Risk management report

The risk management report discusses various dimensions of our enterprise risk management. 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. 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

Our Enterprise Risk Management (ERM) framework encompasses practices relating to the identification, analysis, evaluation, treatment, mitigation and monitoring of the strategic, operational, and legal and compliance risks to achieving our key business objectives. ERM at Infosys seeks to minimize the adverse impact of these risks, thus enabling the Company to leverage market opportunities effectively and enhance its long-term competitive advantage. →

Several risks can impact the achievement of a particular business objective. Similarly, a single risk can impact the achievement of several business objectives. The focus of risk management is to assess risks and deploy mitigation measures. This is done through periodic review meetings of the risk and strategy committee of the Board.

Our core values and ethics provide the platform for our risk management practices. ↓

B. Key components of the Infosys risk management framework

1. Risk governance structure

Our risk management framework is implemented at various levels across the enterprise. The key roles and responsibilities regarding risk management in the Company are summarized as follows:

Level	Key roles and responsibilities
Board of Directors (Board)	• Approving key business objectives to be achieved by the Company. Ensuring that the executive management focuses on managing risks to key business objectives • Reviewing the performance of the risk and strategy committee
Risk and Strategy Committee (RSC)	• Comprises six independent directors : – Ravi Venkatesan, *Chairperson* – Kiran Mazumdar-Shaw – Roopa Kudva – Prof. John W. Etchemendy – Dr. Punita Kumar-Sinha – D. N. Prahlad • Corporate governance oversight with regard to the identification, evaluation and mitigation of strategic, operational, and legal and compliance risks • Monitoring and approving the risk management framework and associated practices of the Company • Reviewing and approving risk-related disclosures
Project teams and individuals	• Adhering to risk management policies and procedures • Implementing prescribed risk mitigation actions • Reporting risk events and incidents in a timely manner

Level	Key roles and responsibilities
Risk council (RC)	• Comprises the Chief Executive Officer, Chief Operating Officer, Chief Financial Officer and Chief Risk Officer • Oversight of risk management practices, including identification, impact assessment, monitoring, mitigation, and reporting • Reviewing enterprise risks to the achievement of business objectives periodically, initiating mitigation actions, identifying owners for mitigation actions, and reviewing progress of mitigation actions • Formulating and deploying risk management policies and procedures • Providing updates to the RSC and the Board from time-to-time on the enterprise risks and actions taken
Office of Risk Management (ORM)	• Headed by the Chief Risk Officer • Comprises a network of risk managers from business units and specialist groups • Facilitating the execution of risk management practices in the enterprise, in the areas of risk identification, impact assessment, monitoring, mitigation and reporting • Providing periodic updates to the risk council and quarterly updates to the RSC on risks to key business objectives and their mitigation • Working closely with business units, business enabling functions and mitigation action owners in deploying mitigation measures and monitoring their effectiveness • Working closely with internal audit, business continuity management services, information security, intellectual property and quality audit teams for identifying, monitoring, and mitigating operational risks
Unit risk managers	• Ensuring units are managed in accordance with the Company's risk management practices • Ensuring compliance with risk management policies and procedures laid out by the Company in their respective business units • Managing risks concomitant with the business decisions relating to their unit, span of control or area of operations • Ensuring effectiveness of risk mitigation actions in their units • Reporting risk events and incidents relating to their unit in a timely manner

2. Business objectives

Our industry and company are in significant transformation, and this has naturally resulted in heightening of risks related to strategic choices, strategy execution along with traditional operational and compliance related risks. The business objectives of the Company are articulated as a set of specific near-term goals, and long-term strategic goals in a corporate scorecard. These goals cover the dimensions of consistent financial performance, market penetration, differentiation of our solutions, momentum of software-enabled services, operational excellence, cost optimization initiatives, attracting and retaining talent, and the long-term sustainability of the organization. In addition, progress of initiatives to mitigate the impact of potential changes to immigration and labor regulations in the United States and other countries are captured in the scorecard.

3. Risk categories

Our risk management framework considers the following broad categories of risks :

Strategy

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. Potential risks to the long-term scalability and sustainability of the organization are also analyzed and mitigated – for example, societal risks relating to the impact of our strategy on the environment, local communities, and conservation of essential resources.

We periodically assess risks to the successful execution of our strategy, such as the effectiveness of strategic programs that are being executed, the momentum in new initiatives, the impact of strategy on financial performance, leveraging of inorganic strategies, effectiveness of organization structure and processes, retention and development of high-performing talent and leadership.

Operational

Risks arising out of internal and external factors affecting policies, procedures, people and systems in our support functions thereby impacting service delivery, compromises our core values or not in accordance with generally accepted business practices or impacting their own service operations 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 violations or non-conformance with laws, regulations, codes of conduct or organizational prescribed practices or contractual compliances are covered in this category – for example, risks of potential litigations, breach of contractual agreement, non-compliance to regulations, potential risk arising out of major regulatory / geo-political changes, potential risk arising out of strategic or business or operational decisions.

4. Risk management processes

Our risk management practices are:

Risk identification, analysis, and evaluation

Mechanisms for identification of risks include annual risk surveys across the Company, industry benchmarking, periodic assessments of the business environment, incident analysis, findings of internal audits, discussions with the risk council and the risk and strategy committee and analysis of the Company's performance relative to the corporate scorecard goals. Risk analysis and evaluation are carried out using scenario-based assessments to decide the potential impact, likelihood of occurrence and in some cases, the detectability of the risk. Estimated risks are compared with established risk criteria and thresholds to determine the priority and method of risk treatment.

Risk treatment

Risk treatment is the process of selecting and implementing measures to alleviate the impact of identified risks.
- Avoid : A decision to nullify the risk by refraining from the activities that cause it
- Share : A decision to share the specific risk with another entity
- Reduce : A decision to reduce the level of risk through targeted mitigation, if not to completely nullify it
- Accept : A decision to allow the risk to remain as is, irrespective of its severity
- Escalate : A decision to escalate the risk to senior management

Risk mitigation and monitoring

Mitigation plans are finalized, owners are identified and the progress of mitigation actions are monitored and reviewed. The risk and strategy committee periodically does a deep dive into understanding the scope and effectiveness of mitigation plans and provides feedback to mitigation teams.

Risk-based approach to strategic planning

At Infosys, the functions of strategic planning and risk management are intertwined. Risks to achieving business objectives are key inputs to the formulation and development of strategy and business planning. Key strategic initiatives are identified to mitigate specific risks. This approach is practiced at various levels of the Company, such as in client account teams, project teams, support departments, and subsidiaries.

Risk reporting and disclosures

Dashboards help track external and internal indicators for each identified risk and assess its severity. The trend line assessment of top risks, analysis of exposure and potential impact are carried out periodically, presented and discussed with the risk council and risk and strategy committee. Key external and internal incidents are reported and reviewed at appropriate fora, such as the Information Security Council and meetings of the executive board. Risks relating to client project execution and client account-level risks are reported and discussed at appropriate levels within the Company. Periodic updates are provided to the Board highlighting key risks, their impact, and mitigation actions. Key risk factors are disclosed in regulatory filings.

C. Risk management highlights for the year

During the year, our risk management practices were primarily focused on the effectiveness of strategic programs in improving our competitive position and differentiation in market segments, the momentum of new initiatives to achieve our long-term business aspirations, our preparedness to address any incidents that may cause business disruptions to our physical and technological infrastructure, strengthening internal controls to detect fraudulent activity, leadership development, leadership succession planning, and monitoring possible impact of changes in our regulatory environment.

We carried out the following risk management activities during the last fiscal :

- Assessed and strengthened the enterprise risk management framework for further standardization of risk identification, assessment and governance of risks across the organization.
- Assessment of our business momentum relative to competition and competitive position in key market segments comprising geographies, industries and service lines were conducted and actions.
- Regularly assessed progress on the execution of strategic programs, specifically, progress on the growth of new software enabled services, impact of automation, performance of subsidiary businesses, leadership succession planning and operating cost optimization. Deep dive assessments were done in identified areas by members of the committee.
- 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 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, information security (cyber-attacks and threat intelligence), women's safety, physical security, succession planning, capital expenditures on infrastructure and business continuity management.
- Monitored key developments in the regulatory environment, especially of the United Kingdom 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.