. This important facet puts us ahead of countries like China and will strengthen our foundations of a democratic debate and better solution for the future. ASSOCHAM is also the "voice of industry" – it reflects the "pain" of industry as well as its "success" to the government. The chamber is a "change agent" that helps to create the environment for positive and constructive policy changes and solutions by the government for the progress of India.

As an apex industry body, ASSOCHAM represents the interests of industry and trade, interfaces with Government on policy issues and interacts with counterpart international organizations to promote bilateral economic issues. ASSOCHAM is represented on all national and local bodies and is, thus, able to pro-actively convey industry viewpoints, as also communicate and debate issues relating to public-private partnerships for economic development.

The road is long. It has many hills and valleys – yet the vision before us of a new resurgent India is strong and powerful. The light of knowledge and banishment of ignorance and poverty beckons us calling each member of the chamber to serve the nation and make a difference.

DEPARTMENT OF CORPORATE AFFAIRS, ASSOCHAM

Santosh Parashar
Additional Director & Head
Email - santosh.parashar@assocham.com

Jatin Kochar
Executive
Email - jatin.kochar@assocham.com

Abhishek Saxena
Assistant Director
Email - abhishek.saxena@assocham.com

Aditya Muvvala
Executive
Email - aditya.muvvala@assocham.com

The Associated Chambers of Commerce and Industry of India

ASSOCHAM Corporate Office:
5, Sardar Patel Marg, Chanakyapuri, New Delhi-110 021
Tel: 011-46550555 (Hunting Line) • Fax: 011-23017008, 23017009
Email: assocham@nic.in • Website: www.assocham.org

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 2,36,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity. Please see www.pwc.com/structure for further details.

Contacts

Neeraj Gupta
Partner, Risk Assurance Services
p.neeraj.gupta@in.pwc.com

Harpreet Singh
Partner, Risk Assurance Services
harpreet.singh@in.pwc.com

Ankur Jain
Partner, Risk Assurance Services
ankur.a.jain@in.pwc.com

Sandeep Agrawal
Director, Risk Assurance Services
sandeep.agrawal@in.pwc.com

Lokesh Gulati
Associate Director, Risk Assurance Services
lokesh.gulati@in.pwc.com

About the authors

This knowledge paper has been co-authored by Sandeep Agrawal, Gaurav Sachdev, Lokesh Gulati, Ruchi Hans, Rananjay Kumar, Manvi Rustagi.

pwc.in

Data Classification: DC0

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

SUB/December2017-11449