Deloitte.

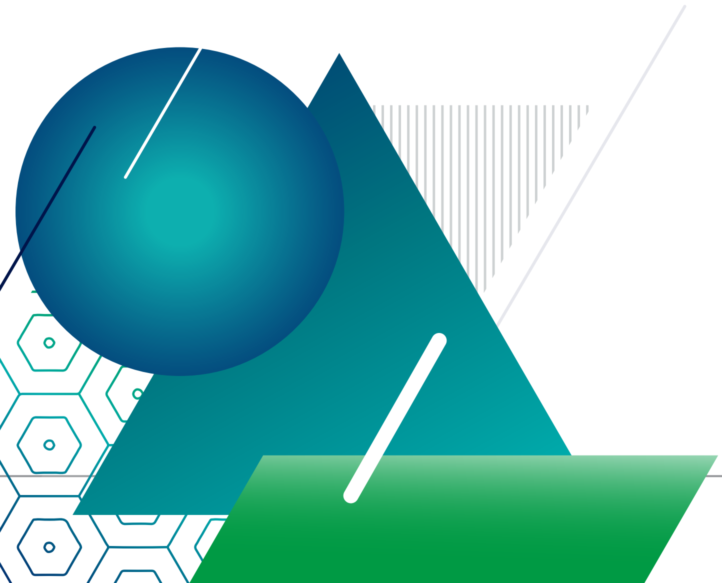
Through the Risk Lens

The future belongs to the prepared

2019

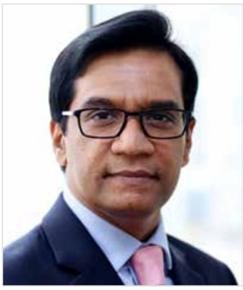
Risk Advisory

Contents



Foreword

Message from the Risk Advisory President



Rohit Mahajan
President – Risk Advisory,
Deloitte Touche Tohmatsu India LLP

Today's global environment is characterised by change, uncertainty, and disruptive innovation. Newer business models, digital transformation, and Industry 4.0 are leading to far reaching changes in the way work is executed. Extended enterprises are becoming a key strategic choice made by most enterprises and regulations are failing to keep pace, in most cases, with the dynamic business environment. Global research indicates:

- Artificial Intelligence (AI) will displace 40 percent of the world's current jobs, and similar disruptors will help create 1.75 million technology-enabled jobs. Fifty-five percent of the Indian workforce will require reskilling by 2022.
- The gap between technological advancements and the mechanism intended to regulate them remains wide. Regulatory policy cycle takes five to twenty years whereas a start-up can adopt disruptive technologies and business models, and turn into a unicorn in half the time.
- There is a trend of leveraging strategic alliances even for core activities, such as developing new products or entering new markets. In Asia Pacific, 71 percent of the alliances signed are furthering the core product development agenda.

These changes have expanded organisations' risk profiles and made them more complex and dynamic. Organisations, as well as their risk leaders, need to be more focussed in understanding these emerging risks and formulating a response strategy to create value and remain relevant in the changing environment.

This publication provides insights on the changes in work, regulation, extended enterprise, the current forces of disruption, the challenges it poses to the organisation, the risks that emanate from these changes, and the recommended response to address these changes.

To lead the change and secure their businesses, organisations will need to consider the following critical issues/risks:

- **Future of work –** Risks associated with digital technology adoption and managing the associated bio-convergence and reskilling imperative
- **Future of regulation –** Fostering the right compliance culture within the organisations' extended value chain while managing an uncertain regulatory landscape.
- **Future of extended enterprise –** Ensuring sustainability, management focus, equity in alliance partnership while minimising the exposure to extended enterprise risks around business continuity, financial solvency, health safety and environment, bribery and corruption, and intellectual property breaches

The need of the hour is to re-evaluate the future of risk, redefine its value proposition; using new age tools, techniques, and methodologies and build a risk intelligent workforce for improved risk sensing and decision making.

Organisations that adapt to these changes will be prepared and very clearly, the future belongs to the prepared.

It has been our endeavour to also understand the industry perspective on these issues, in addition to views from our Subject Matter Expert (SME).

We would like to thank the industry leaders and our subject matter experts for sharing their insights and enriching this publication.

Executive summary

Industry 4.0 is increasingly being characterised by innovation in adopting newer and disruptive technologies leading to interconnected organisations and borderless markets. Alliances and ecosystem partnerships are becoming core to an organisation's strategy.

Technology is augmenting human skills while regulations are still playing catch up with this new normal. And in this new normal, the risk landscape is also registering a shift, which is primarily being shaped by the interrelated changes in Future of Work, Future of Regulation, and Future of Extended Enterprises.

Future of work

- Demographic Shift- Gig workers, millennials, Gen Z
- Digital Technology- AI, 3D printing, IOT, and cognitive computing

Future of regulation

- Regulations unable to keep pace with disruptive business models
- Regulations around data, digital privacy, AI, and cybersecurity
- Responsibility to self regulate

Future of extended enterprise

- Marketplace differentiation by reinventing the value chain through alliances
- Products turning into platforms through ecosystem partners

Future of risk

- Fostering the right compliance culture and maintaining optimum levels of compliance in the face of regulatory uncertainty
- Leveraging Industry 4.0 for technology enabled risk management by design through adoption of IOT, OT, AI & ML
- Prescriptive analytical insights to provide automated intervention to continuously monitor and manage risks
- Usage of behavioural sciences for risk management

Future of work comprises three deeply connected dimensions of an organisation: **work** (the what), the **workforce** (the who), and the **workplace** (the where). The very fabric of work is being altered because of converging demographic and technological trends, which in turn is leading to the rise of new social contracts. Statistics indicate the following:

- Fifty percent of the workforce is likely to be millennials or gen Z workers[1] by 2020.
- Artificial Intelligence (AI) will displace 40 percent of world's current tasks[2], and similar disruptors will help create 1.75 million technology-enabled jobs[3]. Fifty-five percent of Indian workforce will require reskilling by 2022[4].
- By 2025, 20 percent of the workforce will be contract workers[4].

With this shift, new risks have emerged around adopting digital technologies, managing the associated bio convergence (machine-human interaction), reskilling requirements, and extension of workplace boundaries.

To address these risks, organisations can take the following steps:

- Create a digital risk management strategy[5A] to manage the third party, data leakage, and cyber risks.
- Develop a workforce strategy (employee vs. contingent workers) aligned to overall objectives, which will help manage the workforce mix and create a consistent experience across these segments.

This also means the following:

- Policymakers will need to reassess and update policies to define gig economy, ensure access to government and societal benefits, and facilitate access to education.
- Workforce must engage in learning and building tech fluency.

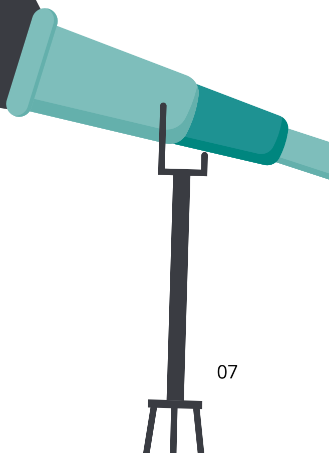
Future of regulation

Sweeping technological advancements are creating a sea of change in today's regulatory requirements and frameworks. This is further compounded by uncertainty in the regulatory landscape.

- Today, 30 percent of countries have no data protection laws; and those that do, lack uniformity[6].
- Regulatory policy cycle takes five to twenty years whereas a start-up can adopt disruptive technologies and business models, and turn into a unicorn in half the time[6].

Given the business models and technology-related disruptions, responsible corporate citizens are now expected to:

- Foster the right compliance culture, especially in fast paced and disruptive business models and
- Self regulate, manage the uncertain regulatory roadmap and expectation gap between regulators and organisations for products, services, and operations.



To address these risks, organisations can consider the following:

- Create a regulatory compliance framework[5B] to enable periodic regulatory risk sensing through social listening and collaboration to develop a strategy to respond to emerging issues.
- Build capability to understand, anticipate, and respond to the changing regulatory landscape and manage regulatory relationships throughout the extended value chain.
- Participate in regulatory sandboxes and collaborate with other organisations, entrepreneurs, academia to test products and identify adaptations to existing regulation.
- Change the current regulatory approach from the current "external imposition" view to a more "risk intelligent" one based on collaboration, transparency, and self-regulation.

Regulators must consider adapting the current regulatory models to include:

- Adaptive, iterative, and collaborative regulation (for example, ISO is working on international standard for drone operations that are likely to be adopted throughout the world.)
- Outcome-based regulation (for example, Australia has developed performance-based guidelines for autonomous vehicles, and these are regularly reviewed.)
- Regulatory sandboxes (for example, Reserve Bank of India has started regulatory sandbox for Fintech players.)
- Risk weighted regulation (for example, Reserve Bank of India has implemented risk based supervision and additional capital requirements for systemically important institutions.)

Future of extended enterprise

Traditional businesses are entering into strategic alliances to thrive in the digital economy. Alliances and ecosystem partners help in improving market/customer reach and shortening the value chain while creating differentiation. Currently in the Asia Pacific region:

- Seventy-one percent of the alliances are entered into for developing new products[7] and
- Twenty-nine percent are for entering new markets[7].

However, not all is well with extended enterprise. Benchmarking data[8] suggests that alliances primary fail due to the following reasons:

- Lack of trust (65 percent), misaligned vision (60 percent), and misaligned culture (45 percent)[8],
- Inequity of commercial terms (50 percent)[8], and
- Lack of governing model (40 percent)[8].

Even though strategic alliances deliver needed capabilities, they create an extended enterprise and expose the organisation to risks in the nature of:

- Sustainability and scalability of the existing partnership,
- Unfavourably negotiated deal terms favouring one side over the other,
- Lack of management attention and cultural mismatch,
- Business continuity, financial solvency, health safety and environment, bribery and corruption, and data risk including intellectual property breaches.

To address these risks, organisations can consider the following measures:

- Evaluate alignment on vision, scope and capabilities, cultural fitment, and commercial equity during alliance partner identification.
- Establish structures and align resources to manage and champion the alliance.
- Set up a holistic governance mechanism with Key Performance Indicators (KPIs) to track the progress and results.
- Define contractually binding independent exit strategy.
- Create a comprehensive Extended Enterprise Risk Management (EERM)[5C] programme, which is technology enabled and has an end-to-end approach to cover the risk universe across the business partner lifecycle.

Having understood the future of work, future of regulation, and future of extended enterprise, it is now clear that organisations' risk profile has expanded and is dynamic and complex. This has a cascading impact on the future of risk.

Future of risk

In the past, risk management was often an exercise in fear and avoidance. Organisations primarily focused on completing necessary, compliance-driven activities. Given the future of work, regulation, and extended enterprise, risks are evolving at an unimagined pace and are becoming more measurable and tangible; it is imperative for risk management functions to accelerate their evolution by:

- Creating a comprehensive Enterprise Risk Management (ERM)[5D] framework,
- Building capability for continuous risk sensing[5E] and encouraging collective risk management through the extended value chain,
- Implementing cognitive technology in a digitally secure and compliant[5F] environment for risk analysis and detection,
- Digital risk management[5A] by deploying pervasive controls through technology such as IoT as part of products, services, and business models to monitor and manage risks in real time,
- Building vigilance and resilience to complement prevention through Continuous Control Monitoring (CCM)[5G],
- Creating an integrated risk and control organisation[5H] enabled by robotics, machine learning, and AI for integrated assurance across the lines of defense (LOD), predictive risk management, and improved control posture,
- Increasing the use of risk transfer instruments to offset costs involved in recovering from a risk event.

There are no rewards without risks. Organisations must have a balanced view of change drivers and disruptors as they will bring in their wake a whole set of new opportunities. To drive performance, the need of the hour is to reimagine the future, through the risk lens.

> “The workplace today is multi-generational. Each group is different from the other. They bring in their own perspective that influences and defines workplace culture. To create a successful workplace and an engaged team, organisations and their HR practices are building a common narrative to weave them all into the workplace fabric while addressing the varied needs and strengths of each.
>
> Regulations today are consistent and uniform across the board. Given the disruption in today’s business environment both digital and workplace related, the “one size fits all” approach should evolve to one that is softer and provides the flexibility and freedom to explain and factor in unique nuances. This distinction will have a positive impact in terms of capitalising on business and workplace disruptions.
>
> Given today’s business environment is a large networked ecosystem, strategic alliances and partnership provide a huge opportunity. The risks from these alliances are manageable if calibrated with thought while considering and crafting the alliance strategy.”

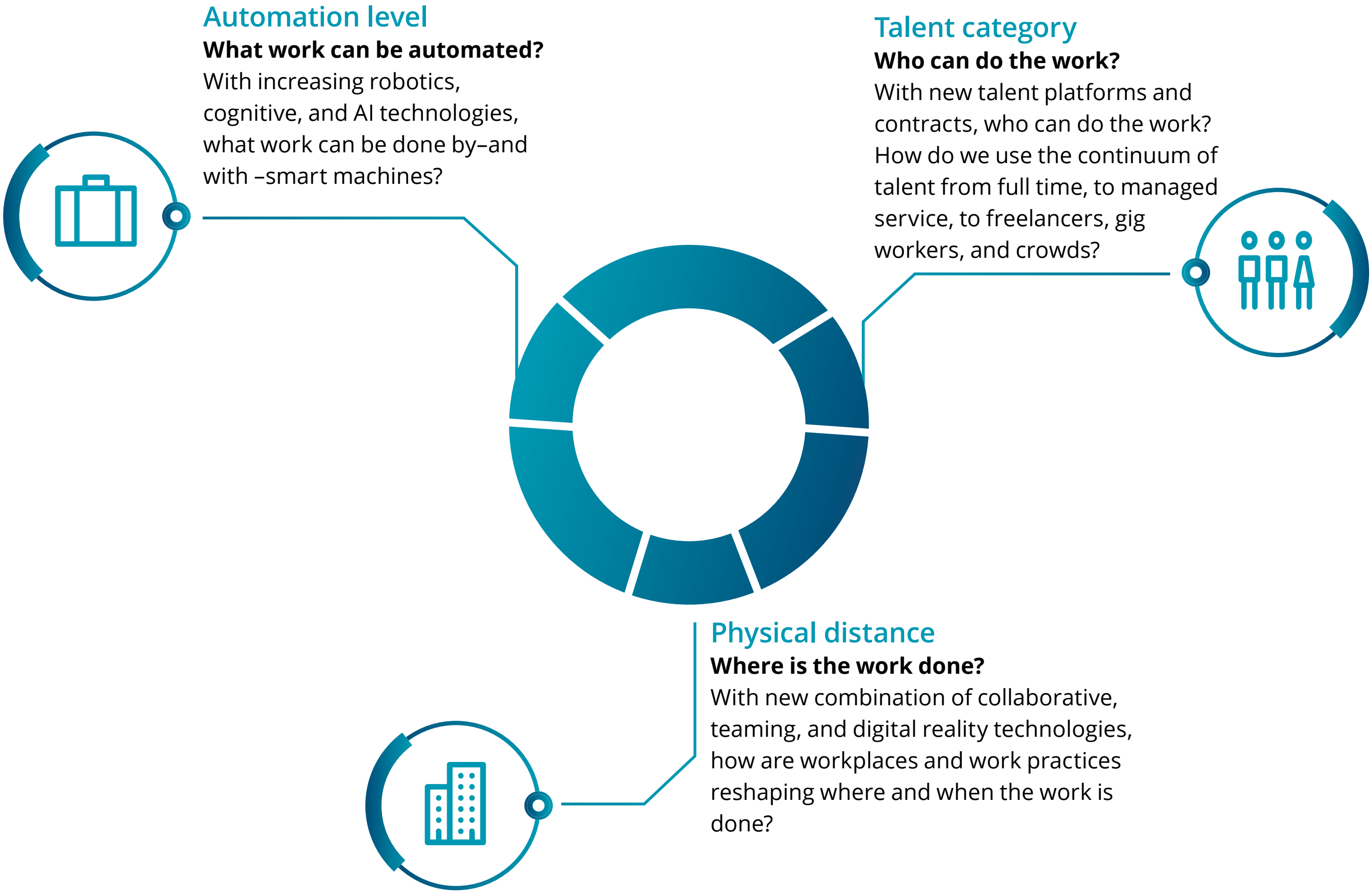
Subramaniam S
CFO, Titan Company Ltd.

Future of work

1. Key disruptors shaping the future of work
2. Emerging risks
3. Risk response

Given the Industry 4.0, economically, markets are increasingly interconnected, businesses are borderless, and technology coupled with extended enterprise ecosystem is leading to innovation and birth of entirely new business models. Demographically, it is estimated that 50 percent of the workforce already comprises millennials and Gen Z workers[1], and Artificial Intelligence (AI) will displace 40 percent of the world's current tasks[3]. By 2025, the freelance or gig economy, which was previously considered supplementary, will move to mainstream and contract workers will replace 22 percent of the permanent workers[4]. Technology will augment the human skills in areas such as problem solving, communication, listening, interpretation, and design and create 1.75 million technology-enabled jobs[3].

These factors are changing the very fabric of work, which comprises three deeply connected dimensions of an organisation: work (the what), the workforce (the who), and the workplace (the where).



Automation level

What work can be automated?

With increasing robotics, cognitive, and AI technologies, what work can be done by–and with –smart machines?

Talent category

Who can do the work?

With new talent platforms and contracts, who can do the work? How do we use the continuum of talent from full time, to managed service, to freelancers, gig workers, and crowds?

Physical distance

Where is the work done?

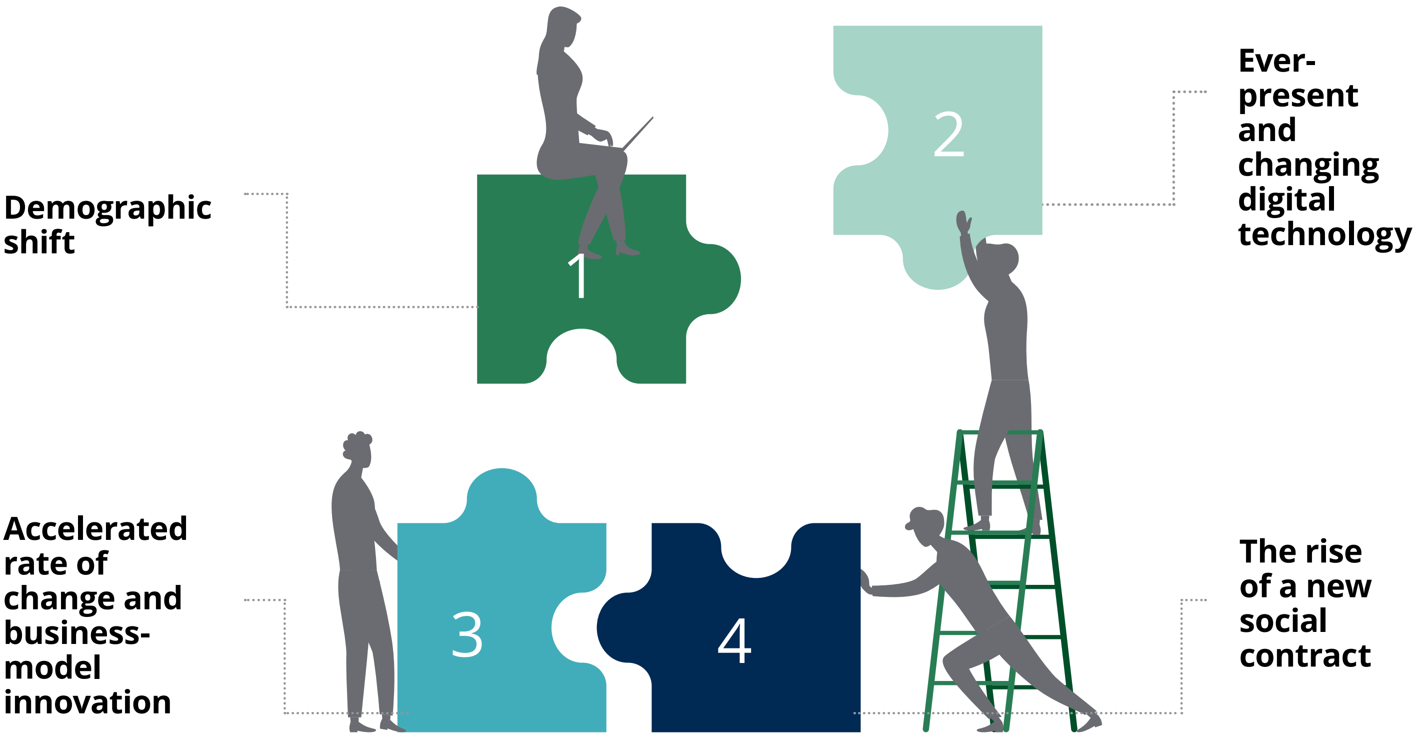
With new combination of collaborative, teaming, and digital reality technologies, how are workplaces and work practices reshaping where and when the work is done?

“After AI and robotics, I believe the next big disruption in the workplace will be the 'gig economy'. The shared economy is fast exploding and is expected to generate $325 Bn. by 2025.

On-demand, project-based employment is the next big thing. The transition to this world will bring about a complete change in the way employees develop and market their capabilities and skills. The question for companies is how to best seize the opportunities linked to 'uberization of work'."

V S Parthasarathy
Group CFO, Group CIO & Member of the Group Executive Board, Mahindra & Mahindra Ltd.

Key disruptors shaping the future of work



Demographic shift

Ever-present and changing digital technology

Accelerated rate of change and business-model innovation

The rise of a new social contract

1. **Demographic shift –** Today, the workforce is diverse in terms of age, culture, gender, etc., and multi-generational with baby boomers, millennials, Gen X working alongside each other. Each group has its own work expectations and working styles. For example, millennials expect greater flexibility, a mobile work environment, and spend a maximum of 16 months with one employer[9]. This contrasts with baby boomers who worked longer with one employer for job and financial stability, and has led to growth in the "gig or freelance economy".

2. **Digital technology –** Now, digital technology is everywhere. According to the Organisation of Economic and Corporate Development, this digital wave will affect 32 percent of jobs across the board. Technologies such as AI, smart mobile devices, 3D printing, sensors, cognitive computing, IoT change the way companies design, manufacture, and deliver almost every product and service. In parallel, social networking tools and apps change the way organisations hire, manage, and support people and leave them more transparent—whether they like it or not.

> "In the future, machines will perform the job and humans will create, tend and protect them."
>
> **Priya Mahadevan**
> Consultant, NASSCOM Future Skills

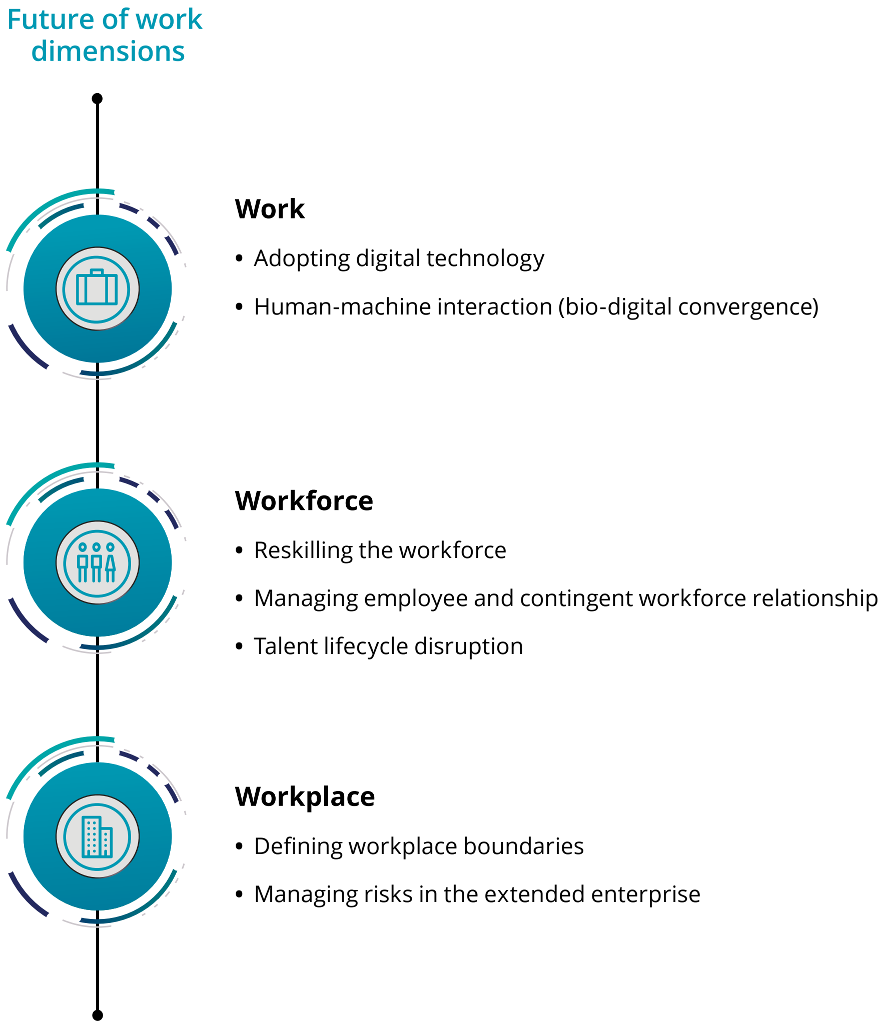
3. **Accelerated rate of change and business model innovation –** Business model innovation is defined as the process of enhancing advantage and value creation by changing the organisation's value proposition and operating model. This is often accompanied with rapid change driven by technology and digital adoption. For example, rapid business model innovation from companies such as Uber and Airbnb is forcing the travel, transportation, and hospitality sectors to respond and reposition themselves to meet new challenges. This is extending the boundaries of workplace and defining the workforce.

4. **New social contract –** A new social contract is developing between companies and workforce, driving major changes in the employer-employee relationship. The days when a majority of the workforce will expect to move up in their careers or across the corporate ladder in one company are over. The millennials and Gen Z workforce wants to work for many employers and demand an enriching experience at every stage. This leads to expectations for a compelling and flexible workplace, and a sense of mission and purpose at work.

> “Imagine an emergency where your mission critical application shuts down and the system automatically generates a distress call that is directed to a chatbot.
>
> The chatbot locates you in a co-working space and connects you to an onsite contractor who is far removed in a different continent to trouble shoot the problem. The contractor puts on his google glasses to consult you and the chatbot and the application is back in operation in no time.
>
> This is the future of work. It will open up multitude of opportunities but will at the same time expose organisations to newer risks around how algorithms and humans interact with data to make real time decisions.
>
> Are you secure, vigilant, and resilient in this faceless, converged and hyper connected world?”
>
> **Santosh Kumar**
> Subject Matter Expert

Emerging risks

The future of work has led to emergence of new risks across the three dimensions of work. The risks are as follows:



Future of work dimensions

Work

- Adopting digital technology
- Human-machine interaction (bio-digital convergence)

Workforce

- Reskilling the workforce
- Managing employee and contingent workforce relationship
- Talent lifecycle disruption

Workplace

- Defining workplace boundaries
- Managing risks in the extended enterprise

Risk response

To address these risks, organisations, policymakers, and people can consider the following measures:

Organisations

- **Create a digital risk management strategy**[5A] to manage third-party data leakage, and cyber risks
- **Redesign work for technology and learning**
  - Facilitate machine-human collaboration
  - Identify and run upskilling programs on technical aspects and soft skills
- **Rethink workforce strategy**
  - Change from traditional employee lifecycle model of "attract, develop, and retain" to "access, curate, and engage"
  - Determine employee contingent workforce mix.
  - Ensure consistent experience across workforce segments
- **Redefine value**
  - Adopt a broader view and focus on creation and delivery of financial value and meaning to the customer

People

- **Engage in lifelong learning**
  - Ensure self-directed learning.
  - Build tech fluency
- **Shape your own career path**
- **Pursue your passion**

Policy makers

- **Reassess policies**
  - Update the definitions of employment to account for freelance/gig economy
  - Ensure provisioning and access to government health, pension, and other social benefits
- **Reimage lifelong education**
  - Extend education facilities to marginalised populations and older generations who cannot transition out of the workforce
  - Design payment structures and incentives to support lifelong education
  - Facilitate access to ongoing education and training throughout a working career that might span 50 years and many different types of work

> "Today's agile world everyday threats and vulnerabilities landscape is evolving in various forms; it is vital to have an independent view to measure effectiveness of risk management controls."

Prabhu Natarajan
Global Cyber Assurance Head,
Temenos India Pvt. Ltd.

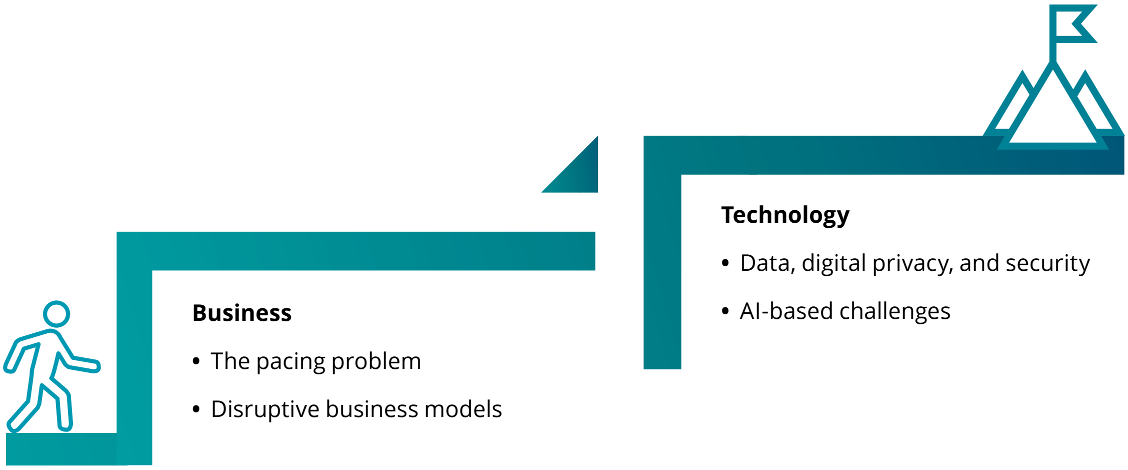
Even though technological advances, demographic shifts, new business models, and social contracts fundamentally change work, workforce, and workplace, this is an opportunity to zoom out and re-imagine learning models, talent practices, work and workforce strategies, policies and regulations to make the future of work more meaningful.

Future of regulation

1. Key disruptors challenging regulations
2. Emerging risks
3. Risk response

Key disruptors challenging regulations

In today’s regulatory environment, technological advancements are bringing in change. Regulators and businesses are challenged to maintain a balance between fostering innovation, enforcing regulation, and addressing the unintended consequences of disruption. Business and Technology are the two main categories disrupting the future of regulation:



Business

- The pacing problem
- Disruptive business models

Technology

- Data, digital privacy, and security
- AI-based challenges

“The governance and risk scenario varies significantly for listed and unlisted companies in terms of complexity of laws, proactiveness, adaptability to change and competency of the responsible person. From a regulatory standpoint, a simple law with maximum governance can help both company and the regulator. This will pave the way for a conducive climate for doing business, enhancing transparency, avoiding non-compliance and to reduce cost of compliance.

Pharma being a highly regulated industry that touches human lives, risk management needs to be embedded in every technical and functional process to distribute products to patients at affordable price with utmost safety.

It’s an imminent need that companies have to hire specialists across geographies to deal with ever changing regulations to protect reputation and to give maximum comfort to the Board on its Governance”.

Sormistha Ghosh
Sr. Vice President – Legal & Secretarial & Chief Risk Officer
Strides Pharma Sciences Ltd.

I. Business related

1. **The pacing problem**
   “Pacing problem” is the gap between technological advancements and the mechanisms intended to regulate them. For example, regulatory policy cycle takes five to twenty years whereas a start-up can adopt disruptive technologies and business models, and turn into a unicorn in half the time[6].

2. **Disruptive business models**
   Disruptive business models cross-traditional industry boundaries. As product and services evolve, they shift from one regulatory category to another. For example, if a ride-hailing company delivers food, it can fall under the jurisdiction of food safety regulators; and if it expands into helicopter services, it will fall under the purview of aviation rules. This constantly evolving interconnected nature of newer business models is challenging for regulators as they need to refresh regulations, maintain consistency, and coordinate across regulators. Business investments are at risk because of the uncertain regulatory landscape.

II. Technology related

3. **Data, digital privacy, and cyber security**
   The growing use of internet-connected devices has created a vast digital footprint—a trend that will only accelerate. Despite the amount of data generated, nearly 30 percent of nations have no data protections laws, and those that do, lack uniformity[6].

   From a regulatory standpoint, the important question is who owns all this data. Is it the user or the service provider who stores it? From a business standpoint, what obligation does the service provider have—to store, protect, and share this data with third parties?

   Another key challenge is cyber security. Malicious cyber activity has become more sophisticated and borderless with its reliance on networked digital infrastructure. For example, autonomous vehicles can be targets of cyberattacks. What precautions should developers and regulators incorporate to ensure malicious hackers will not force vehicles to crash or manipulate signals and cause traffic jams?

4. **AI-based challenges**
   Algorithms are used routinely to make vital financial, credit, hiring, and legal decisions. Given their importance, it is necessary to understand these algorithms and make sense of their decisions. However, algorithms are not open for public scrutiny as organisations hold them closely and often even their creators cannot explain how they work. This is the “black box” problem. Additionally, at least in theory, algorithms should lead to unbiased and fair decisions. However, algorithms may have inherent biases referred to as “algorithmic bias”. This opaqueness and bias causes a challenge to both organisations and regulators.While auditing AI systems to identify non-compliances is difficult, organisations could be held liable for AI breeches and biases. Regulators and organisations need to strategise to handle the associated data risks, protect AI assets and define punitive action in case of AI manipulation.

> “Effective cyber risk management is highly required for business sustenance more than compliance. A dynamic comprehensive technology risk governance strategy supported by human intelligence and machine is the key differentiator that is capable to capture and address the cyber risk in time at root.”
>
> **Dr. Lopa Mudraa Basu**
> Global Head Cyber Security Risk Governance & Compliance,
> NISSAN Motor Corporation

Emerging risks

The business and technology related disruptions have led to an uncertain and complex regulatory landscape for new products, services, and operations. Therefore, leading to the following changes in the risk profile:

- Expectation gap between regulators and organisation on the regulatory requirements and enforcement
- Maintaining optimal levels of compliances within the extended enterprise ecosystem created in today's business models
- Managing compliance information with regulators, third parties, and other industry players
- Failure to foster the right compliance culture
- Addressing the digital privacy, cyber and algorithmic risks

> "With progress in Artificial Intelligence (AI) and cognitive computing, machines may begin to make decision on behalf of humans which may result in unforeseen risks or unpredictable outcomes creating complex liability issues".
>
> **S K Rangaswamy**
> Chief Risk Officer and Head of Internal Audit,
> CholaMS General Insurance

Risk response

As the government policymakers, regulators, and organisations struggle to deal with these disruptors and the emanating risks the following measures can be considered:

I. Regulatory response

To address the critical questions and improve the government to business (G2B) experience, regulators are redesigning their regulatory approach to include the following:

Adaptive regulation

Shift from "regulate and forget" to a responsive, iterative approach.

For example, Finland has reformed its transportation regulation by creating a new transport code that incorporates all transport modes.

Regulatory sandboxes

Prototype and test new approaches by creating sandboxes and accelerators.

For example, RBI has provided Fintech's, access to banking systems within a regulatory sandbox to provide proof of concept and test innovative solutions.

Outcome-based regulation

Focus on results and performance rather than form.

For example, Australia has developed performance-based guidelines for autonomous vehicles and these are regularly reviewed.

Risk-weighted regulation

Shift from one-size-fits-all regulation to a data-driven, segmented approach

For example, RBI has implemented risk based supervision and additional capital requirements for systemically important institutions.

Collaborative regulation

Align regulation nationally and internationally by engaging a broader set of players across the ecosystem

For example, ISO is working on international standards for drone operations that are likely to be adopted throughout the world.

Source: Deloitte Centre for Government Insights Analysis

II. Organisational response

Given the value at risk, organisations can adopt the following internal and external measures:

Periodic scan and sensing
A periodic scan to sense and develop a regulatory compliance strategy and framework[5B] to respond to new issues and disruptions around:

- Technology
- Business models
- Business drivers
- New market opportunities

Cultural shift
Ensure change of approach from the current "external imposition" view to the one that is more risk intelligent based on collaboration, transparency, and self regulation.

Build and develop capability
Most companies will benefit from building capability to:

- Manage and own regulatory relationships.
- Ensure proactive and frequent interaction.
- Develop an appropriate response to the changing regulatory landscape.
- Recruit and retain appropriate talent in this area.

Participation and alignment
As an industry player:

- Set up the precedent for self-regulation, especially for new areas or innovation.
- Participate in regulatory sandboxes and collaborate with private companies, entrepreneurs, academia to test products and identify adaptations to existing regulation.

"An iterative and collaborative process with a robust feedback mechanism should be adopted by regulators involving all relevant stakeholders. Organisations should build capability in terms of sensing eminent changes to regulations so they can proactively engage with regulator and other stakeholders. This capability build will be supplemented through internal or external resources and technology to ensure compliance and be more efficient."

Pankaj Chawda
Assurance, Risk & Internal Controls-ABB India

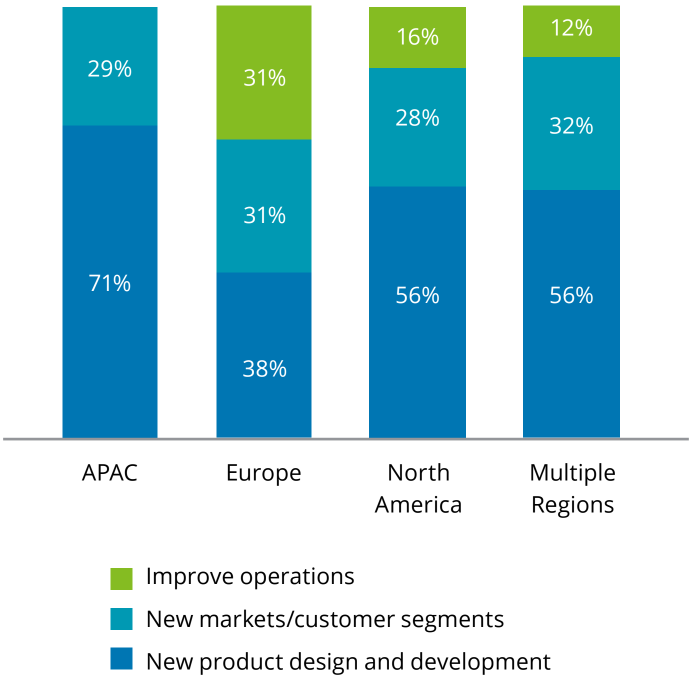
> “In general, regulatory requirements are becoming wider, deeper, and time sensitive across geographies. The data managed and the enabling technology in the process of becoming simpler for end user has become widely complex and massive for corporations.
>
> The traditional static, rule based compliance systems will soon become redundant. To meet this ever evolving process of risk and compliance, organisations need a holistic framework, a technology platform including a robust self-learning mode.”
>
> **Senthilvel Kaliyamurthy**
> Subject Matter Expert

While, the business-related technological advances overwhelm both the regulators and the organisation, these changes provide an opportunity for them to proactively engage and re-examine their ways of working; while providing a definite competitive edge to organisations that can anticipate the future regulatory roadmap. It is also likely that the very factors causing this disruption will reinvent rule making, enforcement and compliance, wherein lies the future of regulation.

Future of extended enterprise

1. Key disruption patterns creating an extended enterprise
2. Emerging risks and risk response

Traditional businesses must reinvent themselves with changes in the business world and domination of technological disruption. Organisations need a clear strategy and seamless execution to keep pace with this change and seize new opportunities. Unique patterns that exist across geographies in terms of digital alliances scope are depicted below[7].



- In APAC, partnerships are geared towards developing new products or solutions.
- Contrast this to Europe, where partnerships are formed to target both external and internal improvements.

Source: Accelerating Digital Ecosystem Development through Strategic Alliances (Deloitte Monitor Analysis)

In terms of industry verticals, 50 percent of the alliances are by Technology, Media, and Telecommunication (TMT) companies[7]. Therefore, this industry vertical dominates the alliance space.

Against this backdrop, alliances are increasingly important as they complement the build or buy options and create an "extended enterprise" that helps traditional businesses gain access to vital external capabilities.

Key disruption patterns creating an extended enterprise

Organisations leverage the extended enterprise to create or address the enlisted patterns of disruption:

1 **Expand marketplace reach**
Make more products available to a larger audience and to fulfill the 'long tail' of demand

2 **Turn products into platforms**
Create a modular and flexible core product to facilitate rapid customisation and scaling

3 **Unlock assets from adjacent markets**
Effectively access and use of underutilised and affordable assets (third party resources) in adjacent markets

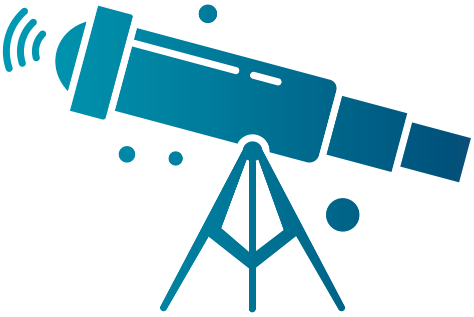
4 **Shorten the value chain**
Restructure the value chain to provide significant benefits to the customer by removing or shifting stages of delivery

Source: Adapted from Deloitte Patterns of Disruption Series

> "In today's disruptive business environment, if successfully managed, strategic alliances create an adaptive ecosystem that is a vital tool to drive technological innovation, thereby decreasing volatility and opening up opportunities while optimising risks."

C Ramanathan
Head of Risk and Controls, United Spirits Ltd.

However, all is not well with the extended enterprise. As depicted below, benchmarking data suggests that alliances primarily fail due to management shortfalls[8].



40%	Trust in alliance relationship
45%	Lack of common vision
50%	Inequity of commercial returns
60%	Cultural misalignment
65%	Unsuitable governance model

Source: Strategic alliances: An essential weapon in the growth arsenal (Alliance Best Practices)

> “In the complex and fast changing environment of innovation, digital transformation, increased regulatory expectations, global macro factors, with heightened client centricity, strategic partners can play an important role; success in future is to strike a balance between the incremental value add from them and change in risk profile of the organisation”
>
> **Prabhakar Arjun Vishwakarma**
> Managing Director Head of Audit for India, State Street India

Emerging risks and risk response

Even though alliances deliver needed capabilities, the extended enterprise exposes the organisation to a unique set of risks. These emerging risks and their potential mitigation across the alliance lifecycle are as follows:

Alliance lifecycle	Key emerging risks		Risk response
Partner identification and selection	Sustainability and scalability of the existing partnership	**Extended Enterprise Risk Management (EERM)^{5C} Framework**	Evaluate alignment on scope, alliance type, ability to unify vision and cultural fitment.
Negotiation and deal structuring	Over-engineering–too prescriptive and comprehensive clauses limiting productivity		• Define a plan to measure both alliance progress and results. • Ensure equity in commercial returns across participants.
	Unfavourably negotiated deal terms favouring one side over the other		
Execution	Lack of management attention and focus		• Establish alliance management systems and structures. • Set up a governance mechanism. • Align resources to manage and champion the alliance. • Manage knowledge exchange dynamics i.e. promote open environment while protecting the core. • Embed governance risk and compliance activities wherever necessary.
	Underperformance due to initially set over-ambitious targets		
	Cultural clash impacting collaboration		
	Potential loss of continuity across all stages of the partnership lifecycle		
	Governance risk and compliance issues – business continuity, financial solvency, health safety and environment etc.		
Exit	High dependency on one partner's capability hindering the speed and ease of the exit		Define independent exit strategy/ disengagement process.

Source: Accelerating Digital Ecosystem Development through Strategic Alliances (Deloitte Monitor Analysis)

> "Alliances and partnerships help organisations pool complimentary skill sets to optimise risks and create value in this challenging and competitive environment. Taking a lifecycle approach to partnerships, whereby organisations identify and address potential risks can help them to not only achieve goals but also more effectively manage ongoing relationships."

Pardhasaradhi Rallabandi
Chief Risk Officer, Northern Arc Capital formerly IFMR Capital

In today's disrupted business environment, the extended enterprise is a source of business value and strategic advantage, since no organisation can function on its own. Hence, organisations will continue to build these alliances and the associated risks will continue to evolve and grow. A comprehensive technology enabled Extended Enterprise Risk Management (EERM) programme across the alliance life cycle is required to seize this advantage and protect value.

Future of risk

1. Risks challenging organisational responses
2. Next steps for improved risk management

Today's global environment is characterised by change, uncertainty, and disruptive innovation. Newer business models, digital transformation, industry 4.0, are leading to changes in work, extended enterprise and regulations. This has expanded the risk universe and made it complex and dynamic. Therefore, organisations and risk leaders are more focused than ever in identifying and managing this dynamic risk landscape.

> "Today, virtually every industry faces risk of disruption driven by advances in technology, innovations in business models, changing consumer preferences and evolving ecosystems. Organisations, which anticipate these risks are more likely to successfully adapt to these changes and continue to create value for their stakeholders.
>
> These call for a shift in the role of the risk management function that needs to migrate the organisation from identifying and managing traditional, operational and predictable risks to developing a broader view of emerging, strategic and often unknown risks.
>
> In addition to driving this transformation, risk officers will also be expected to provide an independent, outside-in view of risks and to focus on building risk resilience within the organisation."

Samita Shah
Group Head Corporate Finance & Risk Management, Tata Steel

Risks challenging organisational responses

People Related Risks
People Strategy:

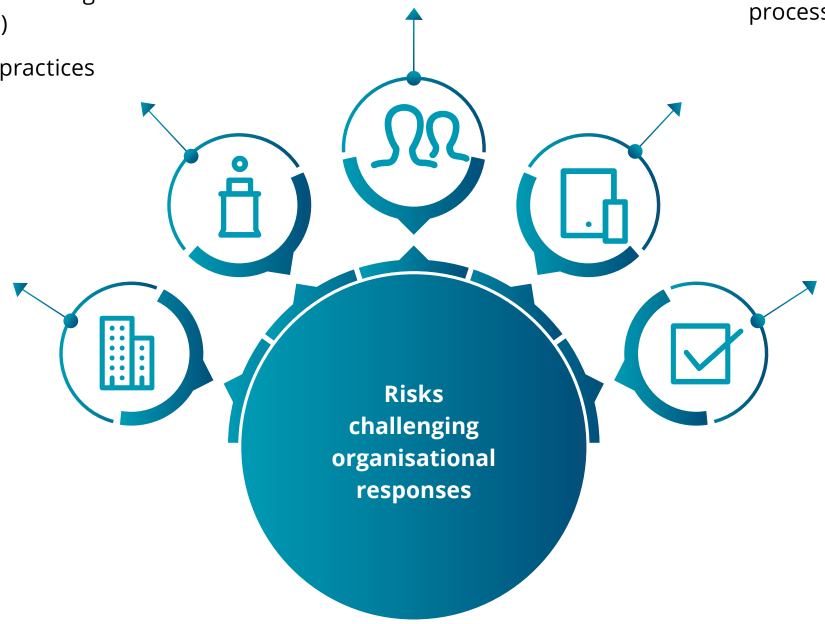
- Managing a multi-generational workforce
- Redefining talent lifecycle
- Ensuring digital readiness
- Reskilling workforce
- Using the "gig economy"
- Diversity and inclusion
- Driving engagement

Reputational Risks

- Corporate governance failure
- Regulatory responsibility
- Employment conditions
- Product quality
- Customer working practices
- Social media (combating misinformation)
- Environmental practices

Digital/Technology Risk

- AI risks (black box problem, algorithmic bias)
- Cybersecurity
- Data risks (accuracy, security, privacy)
- Digital ethics
- Automation (operational process and controls)



Extended Enterprise

- Managing sustainability, scalability, cultural mismatch
- Managing inequitable terms, exit rules
- Managing exposure to business continuity, financial solvency, health safety and environment, bribery and corruption, and data risk including intellectual property breaches

Compliance/ Regulatory Risks

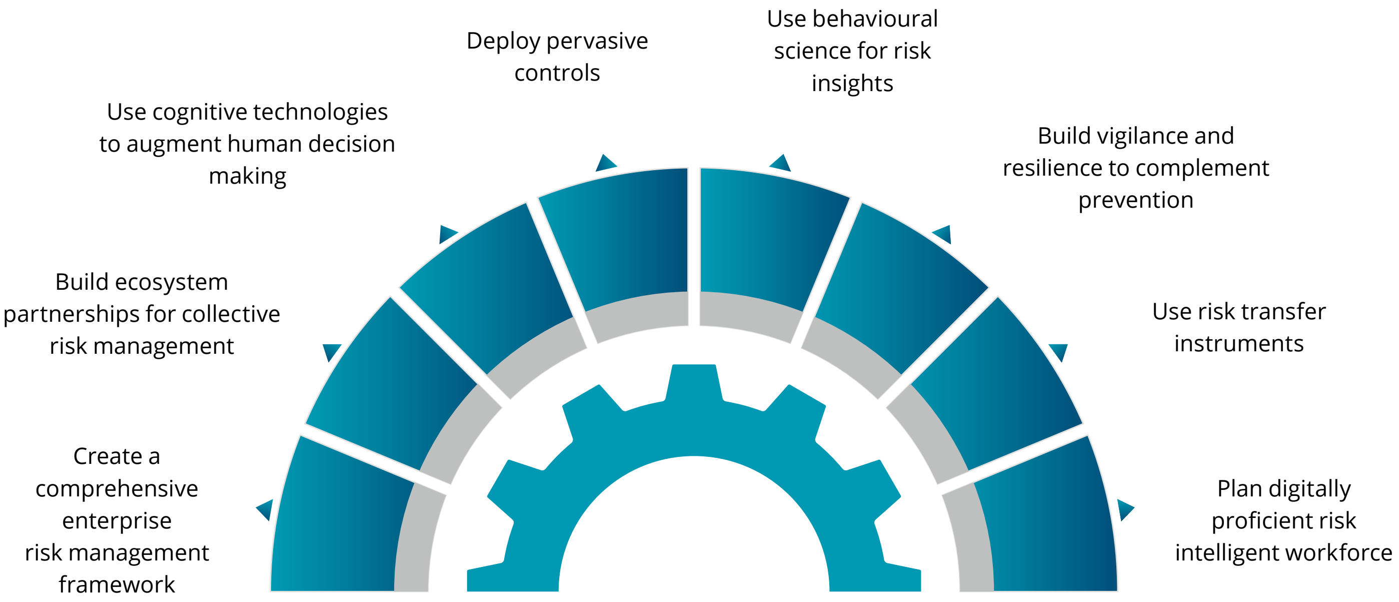
- Managing complex structure, uncertain landscape
- Managing expectation gap for newer products, services, and operations
- Fostering a compliance culture
- Maintaining optimal levels of compliance

> "In future, risk management will transcend the mechanics of metrics, measurements, and models and enable insight-rich approaches to underpin business strategies and processes. Risk agenda will hopefully be driven by convergence amongst the three lines of defense, with the common objective of keeping the risks within the organisation appetite"

Anil Kishora
Chief Risk Officer and Deputy Managing Director, State Bank of India

Risk management future imperatives

The emerging risks and risk responses for changes related to “future of work”, “future of regulation” and “future of extended enterprise” have already been covered in the respective sections. Beyond these, the additional steps that organisations can adopt for effective risk management are enlisted as follows:


Create a comprehensive enterprise risk management framework
Build ecosystem partnerships for collective risk management
Use cognitive technologies to augment human decision making
Deploy pervasive controls
Use behavioural science for risk insights
Build vigilance and resilience to complement prevention
Use risk transfer instruments
Plan digitally proficient risk intelligent workforce

> “Risk landscape is ever evolving. The challenge in hand for organisations is to figure out a way to deal with not only business as usual, but also navigate through disruptive forces to successfully deliver strategic imperatives. When risks do materialise and culminate into crisis, organisation’s response and resilience goes through a litmus test.
>
> Boards are now keen to understand the overall risk governance framework that extends throughout the value chain. From a monitoring and oversight perspective the expectation is to demonstrate an integrated assurance framework with a ‘test once, satisfy all’ philosophy leveraging AI, BOTs, analytics and other digital enablers.”
>
> **Sandeep Sarkar**
> Partner, Deloitte India

1. **Create a comprehensive enterprise risk management framework (ERM)[5D]** with building blocks such as governance frameworks; tools for risk management and operational discipline; methodology to deliver change, manage high risk events.

2. **Build ecosystem partnerships for continuous risk[5E] sensing and collective risk management**
The network economy demands collective risk management. As businesses engage deeply with a large number of external stakeholders (vendors, peers, innovators, regulators, etc.), organisations need to build risk sensing capability and use this collective ecosystem or extended value chain to identify, manage, and reduce risks.

3. **Use cognitive technologies to augment human decision making**
Driven by development in AI and easy access to big data, organisations will rely on smart systems to assist and at times even replace human-led risk management. Cognitive technology/BOT's/Robotic Process Automation when implemented in a secured and compliant environment[5F] can significantly risk by improving enhance risk analysis and detection[10].

> "At Quikr, we look at fraudulent activities as a business problem to be solved and use combination of technology, human effort, advocacy, and policies to moderate our listings. While technology filters is an added advantage, phone verification for authentication in such cases is necessary too. With advancement in technology, complexity of such activities will only increase and businesses such as ours will continue to invest in measures to tackle this Tom and Jerry chase."
>
> **Pranay Chulet**
> Founder and CEO, Quikr

4. **Deploy pervasive controls**
Pervasive controls will be deployed as part of products, services, and business models to monitor and manage risks in real time. The current environment, which is sensor-enabled and hyper-connected coupled with Digital Risk Management[5A] facilitates this practice. Singapore-based TrustSphere, whose clients include financial services firms, specialises in trying to uncover the relationships that an employee has through digital interactions—attempting to reduce the risks of illegal collusion and internal fraud.

5. **Use behavioural science for risk insights**
Behavioural science can be used to understand risk perception, influence risk behaviour, and improve risk related decision making. Fujitsu has built a platform that uses psychological profiling to ramp up computer security in the workplace. It is done by identifying the users who are most vulnerable to cyberattacks basis on their browsing pattern. This was developed after consulting social psychology experts and surveying more than 2,000 Japanese users, half of whom had experienced attacks, to determine which traits make some users more vulnerable to viruses, scams, and data leaks.

6. **Build vigilance and resilience to complement prevention**
Risk prevention methods can never be foolproof. Increasing investment in preventative approaches often yields only marginal benefits. Therefore, organisations are expanding their approaches to focus on vigilance (detecting patterns that may indicate or even predict risk events) and resilience (the capacity to rapidly contain and reduce the impact of risk events) through Continuous Control Monitoring (CCM)[5G]. These activities will continue to rise in importance: monitoring emerging threats, identifying anomalies in business processes, managing stoppages from third-party vendors, and preparing for risk-related workplace disruptions.

> "In future, only those auditors will be successful who can optimise assurance for an integrated and digital world."
>
> **Rajiv Gupta**
> Senior Vice President, Diageo Business Services

7. **Create an integrated risk and control organisation[5H]**
   Virtually all (95 percent)[11] of the organisations report deploying the three lines of defense but face challenges eliminating overlap. So organisations should consider creating an integrated risk and control organisation enabled by robotics, machine learning, artificial intelligence, and analytics to support across all the LOD. This will also help evolve from a traditional risk management approach, which was manual and reactive to a more mature and advanced set-up that is automated, predictive, and ensures near real-time monitoring.

> "Technology is disrupting business models, product definitions and business processes. For risk management to stay relevant, it would also need to re-invent itself using building blocks like AI, RPA, analytics, IOT as levers. ".
>
> **Anthony Crasto,**
> Partner, Deloitte India

8. **Use risk transfer instruments**
   Organisations will increasingly use risk transfer instruments, such as insurance, contracts, and novel financial instruments, to protect themselves from risks. Insurance coverage programmes include Cyber Liability Insurance Coverage (CLIC), to help organisations mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach or similar event. In healthcare, some of the largest medical device manufacturers are negotiating experimental deals with hospitals to take on performance-based financial risk for their implants. Risk-sharing agreements are structured such that the manufacturer returns a percentage of the device's price if it does not meet certain performance goals or fails within a set period.

9. **Accelerate adoption of analytics and automate**
   Risk management must prioritise adoption of advanced analytics. Inexpensive tools can be used for cleaning, organising, and analysing data. Alternative resourcing models that provide flexible access to the needed skills while building the in-house talent pool should be considered.

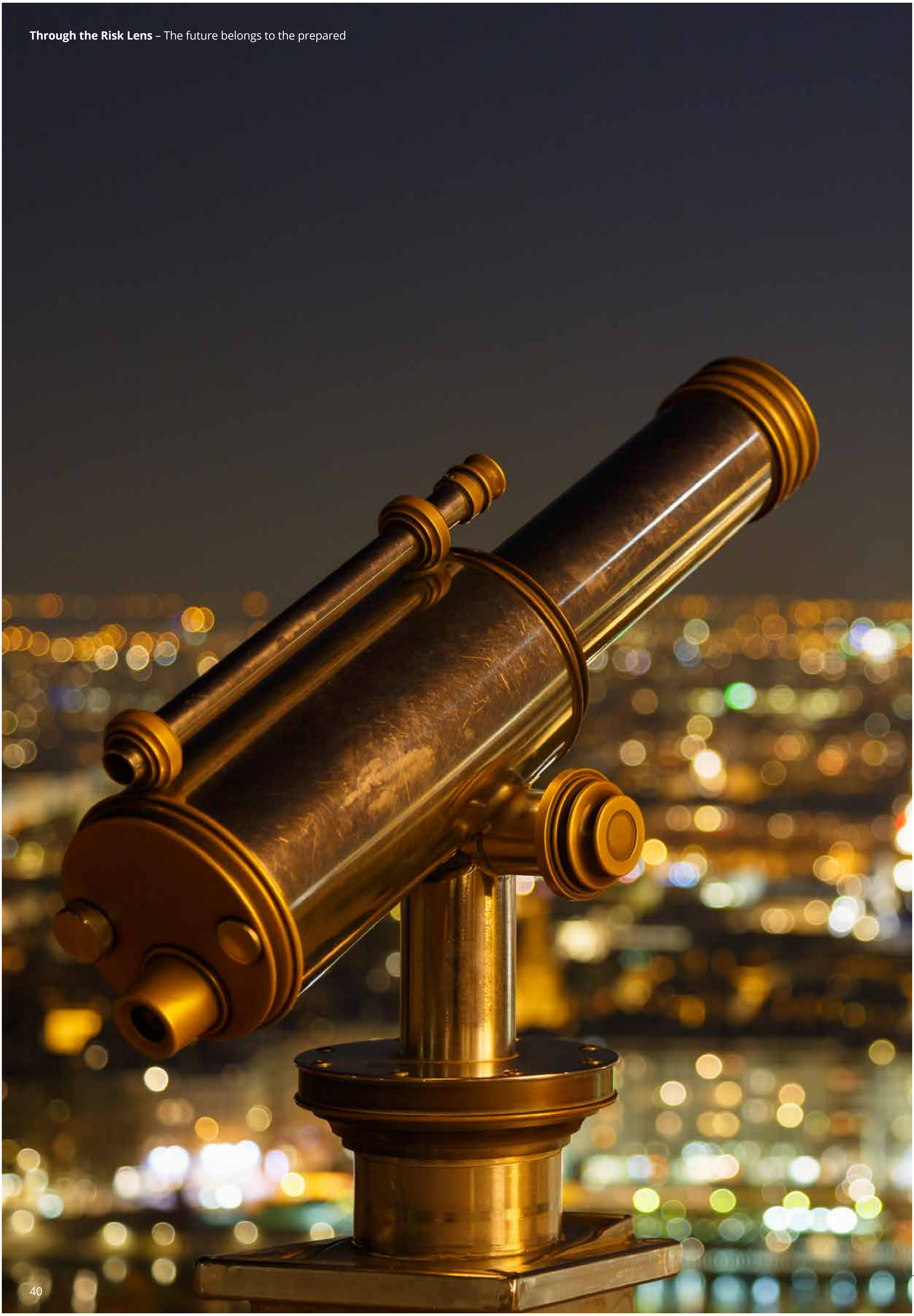
   Advanced analytics, coupled with RPA and real-time reporting mechanisms can enable the function to provide continuous assurance. Ideally, this will automated root-cause analysis of incidents to indicate behavioural and process patterns and solutions.

> "Digital technologies have disrupted the business by empowering customers through self-help tools and new ways of seeking information. The risk management often requires changes to suit the new environment, which trigger new types of risks including the data and digital risks. The rise of analytics require greater amount of inter-connectedness while negotiating the data and IT systems constraints. The internal control framework should be robust enough and designed to cover all new types of risks. The model can be optimised with constant check on the risk basket to build a most effective risk management framework."
>
> **Raman N**
> Head Internal Audit, Sundaram Finance

10. **Build a digitally proficient and risk intelligent workforce**
    Risk management professionals and employees must be trained to work with emerging technology and in new disciplines such as automation, blockchain, cybersecurity, cloud to manage the associated risks. It is also equally important for risk functions to cultivate digitally proficient talent to embed analytics, continuous control monitoring and new methodologies, and agile principles in risk management. Organisations need to improve the level of risk awareness and responsibility to improve the risk culture and create a risk intelligent workforce that complements its overall risk management strategy.

> “Days of having a strong perimeter for your enterprise with private cloud, data centres, firewalls, etc., are fading away very quickly and the new perimeter is going to be the identity”.
>
> **Giri Govindarajulu**
> CISO, Cisco APAC

In the past, risk management was often an exercise in fear and avoidance. The organisations’ primary focus was to complete the necessary, compliance-driven activities. While risks evolve at an unimagined pace and become more measurable and tangible, it is imperative for risk management functions to accelerate their evolution and view risks in terms of their potential to drive performance and value. The future of managing risk lies in the hands of businesses and forward-thinking risk managers who will ride the tide of change and convert risks into game-changing opportunities.



References and further readings

1. Millennial Insights for the 2020 Labor Market
2. Fortune, Artificial Intelligence Briefing dated Jan 10,2019
3. World Economic Forum, The Future of Jobs Report
4. The Indian Express, Future of Work in India Report
5. Deloitte Publications Suggested Further Reading
    A. Managing Risks in Digital Transformation
    B. Ensuring Regulatory Compliance
    C. Extended Enterprise Risk Management (EERM)
    D. Enterprise Risk Management (ERM) A 'Risk-Intelligent' Approach
    E. Risk Sensing The (evolving) State of Art
    F. Risk Management For and By the BOT, Secured BOT series
    G. Next Wave of Continuous Control Monitoring (CCM) Solution
    H. Risk and Controls Centre of Excellence
6. William D Eggers et al., The Future of Regulation
7. Mohit Mehrotra et al., Accelerating Digital Ecosystem Development through Strategic Alliances (Deloitte Monitor Analysis)
8. Will Engelbrecht et al., Strategic alliances: An essential weapon in the growth arsenal (Alliance Best Practices)
9. The News, Meeting the Millennial Challenge
10. Deloitte Global Risk Management Survey 11th Edition
11. Deloitte's 2018 Global Chief Audit Executive Research Survey
12. Jeff Schwartz et al., What is the future of work?
13. Jeff Schwartz et al., The Future of the Workforce Critical Drivers and Challenges
14. Jeff Schwartz et al., Future of Work Forces of Change
15. Nancy Albinson et al., The Future of Risk, New Games New Rules
16. Nancy Albinson et al., Future of Risk in the Digital Era
17. John Hagel III et al., Patterns of Disruption Series
18. Will Engelbrecht et al., Strategic alliances: An essential weapon in the growth arsenal
19. Terry Hatherell et al., The future of audit is now
20. Emily Mossburg et al., Value Based Data Risk Management, Deloitte Publication
21. Deloitte Extended Enterprise Risk Management Global Survey 2019

Contacts

Rohit Mahajan
President Risk Advisory
rmahajan@deloitte.com

Gaurav Shukla
Partner, Deloitte India
shuklagaurav@deloitte.com

Anthony Crasto
Partner, Deloitte India
acrasto@deloitte.com

Sandeep Sarkar
Partner, Deloitte India
sarkars@deloitte.com

Ramu N
Partner, Deloitte India
ramun@deloitte.com

Primary Contributors

Santosh Kumar

Johar Batterywala

Deepa Seshadri

Afshan Khayum

Deepti Berera

Rati Acharya

Prachi Ranavat

Ira Gopal

Ankita Chawla

Kinan Zahed

Anisha Lalwani

Deloitte.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.