Enterprise Risk Management

Halliburton's risk-assessment process relies on a consistent, systematic, integrated approach to risk and includes an annual review of items that have the potential to impact our business continuity, strategy, and crisis management. Halliburton reports to the Board of Directors on the results of the risk-assessment process. This process is part of Halliburton's Enterprise Risk Management (ERM) program, which is designed to identify, mitigate, and manage enterprise-level risks to our organization as well as other strategic risks.

Our Risk Management Sustainability Commitments

- Streamline risk categories, risk identification, and risk management to ensure alignment with Halliburton strategy and focus on what matters most.

- Enhance cross-functional visibility to and collaboration among key stakeholders throughout the organization to ensure a consistent, uniform, and strategic approach to risk assessment, identification, and mitigation.

Annual Enterprise Risk Assessment

Halliburton's annual risk-assessment process continued in 2024. We conduct this process in collaboration with a global leader in ERM programs. This streamlined and collaborative approach to strategic risk assessments is one way we identify and prioritize top risks.

The process consists of annual workshops that facilitate open dialogue, debate, and existent and emergent risk evaluation. This year, 66 Halliburton executives participated to discuss, evaluate, and score risks based on their potential impact, likelihood of occurrence, and risk-mitigation preparedness. Workshop results provided valuable feedback to help us focus our attention on risk-mitigation and opportunities for process optimization. We incorporate insights gained into upcoming plans and utilize them to help Halliburton minimize risks and maximize opportunities as we achieve our strategic plans.

Global IT Infrastructure

Halliburton's IT strategy includes infrastructure, networks, and applications that provide agility, scalability, and flexibility to our business and customers. This design aligns with and supports our broader digital and automation strategy.

Maintenance of ubiquitous global connectivity at Halliburton is key. To provide the most cost-efficient resources for our users and locations, we conduct ongoing updates to our internal and external connectivity options.

We also continue our efforts to rationalize and optimize all applications deployed to cloud-based digital platforms. This includes applications that are new to the cloud as well as those we migrated from previous platforms.

Field employees use Sensori™ fracture monitoring service for real-time subsurface analysis

Cybersecurity

Halliburton takes every threat to cybersecurity seriously. In 2024, Halliburton increased cybersecurity oversight by appointing a new Chief Information Security Officer who is independent of our IT and Technology functions.

We invest significant resources to protect our systems and data. We do this in ways that align with industry standards, such as the National Institute of Standards and Technology (NIST) Cyber Security Framework, NIST 800-53, NIST 800-82, and International Electrotechnical Commission 62443.

In 2024, Halliburton continued to perform Operational Technology (OT) security assessments and remediation for all of our product lines. These remediation activities strengthen governance of cyber controls, enable us to evaluate and mitigate evolving cyber risks, and improve our product line network segmentation, monitoring, and endpoint security management.

We require all Halliburton personnel to complete our annual cybersecurity training course and OT Security training. This helps equip our employees to be more vigilant about cybersecurity threats.

Training on select subjects, such as phishing and privileged access management, is required for specific groups of Halliburton personnel. We maintained optional access to these courses for the rest of our employee population.

We further strengthened our information security posture this year by improving security for all employees and contractors. We are implementing solutions that provide a uniform experience for employees who work at home and in the office with advanced off-network protection for user endpoints and improved security visibility.