

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) 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 boosts the performance of the organization. The ERM unit functions as a decision-enabler which not only seeks to

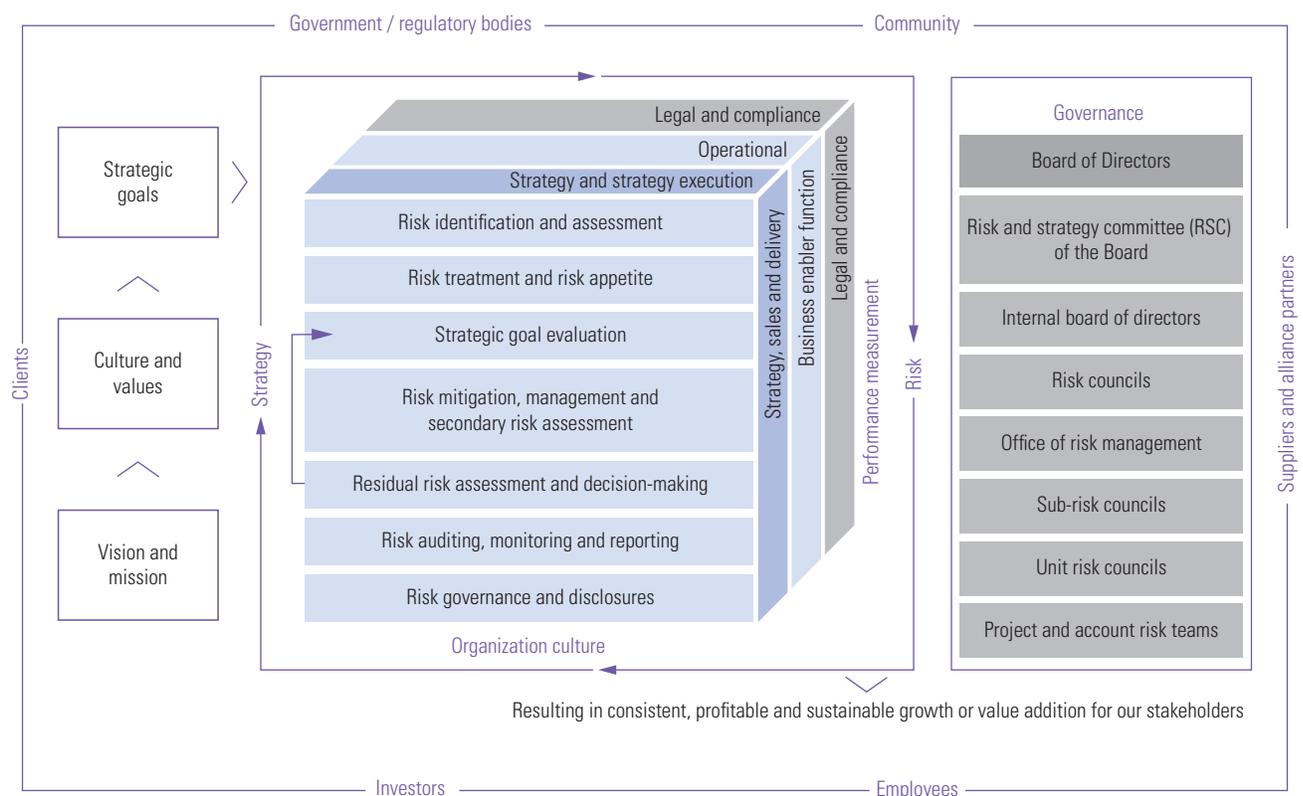
minimize the impact of risks but also enables effective resource allocation based on the risk impact ranking and risk appetite. Strategic decisions are taken after careful consideration of risks based on secondary risks and residual risks.

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 the multiplied impact of the same while framing our risk responses.

B. Key components of Infosys Enterprise Risk Management program

Framework: We adopted a new integrated ERM framework that is being implemented across the organization by the risk management office. The new 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.

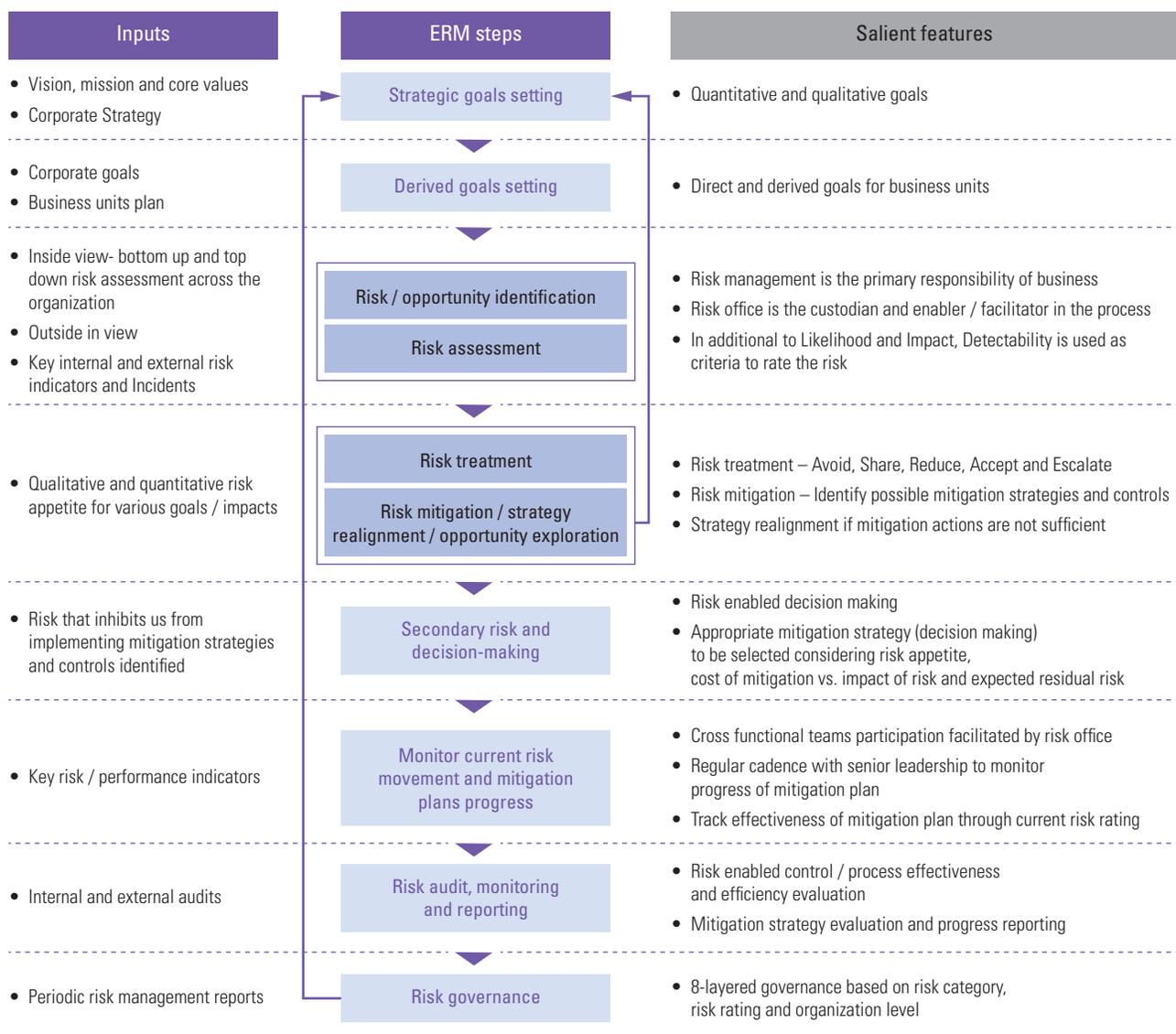
Operational: Risks arising out of internal and external factors affecting policies, procedures, people and systems in our support functions, thereby impacting service delivery / operations, compromising our core values or not in accordance

with generally accepted business practices are covered in this category – for example: 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 cyber security.

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: The Infosys ERM framework defines risks and the steps to identify, assess and mitigate risks. Secondary risks and residual risks are used as key inputs for deciding the mitigation strategies.

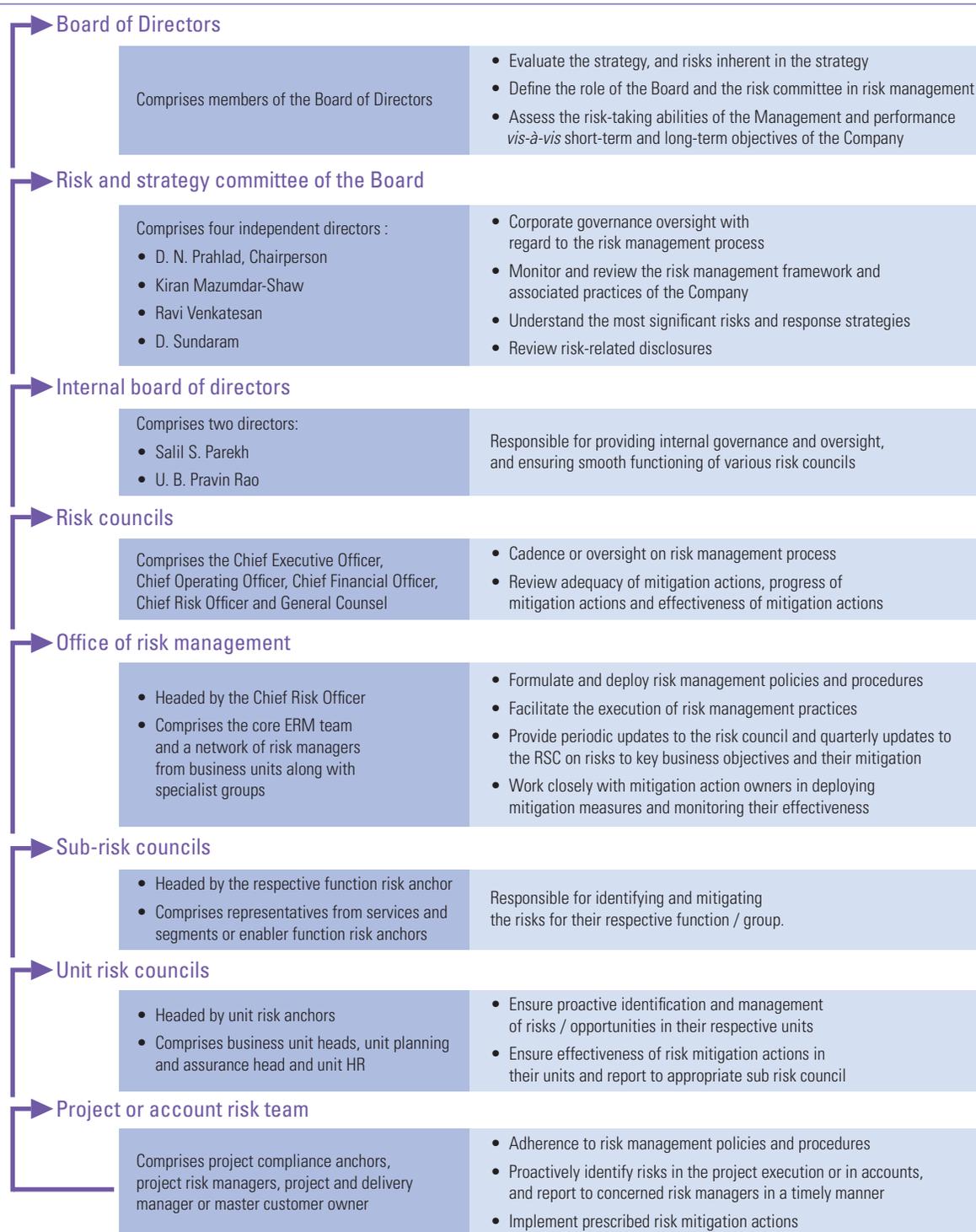
Infosys Integrated Enterprise Risk Management Framework



Risk governance structure: Risks identified by risk management functions or roles at different levels in the organization are presented at appropriate councils in the governance structure. 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 and strategy committee of the Board on a quarterly basis.

Risk governance structure



C. RISC360 integrated risk and auditing platform

RISC360 is a common Governance, Risk management and Compliance (GRC) platform that combines three lines of defense under one umbrella to enable risk-based decision-making and auditing. The iGRC platform gives a consolidated risk and strategic goal view to the leadership to enable quick and effective decision-making across enterprise risk, internal audit, Sarbanes-Oxley Act (SOX) compliance 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.

D. Risk management highlights for the year

During the year, our focus was on extending adoption of the new 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, progress on US localization, the growth of new software-enabled services, impact of automation, performance of subsidiary businesses, enhancement of traditional offerings, leadership succession planning, operating cost optimization and capital allocation policy.
- 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 information security risks (cyber-attacks and threat intelligence) and continue 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 in the regulatory environment, especially key geographies such as the United Kingdom, continental Europe, Australia and the United States of America, relating to immigration laws, minimum wages and impact to businesses of our clients.
- Monitored the availability of natural resources, such as water and power, and its impact on our operations.