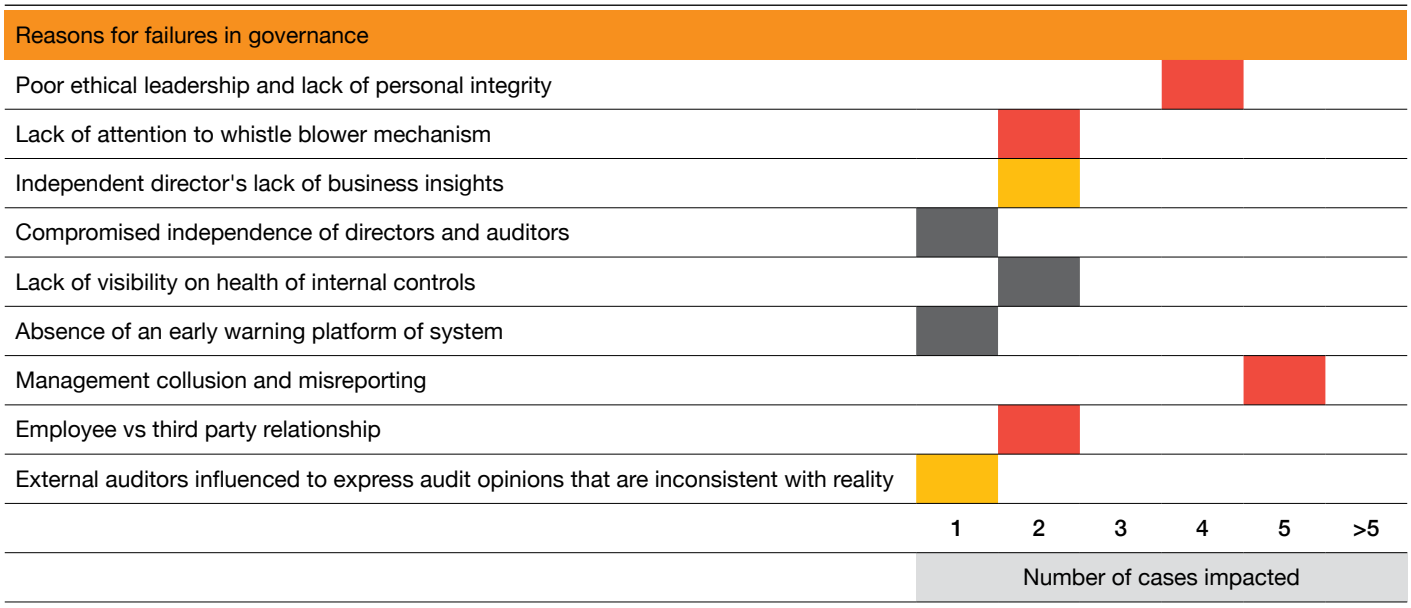
The future of business risk management

pwc

The increasing rate of failure in corporate governance in the business world is worrisome. Moreover, pressure to meet growth targets, personal aspirations, all-pervasive disruptions and the desire to paint a rosy picture to stakeholders are some of the pressure points businesses and business leaders are facing today.

A quick analysis of major corporate failures in the last couple of years provides some interesting insights.



Colour key for the diagram:

Low financial impact | Medium financial impact | High financial impact

Source: Primary research conducted by PwC India on the basis of recent media reports on failure in corporate governance in India, 2019

Today, most instances of failure and fraud in India's corporate world include:

- Misreporting (over and under reporting) of key indicators of performance in business (e.g. sales, margins, ROI and capital project cost etc.)
- Misappropriation of company funds by employees and third parties (e.g. suppliers, customers and service providers)
- Theft of intellectual property and trade secrets
- Mis-statements in financial accounting (e.g. loans disguised as sales, showing an increase in the reasonable expected life of assets, and inflation of the value of assets)
- Misappropriation of assets (e.g. skimming cash and misusing company assets)
- Manipulation of stock price using cartel or insider information
- Theft of cash, physical assets and/or confidential information
- Bribery and corruption
- Consumer fraud (e.g. bogus telemarketing and emails, Ponzi schemes, phishing, theft of ID and other schemes)

When speaking of governance, we generally refer to the qualitative and quantitative aspects of governance. 'Qualitative' refers to the culture, ethics framework, organisational structure, etc. of a business and 'quantitative' to measures including internal controls, compliance and audit.

While governance is not at a very high level of maturity in many corporates in India, a great advantage in the current environment is that businesses are becoming highly digitised and data-driven, which makes it easier for them to adopt technology-driven governance frameworks.

Implementation of a 'digitally enabled risk intelligence map' should enable assessment of quantitative aspects of governance in a holistic manner.

A digital risk intelligence map (DRIM) provides a single window view of the risk profile of an organisation, and is collated on the basis of a risk indicator-related assessment of various parameters across diverse functions and the types of risks to which an organisation is vulnerable.

This means that the entire organisational data of an organisation, including related external data points, comes together on a platform that hosts and analyses the data to publish a single dashboard with drill-down capabilities, which highlights the occurrence of risk across the Board.

However, this is easier said than done, since the exercise necessitates multiple steps being taken in a structured manner to arrive at this conclusion.

Gain an understanding of risk-related dimensions applicable to the industry and across business functions

The dimensions could include internal controls, fraud, compliance, security, financial reporting, and regulatory and strategy-related issues. For example, how critical is its cyber security risk to an organisation and which of its specific functions (e.g. customer profile and employee data or product platforms) are the most susceptible to such risks needs to be assessed.

Understand how such risks can be quantified

This means defining the key risk-related indicators that can assess and quantify the risks identified at step 1. For example, there may be several indicators of the bad credit portfolio of a bank, ranging from its default rate, early conversion of loans into NPA ratio, overexposure of its loan portfolio to a specific industry, segment or product, or frequent degrading of credit ratings in its loan portfolio.

Therefore, in such an exercise, care needs to be taken to select the indicator that represents the risk in the best possible manner and is not arbitrary.

Map data points and sources for risk indicators

This is a qualitative and quantitative assessment, where it is not just necessary to identify the data points, but to also rate the quality of data available. This may result in identification of key risk indicators (KRIs) when no data is currently in the process of being captured. However, it can become an input for an organisation to begin capturing such data to enable monitoring of its KRI.

Understand the design of outcomes and implementation of DRIM

This involves developing a technical blueprint of the entire IT architecture of an organisation, including its billing, delivery and banking or collection systems; online portals, accounting systems and external feeds to understand how all disparate or integrated systems can be connected to extract relevant data and use this for analysis.

Blueprinting includes a functional blueprint of the design of the outcome an organisation wants to implement. It enables an enterprise to remain focused on achieving its end results, e.g. the form and shape of its risk intelligence map or what exactly its KRI on its credit risk concentration will look like in the dashboard.

Implement database and analytics framework

A well-designed data architecture for risk analytics not only helps organisations manage risk, but also enables them to gauge their business growth and cost management opportunities. For example, a database with an accumulation of customer-related data to assess completeness of information for KYC-related purposes and customers' credit card spending-related data gathered for fraud analytics can also be utilised to categorise customers in various segments and be linked with their credit card spending pattern. In addition, it will enable organisations to analyse whether those who generally opt for zero interest EMIs can be offered 'alliance partner' products in the same category in which customers are most likely to spend.

Some important technical aspects to be considered at this step:

- Ensuring integrity and completeness of data
- Following strong standards to model, script or query data to ensure efficient and accurate implementation of the code
- Putting in place a framework that enables real time risk monitoring
- Choosing the right tools for analytics and the agile environment that supports continuous upgrading and enhancement (cloud and emerging advanced analytics platforms such as 'data lake' and predictive analytic tools)
- Engaging people who understand data, business, risk and analytics

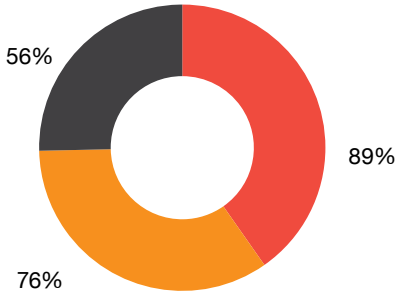
Action required

Generating analytical outcomes is an important goal that needs to be achieved, but it is of no use if it is not assigned to the right people who will take the right action. For a risk intelligence map to be effective for an organisation, it is not only the CRO, CAE or CFO who should be responsible, but people who can work on KRI outcomes to mitigate such risks should be also be given this responsibility. The KPIs of such people need to reflect the relationship of such responsibility with the carrot and stick method. For example, a mitigation measure for a KRI (such as billing-related errors) may require a system or ERP configuration upgrade, so there is no need to track and ensure that action is taken in time.

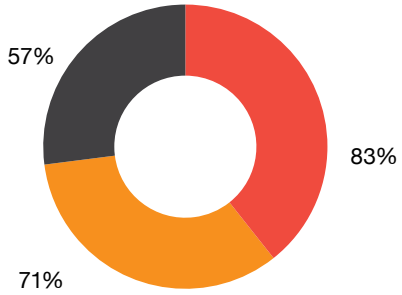
The dynamic nature of risk needs to be countered with proactive mitigation strategies that will be triggered by predictive risk identification and application of control monitoring frameworks. Such frameworks will align risk stakeholders and enable them to work in parallel with business to mitigate organisations' operational risks and achieve their goals. In this case, embedding advanced analytics is pivotal for risk-related decision-making, and involves utilising machine learning and Artificial Intelligence (AI) on data from internal or external sources.

Organisations with dynamic risk functions have distinct advantages.

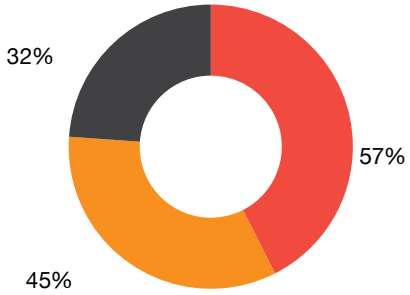
Effective at managing risks on digital journey



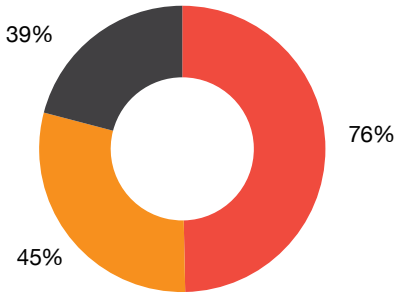
Ahead of or on track with digital roadmap



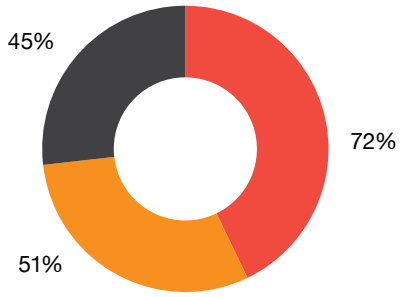
Willing to take on more risk than in the past



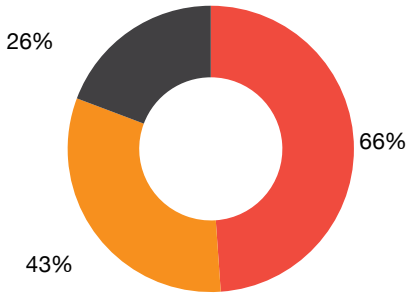
Meeting or exceeding expectations of enhanced decision-making



Meeting or exceeding expectations of improved customer experience



Meeting or exceeding expectations of revenue growth



Dynamics Actives Beginners

Source: PwC Governance Insights Centre

This then requires monitoring by a CRO or CAE to ensure that their actions are steered in the right direction and show systemic improvement over a period.

This is a journey of continuous improvement and evolution, so one should not think that once these steps are taken, the journey is over

In fact, in this dynamic world, with disruption everywhere and in everything (including businesses and the way they manage their risk needs to evolve), there is a need for organisations to look at new areas of risks, the different dimensions of data. Moreover, they should give continuous thought to the parameters incorporated in the framework given above, e.g. a disrupting technology that enables customers to use everything on a need basis instantaneously at a significantly reduced cost and superior convenience rather than buying and owning a product which may not be a risk today, but could be one tomorrow. But such steps can only be taken when such issues appear on the horizon and thereafter find their place on a business risk intelligence map.

Some leading corporates have begun taking steps in this direction, but their approach varies, based on their level of maturity in areas including data, digitisation, and availability of resources, skills and priorities.

Maturity level	Initiated	Expanded	Mature
Use of technology	Continuous monitoring of business risks through analytics	Continuous monitoring combined with predictive analytics for high risk areas	Sophisticated early warning system/ Digital Risk Intelligence map enabling real time and proactive monitoring of business risks (internal and external)
Coverage	Internal business operational and financial risks	Internal business: operational and financial risks	Internal and external risks to business (operational, financial, compliance and strategic)
Data	Primarily ERP data	All internal data sources (ERP and customised systems)	Internal and external data sources
Initiator/Implementer	Head of Audit/CRO initiated	Head of Audit/CRO initiated	CEO/CFO/CRO/Head of Audit
Owner – business risks	Second line of defence (Risk Management/Controllership functions)	Second line of defence (Risk Management/Controllership functions)	Business functions and process owners
Owner – red flags	Head of Audit/Head of Forensics	Head of Audit/Head of Forensics	Head of Audit/Compliance/Forensics
Enabler	CIO	CIO	Chief Digital Officer
Benefits	Continuous identification of critical lapses in controls, revenue or cost leakage to enable business to take immediate action Increased assurance to the board and the management on managing risks	Continuous identification of critical lapses in controls/revenue or cost leakage to enable business to take proactive action Proactive handling of critical failures through predictive analytics Increased assurance to the board and the management on managing risks	Real time and proactive monitoring of critical business risks Aggregated view of business risks High level of assurance to the board and the management on managing risks
Real life cases	A large multinational in the retail and consumer space identifies multi-million dollars' worth of revenue and cost leakages, remediates issues as and when they occur, and in some cases, systemically 'fixes' and improves systems.	A global insurance company monitors critical risks across its functions, proactively detects potential fraudulent policies and claims it prevents such transactions before final processing.	A large multinational bank gains an integrated view of risk across its business, functions and risk dimensions, supported with key risk indicator-related quantification; is able to take proactive action to prevent serious failures in its business across various dimensions, including NPA, liquidity, cyber and credit risks in time.

To conclude, while you may or may not feel confident about treading this path, you will soon realise that managing risks in the traditional way will be outdated and rendered completely ineffective in the near future (e.g. if one had to adopt measures to monitor risk that were used 20 years ago, would this be acceptable?). So we need to remember that the future is approaching fast, and it is better to prepare ourselves in time to meet it head on.

56%

CAEs are concerned that their failure to adopt technology in their assessment of risk and controls will diminish their value to their organisations.

18%

CAEs are usually using technology effectively in their functions.

75%

Those using technology effectively deliver better quality of output.

Source: PwC Global CAE survey 2018

How PwC can help you on this journey

PwC offers integrated solutions that embed industry, risk and technology intelligence and capabilities that can serve your needs holistically and help you build a digital risk intelligence platform in your company.

Contact us for more details and discussions.

Contributed by

Shreyans Dudheriya
Executive Director and Leader – Risk Analytics | Risk Assurance Services | PwC India
M: 9717007225
E: Shreyans.dudheriya@pwc.com

Prashant Nagwanshi
Director- Risk Assurance Services | PwC India
M: +91 9717397505
E: prashant.nagwanshi@pwc.com

Supported by

Kaushal Dugar
Manager- Risk Assurance Services | PwC India
M: 9899715839
E: kaushal.dugar@pwc.com

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune.

For more information about PwC India's service offerings, visit www.pwc.com/in

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

pwc.in

Data Classification: DC0

SG/May2019-17562