Risk management report

The risk management report discusses various dimensions of our enterprise risk management function. The risk-related information outlined in this section may not be exhaustive. The discussion may contain statements that are forward-looking in nature. Our business is subject to uncertainties that could cause actual results to differ materially from those reflected in the forward-looking statements. If any of the risks materializes, our business, financial conditions or prospects could be materially and adversely affected. Our business, operating results, financial performance or prospects could also be harmed by risks and uncertainties not currently known to us or that we currently do not believe are material. Readers are advised to refer to the detailed discussion of risk factors and related disclosures in our regulatory filings, and exercise their own judgment in assessing risks associated with the Company.

A. Overview

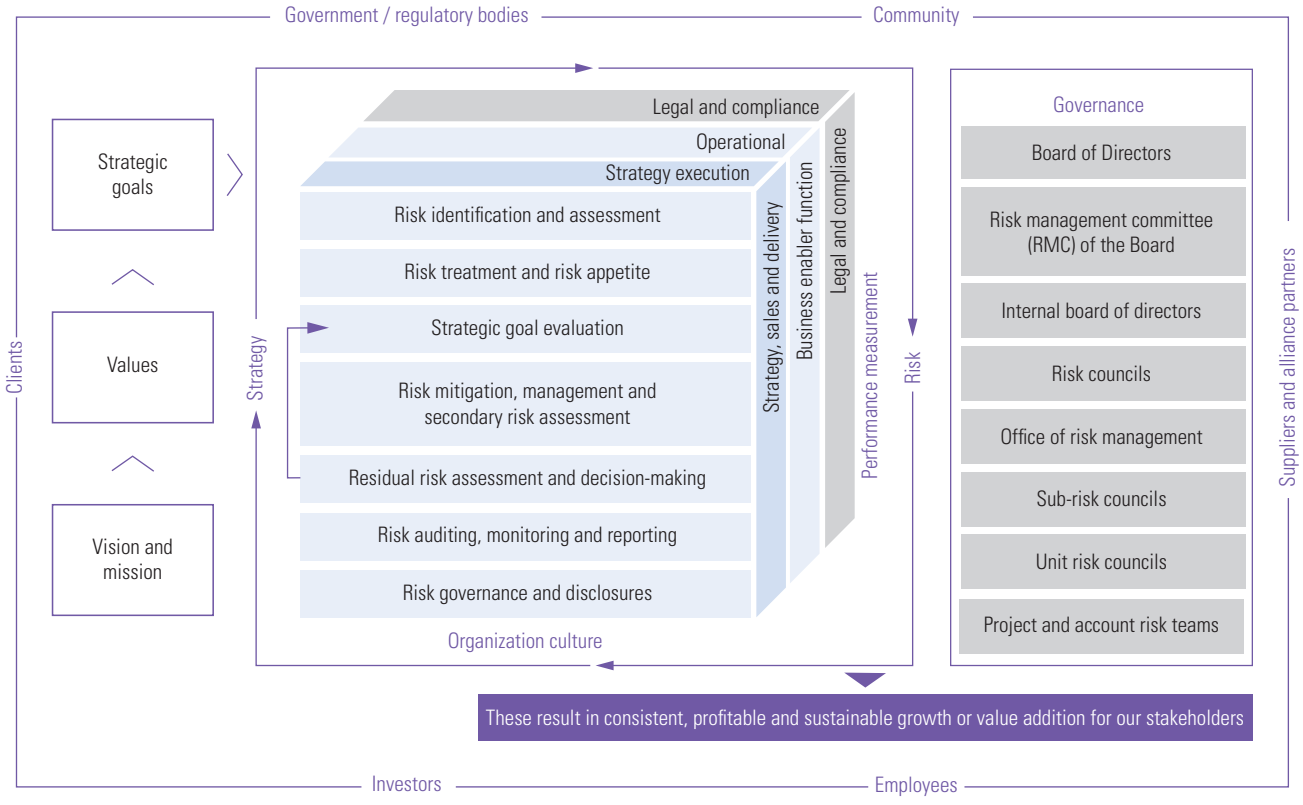
The Infosys Enterprise Risk Management (ERM) function enables the achievement of strategic objectives by identifying, analyzing, assessing, mitigating, monitoring and governing any risk or potential threat to these objectives. While achievement of strategic objectives is the key driver, our values, culture, obligation and commitment to employees, customers, investors, regulatory bodies, partners and the community around us are the foundation on which our ERM framework is developed. Systematic and proactive identification of risks and mitigation thereof enable effective or quick decision-making and boost the performance of the organization. The ERM function is a decision-enabler which not only seeks to minimize the impact of risks but also enables effective resource allocation based on the risk impact ranking and risk appetite. Strategic decisions are taken after careful consideration of primary risks, secondary risks, tertiary risks and residual risks.

Our ERM framework encompasses all the risks that the organization is facing under different categories, such as strategic, operational, and legal and compliance risks. Any of these categories can have internal or external dimensions. Hence, appropriate risk indicators are used to identify these risks proactively. We take cognizance of risks faced by our key stakeholders and their cumulative impact while framing our risk responses.

B. Key components of Infosys Enterprise Risk Management Framework

We have adopted an integrated ERM framework that is being implemented across the organization by the risk management office. The framework is based on international standards and tailored to suit our business needs.

Infosys Integrated Enterprise Risk Management Framework



Risk categories: Our industry and Company are in significant transformation, and this has naturally resulted in the heightening of risks related to strategic choices and strategy execution along with traditional operational and compliance-related risks.

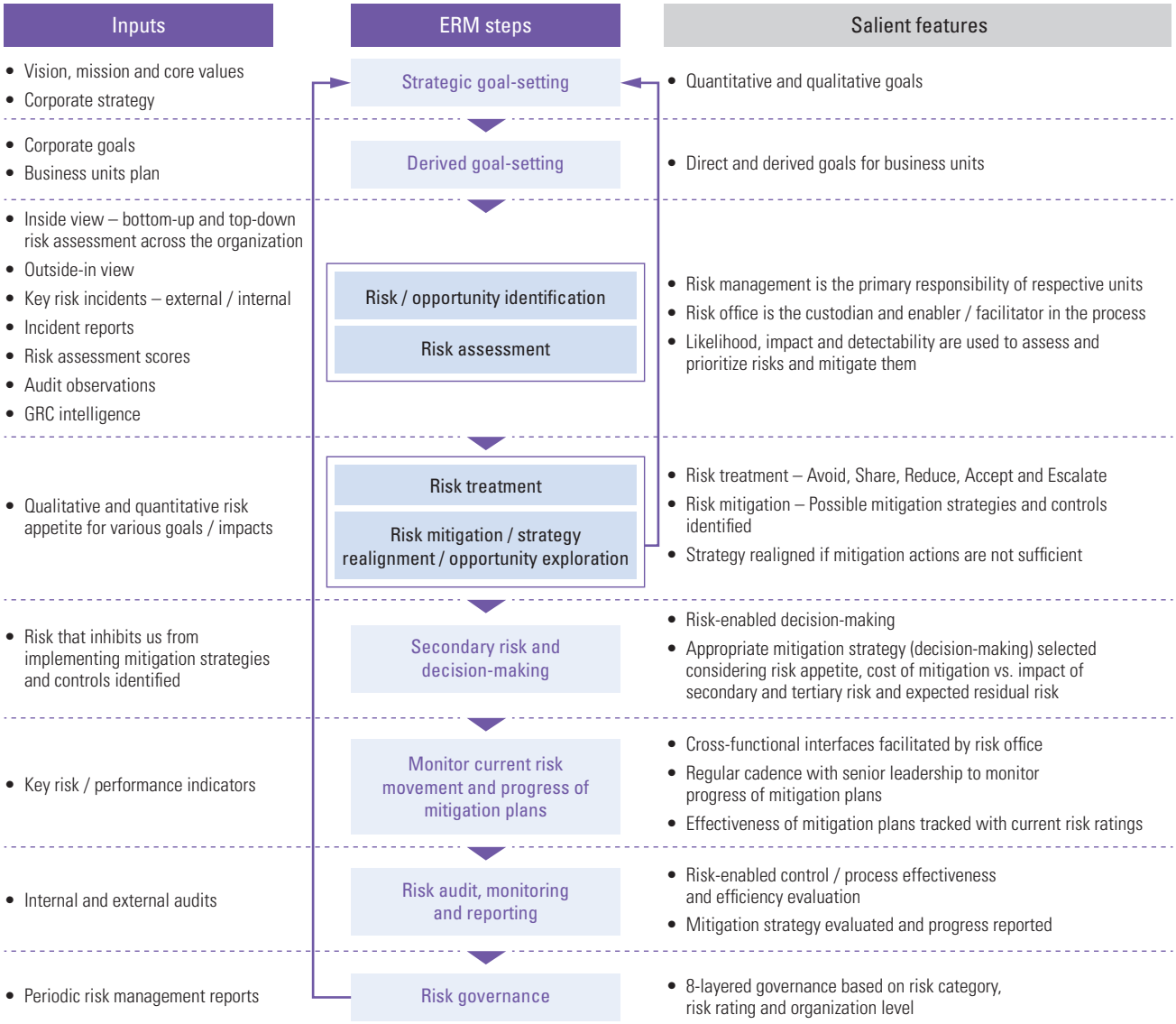
Strategy and strategy execution: Risks arising out of the choices we have made in defining our strategy and the risks to the successful execution of these strategies are covered in this category – for example, risks inherent to our industry and competitiveness are analyzed and mitigated through strategic choices of target markets, the Company's market offerings, business models and talent base. Details of the Company's strategy are described in other sections of this document.

Operational: Risks arising out of internal and external factors affecting policies, procedures, people and systems in our support functions, thereby impacting service delivery or operations, compromising our core values or not in accordance with generally accepted business practices are covered in this category – for example, risks of inefficiencies in internal processes, risks of business activity disruptions due to natural calamities, terrorist attacks or war or regional conflicts, or disruptions in telecommunications, system failures, virus attacks or breach of cybersecurity.

Legal and compliance: Risks arising out of threats posed to our financial, organizational, or reputational standing resulting from potential litigations, violations or non-conformance with laws, regulations, codes of conduct or organizational prescribed practices or contractual compliances are covered in this category along with potential risks arising out of major regulatory / geopolitical changes or risks arising out of strategic or business or operational decisions.

Risk management processes: Our ERM framework defines the steps to identify, assess and mitigate risks. Secondary risks and residual risks are also used as key inputs for deciding the mitigation strategies.

Infosys Integrated Enterprise Risk Management Framework



Risk governance : We have adopted a multi-level governance structure to monitor and report risks and risk mitigation activities. Critical risks or cross-functional risks at each level are escalated to the next level in the governance structure. Critical risks under different categories of risks at the Group level are reviewed by the Chief Executive Officer, Chief Operating Officer, Chief Financial Officer, Chief Risk Officer and General Counsel in various councils. Critical risks from these councils are presented to the Internal Board of Directors and then to the risk management committee of the Board on a quarterly basis.

Risk governance structure

Board of Directors

Comprises members of the Board of Directors	• Evaluate the strategy, and risks inherent in the strategy • Define the role of the Board and the risk committee in risk management • Assess the risk-taking abilities of the Management and performance *vis-à-vis* short-term and long-term objectives of the Company

Risk management committee of the Board

Comprises four independent directors : • D.N. Prahlad, Chairperson • Kiran Mazumdar-Shaw • Michael Gibbs • D. Sundaram	• Oversee corporate governance with regard to the risk management process • Monitor and review the risk management framework and associated practices of the Company • Understand the most significant risks and response strategies • Review risk-related disclosures

Internal board of directors

Comprises two directors: • Salil Parekh • U.B. Pravin Rao	Responsible for providing internal governance and oversight, and ensuring smooth functioning of various risk councils

Risk councils

Comprises the Chief Executive Officer, Chief Operating Officer, Chief Financial Officer, Chief Risk Officer and General Counsel	• Cadence or oversight on risk management process • Review adequacy, progress and effectiveness of mitigation actions

Office of risk management

• Headed by the Chief Risk Officer • Comprises the core ERM team and a network of risk managers from business units along with specialist groups	• Formulate and deploy risk management policies and procedures • Facilitate the execution of risk management practices • Provide periodic updates to the risk council and quarterly updates to the RMC on risks to key business objectives and their mitigation • Work closely with mitigation action owners in deploying mitigation measures and monitoring their effectiveness

Sub-risk councils

• Headed by the respective function risk anchor • Comprises representatives from services and segments or enabler function risk anchors	Responsible for identifying and mitigating the risks for their respective function / group.

Unit risk councils

• Headed by unit risk anchors • Comprises business unit heads, unit planning and assurance head and unit HR	• Ensure proactive identification and management of risks / opportunities in their respective units • Ensure effectiveness of risk mitigation actions in their units and report to appropriate sub-risk council

Project or account risk team

Comprises project compliance anchors, project risk managers, project and delivery manager or master customer owner	• Adhere to risk management policies and procedures • Proactively identify risks in the project execution or in accounts, and report to concerned risk managers in a timely manner • Implement prescribed risk mitigation actions

C. Risk Library

The Office of Risk Management has defined a multi-layered risk register. At the highest level, risks to achieving the Company's strategic goals of Scaling Agile Digital and Energizing the Core and to ensuring organizational hygiene (pertaining to effectiveness, efficiency, security, integrity, compliance and governance) are captured. These risks are further broken down into various sub-risks specific to strategic initiatives, processes or functions. Further down the risk register hierarchy are risks pertaining to sub-processes, and control risks.

Quantitative exposure from risks at various levels are aggregated to assess the overall risk exposure of the Company. This hierarchy ensures that there is one common risk library across the Company.

The common risk register is enabled on the Company's iGRC technology platform as explained in the next section.

D. RISC360 integrated risk and auditing platform

RISC360 is the Company's Governance, Risk management and Compliance (GRC) program that combines three lines of defense under one umbrella to enable risk-based decision-making and auditing. The Company has implemented a technology platform, iGRC, to support the program. The iGRC platform gives a consolidated view of strategic goals and associated risks to the leadership to enable quick and effective decision-making across enterprise risk, internal audit, compliance to the Sarbanes-Oxley Act (SOX) and corporate audit. Integration of these functions using one common platform ensures that audits are based on risks tied to the overall ERM framework and the organization gets the benefits of synergies amongst different lines of defense.

E. Risk management highlights for the year

During the year, our focus was on extending adoption of the integrated ERM framework across the organization and strengthening the risk management program.

As part of monitoring key risks, the risk management office :

- Assessed our business momentum relative to competition and competitive position in key market segments comprising geographies, industries and service lines
- Regularly assessed the progress of the execution of strategic programs, specifically the progress on US localization, the growth of digital services, impact of automation, talent fulfilment / forecasting, subsidiary businesses performance, enhancement of traditional offerings, and leadership succession planning
- Regularly assessed the business environment, including trend line of key external indicators and internal business indicators such as client concentration, client technology spend, growth of top clients and revenue bookings from large outsourcing engagements. Reviewed risks in new countries before business penetration
- Reviewed and assessed risks associated with customer contract management process
- Reviewed information security risks (cyber attacks and threat intelligence) and privacy related risks in GDPR. It continued to monitor the progress of mitigation actions
- Reviewed key operational risks and actions based on inputs from the internal risk register, external assessments, internal audit findings and incidents
- Reviewed operational risk areas including client service delivery, retention and engagement of employees, reskilling of employees, brand attractiveness, women's safety, physical security, capital expenditures on infrastructure, and business continuity management
- Monitored key developments (such as Brexit, changes to immigration laws, minimum wages, and impact to the businesses of our clients) in the regulatory environment, especially in key geographies such as the United Kingdom, continental Europe, Australia and the United States of America
- Monitored the availability of natural resources, such as water and power, and its impact on our operations.