Risk Survey 2018
Transforming Risks into Opportunities
For private circulation only
Contents

Foreword 5
Introduction 7
Building Future-Ready Risk Management Functions 10
Key Risk Function Priorities: Identify, Mitigate, Raise awareness 16
An Organisation's Perspective: Identifying key risks 20
Future of Risk: Integrated risk management strategy 28
Conclusions: The road to accelerated performance 36
About the Survey 37
The risk landscape is evolving. Every day’s headlines bring new reminders that the future is on its way, and new risks and response strategies are around every corner. Risk leaders are faced with new challenges and opportunities at a pace very different from that of the past. How is India Inc. equipping itself to manage the emerging and dynamic risk landscape?

Deloitte India’s Risk Advisory practice is pleased to present the Risk Survey 2018. The survey report aims at providing insights on the approach to risks in Indian organisations, based on the responses from over 100 Indian companies/organisations. We would like to take this opportunity to express our sincere gratitude to all the participants for their inputs.

The results were intriguing. Leading risk management practices are gaining wider adoption. Boards of Directors are actively investing time and resources in the oversight of risk management. The Chief Risk Officer (CRO) position has gained wider acceptance in organisations and risk is increasingly seen as a value enabling function.

The progress has been undeniable, but in the years ahead, organisations are likely to face different challenges pertaining to risk management. We are in the midst of the Fourth Industrial Revolution—and this one goes far beyond automation. Smart and connected technologies are transforming the manner in which parts and products are designed, made, used, and maintained. By ushering in a digital reality, organisations are using cognitive computing. Identifying the emerging risks proactively is the #1 priority for risk teams. However, risk professionals have before them a challenge to not only keep pace, but also think one step ahead in an attempt to foresee emerging risks and collaborate with business to build mitigation strategies.

The question that Boards of Directors have to ask is whether their organisation has given due importance and devoted sufficiently skilled resources to this key function. The evolving nature of risks in the ecosystem will require organisations to re-evaluate their skillsets and resources to be better prepared to address these risks.

Through this report, we intend to spark a conversation around how risk management functions and practices need to evolve and take a value-focused approach to risk management. This would help them embrace complexity to accelerate performance. We believe that the organisations that shift their mind-set from risk averse to risk aware will be able to lead in their industry, navigate risks and opportunities more effectively, and disrupt the traditional and obsolete systems and processes through innovation.
Introduction

Risk has different implications for different organisations. The findings of our survey reflect the unanimity in identifying cyber security, technology disruptions and regulatory risks as the top three risks – both in present times and in a time span of three years from now. There is also a consensus on the aspect of cyber security and technology disruptions outweighing regulatory risks, three years from now. While there are no surprises here, we believe that the volatility and complexity of each of these risks will continue to increase.

When leaders of organisations were asked how well the cyber security and technology-related risks are currently managed, 64% responded that it is either ‘inadequate’ or ‘needs to improve’. There are four key factors that impact the organisation’s ability to deal with these emerging risks:

- Involvement of the Board of Directors and senior management;
- Availability of skilled risk management professionals;
- Ability of the business teams to interpret data for actionable insights; and
- Adequate budget and resources.

The survey indicated that nearly two-thirds of the organisations have a medium to low preparedness on each of the above factors. This clearly indicates that organisations have some distance to travel in their journey towards creating an effective risk management function.

Creating the right structure and identifying the right expectations and responsibilities are important considerations for an effective risk management function. However, only 61% of the organisations had a full-time Chief Risk Officer (CRO) role as a part of the senior management or reporting to the senior management with adequately staffed risk teams; and only 47% of the organisations with revenues in excess of INR 2,000 crores had 12 or more individuals as part of their risk function.

Organisations were also divided on how they viewed risk management – few of them harness risks to find future opportunities and drive returns (a value focussed approach), and the others use risk management with an aim to drive compliance and prevent losses.

Given the findings of the survey responses, we believe that the benefits of a value-focused approach to risk management are far more significant. The first benefit is a heightened corporate performance; organisations are more likely to achieve better financial and operational performance than their competitors. The second benefit is the competitive advantage; business leaders are better able to manage costs and improve customer relationships, giving them a competitive edge over the other players in the market. Lastly, organisations can gain from an enhanced brand and reputation; they experience improved risk protection and reputational resiliency.
According to us, there are some clear themes emerging from the survey findings:

**Elevate the conversation**
Organisations should consider the need to have a full-time CRO as part of the senior management. The Board of Directors too need to enhance their participation in the risk agenda and perhaps create a Board level Risk Committee. The CRO should have a direct line of reporting to this Committee, in addition to the Chief Executive Officer. Risk considerations must be embedded into strategy and continuously monitored.

**Right-skill the function:**
There is a clear need to attract professionals with diverse skills, as also retrain and upskill the existing risk professionals. Organisations also need to consider the role of external experts – academia, professionals, and experts, as well as internal business teams, to augment risk related capabilities.

**Use technology to enable the risk function:**
Risk teams need to adopt and invest in technology and analytical tools. This will aid them to scan vast amounts of data being generated, both internally and externally, and convert that into meaningful and actionable insights.

**Create a risk-aware culture:**
Timing is everything. There are several important shifts expected in the next few years, making it imperative for business leaders to react quickly to these shifts. The scope and responsibility of managing risks need to expand beyond the domain of a select few. For organisations, building a risk-aware culture and identifying opportunities for value creation and loss avoidance are becoming increasingly important, along with compliance management.
Elevate the conversation

Right-skill the function

Use technology to enable the risk function

Create a risk-aware culture
Building Future-Ready Risk Management Functions

We believe that while the role and perception of the risk management function has considerably evolved in recent times, there is a need to further enhance the role, scope and skill-sets of this increasingly critical function. Increasing pressure from regulators, vendors and customers, along with threats from industry disruptors and competitors, has made the identification of risks and rigor around implementation of appropriate mitigation measures of paramount importance.

Current Risk Management Structure

- In-house team: 64%
- Fully outsourced external service provider: 34%
- Co-sourced with external service provider: 2%
of the organisations surveyed had an in-house team manning the risk management function.

of organisations have a full-time Chief Risk Officer (CRO), either as a part of their Leadership team (40%) or directly reporting to the Leadership team (21%). Thus, we see the notable adoption of the CRO position in organisations as an evolving trend in Indian organisations, as they realise the benefits of having a full-time CRO position (Refer to the next page for our view on the Ideal Role of a CRO).

of the companies with a turnover in excess of INR 2,000 crores have 12 or more personnel (including in-house and outsourced).

of the respondents indicated that they harnessed risk to find future opportunities for the organisation and drive returns.

have less than 5 personnel as part of their risk teams.

indicated that risk management is the responsibility of each business/function and there is no separate CRO role. Among the roles of the CRO, challenging business assumptions and strategy execution, and monitoring risk mitigation measures implemented by business are essential ones. In our view, both these roles need to be independent of each other.

indicated that their purpose of risk management was to remain compliant with regulations and prevent losses. Not surprisingly, organisations with full-time CRO roles harnessed risk to find future opportunities for the organisation and drive returns. This view is consistent with Deloitte’s experience that the most experienced CROs see risk management as a performance accelerator.

of the organisations used a co-sourced model. Given the multifarious nature of risks and the pace at which they are evolving, we believe that organisations should further explore co-sourcing models with academia, think-tanks, professional firms and experts to permit organisations to benefit from their experience.
In our view, organisations must critically evaluate the need to have a full-time CRO as part of their senior leadership team. The risk management function must be adequately staffed, and perhaps co-sourced considering the multifarious skills required for an effective risk management function. The reality is that opportunity doesn’t exist without risk. But when risk is taken strategically—with a value-focused approach—new opportunities to accelerate performance emerge. These opportunities have the ability to enhance reputation, market positioning, and competitive advantage. Risk management teams must focus not only on compliance, but also on how they can help accelerate performance.
Role of a CRO

01. Determine the company’s risk appetite and quantify the amount of risk the company should take on.

02. Integrate risk management priorities into the company’s overall strategic planning.

03. Assist in the development of strategic action plans to mitigate the impacts of the primary threats.

04. Monitor the progress of risk mitigation efforts.

05. Oversee funding and budgeting of risk management and mitigation projects.

06. Communicate with the company stakeholders and board members about the risk profile and assessments.
To ensure the right risk posture, organisations must have an independent external check and balance for their processes. They need to have a centralised system that functions like a lighthouse in the organisational setting.
Key Risk Function Priorities
Identify, Mitigate, Raise awareness

Risk functions are expected to focus on a plethora of tasks to maximise the value derived from various areas that risk covers. The function attempts to deliver solutions by being proactive rather than reactive. Besides trying to deliver value by performing the traditional tasks such as continuous monitoring and raising of red flags, it must transcend to support business objectives and strategy. The survey result indicate the following top priorities for the risk management function:

Priority 1: Identifying existing and new risks proactively

Deloitte research suggests that evolved organisations have begun using Risk Sensing tools and techniques (For more information, refer to the next page) to aide this activity. Risk also occupies a prominent slot in Board meetings with more proactive Boards interacting with think tanks, academia and industry experts to gain a better insight into this complex and evolving topic.

Priority 2: Risk Mitigation

Given the volatile, uncertain, complex and ambiguous (VUCA) environment, mitigation strategies are taking on varied meanings. Cognitive technologies are augmenting human decision making, controls are becoming all pervasive, vigilance and resilience compliment prevention practices, behavioural sciences inform risk insights and risk transfer is broadening in scope and application (For more information, refer to the next page)

Priority 3: Raising risk awareness

Approach to managing and responding to risk has changed due to market volatility. It no longer remains the domain of a certain set of individuals. In our view, risk management teams must use a combination of the following strategies to raise risk awareness throughout the organisation:

• Elevate profile of risk management
• Integrate risk into strategic planning
• Decentralise risk management processes
• Provide risk training across the organisation
What is Risk Sensing?
Risk sensing combines human insights and advanced analytics capabilities to identify, analyse, and monitor emerging risks. It has become a key component of many organisations’ arsenal to manage risks in their business model, long-term viability, and ability to create value. Risk sensing is carried out by identifying and monitoring strategic risk indicators of events, trends, and anomalies in structured and unstructured data from internal and external sources. These indicators are then compared and mapped to the organisation’s risk tolerance levels and thresholds. Risk Sensing is a combination of technological capability and human insight that gives risk sensing its detection and analytical powers, when aligned appropriately. Hence, it is imperative that the Risk Sensing program includes business analytical specialists, sector analysts, and data scientists.

Here are four steps to consider when framing and implementing a risk sensing program:

1. Identify the strategic risks to be monitored, and the scope of the effort
2. Define the elements required to enable strategic risk monitoring
3. Configure the platform to enable scanning, analysing, and tracking of strategic risks
4. Continue monitoring the data sources and generating ongoing insights

Trends in Risk Mitigation

Cognitive technologies augment human decision-making
Driven by developments in artificial intelligence (AI) and easy access to huge amounts of data, smart systems will assist, and at times even replace, human-led risk management.

Controls become pervasive
In a sensor-enabled, hyper-connected environment, organisations will deploy pervasive controls as part of their products, services, and business models to monitor and manage risk in real time.

Behavioural science informs risk insights
Advances in behavioural sciences will fuel efforts to understand risk perceptions, influence risk behaviours, and improve risk-related decision-making.

Vigilance and resilience complement prevention as leading practices
Organisations are realising that 100-percent risk prevention is not feasible, so investment in vigilance (detecting risk events as they happen) and resilience (containing and reducing the impact of risk events) will increase.

Risk transfer broadens in scope and application
Risk transfer instruments, such as insurance, contracts, and novel financial instruments, will increasingly be used by organisations to protect them from a wider range of risks – cyberattacks, climate change, geopolitical risks, terrorism, business disruptions, and more.
The emerging trend is that companies are realising how vulnerable their reputation can become. It is a classic case of infinite causes, finite impact.

The classical theories have relied on root cause analysis and prevention, which still holds true but organisations are now required to be more proactive about safeguarding reputation. This asset is intangible and hence, you can’t build inventory for a rainy day. Also this reflects more in public perception than on the balance sheet. All in all this requires a different approach than a traditional one.
An Organisation's Perspective

Identifying key risks

We asked our survey respondents to rank risks impacting their organisations today and three years from now. There was an overwhelming concurrence on Cyber Security, Technology Disruption, and Regulatory Risks being the top 3 risks impacting organisations both in the present day scenario and in three years from now. However, the focus on Cyber Security and Technology Disruptions is expected to intensify over a three year period, whereas Regulatory Risks seems to follow a declining trend. This is in consistency with the global trends.

In our view, the intensity with which these risks are evolving has increased and is expected to challenge organisations to not only keep pace, but perhaps, move one step ahead. In the following pages, we will provide our viewpoints on how risk management functions could think about approaching these top emerging risks.

Emerging Trends in Risk Management

01. Cyber Security

02. Technology Disruptions

03. Regulatory Risk
Top three current risks

- **44%** Regulatory Risks
- **31%** Cyber Security
- **25%** Technology Disruptions

Top three risks three years from now

- **36%** Cyber Security
- **33%** Technology Disruptions
- **31%** Regulatory Risks
01. Taking a holistic view on cyber risk
A fundamental shift is occurring in the management of cyber risk. The idea that cyberattacks are increasingly likely—and perhaps inevitable—is beginning to take hold among executives and boards. Business leaders are realising that we are a part of an interconnected world dependent on technologies that are designed to share information, not to protect it. They recognise that they have to trust people— their own employees and the third parties they do business with—to handle sensitive information and operate in critical infrastructure.

There are many ways a cyber-incident can affect an organisation, and the impacts vary, depending on the nature and severity of the incident. In general, there are 14 “impact factors” that business leaders should consider when preparing for cyber incidents (see illustration). Some are well-known, direct costs commonly associated with cyber breaches; others are more far-reaching, intangible costs that are both more difficult to quantify and often hidden from public view.

For many organisations, becoming truly resilient to cyberattacks calls for a shift in mind-set that changes how they perceive cyber risk and its potential impacts. It requires organisational transformation that broadens the scope of involvement at the top of the organisation and instils focus on business risk beyond technology controls. It involves the ability to re-prioritise and refocus investments on mitigating likely outcomes, based on a broad understanding of attackers’ motives and the ability to anticipate high-impact scenarios. Many will find the following to be useful steps.

14 Cyberattack impact factors

Above the surface
Better-known cyber incident costs
- Attorney fees and litigation
- Customer breach notification
- Regulatory compliance
- Loss of intellectual property
- Post-breaching customer protection
- Cybersecurity improvements
- Public relations

Below the surface
Devaluation of trade name
- Increased cost to raise debt
- Impact of operational disruption or destruction
- Lost value of customer relationships
- Value of lost contract revenue
- Insurance premium increases

Source: Deloitte Report- Beneath the surface of a cyberattack
Convene the right team.
Evaluate organisational readiness by bringing together the right business and technical leaders to develop a list of high risk cyberattack scenarios.

Identify top risk areas and assets.
In some enterprises, particular data sets, computer systems, control devices, or other digital assets represent high value unto themselves. In others, the value of information and technology assets is tied to the criticality of the business processes and the relationships they enable.

Right-size spend to reduce incident impact.
Budgets will never be big enough if the aim is to try and prevent every possible incident. It is likely more important to invest in a more risk-focused manner.

Modernize the meaning of “readiness”.
With awareness of what matters most to the organisation, plans can be made to involve the various parties needed to protect, defend, and recover if those things are compromised. Incident response plans can be appropriately broadened—and rehearsed—to anticipate and prepare for the high-risk cyberattack scenarios identified.

Do more than prepare. Cyber readiness is not just about what happens after an attack.
Right now, malware is sitting undetected on networked systems within an organisation or on the devices of partners, vendors, or employees. There may be ill-intended users within the walls of the company who could use authorised access to inflict damage. In some areas, tighter security practices may be warranted. Other areas may be technically impossible or impractical to secure further, but might warrant stronger capabilities to detect potentially malicious activity. Every organisation should institute some variation of a secure, vigilant, and resilient approach that is aligned to its cyber risk posture and program.
02. Managing technology/digital risk

Nowadays, organisations are moving towards Digital Transformation within their businesses with an aim to create new opportunities and capabilities for future growth. Enterprises should now focus on integrating risks right from the design phase in which they undertake digital transformation. Advent of digital enablers in the business poses new set of risks which are beyond traditional cyber security, thereby leading to the need of a risk framework for your digital journey. This risk framework should cover aspects not just around technology, but also operations, third-party ecosystem, data privacy, and regulatory amongst others.

Industry 4.0 signifies the promise of a new Industrial Revolution—one that marries advanced production and operations techniques with smart digital technologies to create a digital enterprise that would not only be interconnected and autonomous but could communicate, analyse, and use data to drive further intelligent action back in the physical world. It represents the ways in which smart, connected technology would become embedded within organisations, people, and assets, and is marked by the emergence of capabilities such as robotics, analytics, artificial intelligence and cognitive technologies, nanotechnology, quantum computing, wearables, the Internet of Things, additive manufacturing, and advanced materials.

While Industry 4.0 plans to enhance digital capabilities throughout the value chain and drive revolutionary changes to connected devices, it also brings with it new risks for which the industry is unprepared. Developing a fully integrated strategic approach to risk is fundamental to manufacturing value chains as they marry operational technology (OT) and information technology (IT)—the very force driving Industry 4.0.

Every organisation has to rapidly learn and adapt to the new ABCDs – Artificial Intelligence and Analytics, Blockchain and Big data, Cloud and Cyber, Digital platforms and more. Business ecosystems, the permeation of AI, advances in quantum computing, and the rapid evolution of cloud and fog computing is going to fundamentally change businesses and business models. Companies that proactively embrace these opportunities in risk-intelligent, agile ways will differentiate themselves and win in the marketplace.
Across Deloitte, we talk to clients about three aspects of digital risk:

**Strategy**
- How are you transforming your business models?
- Are you considering disruptive M&A and/or ecosystems for growth in new business models?
- How are you engaging your board to build confidence that the new business models and digital risks are being comprehended and addressed properly by management?

**Governance**
- How are accountability and decision-making evolving in context of increased reliance on technology and robotics?
- What are the brand risks and how is the importance of public perception, integrity and trust factored into proactively addressing them?
- How are third-party risks being handled in the world of connected, but decentralized, ecosystems?
- Are you comprehending and mitigating algorithmic risks?

**Execution**
- Are you positioned to execute with agility, failing fast if needed?
- Are you prudently balancing risks and opportunities?
- How are you managing changes with your teams across the organisation both in terms of developing digital fluency and coexisting with robots?
- What are you doing to attract, develop and retain your workforce of the future?
- What culture changes are necessary for your organisation to be successful?
03. How Regulatory risk can preserve value and power performance?

Over the last few years, there has been a significant change in the regulatory scenario in India in terms of new regulations, and an increased enforcement of regulations by the regulators.

Emerging regulations – cross border impact:
Risks are not limited to a specific geography or developed economies. For example, the recent increase in data privacy and hacking cases have not only impacted the developed economies, but also affected India. There is an increasing focus on cyber security and data privacy, resulting in the need for new regulations in India and globally. The enhanced nature of regulations addresses both risk mitigation in the interest of customers, investors or citizens, and the alignment of the country’s landscape to the global regulatory standards. In the next few years, we will see the introduction of new regulations and amendment of existing regulations, making them more effective and enforceable.

Social Media – Strong tool for creating awareness:
Various means of communication, including social media are used to create awareness on regulations, cases of non-compliance, and their implications. Consumers, customers and investors are using social media as a platform to report issues, raise concerns or even highlight matters (relating to products, environment, health and safety) which can lead to serious implications for organisations, if they do not take compliance matters seriously. For example, if companies do not adhere to environmental norms or product safety norms, customers and stakeholders are very agile to voice their concerns on social media. If not addressed in a timely manner, this can affect the company or brand severely.
Building capabilities – Strong structure:
Companies are realising the importance of regulatory risks affecting their businesses. They are ensuring that they understand the regulatory landscape in all the regions/countries where they operate and implement structures and frameworks to comply with the various regulations. Compliance structures/teams have been set-up within companies to manage these risks effectively. Most companies are seeking guidance and assistance from external specialists to understand the nature of regulations and seek support in implementing frameworks and mitigations measures.

Compliance with regulatory requirements will lead to increased compliance costs, however companies need to treat this as investments since compliance with these regulations will give them the license to operate, protect their brand and reputation and ensure business continuity. Companies also need to ensure that they implement effective monitoring processes to ensure compliance activities are done on a timely basis and non-compliances are tracked and reported to the appropriate forums.

Regulatory Changes – A business opportunity:
Regulatory changes may be a cost to companies but they also create business opportunities for many other organisations. For example, the regulatory changes and updates in the Financial Sector have created various opportunities for fintech companies to support the regulators by developing new technologies. Companies are implementing automated solutions for business processes to ensure compliances rather than relying on manual processes, which are prone to errors and frauds.

Risk Survey 2018 | Transforming Risks into Opportunities
Organisations are using risk management to achieve various objectives. Business sustainability has emerged as the top impacting factor, whereas business strategy, business growth and profitability were other key impact areas. In our view, this is representative of the integral role that risk management assumes. Given the VUCA world that organisations operate in, tightly integrating risk management into business strategy and operations becomes critical to sustainable growth.

A well-defined and well-understood risk management strategy is essential to ensure a structured and comprehensive approach towards identifying, assessing and managing risks. According to us, essential building blocks for an integrated risk management strategy include:

1. A well-laid out risk governance framework integrated with the organisation’s operating model.
2. Constant vigilance on early warning risk indicators to respond to emerging risks and changes in risk profiles, almost on a real time basis.
3. Holistic assessment of emerging issues and incidents to enable recalibration of the risk management strategy.
4. Well understood contingency plans and escalation protocols that can be deployed without any delay is key to minimize the risk response time.
5. The right tone at the top that builds the organisational ethos that operates within the defined risk appetite and threshold.
6. An open and transparent culture that promotes the right level of dialogue on risks between the board, executive management and the risk owners.

54% of the organisations consider Sustainability as a high impact area
45% of the organisations consider Business Growth as a high impact area
41% of the organisations consider Business Strategy as a high impact area
40% of the organisations consider Profitability as a high impact area
Having a well-defined organisation risk strategy is the first step. The findings suggest that:

- **61%** of the survey respondents mentioned that they had a **well-defined** organisation risk strategy.
- **12%** of the survey respondents **did not have a well-defined** organization risk strategy.
- **27%** of the survey respondents were **undecided**.

Once an organisation has a well-defined risk strategy it is imperative for the same to be kept live given the pace at which newer risks are emerging and existing ones are evolving. Our survey results tell us that CEOs and Boards perhaps need to increase the frequency of interactions with their CROs. 46% of the survey respondents mentioned that the CRO interacts with the CEO on a quarterly basis, whereas 6% responded that this interaction is conducted on an annual basis (which in our view is significantly low). The balance 48% mentioned that their CROs met with their CEO on an ad-hoc basis. While ad-hoc access is at times required, we would recommend that the CROs establish at minimum a quarterly rhythm of interacting with the CEO. When it comes to interacting with the Boards, CROs seem to have a more defined schedule – 59% of CROs meet with their Boards on a quarterly basis. We would recommend that CROs allocate a time slot at each of the Board meetings to talk through emerging risks, as well as actions taken to address existing risks.
The survey also attempted to understand the frequency with which the Board undertook certain activities in relation to their overall risk management strategy. 37% of the survey respondents mentioned that they reviewed their overall risk management policy and framework, and 43% mentioned that they review the effectiveness of the risk management strategy, on a quarterly basis. Due to the dynamic nature of risk today, the mentioned frequency of reviews does not seem to be adequate. We also note that more than three-fourth of the organisations surveyed, conduct executive sessions with their CRO. This is again reflective of the importance of the role and emphasises the need for a full-time CRO, independent from operating management.

### Strategy for risk management in organisations

<table>
<thead>
<tr>
<th>Activity</th>
<th>Annually</th>
<th>Quarterly</th>
<th>Monthly</th>
<th>Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review overall risk management policy and framework</td>
<td>7%</td>
<td>5%</td>
<td>37%</td>
<td>51%</td>
</tr>
<tr>
<td>Review risk management reports and mitigation adequacy</td>
<td>5%</td>
<td>7%</td>
<td>67%</td>
<td>21%</td>
</tr>
<tr>
<td>Review effectiveness of risk management strategy</td>
<td>9%</td>
<td>3%</td>
<td>43%</td>
<td>21%</td>
</tr>
<tr>
<td>Review and drive organisational risk culture</td>
<td>12%</td>
<td>9%</td>
<td>39%</td>
<td>40%</td>
</tr>
<tr>
<td>Conduct executive sessions with the Chief Risk Officer</td>
<td>23%</td>
<td>8%</td>
<td>34%</td>
<td>35%</td>
</tr>
</tbody>
</table>

Given the current environment of rapid changes in business models, technology disruptions and regulatory changes, in our view most organisations should consider adopting a quarterly timetable (if not more frequent) to review their risk strategy, implementation of mitigation measures and organisational risk culture. In our view, the absence of frequent reviews will result in lack of alignment between corporate strategy and risk management. In form, the needle seems to have moved on the risk management framework and strategy but in substance, there is still some way to go to align risk management with corporate strategy, knitting together risk tolerance to executive decision making and focusing on risks that matter, which will help organisations create long-term value and not just value preservation.
Considering the dynamic nature of risks and the velocity of their onset, an integrated risk management strategy will only be effective if the necessary investments are made in the tools, technologies, and skills. This needs to be done in collaboration with business units to identify and mitigate risk. We asked corporate India on the extent of adoption of these enablers in their risk management programs in the last 3 years, and the findings suggest that while there is high level of collaboration with the business units, the investment in tools and the right skills sets leaves a lot to be desired.

- 32% of the organisations had low automation within their risk management processes.
- 34% of the respondents had low adoption of analytics for analysing risk triggers.
- 34% of the organisations surveyed had not reskilled their risk management team or moved personnel from business units into the risk management unit to deal with the complex and rapidly changing business environment.
96% of organisations surveyed mentioned that currently their risk management approach enabled regulatory compliance. This is perhaps indicative of the mind-set with which organisations approached risk management. However, there is also clear acknowledgement that risk management needs to invest in enhancing risk information systems and technology infrastructure, as well as enhancing quality, availability and timeliness of risk data. While technology and data would enhance risk management capabilities, human intelligence would continue to remain at the centre. To that, organisations surveyed acknowledged the need to re-skill existing risk professionals, and also attract risk management professionals, who can work in collaboration with the business functions to achieve the end goal.

<table>
<thead>
<tr>
<th>Risk management activities that impact businesses</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increasing involvement of the Board of Directors in risk management</td>
<td>35%</td>
<td>45%</td>
<td>20%</td>
</tr>
<tr>
<td>Enhancing risk information systems and technology infrastructure</td>
<td>29%</td>
<td>51%</td>
<td>20%</td>
</tr>
<tr>
<td>Enhancing quality, availability and timeliness of risk data</td>
<td>35%</td>
<td>51%</td>
<td>13%</td>
</tr>
<tr>
<td>Collaboration between business units and the risk management function</td>
<td>45%</td>
<td>45%</td>
<td>10%</td>
</tr>
<tr>
<td>Reskilling existing risk professionals to meet demands of future technologies and risk of the future</td>
<td>21%</td>
<td>48%</td>
<td>32%</td>
</tr>
<tr>
<td>Attracting risk management professionals with future-ready skills</td>
<td>24%</td>
<td>46%</td>
<td>29%</td>
</tr>
<tr>
<td>Regulatory compliance</td>
<td>70%</td>
<td>26%</td>
<td>5%</td>
</tr>
<tr>
<td>Securing adequate budgets and resources for the risk management function</td>
<td>27%</td>
<td>57%</td>
<td>16%</td>
</tr>
</tbody>
</table>
In our view, the need of the hour is to embrace an open and transparent risk culture which enables real time engagement of key stakeholders. This engagement needs to be achieved through effective use of technology enablers which will lead to collaborative risk management and decision making. Risk organisations need to significantly leverage analytics, conduct scenario planning and predictive modelling to bring in an element of foresight in risks that really matter to enable sustained value creation. When organisations are becoming more and more innovative to address ever increasing disruptions, it is important that risk management functions also keep pace. A futuristic risk organisation can be created only through an overhaul of its traditional skills and technology matrix.
Effective risk management is as much about value creation as it is about value protection. Having an optimum risk framework and associated processes is important for developing the capability to recognise such opportunities. This, in turn, calls for a change in the risk management mind-set.
Conclusions
The road to accelerated performance

In order to channelise risk for accelerating performance, organisations can adopt several leading practices that are driven by strategy, culture, and measurement.

**Strategy:** Have clarity on the structure, roles and responsibilities of the risk management structure and staff the risk management function adequately. Break down the wall between risk management and strategic planning. Risk professionals and business leaders must share ideas on the threats and opportunities facing the organisation. Only by openly discussing business problems can the two sides understand the other’s point of view and act on this knowledge.

**Culture:** Create a culture, in which, risk management is everybody’s business. Get the board and leadership involved in risk conversations and educate professionals to understand their role in risk management. This change doesn’t occur simply by telling employees that risk is everybody’s business. Individuals must be trained to identify risks; to calibrate their response; and, ideally, to act on the knowledge that for every threat, there is a business opportunity.

**Measurement:** Employ technology and data analytics to measure risk and predict trends. Data analytics is a major enabler of a value-focused risk strategy. Business has reached a level of complexity that demands a more scientific approach to the information generated inside and outside the organisation. Technology is only as good as the people who use it. Data analytics requires skilled people to ask the right questions to uncover the most useful answers.

Ultimately, risk management is a story of human judgement, in which, executives understand that risk management is a means to achieve a lot more than safeguarding the business. For those who can use the uncertainties to their advantage, the future looks bright. Are you a CEO who is ready to take calculated risks? Consider transforming your focus—from a traditional enterprise risk management approach to one that’s more agile and strategic—to reposition risk and accelerate your organisation’s performance.
About the Survey

Deloitte India Risk Advisory surveyed more than 100 C-Suite stakeholders covering board level executives, CEOs, CFOs, CRO, Business Leaders, and Heads of Internal Audit. To get a reasonable understanding of the risk culture in the Indian organisation, we gathered responses from organisations belonging to a diverse set of industries that covered both private companies and public companies with turnover ranging from less than INR 500 crores (15%), INR 500 – 2000 crores (23%), INR 2000 – 7500 crores (22%), and more than INR 7500 crores (40%). Industries surveyed include Consumer Business & Industrial Products (35%), Life Sciences & Healthcare (8%), Financial Services (16%), Government and Public Services (7%), Energy & Resources (5%) and Technology, Media & Telecom (29%).
Contacts

Rohit Mahajan
rmahajan@deloitte.com

Sandeep Kumar
kumarsandeep@deloitte.com

Shree Parthasarathy
sparthasarathy@deloitte.com

Ramu N.
ramun@deloitte.com

Anthony Crasto
acrasto@deloitte.com

Maninder Bharadwaj
manbharadwaj@deloitte.com

A.K. Viswanathan
akviswanathan@deloitte.com

Primary Contributors

Burzin Dubash

Rati Acharya

Priyanjali Moulik

Santosh Kumar

Amit Kumar

Tushna Vevaina

Payal Agarwal

Shalaka Kaprekar

Dhruv Srivastava