



Risk Management Report FY 2024-25



Risk Management

Strengthening Resilience, Enabling Growth

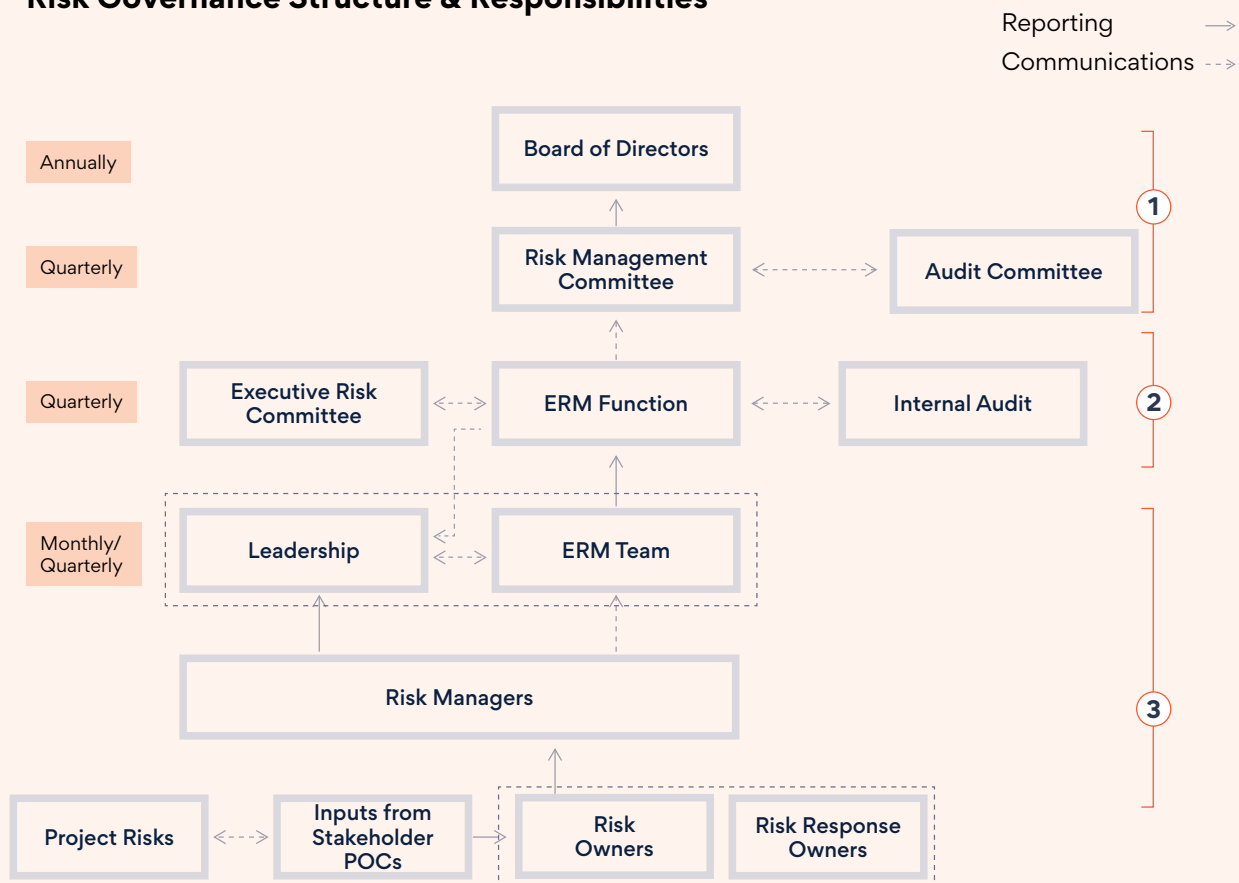
At Persistent Systems, we are committed to embedding a robust risk management culture that enhances organizational resilience and sustainable growth. Our Enterprise Risk Management (ERM) framework proactively identifies, assesses, and mitigates risks across economic, geopolitical, technological, and ESG landscapes. Guided by the Risk Management Committee (RMC) of the Board, we continuously refine our risk approach to ensure alignment with our long-term business objectives.

Approach to Risk Management

Our structured Risk Management framework integrates policies, processes, governance mechanisms, and awareness initiatives to strengthen risk oversight across the organization.

The ERM function collaborates with business units and leadership to facilitate risk identification, assessment, and mitigation, ensuring alignment with strategic priorities. Through this approach, we enable informed decision-making, minimize uncertainties, and drive business continuity in an evolving risk landscape.

Risk Governance Structure & Responsibilities



1 Risk Governance and Oversight

The Risk Governance and Oversight layer comprises the Board and Risk Management Committee, who will play a pivotal role in framing and approving the ERM Policy and guidelines for the organization.

2 Risk Infrastructure and Management

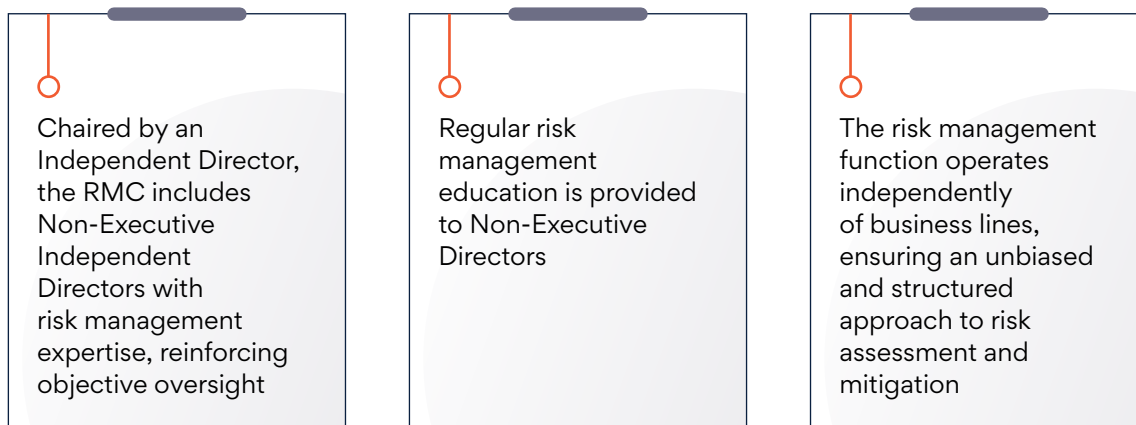
The Risk Infrastructure and Management layer comprises the Executive Risk Committee, ERM Function (CRO and ERM Team) who shall support risk governance and oversight function play a pivotal role in implementation of ERM framework in Persistent Systems.

3 Risk Ownership

The Risk Ownership layer comprises Risk Owners and various Risk Committees who shall be responsible for performing risk management activities in Persistent Systems.

Risk Management Committee (RMC)

The dedicated Risk Management Committee (RMC) plays a crucial role in safeguarding the long-term stability and success of Persistent Systems. Persistent Systems has a risk governance framework with Board-level risk oversight. As a dedicated Risk management committee at the Board-level, oversees industry-specific risks and strengthens Persistent System's risk management framework, ensuring proactive identification and mitigation of risks.



Composition of the Risk Management Committee of the Board of Directors as of March 31, 2025

Name of the Director	Designation	RMC attendance
Mr. Praveen Kadle	Chairman of the Committee and Independent Director	04
Mr. Arvind Goel	Independent Director	04
Prof. Ajit Ranade	Independent Director	04
Mr. Sandeep Kalra	Chief Executive Officer and Executive Director	04
Mr. Debashis Singh	Chief Information Officer	04

The Committee has been established with the authority and responsibilities, including but not limited to formulating a detailed risk management policy that includes:

- A framework for identifying internal and external risks specifically faced by the listed entity, including financial, operational, sectoral, sustainability (particularly ESG-related risks), information, cybersecurity risks, or any other risks as determined by the Committee.
- Measures for risk mitigation, including systems and processes for internal control of identified risks.

- A business continuity plan.
- Ensuring appropriate methodologies, processes, and systems are in place to monitor and evaluate risks associated with the business of Persistent Systems.
- Monitoring and overseeing the implementation of the risk management policy, including evaluating the adequacy of risk management systems.
- Periodically reviewing the risk management policy, at least once every two years, considering changing industry dynamics and evolving complexity.
- Keeping the Board of Directors informed about the nature and content of its discussions, recommendations, and actions to be taken.
- Reviewing the appointment, removal, and terms of remuneration of the Chief Risk Officer (if any) under the purview of the Risk Management Committee.
- Seeking information from employees, obtaining outside legal or professional advice, and securing the attendance of relevant external experts when necessary.



For more details, refer to Page 170 of

Risk Management Committee

Enterprise Risk Management (ERM) Function



Persistent System's Enterprise Risk Management (ERM) framework aligns with ISO Standard 31000:2018 Risk Management – Guidelines, COSO: ERM - Integrating Strategy and Performance (2017), and relevant regulatory requirements in India. Our ERM framework takes a comprehensive approach to managing the full spectrum of risks faced by Persistent Systems, with a focus on those critical to its strategic success. It provides structured guidance for identifying, assessing, measuring, monitoring, and addressing risks across the enterprise, ensuring alignment with strategic objectives and risk appetite. The ERM function regularly reports risks to executive leadership and the Risk Management Committee (RMC) of the Board for ongoing oversight.

Our Enterprise Risk Management (ERM) function is designed to enhance a proactive risk management culture across the organization. It collaborates closely with various organizational units and their leadership to facilitate the risk management process. The philosophy of Risk Management at Persistent Systems is highlighted in the below objective:

- Promote an effective risk management system that supports Persistent's growth strategy, business objectives, and ensures resilience to the business dynamics.
- Improve institutional decision-making by giving senior management and Board of Directors timely and accurate information that helps them better comprehend the risks and possibilities at the enterprise level, and then propose mitigation plans to achieve the desired objectives.
- Enhance Persistent System's capacity to achieve its legal, regulatory, and policy compliance obligations.
- Strengthen the business's capacity to recognise its most important resources and put strategies in place to protect and strengthen them.
- Establish a process to identify and assess risks that may impact the business continuity of Persistent and define response and recovery plans for such risks.
- Proactively identify potential opportunities and risks to prepare for future breakthroughs and obstacles.

- Strengthen the organization's capacity to comprehend and control risk exposures and establish a culture of responsible risk-taking.
- Integrate opportunity and risk assessment analysis into Persistent System's periodic planning procedures (for example, strategic planning, annual budget cycle, etc.).



Enterprise Risk Management (ERM) Process Flow

- Identifying plausible uncertainties or risks that may impact the successful achievement of functional, organizational, and business objectives or threaten business continuity.
- Categorizing risks into financial, operational, reputational, regulatory, extended enterprise, strategic, sustainability, and technology for assessment.
- Analysing and assessing the potential impact, likelihood, and velocity of existing and newly identified risks.
- Determining the readiness to manage identified risks.
- Evaluating the results of the risk analysis against established risk criteria.
- Prioritizing risks based on criticality to decide on the appropriate risk management strategy.
- Formulating risk response strategies to evade, prevent, or eliminate root causes of risks and risk events, especially for key risks.
- Integrating mitigation plans devised by risk owners into day-to-day activities and monitoring them closely.
- Monitoring and reviewing risks on a periodic basis for continuous risk assessment.
- Re-evaluating the risk environment and updating mitigation plans if necessary.
- Reporting relevant risk information to the Risk Management Committee of the Board in a timely manner for risk-informed decision-making.

Risk Management Processes

Risk Review



- Risks are analysed based on impact, likelihood, and velocity to assess potential consequences.
- Assessed risks are prioritized using predefined criteria to guide management strategies.
- A key component of this process is defining Persistent System's Risk Appetite and Tolerance, ensuring alignment with strategic objectives.
- Defined process for Risk Appetite and Tolerance identification along with Key Risk Indicators (KRIs).

Defining Risk Appetite Statements

- The first step in determining the risk appetite and tolerance is to articulate it through Risk Appetite Statements.
- Risk Appetite Statements shall be defined taking into consideration the strategies, acceptable level of risk that Persistent Systems is willing to assume to achieve its strategy, and Persistent System's internal and external context.
- Risk appetite statements shall incorporate tolerance limits, which, if breached, would necessitate immediate escalation and management action.
- Risk Appetite statements have been defined across various operations for PSL. These statements are to be reviewed annually and approved by the Board.

Implementing and Operationalizing Risk Appetite Statements

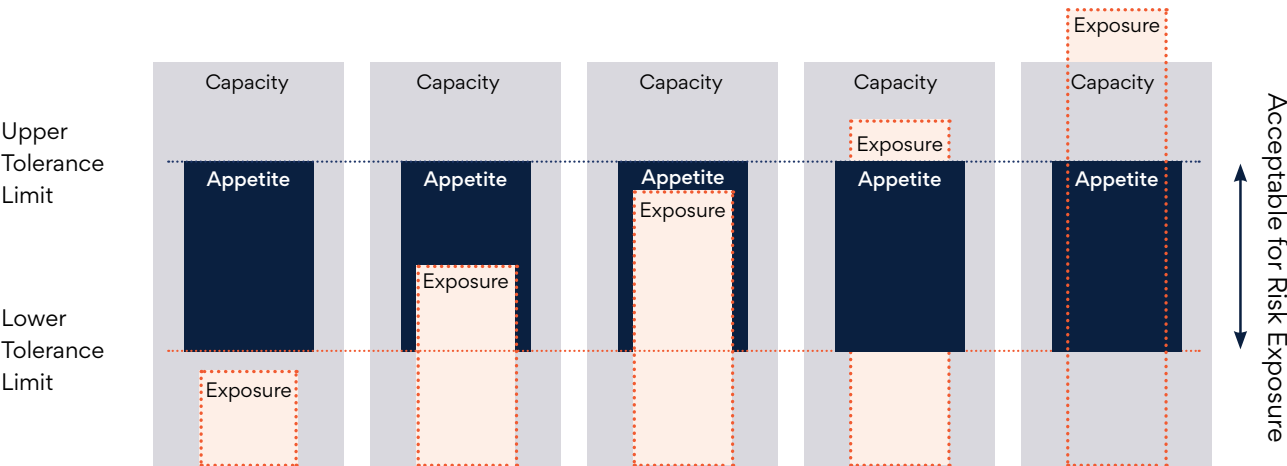
Risk Appetite Statements are driven by the risk philosophy defined by the Board and Management. These may be qualitative or quantitative in nature and allow Business Units and Corporate Functions to measure risks while making business and operational decisions. Once risk appetite is defined and implemented, it is essential to continuously monitor Persistent's actual risk exposure to ensure alignment with risk tolerance levels.

Risk Exposure

- The Board of Directors shall evaluate the risk exposure of Persistent Systems on a quarterly basis, including exposure towards strategic and emerging risks and associated response plans.
- The risk exposure of Persistent Systems shall be measured by assessing enterprise risks using the Risk Assessment Scales defined as per the Risk Appetites adopted by the Board.
- For each risk exposure scenario (as illustrated below), corrective action shall be required depending on where the risk exposure lies, i.e., whether to increase or decrease the amount of risk Persistent Systems is exposed to. Alternatively, Persistent Systems may need to re-assess its risk appetite to achieve its business strategy.
- To maintain compliance and ensure **risk exposure remains within acceptable limits**, Persistent Systems conducts regular audits to assess the effectiveness of risk management strategies.



Risk Exposure Scenarios



Strategy under threat	Desired range	Escalation	Strategy under threat	Company under threat
Risk exposure is less than the lower tolerance limit. Corrective action needed to evaluate opportunity to take additional risks to achieve strategy	Risk profile is between the upper and lower tolerance limit. This is the optimal range	Risk profile is near the upper tolerance limit. Escalation may be considered for corrective action and explore additional risk controls to avoid breach	Risk profile exceeds the upper tolerance limit. Immediate corrective action must be taken to limit risk exposure	Risk profile exceeds risk capacity. Company must enact response and recovery plans to prevent an impending crisis

Risk Management Process Audits

To ensure a robust risk management framework, Persistent complies with multiple ISO standards, including Information Security, Quality, Business Continuity, Privacy, Environment, Health & Safety, and ESG.



- We conduct both internal audits of risk management processes and external independent third-party audits on an annual basis.

- These audits evaluate risk identification, impact, and mitigation strategies across key focus areas including Cyber Security, Data Privacy, Sustainability, Environmental & Climate Risks, and Health & Safety.



For more details.

[Refer to certifications](#)

Risk Culture

Risk management is a shared responsibility across the organization, ensuring a structured, consistent, and effective approach. Our ERM framework integrates policies, processes, governance mechanisms, and awareness programs to embed a strong risk-aware culture.

To strengthen risk capabilities across all levels, our ERM framework focus on:

- Regular training for Non-Executive Independent Directors and the Board.
- Company-wide education programs to enhance risk awareness.
- Integration of risk criteria into service development and Business models.
- Incorporation of risk metrics into leadership scorecards & KRAs, with a direct link to financial incentives.

Risk Managers and Risk Owners

Risk Governance Framework

Persistent Systems has established three pillars of risk management responsibilities in its Governance structure as Risk Oversight, Risk Infrastructure and Management, and Risk Ownership, that cascades the scope of activities to senior management and all employees, across the subsidiaries of Persistent Systems.

Persistent Systems has a risk governance framework with details outlined below:

1

Operational and Functional Risk Ownership (first line):

Organizational Units and Functional Units have identified Risk Managers and Risk Owners, they are responsible for identifying, managing and mitigating risks through support provided by key support teams such as Contract Management, Information Security, Project Risk Management and ERM Team. Regular governance & cadence is setup for effective risk management.

2

Risk Management and Compliance Oversight (second line):

A dedicated ERM Team exists as a second line of defence to strengthen and embed proactive risk management culture across the organization. This team works closely with the various organizational units and their leadership to facilitate the risk management process. As a process, the Chief Risk Officer (CRO) reports the risks to the Executive Leadership and Risk Management Committee (RMC) of the Board each quarter for their regular review.

3

Independent Audit Unit (third line):

An internal audit function that provides independent assurance on the effectiveness of risk management and compliance processes.



Key risks & emerging risks with Business Impact and Mitigation Approach

Cyber-attack and Hacking Risk

Type	Risk Category	Magnitude	Likelihood
Risk	Technology & Cyber / Extended Enterprise	High	Possible
Business Impact	> External attacks, malware, compromised credentials, Business email compromise via phishing and other cyber security risks may result in data loss and loss of reputation.		
Mitigation Approach	> Risk <ul style="list-style-type: none"> • Robust Information Security Management System (ISMS) centred around comprehensive Information Security policies based on industry best practices and leading security frameworks, with a continuous reinforcement of security controls to ensure the confidentiality, integrity, and availability of information assets • Multi-layered governance process with Executive and Board oversight • Certifications such as ISO 27001, ISO 27017, ISO 27018, ISO 27701, and SOC 2 Type II attestations to demonstrate our commitment to cybersecurity • Continued investment and deployment of state-of-the-art technologies such as Zero Trust architecture, Advanced endpoint protection solution, Dark / Deep web monitoring, etc. to secure corporate infra, data & applications • Access controls including Multi Factor Authentication for secure access to enterprise applications/network, special handling of privileged administrator accounts, rigorous access management & monitoring of all cloud deployments • Mandatory training and adequate awareness measures across employee life cycle ensure a strong human firewall • Implementation of enhanced Data Leakage prevention platform to protect critical data • Encryption of data, data back-up and recovery mechanisms for ensuring business continuity aligned to ISO 22301:2019 • Established threat intelligence, security monitoring and incident response processes to detect and respond to cybersecurity threats and incidents coordinated through a 24x7 Security Operations Centre • Internal and external audits and red teaming to validate effectiveness of controls 		
Financial Implication	> Negative <ul style="list-style-type: none"> • May cause operational disruptions, impacting business continuity. • Could result in legal fines and penalties due to regulatory non-compliance. • May negatively affect brand reputation and customer relationships. 		

Data Privacy

Type	Risk Category	Magnitude	Likelihood
Risk	Regulatory / Reputational	High	Possible
Business Impact	<ul style="list-style-type: none"> Persistent operates globally and hence needs to be compliant with the data privacy laws across countries where we operate Unauthorised use or disclosure of employee or Company or customer data may lead to either breach of customer contract or fines/penalties from regulators and / or damage to Persistent System's reputation 		
Mitigation Approach	<p>Risk</p> <ul style="list-style-type: none"> Robust Privacy Information Management System (PIMS) to safeguard personal data and ensure compliance with applicable legal, regulatory, and contractual obligations pertaining to data privacy and protection Global privacy policy covering all geographies, all areas of operations, and stakeholders Data Loss Protection (DLP), Data Classification and Data Encryption technologies are deployed to protect personal information Access controls including Multi Factor Authentication, Privileged administrator account management tools are deployed. All access provisioning is on a need-to-know basis and access reviews are performed on a regular basis Dedicated Data Protection Officer and Privacy team Continuous strengthening of global privacy program through monitoring of regulatory mandates, revalidation of existing frameworks, policies and processes and ensuring applicability to customer contracts Technical and organization measures such as PII Inventories, Privacy Impact Assessment, Incident Management Procedures and Systems, Breach Notification Management, Data Subject Rights Request Management, etc. Development of products & applications, including change in processing of personal data go through appropriate privacy assessments and approval Vendors and third parties are subjected to risk assessment and contracted with appropriate privacy obligations Mandatory training on data protection, Privacy by Design, and global privacy regulations. Continuous awareness campaigns through blog posts, email broadcasts, and online events Periodic reviews and audits by independent audit firm to verify compliance to obligations in addition to internal audits across the ecosystem Certified under ISO 27701:2019 — Privacy Information Management System, ISO 27018:2014 — Securing Personal Data in Cloud and SOC 2 Type 2 Attestation 		
Financial Implication	<p>Negative</p> <ul style="list-style-type: none"> Risk of operational disruptions, affecting business processes. Potential legal fines and penalties for non-compliance. Adverse effects on brand reputation and customer trust. 		

Foreign Exchange Risks

Type	Risk Category	Magnitude	Likelihood
Risk	Financial	Low	Possible
Business Impact	<p>Persistent Systems operates in the global environment and has maximum business from US geography hence Currency fluctuations is a major risk.</p>		
Mitigation Approach	<p>Risk</p> <ul style="list-style-type: none"> Net foreign exchange earnings are hedged on a 12-month rolling basis, covering 45% to 70% of net open positions. Guidance from the Board members is obtained every quarter regarding hedging quantum. Close monitoring of exchange rate movement is done. 		
Financial Implication	<p>Negative</p> <ul style="list-style-type: none"> Fluctuations in currency exchange rates may directly affect Persistent System's profitability. 		

Geo-Political and Macro-Economic Risk

Type	Risk Category	Magnitude	Likelihood
Risk	Strategic / Sectoral	Medium	Possible
Business Impact	> Changing Geo-political landscape in multiple regions - Change in Govt. & their policies (US, Europe, UK); Extended war scenarios in Middle East and Ukraine / Russia, Macroeconomic headwinds due to potential tariffs changes, energy price increase and customer discretionary spends, leading to potential impact on growth opportunities		
Mitigation Approach	> Risk <ul style="list-style-type: none"> Conduct “Country Risk Assessments” based on PESTEL Framework Engaged with geo-political consultants to get insights on the changing geopolitical landscape Monitoring and reporting of geo-political risks to the RMC of the Board Geo-Diversification for growth planned via Europe and other geographies Enhanced focus on customer connects and relationships Persistent Systems is ISO 22301 certified and regular BCP testing is performed 		
Financial Implication	> Negative <ul style="list-style-type: none"> Potential shifts in customer outlook may lead to reduced demand for Persistent System’s services. Increased operational costs due to geopolitical or macroeconomic uncertainties. 		

Talent demand and employee attrition

Type	Risk Category	Magnitude	Likelihood
Risk	Talent / Operational	Medium	Possible
Business Impact	> <ul style="list-style-type: none"> Market forces – After the great resignation phase post-COVID, the talent market has stabilized over the past year. However, there is a slight uptick in voluntary attrition. The demand for emerging technologies remains high, with AI reshaping the talent landscape. Specialized digital skills command substantially higher, differentiated compensation, impacting talent hiring and retention. Our high-demand skill capabilities make our trained talent pool susceptible to headhunting and competitive offers. Employee preferences — Hybrid working seems to be employee’s preference 		
Mitigation Approach	> Risk <ul style="list-style-type: none"> Employee Development and Growth — Focus on employee development and upskilling, enabling them to build their careers has been a part of the ‘Persistent way’ of working. Persistent University offers an excellent platform for employee to acquire skills, stay relevant and enhance their skills and competencies. Persistent Systems invests in up-skilling of its associates in new age digital technologies and runs Persistent’s Digital Engineering Academy (PDEA). PDEA runs upskilling programs in Cloud, Data, Gen AI etc. Employee engagement and all-round wellbeing — All round wellbeing of our employee, has been central to our employee engagement approach, which covers physical, financial, and psychological wellbeing. We conduct regular surveys to seek input from employee on various aspects of their work to understand their engagement and expectations. Input thus received is processed to make necessary improvements in processes and policies Employee Experience — We will continue to focus on elevating employee experience through ‘Do It Yourself’ approach through simplified processes and tools. This will help to enhance employee engagement and employee productivity. Persistent brand — Our consistent growth over last several quarters, scale of operations and geographical presence has been helping us continue to position Persistent Systems as a leading brand in the industry. We continue to invest in branding initiatives Inclusive Workplace — Persistent Systems provides a diverse and inclusive workplace which promotes creativity, diversity, inclusivity, and enhanced work culture 		
Financial Implication	> Negative <ul style="list-style-type: none"> Increased attrition, particularly in niche digital skills, may disrupt ongoing delivery operations and impact project execution. Potential revenue loss due to resource gaps and increased hiring/training costs. 		

Credit Risk

Type	Risk Category	Magnitude	Likelihood
Risk	Financial	High	Possible
Business Impact	> Delay in collection of customer dues as a result of the global economic situation		
Mitigation Approach	> Risk <ul style="list-style-type: none"> Persistent Systems has adopted an effective receivables management system to monitor and control the outstanding receivables Credit Risk is managed through policies, procedures, and controls as a part of customer credit risk assessment Persistent Systems has adopted expected credit loss model, based on profile of the customer and aging pattern, to assess the impairment loss or gain on trade receivables 		
Financial Implication	> Negative <ul style="list-style-type: none"> Delayed or non-collection of dues may disrupt cash flow and increase financial strain. Potential rise in operational costs due to outstanding receivables. 		

Sustainability Risks – Climate change

Type	Risk Category	Magnitude	Likelihood
Risk & Opportunity	Sustainability – ESG / Operational	Low	Unlikely
Business Impact	> <ul style="list-style-type: none"> Climate change is affecting the frequency and severity of certain extreme weather events, including heat waves, cold waves, tornadoes, tropical cyclones, floods, seasonal diseases, epidemics, and pandemics. Extreme weather events can pose risks to human safety and business operations. Customers appreciate vendors committed to helping them achieve sustainability goals Ignoring environmental regulations can lead to legal issues and hinder best practices 		
Mitigation Approach	> Risk <ul style="list-style-type: none"> Persistent System's facilities across India are ISO 14001:2015 certified by external third parties. Persistent Systems has distributed operations, enabled remote working, focused on agile delivery, and periodically tested business continuity plans. Delivery centres are designed to withstand extreme weather events Employee awareness around conservation of resources is built to strengthen business resilience and align resources with Persistent Systems. The CISO of Persistent Systems and the team ensures implementation of business continuity at project, customer, region, location, function level and run internal audit checks to verify the implementation of the controls Persistent Systems is certified – ISO 27001 for information security and ISO 22301 for business continuity We continuously invest in R&D to enhance existing and develop new solutions that boost our clients' efficiency, generating positive environmental and social impact. Recognizing the growing importance of ESG goals, we're actively exploring ways to integrate them even deeper into our future offerings. Our climate action goals include: <ul style="list-style-type: none"> Maintain Carbon Neutrality for Scope 1 and Scope 2 emissions every year Sourcing of 100% Renewable energy across owned locations by FY 2025-26 Achieve net-zero greenhouse gas emissions across the value chain by FY 2049-50 The progress on above goals is shared biannually with the SRC and ESG committee of the Board for review and guidance. The organization focuses on reducing its carbon footprint by promoting environmental sustainability. Its initiatives include tree planting, which contributes to carbon sequestration and air quality improvement efforts. Persistent is committed to driving renewable energy adoption, optimizing energy use, and working with communities to address climate change. Publishing the ESG and BRSR annual report fulfils regulatory reporting requirements and transparently communicates our progress on ESG goals to our stakeholders Crisis Management framework development in FY 2025-26 which includes Early Warning Systems for efficient monitoring and communications <p>Opportunities</p> <ul style="list-style-type: none"> Proactive Climate risk assessment ensures we are equipped to deal with adversities. Focus on using technology that supports low carbon emissions and reduce carbon footprint. 		
Financial Implication	> Negative <ul style="list-style-type: none"> Climate change, resulting in extreme weather events, poses sustainability risks by threatening human safety and disrupting business operations. <p>Positive</p> <ul style="list-style-type: none"> Growing corporate focus on carbon footprint reduction presents new business opportunities for Persistent Systems to offer technology-driven sustainability solutions. Persistent System's proactive environmental initiatives enhance brand reputation, making it a preferred partner for organizations with aligned sustainability goals. 		

Water Scarcity Risk

Type	Risk Category	Magnitude	Likelihood
Risk & Opportunity	Sustainability – ESG / Operational	Medium	Possible
Business Impact	<ul style="list-style-type: none"> Water conservation is essential for the sustainability of our planet. Declining groundwater levels and altered rainfall patterns pose significant risks, potentially leading to a global water crisis. 		
Mitigation Approach	<p>Risk</p> <ul style="list-style-type: none"> Water resource analysis has been conducted for all global locations and categorized according to the 'Aqueduct Water Risk Atlas'. Vulnerability identification and location-specific mitigation plans have been implemented to monitor water consumption. Conservation and efficiency measures are enforced through operational control and all owned facilities are equipped with rainwater harvesting systems to recharge groundwater. Groundwater sources are considered a last resort. Frequent awareness sessions on sustainable water management are conducted. <p>Opportunity:</p> <ul style="list-style-type: none"> We engage in CSR activities, such as integrated watershed development programs and the provision of open wells for drinking water, to raise awareness and support community development. Proactive ESG measures and CSR initiatives taken by Persistent Systems strengthen its brand, thus making it attractive to organizations seeking an IT Services partner with a shared vision. Additionally, it also helps attract and retain younger talent. 		
Financial Implication	<p>Negative</p> <ul style="list-style-type: none"> Water scarcity and associated constraints could disrupt business operations and affect long-term sustainability <p>Positive:</p> <ul style="list-style-type: none"> CSR initiatives will enhance brand visibility within society, making Persistent Systems an attractive employer for younger talent. These initiatives contribute to the upliftment of society by supporting broader social causes. 		

Global Regulatory Risks (Emerging Risk)

Type	Risk Category	Magnitude	Likelihood
Risk & Opportunity	Regulatory / Reputational	High	Possible
Business Impact	<ul style="list-style-type: none"> Risk of non-compliance with existing statutory regulations, new regulations, or amendments to existing regulations (e.g., immigration, payroll and social security, taxation, employment laws, data privacy laws etc.) where Persistent operates globally, may have an impact Persistent Systems operates globally in major markets and industries. There is an inherent risk of non-compliance with the ever-evolving legal landscape resulting into frequent legal updates and changes in regulatory requirements/disclosures (including regulations related to ESG, ethical, and hygiene practices) that are applicable to our business 		
Mitigation Approach	<p>Risk</p> <ul style="list-style-type: none"> Persistent uses a professional Compliance Manager Tool to report and monitor the regulatory compliances applicable to Persistent Systems Persistent also updates the Tool on ongoing basis with the amendments in the existing regulations and inclusion of newly introduced legislations, if any A framework is in place to assess the correctness of the compliances which have been reported in the Tool The Compliance status is placed before the Audit Committee of the Board of Directors and the Board of Directors of Persistent in their quarterly meetings Persistent Systems has also appointed local consultants in various geographies to advise and help Persistent Systems to ensure the compliances in respective geographies Persistent Systems has a dedicated ESG function for the oversight of any ESG related regulatory compliance changes. Company has been certified in- ISO 14001:2015 Environmental Management System and ISO 45001:2018 Occupational Health and Safety Management System <p>Opportunities</p> <ul style="list-style-type: none"> Provide services to customers to enable them to meet their ESG-related requirements 		
Financial Implication	<p>Negative</p> <ul style="list-style-type: none"> Non-compliance with global regulations may lead to penalties, legal repercussions, and reputational damage. <p>Positive</p> <ul style="list-style-type: none"> Evolving ESG regulatory requirements and disclosure standards create new business opportunities for Persistent to offer technology-driven solutions that help customers achieve their sustainability goals. 		

Energy Demand Risk (Emerging Risk)

Type	Risk Category	Magnitude	Likelihood
Risk & Opportunity	Sustainability – ESG	Medium	Possible
Business Impact	<ul style="list-style-type: none"> The development of emerging technologies and AI may result in increased global energy consumption, which could lead to higher carbon emissions. 		
Mitigation Approach	<p>Our climate action goals include</p> <ul style="list-style-type: none"> Maintain Carbon Neutrality for Scope 1 and Scope 2 emissions every year <ul style="list-style-type: none"> Sourcing of 100% Renewable energy across owned locations by FY 2025-26 Achieve net-zero greenhouse gas emissions across the value chain by FY 2049-50 Persistent Systems has made significant strides in renewable energy adoption and resource management by enhancing energy efficiency through investments in renewable energy and the development of energy-efficient infrastructure, certified by the Indian Green Building Council (IGBC) and Leadership in Energy and Environmental Design (LEED). Decarbonization roadmap with strategies aligned with SBTi guidelines to achieve emissions reductions. All owned campuses are equipped with rooftop solar generation and connected to 2 windmills via open access, additionally Persistent Systems purchases renewable energy through Green Tariff's from DISCOM's. <p>Continuous improvement to monitor and evaluate the environmental performance of new technology, identify areas for enhancement, and implement corrective measures as part of an ongoing process.</p> <p>Green procurement policy enabling buyers to evaluate the suppliers based on emissions from Purchase of goods and services</p> <p>Opportunity</p> <ul style="list-style-type: none"> As corporations strive to reduce carbon footprints and focus on environment-friendly products and services, it also opens up new business opportunities for Persistent to provide technology-led solutions and services to these organizations. We help our customers to migrate their workloads from data centres to the cloud, thus reducing their carbon footprints. 		
Financial Implication	<p>Negative</p> <ul style="list-style-type: none"> Increased energy consumption may challenge the achievement of emissions reduction targets. <p>Positive:</p> <ul style="list-style-type: none"> Assisting customers in cloud migration strategies can unlock new business opportunities for Persistent Systems. 		

GenAI Risk (Emerging Risk)

Type	Risk Category	Magnitude	Likelihood
Risk & Opportunity	Strategy / Technology	Medium	Likely
Business Impact	<p>PSL recognize the risks associated with GenAI, which includes potential data privacy and cyber security vulnerabilities, intellectual property challenges related to AI-generated content, biased outputs, accuracy, and reliability concerns with AI-generated information, the evolving regulatory landscape adds a risk of non-compliance</p>		
Mitigation Approach	<ul style="list-style-type: none"> Emphasizing self-regulation and adherence to Responsible AI principles Risk-based approach for reducing risks associated with usage and build an effective policy over time to govern the usage of AI Responsible AI Council to oversee and direct usage norms Keeping human-in-the-loop system to review AI generated data Ensuring clarity on the terms of use and liability in AI deployment policies Continue to provide a secured private instance and safe environments for accessing Generative AI applications <p>Raise awareness among employees in responsible use of GenAI tools, from validation of outputs to refraining from using materials that could be subject to copyright</p> <p>Ongoing monitoring of regulatory changes</p> <p>Development of AI management system leading to ISO 42001 certification in FY 2025-26 to manage associated risks and entire lifecycle of AI.</p> <p>Opportunity:</p> <ul style="list-style-type: none"> AI for Tech: Launch of a fully integrated end-to-end solution (SASVA 2.0) from ideation to post-deployment operations for businesses across industries to drive innovation, enhance customer experiences and productivity gains AI for Business: Engaged with multiple customers on GenAI opportunities 		
Financial Implication	<p>Negative:</p> <ul style="list-style-type: none"> PSL recognize the risks associated with GenAI, which includes potential data privacy and cyber security vulnerabilities, intellectual property challenges related to AI-generated content, biased outputs, accuracy, and reliability concerns with AI-generated information, the evolving regulatory landscape adds a risk of non-compliance <p>Positive:</p> <ul style="list-style-type: none"> PSL leveraging AI for Tech – launch of integrated end-to-end solutions for ideation to post deployment. AI for Business is also explored with multiple customers for new opportunities 		

Emerging Risks

Risk 1: Global Regulatory Risks (Emerging Risk)

Type: Risk & Opportunity

Risk Category: Geopolitical

Magnitude: High

Likelihood: Possible

Financial Implication: Both (Positive & Negative)

Description	Global regulatory risks refer to the uncertainties arising from evolving international laws, compliance requirements, and policy changes that impact businesses. In the IT sector, these risks include stringent data protection laws, cybersecurity mandates, AI governance frameworks, and cross-border regulatory conflicts. Rapid shifts in global regulations require organizations to adapt their risk management strategies to ensure compliance while maintaining operational resilience and business continuity.
Impact	<p>Regulatory Compliance Risks: Non-compliance with existing or newly introduced statutory regulations, such as immigration, payroll, social security, taxation, employment laws, and data privacy, across global operations may lead to legal penalties, reputational damage, and financial implications.</p> <p>Evolving Legal Landscape: As a globally operating Company, Persistent Systems faces inherent risks due to frequent legal updates and changing regulatory requirements, including ESG, ethical standards, and workplace hygiene practices, which necessitate continuous monitoring and adaptation.</p> <p>Business Impact: Failure to comply with regulatory changes can result in fines, operational disruptions, increased compliance costs, and potential restrictions on market access, impacting Persistent's growth and sustainability.</p>
Mitigation	<p>Risk</p> <ul style="list-style-type: none">• A Compliance Manager Tool is used to track and oversee all applicable regulatory requirements.• The tool is regularly updated to incorporate amendments to existing regulations and newly introduced legislations, ensuring ongoing compliance.• A structured assessment process verifies the accuracy of reported compliance status.• Compliance reports are presented at regular intervals to the Audit Committee and Board of Directors for review and governance.• Local consultants across various geographies provide advisory support to ensure adherence to country-specific regulations.• A dedicated ESG function oversees compliance with evolving ESG-related regulatory requirements. <p>Opportunity:</p> <ul style="list-style-type: none">• To provide sustainability as a service offering to customers

Risk 2: Energy Demand Risk (Emerging Risk)

Type: Risk & Opportunity

Risk Category: : Environmental

Magnitude: Medium

Likelihood: Possible

Description — **Energy Demand Risk** in the IT sector arises from the increasing power consumption required to support expanding data centre infrastructure, cloud services, and AI-driven operations. Rapid technological advancements and the growing demand for high-performance computing contribute to rising energy needs, making companies more susceptible to fluctuations in energy availability, regulatory changes, and cost volatility. Additionally, evolving global energy policies, carbon reduction commitments, and stricter efficiency regulations present challenges in managing energy demand while ensuring compliance with sustainability standards.

Impact — **Increased Energy Consumption:** The adoption of emerging technologies, including AI and advanced computing, may lead to higher energy usage, impacting operational costs and sustainability goals.

Carbon Emissions Challenges: Rising energy demand could contribute to increased carbon emissions, necessitating enhanced carbon management strategies to align with sustainability commitments.

Regulatory & Compliance Risks: Strengthening global climate regulations may impose stricter emissions reduction targets, requiring PSL to invest in energy-efficient infrastructure and renewable energy solutions.

Client & Market Expectations: Growing emphasis on sustainable IT solutions may drive the need for PSL to innovate in low-carbon technologies, influencing product development and service offerings

Mitigation — **Risk**

- Our climate action goals include:
 - Maintain Carbon Neutrality for Scope 1 and Scope 2 emissions every year
 - Sourcing of 100% Renewable energy across owned locations by FY 2022-26
 - Achieve net-zero greenhouse gas emissions across the value chain by FY 2049-50
- Persistent Systems has made significant strides in renewable energy adoption and resource management by enhancing energy efficiency through investments in renewable energy and the development of energy-efficient infrastructure, certified by the Indian Green Building Council (IGBC) and Leadership in Energy and Environmental Design (LEED).
- Decarbonization roadmap with strategies aligned with SBTi guidelines to achieve emissions reductions.
- All owned campuses are equipped with rooftop solar generation and connected to 2 windmills via open access, additionally Persistent purchases renewable energy through Green Tariff's from DISCOM's.
- Continuous improvement to monitor and evaluate the environmental performance of new technology, identify areas for enhancement, and implement corrective measures as part of an ongoing process.
- Green procurement policy enabling buyers to evaluate the suppliers based on emissions from purchase of goods and services

Opportunities

- As corporations strive to reduce carbon footprints and focus on environment-friendly products and services, it also opens up new business opportunities for Persistent Systems to provide technology-led solutions and services to these organizations.
- We help our customers to migrate their workloads from data centres to the cloud, thus reducing their carbon footprints.

Emerging Risks

Risk 1: GenAI Risk (Emerging Risk)

Type: Risk & Opportunity

Risk Category: Technological

Magnitude: High

Likelihood: Possible

Financial Implication: Both (Positive & Negative)

Description	<p>— The integration of Generative AI (GenAI) in the IT sector presents risks related to data privacy, cybersecurity threats, intellectual property rights, and algorithmic bias. The reliance on large datasets increases exposure to regulatory non-compliance, while AI-generated content raises concerns about misinformation and ethical accountability. Additionally, the high computational power required for GenAI leads to increased energy consumption and carbon footprint, impacting sustainability goals. As global regulations around AI governance evolve, IT companies must implement robust risk management frameworks to ensure compliance, security, and responsible AI deployment.</p>
Impact	<p>— PSL recognize the risks associated with GenAI, which includes potential data privacy and cyber security vulnerabilities, intellectual property challenges related to AI-generated content, biased outputs, accuracy, and reliability concerns with AI-generated information, the evolving regulatory landscape adds a risk of non-compliance.</p>
Mitigation	<p>— Risk</p> <ul style="list-style-type: none"> • Emphasizing self-regulation and adherence to Responsible AI principles • Risk-based approach for reducing risks associated with usage and build an effective policy over time to govern the usage of AI • Responsible AI Council to oversee and direct usage norms • Keeping human-in-the-loop system to review AI generated data • Ensuring clarity on the terms of use and liability in AI deployment policies • Continue to provide a secured private instance and safe environments for accessing Generative AI applications • Raise awareness among employees in responsible use of GenAI tools, from validation of outputs to refraining from using materials that could be subject to copyright • Ongoing monitoring of regulatory changes • Development of AI management system leading to ISO 42001 certification in FY 2025-26 to manage associated risks and entire lifecycle of AI. <p>Opportunity:</p> <ul style="list-style-type: none"> • AI for Tech: Launch of a fully integrated end-to-end solution (SASVA 2.0) from ideation to post-deployment operations for businesses across industries to drive innovation, enhance customer experiences and productivity gains • AI for Business: Engaged with multiple customers on GenAI opportunities

Risk Management Certification

Cyber Risk Management Certifications



ISO
27001:2022



ISO
27017:2015



ISO
22301:2019



ISO
27018:2019



SOC 2
Type II



ISO
27701:2019

Standards we adhere to



ISO
31000:2018



NIST
CSF



NIST
RMF



Persistent Systems Limited

CIN: L72300PN1990PLC056696

Registered Office


Bhageerath, 402 Senapati Bapat Road
Pune 411 016, India

Tel: +91 20 6703 0000


Fax: +91 20 6703 0008


info@persistent.com

www.persistent.com

 persistent-systems

 Persistentsys

 PersistentSystems

 persistent_systems