ENTERPRISE RISK MANAGEMENT POLICY OF INFOSYS LIMITED

1. Objective

The purpose of this Enterprise Risk Management (ERM) Policy ("Policy") is to institutionalize a formal risk management function and framework in Infosys Limited ("Company" or "Infosys"). This Policy is drafted in accordance with the guidelines provided [under the charter of the Risk Management Committee ("RMC") of the Board of Directors ("Board")], and pursuant to Section 134 of the Companies Act, 2013 and relevant regulations of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 as amended.

2. Scope

This Policy (along with the charter of the RMC) is applicable to the Infosys Group, including its subsidiaries, acquired entities and to all processes or functions in such entities.

3. Philosophy and approach to risk management

Infosys' ERM philosophy is to enable the achievement of the Company's strategic objectives by identifying, analyzing, assessing, mitigating, monitoring, preventing, and governing any risks or potential threat to these objectives. While the achievement of strategic objectives is a key driver, our values, culture and our obligation & commitment to employees, customers, investors, regulatory bodies, partners, and the community around us are the foundation on which our risk management philosophy is based. The systematic and proactive identification of risks and mitigation thereof shall enable effective or quick decision-making, enable business continuity, and shall improve the performance of the organization.

4. Office of Enterprise Risk Management

The Company shall set up a unit (Office of Risk Management or Risk Office) with sufficient independence and authority for ERM, headed by the Chief Risk Officer. The objective of the unit will be to:

- embed a consistent approach to risk-based decision making in the Company's processes and culture that is aligned to the achievement of the Company's strategic objectives,
- minimize the adverse impact of risks to the enterprise and its operations, thus enhancing its long -term competitive advantage,
- identify opportunities to proactively convert risks into opportunities to deliver improved performance,
- design and implement an ERM Framework, monitor the key risks to the enterprise and associated mitigation plans, and report these to the CEO, CFO, General Counsel and such other management personnel as may be necessary and the RMC of the Board.

The unit will work closely with other related risk management functions of the Company such as legal, information security, finance, data privacy, etc.

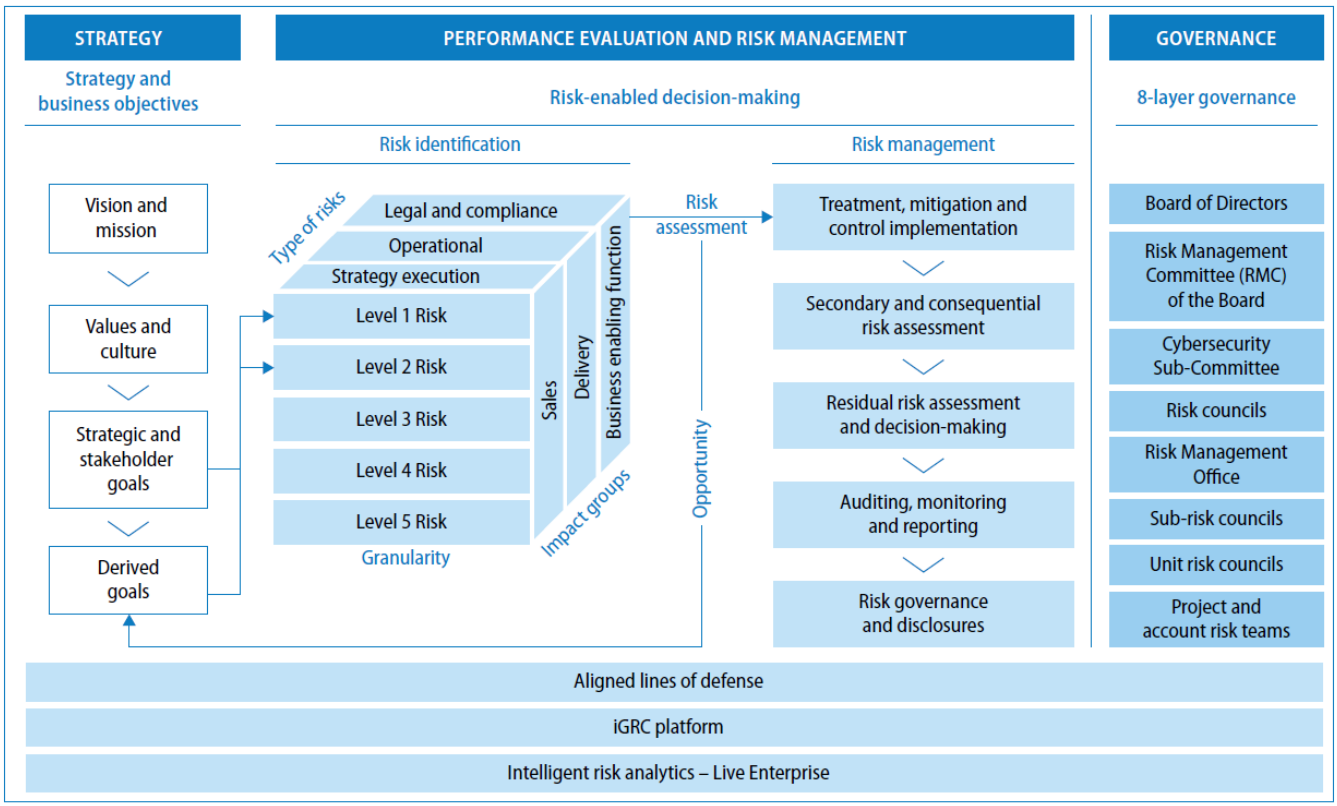
5. Enterprise Risk Management Framework

The Company has defined an ERM Framework that is based on industry standards and encompassing all risks that the organization is facing internally or externally under different categories such as strategic, operational,

legal and compliance risks including sectoral, ESG, AI and cyber security risks. The framework prescribes detailed procedures and guidelines for contextualization of risks by linking it to strategic objectives, identification, assessment, mitigation, any internal controls, communication, monitoring and governance. Appropriate risk indicators shall be used to identify risks proactively. The framework shall take cognizance of risks faced by key stakeholders and the multiplied impact of the same on the organization which may impact business continuity while framing risk responses.

Risk management 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 risks and opportunities. The framework prescribes approaches to identify and measure Primary, Secondary, Consequential, and Residual Risks which enable efficient decision making.

The salient components of the Company's Risk Management Framework are illustrated below:



6. Enterprise Risk Management Rollout

Achieving strategic objectives by proactively managing the risks shall be the responsibility of the Company's management at all levels. Risk management shall be embedded into day-to-day decision making of every function of the Company. People at different levels shall identify and manage the risks within their purview. Identification of risks and bubbling up to the right decision makers shall be actively encouraged and different forums shall be provided for such discussions.

Functions across sales, delivery and business enablers including those in various geographies shall be included in the roll out of the risk management program. Subsidiaries and acquired entities shall also adopt the group's Risk Management Framework and report accordingly. Processes put in place by the Risk Office shall duly enable identification and assessment of top-down and bottom-up risks.

The Risk Office shall have access and visibility to various parts of the organization and data that is required to enable effective risk management.

The ERM program shall be automated with an effective GRC (Governance, Risk and Compliance) solution to enable better visibility, tracking and governance. The program and associated systems shall be updated to adopt and/or comply to applicable regulations, if any.

7. Risk Culture and Adoption

While a top-down mandate is required to implement ERM, having a conducive risk culture will ingrain it into various parts of the organization. To achieve that, Management and the Risk Office shall demonstrate the benefits of having an effective ERM program and encourage business leaders to proactively identify risks or challenges. There shall be free and open forums at various levels in the organization to discuss risks or challenges to the business, bubbling up to the right level of leadership. Business leaders shall take the responsibility for proactively managing the risks and achieve the stated goals.

8. Aligning Enterprise Risk Management with other Lines of Defense

ERM is an umbrella function looking into various aspects of risks from strategic, operational, financial, and tactical perspective. Risk Office enables identification of potential risks and mitigation plans. In addition to Risk Office, there are other risk identification / mitigation functions which are working and safeguarding the organizations assets such as audit, business continuity, compliance, information security, data privacy etc. The Risk Office shall align with these functions and exchange information where required to ensure all pertinent risks are captured and comprehensive solutions are implemented.

9. Governance

The ERM Framework shall provide for comprehensive governance detailing the structure, participants, charter, roles and responsibilities, periodicity of meetings and broad contours of the topics that can be discussed in these meetings. The governance structures shall enable oversight on various risks and allow for bubbling up of risks to the right level of leadership including to the RMC of the Board.

10. Periodic maturity assessment, improvement, and innovation

Periodic assessment of the adequacy of ERM framework, function, mapping against any available risk maturity models and identifying the areas of improvement shall be done to ensure continued relevance of program and framework to the organization. Such review and assessment shall be carried out in at least once every two years by the Risk Office in accordance with the directions given by the RMC.

11. Review and approval of the policy

The Chief Risk Officer shall propose this Policy or any changes to this Policy to the RMC of the Board. This Policy shall become effective upon their approval. This Policy shall be reviewed as deemed necessary by the RMC at least once in two years, including by considering inter alia the changing industry dynamics and evolving complexity.

12. Terms used in this document

Primary Risk	is any uncertainty, event and/or scenario that may inhibit or prevent the organization from achieving its stated business goals, vision and mission.
Secondary Risk	is any risk that inhibits the implementation of identified mitigation strategies and controls.
Residual Risk	is the risk that remains after risk treatment.
Consequential Risk	is an unintended consequence of implementing mitigation actions for primary risks.
Risk Impact Ranking	is the ranking given to a risk based on impact of occurrence, likelihood of occurrence and detectability. Risks are ranked as Critical, High, Medium or Low.
Risk Appetite	is the amount of risk or exposure the organization is willing to accept in pursuit of its goals.
Lines of Defense	refers to risk assessment done by functions/units, corporate audit teams and external audit teams.

13. References and Links

The charter of the RMC is available at https://www.infosys.com/investors/corporate-governance/documents/risk-management-committee-charter.pdf

14. Limitations and Amendment

In the event of any conflict between the provisions of this Policy and of Companies Act, 2013 and relevant regulations of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("Applicable Law"), the provisions of Applicable Law shall prevail over this Policy. Any subsequent amendment / modification to the Applicable Law shall automatically apply to this Policy.

****