Risk management report

"During the fiscal, businesses around the world, including ours, faced several macro risks such as the continued impact of the pandemic, geo-political events in Eastern Europe, tightening of supply chains, demand for talent and inflation. Our enterprise risk management processes were instrumental in keeping the Company focused on our most important priorities toward all our stakeholders."

Deepak Padaki
EVP and Group Head – Corporate Strategy, and Chief Risk Officer

Note: 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.

Our Enterprise Risk Management (ERM) function enables the achievement of the Company's strategic objectives by identifying, analyzing, assessing, mitigating, monitoring and governing any risk or potential threat to these objectives. While this is the key driver, our values, culture and commitment to stakeholders – employees, customers, investors, regulatory bodies, partners and the community around us – are the foundation for our ERM framework.

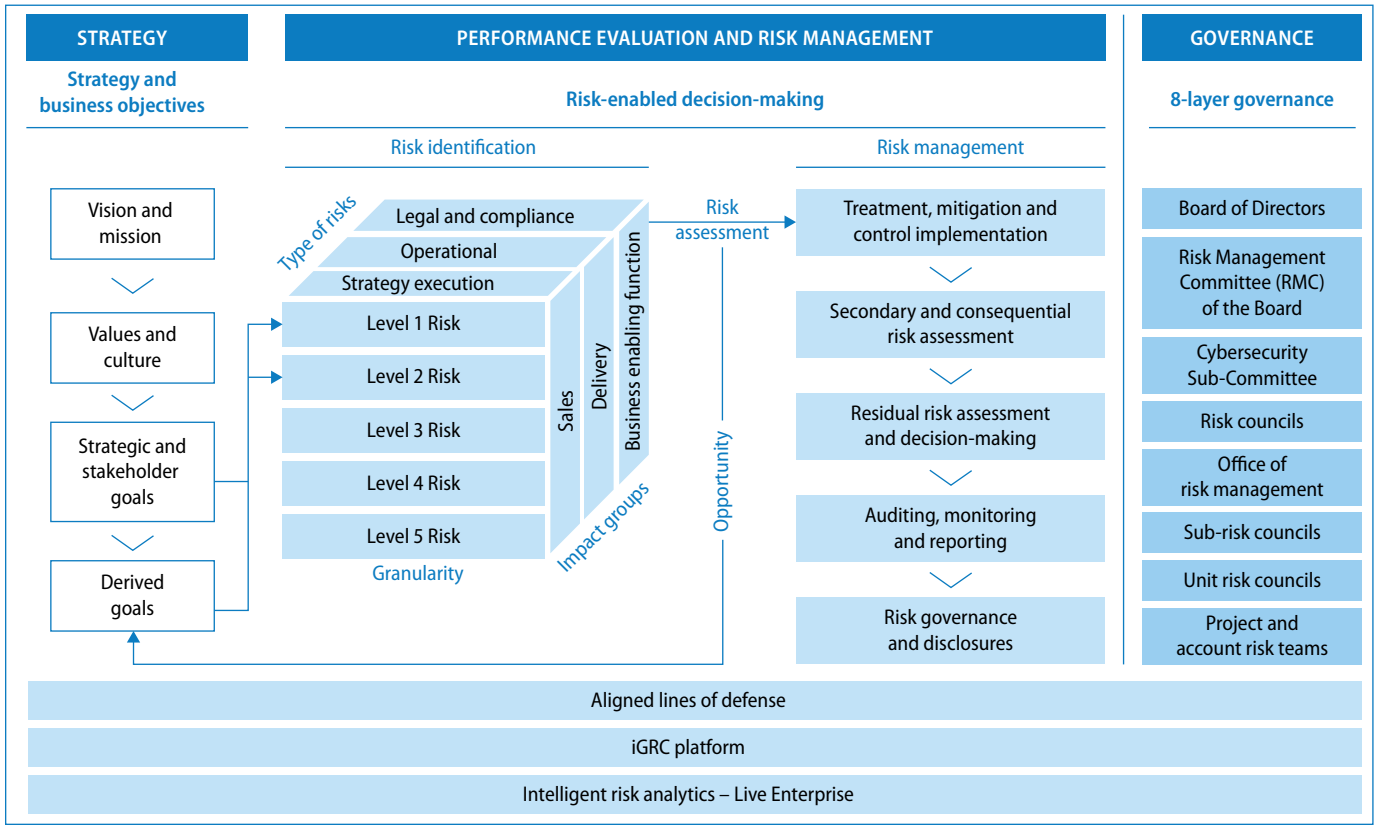
The systematic and proactive identification of risks, and mitigation thereof, enables our organization to boost performance with effective and timely decision-making. Strategic decisions are taken after careful consideration of primary risks, secondary risks, consequential risks and residual risks. The ERM function also enables effective resource allocation through structured qualitative and quantitative risk impact assessment and prioritization based on our risk appetite. Our ERM framework also enables the identification of underlying opportunities during risk assessment, which are then further evaluated and actionized by the business. Our ERM framework encompasses all of the Company's risks, such as strategic, operational, and legal & 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.

Strategy and strategy execution	The risks arising out of the choices we have made in defining our strategy and the risks to the successful execution of our strategy are covered in this category. For example, risks inherent to our industry and our competitiveness are analyzed and mitigated through strategic choices of target markets, our market offerings, business model and talent base.
Operational	The risks affecting our policies, procedures, people and systems, thereby impacting service delivery or operations, or compromising our core values or business practices are covered in this category. For example, risks such as inefficiencies in internal processes, business activity disruptions due to natural calamities, climate change events, human conflicts, system failures and cybersecurity attacks.
Legal and compliance	The risks arising out of threats posed to our financial, organizational, or reputational standing resulting from litigations, non-conformance with laws, regulatory or geo-political developments, codes of conduct and contractual compliances are covered in this category.

Integrated Enterprise Risk Management Framework

We have adopted an integrated ERM framework that is implemented across the organization by the risk management office. Our ERM framework is developed by incorporating the best practices based on COSO and ISO 31000 and then tailored to suit our unique business requirements.

Integrated Enterprise Risk Management Framework



Salient features of our Enterprise Risk Management program

Our ERM program adopts unique methods to identify risks, evaluate potential impact and promote risk awareness across the organization.

Enterprise Risk Management program

Salient features

Secondary, consequential and residual risks

Secondary risks are threats that could impede the mitigation of primary risks. Consequential risks are the unintended consequences of primary mitigation, and residual risks are those risks that are left over after mitigation.

Aggregation and accumulation

Exposure for same risks are aggregated as it goes up the hierarchy. This provides enterprise-wide view to the leadership. Cumulated risk view is also provided to understand total exposure arising out of all risks at a unit level.

Process risk frameworks

Process-specific risk frameworks have been developed for decision-making, for example, frameworks for customer risk, vendor risk, contractual liability, contractual weighted-risk and credit risk.

Intelligent risk analytics – Live Enterprise

Internal and external risk and performance indicators, loss incidents are used real-time to identify, analyze and assess potential issues that could negatively impact strategic goals.

RISC360 : iGRC

RISC360 is the Company's Governance, Risk management and Compliance (GRC) program that combines three lines of defense under one umbrella. This enables risk-based decision-making and auditing. The Company has implemented a technology platform, iGRC, to provide a consolidated view of risks to strategic goals.

Risk culture

Our risk culture encourages open and upward communication. Coupled with our belief systems and core values, this drives behavior, guides daily activities and decision-making throughout the organization. We encourage sharing of knowledge and best practices, continuous process improvement and a strong commitment to ethics and integrity.

Highlights of fiscal 2022

During fiscal 2022, we extended the adoption of the integrated ERM framework across the organization, strengthening our risk management program with a technology platform and enhancing the risk culture. The risk office played a key role in identifying, assessing and managing primary and secondary risks – so as to ensure the smooth delivery of services to our clients, transparent communication with all stakeholders and fulfilling our social responsibility while ensuring employee safety and health.

The risk office assessed, monitored and reported on risks related to strategic programs covering sales, cost optimization, automation, employee engagement and retention. Specifically, these included risks arising from the multiple waves of the pandemic, readiness for post-pandemic operational resilience, geopolitical and macro-economic events such as the conflict in Eastern Europe, contractual liabilities, heightened cybersecurity threats, employee attrition and data protection regulations.

While the Company tracks several risks to its business as mentioned in the *Management's Discussion and Analysis* section of this Integrated Annual Report, the key risks are described below along with the Company's approach to mitigate them.

Key risks	Mitigation approach
Adverse geo-political, economic or health events may impact demand for our offerings and /or technology and talent supply chain.	Broad-based growth to reduce concentration in any single region, client or industry, operational agility to assess and respond to situations
Commoditization of traditional offerings may impact our market share and profitability.	Investment in launching innovative new offerings, a broad portfolio of interconnected services and solutions, and focused growth of digital capabilities
Talent attrition beyond acceptable levels may impact our ability to staff projects or optimize cost structures.	Employee engagement and care, holistic employee retention and recognition policies, focus on career and leadership development
Cost inflation may impact our cost structure and longer-term profitability.	Effective operations with sustainable cost optimization levers, automation and planned capex program
Disruptive technologies such as cloud, software-as-a-service and automation software may diminish the value of some of our service offerings (emerging risk).	Robust alliance strategy, consulting and industry-domain-knowledge-led solutions, reskilling program for employees into newer technologies and methodologies, and large deal program
Cyber attacks that breach our information network or failure to protect sensitive information of our stakeholders in accordance with applicable laws may impact our operations or result in significant regulatory penalties.	Robust cybersecurity framework, controls, governance, preparedness for response to incidents, insurance, region-specific data protection controls and awareness campaigns
New regulations or amendments to existing regulations (e.g., immigration, wages, tax, sanctions) may have an adverse impact on our operations (emerging risk).	Active engagement with policymakers and trade associations, well-governed compliance framework and controls, and de-risked operations
If our employees operate remotely for extended periods, it may adversely impact their productivity, our information security controls and the social capital of the organization.	Implement a hybrid operational model that balances client requirements, evolving employee preferences, legal requirements and information security risks
Physical disasters or climate change events may adversely impact our operations.	Well-established and tested business continuity plans, crisis management policy, distributed operations, sustainability and community engagement initiatives

Cybersecurity risk management

Cyber risks, being one of the key risks, is managed through multi-layered controls with a defense-in-depth approach starting from the thoughtfully-crafted Cybersecurity Strategy, supplemented by policies, processes and controls (preventive, detective, and corrective). Our strategy is focussed on four areas: transparency & experience, continual improvement & compliance, cyber resilience, and building & maintaining a positive cybersecurity culture within the organization, thus making cybersecurity a sustainable and repeatable process throughout the organization.

A high-level working group, the enterprise Information Security Council (ISC) has been established, which is responsible for governing and overseeing the Information Security Management System (ISMS) at Infosys. ISC focuses on establishing, directing, monitoring, and executing the information security program with representation from various departments and business units at Infosys and reports to the Operational Risk Council for highlighting key risks to the executive leadership.