Management Approach: Risk Management

Stantec continually identifies and manages potential risks and uncertainties facing our business at the enterprise and project levels, including climate risks.

Commitments and Practices

Responsibility for risk management is shared across the organization—from our Board of Directors, which establishes overall risk appetite and provides strategic direction and guidance on risk management, to senior executives, who are responsible for implementing risk management practices, to our employees, who apply risk management in day-to-day operations and decision making. Our programs are subject to internal and third-party audit.

In Our Operations

Stantec's approach to risk management includes Enterprise Risk Management (ERM), an Integrated Management System (IMS), and Business Continuity Management (BCM). We incorporate climate-related risk management throughout. Our practices and risk mitigation measures evolve as risks change and new risks emerge.

Enterprise Risk Management

Stantec's ERM program aligns with the ISO 31000:2018 Risk Management Standard (ISO 31000) and includes policies, practices, and systems to address our principal risks, which include, among others, cybersecurity, health and safety, project delivery, talent management, macroeconomic, market, geopolitical, fraud and ethics, organic growth, acquisitions and integrations, climate transition, and regulatory risks. We embed risk management approaches across the organization to support the business in making risk-aware decisions.

Our ERM process involves the continuous identification, analysis, evaluation, treatment, monitoring, and communication of risks. We evaluate principal and emerging risks and view each risk in relation to other risks because the risks considered, and the actions taken to mitigate them, may create new risks to the Company. Our ERM program allows us to address the interdependencies and interconnectedness of risks.

Governance

Stantec's Board of Directors provides strategic direction to and guidance on risk management. It has delegated responsibility for oversight of Stantec's ERM program to the Audit and Risk Committee (ARC), with our chief financial officer responsible for implementing the program. In addition to the ARC, the Sustainability and Safety Committee (SSC) provides oversight with a focus on health and safety and additional focuses on environmental, social, and governance (ESG) risks, including climate-related risks and the transition to a sustainable, net-zero economy. The Corporate Governance and Compensation Committee is responsible for corporate governance and ensures that management maintains policies designed to support an effective compliance, integrity, and ethics program.

The C-suite is directly accountable to the board for all risk management and risk mitigation practices. With the C-suite's oversight, responsibility for risk management is shared across the organization and is embedded into our day-to-day operations as well as in our key decision-making processes, such as strategic planning and project go or no-go decisions.

The C-suite is supported by numerous teams—Legal; Health, Safety, Security, and Environment (HSSE); Information Technology (IT); Finance; Corporate Sustainability; and others—that provide risk management and compliance functions across the organization and work with management to design and monitor appropriate risk mitigation.

Risk Identification and Assessment

We define our principal risks as those that may adversely and materially affect our business, financial position, results of operations, prospects, or our ability to deliver value to interested parties. We closely align the identification of our principal risks with the Company's strategic planning process, such that Stantec's key strategic initiatives are considered against our stated risk appetite and are appropriately managed to advance our strategy and deliver value to our shareholders.

Once identified, risks are analyzed and ranked based on inherent (before considering risk mitigation) and residual (after considering risk mitigation) risk scores that consider each risk's likelihood and impact. A risk's likelihood gauges the probability of the risk occurring, and its impact reflects our assessment of financial and strategic business consequences, including impacts to people, interested parties, reputation, compliance, clients, operations, and our financial position. Assessing both inherent and residual risks allows management to determine whether current risk management techniques are sufficient or if additional risk mitigation is required.

Stantec implements the guiding principles of ISO 31000 by following processes and practices to ensure that our ERM program is dynamic, inclusive, structured, responsive to Stantec's business, and based on the best available information. Accordingly, in the risk identification and assessment process, our ERM practitioners work closely with our senior leadership as well as experts who lead Stantec's other risk management functions, including Risk Management, Practice Services, HSSE, IT, Internal Audit, and Corporate Sustainability. We derive information from the Company's practice, geographic, and business operating unit leaders, and draw on the expertise of our Board of Directors.

Identified principal risks are entered into an internal risk register and a heat map which are updated and reported to the ARC on a quarterly basis. Each principal risk has corresponding controls and mitigation measures which are assigned to and executed by members of our management team. Policies and procedures are established and implemented to help ensure our response to a risk (avoiding, accepting, reducing, or sharing risk) aligns with our risk tolerance and appetite.

Please refer to Stantec's Annual Report for additional information on our principal risks.

Integrated Management System

Stantec's certified IMS delivers a disciplined and accountable framework that defines Company procedures, monitors risks and hazards, reduces inefficiencies, maximizes Company resources, and enables the implementation of our Sustainability Program. Our Practice Services team monitors operational compliance with risk mitigation strategies by conducting internal practice audits each year and is subject to annual external audits to assess compliance with Stantec's IMS.

Stantec's centralized IMS consists of global ISO certifications for Quality Management (ISO 9001:2015), Environmental Management (ISO 14001:2015), and Occupational Health and Safety Management (ISO 45001:2018). Additional certifications are held for IT Service Management (ISO/IEC 20000-1:2018) and Information Security Management (ISO/IEC 27001:2022). Stantec has achieved global ISO certification across the majority of its operations and geographies for the Quality Management, Environmental Management, Occupational Health and Safety Management and Information Security Management standards. Practice Services provides valuable feedback to the ERM program in identifying emerging risks, changes to principal risks, or areas for further improvement.

To help project teams manage and reduce future risks, Stantec's IMS includes a Lessons Learned process.[1] Extracting lessons from Stantec projects and translating them into recommendations helps us avoid repeating the same problems and enables us to replicate successful practices on other projects. Additionally, IMS maintains a Correction and Preventive Action system. This database is designed to identify root cause of quality conformity issues and implement corrections and appropriate actions to prevent recurrence in the future, effectively preventing future issues and improving overall quality by addressing root causes.

Client satisfaction is tracked and monitored through a series of surveys, including a net promoter score.[2] This allows us to periodically pulse our clients to understand how they feel about Stantec and provides us year-over-year insights into the health of our relationships.

While reviewing the IMS each quarter, executive leaders consider project management, leading and lagging health and safety indicators, progress against environmental goals, client feedback, and claims statistics. A quarterly IMS report is shared with the Board's ARC.

Business Continuity Management

Certain events, such as a cyber incident, natural disaster, communications outage, or pandemic, can interrupt our operations or prevent us from delivering services to our clients. Material business continuity risks to Stantec include the loss of IT systems, the impact of a pandemic on our operations, and emergency events that may impact our service delivery to clients at either the project or office level. Stantec has a comprehensive BCM program to identify, plan, and mitigate business continuity risks. Our BCM framework includes the following plans

- Corporate Crisis Management Plan
- Information Security Incident Response Plan
- Regional IT Disaster Recovery Plan
- Pandemic Preparedness Plan
- Emergency Response Plans at the local office level

A dedicated BCM governance team regularly reviews and updates Stantec's BCM program to ensure it continues to appropriately respond to and address interruption events. As part of this effort, these plans are subject to both internal and external audits.

Our IMS incorporates planning for business continuity to decrease the impacts of events such as extreme weather resulting from climate change, which could prevent us from delivering services to our clients. For example, if employees are impacted by floods, hurricanes, forest fires, or earthquakes, teams quickly activate disaster recovery programs and keep the business functioning during these challenges.

Climate Risks

Stantec's risk management approach strives to proactively address and mitigate emerging ESG risks, including climate-related risks, by developing appropriate policies and procedures. We track regulations and frameworks that might affect our Company, the way we deliver our services, and our clients.

Our risk management processes consider climate change, and we evaluate climate-related risks for potential short-, mid-, and long-term impacts. Climate risks have been identified at enterprise, operational, and project levels.

[1] Lessons Learned is an industry nomenclature to describe the sharing of knowledge or understanding gained by experiences that may have a positive or negative impact on a company.

[2] A net promoter score is an industry recognized benchmark for client loyalty where respondents rate how likely they are to recommend a company.

Stantec's ERM, Strategy, Finance, and Corporate Sustainability teams proactively identify, analyze, and manage climate-related risks. At enterprise level, Stantec identifies and monitors transitional and physical climate-related risks and has established task forces to manage these risks. Please refer to our Annual Report for information about our climate-related risks.

Operationally, Stantec has carbon management and reduction programs in place, and we evaluate weather-related risks when looking at new office space. Significant environmental impacts are also incorporated into Stantec's ISO 14001-certified EMS. Environmental risks, including those pertaining to climate, are considered within the required aspects and impacts registers. We follow ISO 14001 guidance to identify relevant environmental aspects and determine which activities have an impact on the environment under normal, abnormal, and emergency operating conditions.

While Stantec's Board carries out its risk oversight mandate, ESG risks are specifically the responsibility of the Executive ESG Committee and the Board's SSC.

Supporting Clients

Each project has unique risk conditions, and our overall project management process helps keep them top of mind for our project teams. Stantec's Project Management (PM) Framework provides a scalable framework to promote a pragmatic and disciplined approach to project delivery. It includes the critical tasks for managing risks and achieving quality delivery on typical projects.

For projects with risks that have the potential for significant financial or reputational impacts, we have a formal project risk review practice involving Project Risk Review Committees that consist of senior Stantec leaders and subject matter experts. Active projects are managed by project managers assigned through our project manager prequalification process who have competencies and experience appropriate for the project. In addition, project-independent reviewers are responsible for monitoring project planning and management through the project lifecycle, including financial performance and risk.

At a project level, Stantec's PM Framework considers sustainability topics such as climate change, air and water quality, energy and resource use, human rights, ethics, stakeholder engagement, and Indigenous relations. Impacts are evaluated during the proposal and the health, safety, security, and environmental planning stages and then reviewed through project audits.

Specific to climate, at a project level Stantec's Climate Solutions group and subject matter experts within each business operating unit review future climate impacts when approaching our designs. Our internal guidance outlines an enterprise-wide protocol for informing clients of the potential for increased risk of adverse impacts on their project due to climate change.

Accountability

We continually promote and communicate our commitment to quality, environmental stewardship, and continuous improvement. Stantec has formal mechanisms to encourage suggestions for process enhancements to address nonconformances and to identify opportunities for improvement and corrective action. We

- Have a comprehensive Code of Business Conduct (Code) that provides a framework for ethical decision making and outlines procedures to report any concerns about accounting, internal controls, auditing, or other financial or nonfinancial matters, including violations of applicable laws, regulations, or internal policies. For further information see our Management Approach: Ethics and Compliance.
- Monitor, via the ERM program, enterprise risks through ongoing management activities, separate evaluations, and the quarterly review of each risk's inherent and residual scores.

- Conduct independent audits over key financial and operational processes and develop an annual audit plan in consultation with management using a risk-based approach. Annually, we conduct independent assurance testing over financial and information technology controls in support of Sarbanes-Oxley certifications.
- Conduct internal practice audits annually that cover all regions and business lines (for compliance with ISO 14001, 45001, 9001, and IMS requirements) and are externally audited each year by an independent certification and accreditation body.
- Track client satisfaction by conducting surveys to assess performance, identify and prioritize improvement, and year-over-year relationships (satisfaction consistently measures above 90%).
- Identify, review, approve, communicate, and document the impacts of practice changes; initiate change management procedures; review unintended consequences of changes; and act to mitigate adverse effects.
- Include quality management targets as key performance indicator in Stantec's executive sustainability pay link.

Material Topics / Value Chain Nodes Covered:

Risk Management – Overall / Operations

Risk Management – Climate / Operations, Downstream (Clients)

See all Stantec Management Approaches