G2

Enterprise Risk Management

Halliburton takes a consistent, systematic, and integrated approach to our Enterprise Risk Management (ERM) program, which our Board of Directors oversees. Designed to identify, mitigate, and manage enterprise-level risks to our organization, our ERM assessment process includes a review of items that may impact company strategy, business continuity, and crisis management — among other strategic risks to the Company.

Our Risk Management Sustainability Commitments

- Streamline risk categories, risk identification, and risk management to ensure best alignment with Halliburton strategy and place a critical focus on what matters most.
- Enhance cross-functional visibility to and collaboration among key stakeholders throughout the organization to ensure consistency, uniformity, and a strategic approach to risk assessment, identification, and mitigation.

2021 HIGHLIGHTS

Enhancements to Risk Controls

Through our risk assessment process, we continually review our risks to ensure that the Company focuses on those with the greatest potential impact to our organization. We embed any identified risks into our strategic planning for the years ahead.

In 2021, as part of the risk identification phase of our assessment, our ERM group surveyed a broad group of more than 190 leaders representing different parts of the Company around the world and interviewed 29 senior-level, strategic leaders. We reported the findings to the Board of Directors' Audit Committee, as well as to leaders who manage a part of the organization with an identified risk.

Global IT Infrastructure

Halliburton is on a strong path to advance our digital capabilities — doing so will allow us to reduce capital expenditures, enhance security, speed delivery, and improve service quality (SQ). A shift is underway to transfer applications and data from our physical data centers into a cloud-based digital platform while retaining a smaller number of network hubs that ensure secure access to cloud resources. When we complete this initiative, our physical footprint contained within these network hubs will decrease by 77% from 2020. Last year, our team transferred significant amounts of our computer and storage workload to the cloud and are on target to complete all scheduled moves by the third quarter of 2022.

Cybersecurity

The frequency and sophistication of global attacks on corporate IT systems containing sensitive information have increased. Halliburton takes each threat seriously and dedicates significant resources to protect our IT systems and data, in alignment with industry security standards, such as the International Organization for Standardization (ISO) 27001 and the National Institute of Standards and Technology (NIST) 800-53. In response, our Board of Directors now receives quarterly updates on cybersecurity matters, and our Audit Committee receives an annual, in-depth review.

The Landmark iEnergy® platform completed a System and Organization Controls (SOC 2) Type 1 audit for security and availability. An SOC 2 Type 1 audit evaluates and certifies design effectiveness of IT system controls. The platform is currently undergoing an SOC 2 Type 2 audit, which certifies that controls are in place and working as designed.

Halliburton employees share their knowledge and contribute to many industry organizations. In 2021, our Chief Information Security Officer served as board member and treasurer for the Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC), an organization that shares intelligence on cybersecurity incidents, threats, vulnerabilities, and best practices to improve security measures within companies throughout our industry.

Halliburton subscribes to best-practice design philosophies for IT systems that include "zero trust," which uses techniques such as:

- Multi-factor authentication to verify the credentials of users' identities and devices
- "Defense in depth," which puts in place multiple layers of protection
- "Least privilege," which limits the content that individual users can access

Our cybersecurity team includes thought leaders who expand knowledge of their expertise. Team members contributed to the following publications for the World Economic Forum Cyber Resilience in Oil and Gas community:

- *Cyber Resilience in the Oil and Gas Industry: Playbook for Boards and Corporate Officers*
- *Advancing Supply Chain Security in Oil and Gas: An Industry Analysis*

Through the pandemic, as employees work remotely and access our Company systems, stringent security measures are vital to protect our computing assets, networks, data, and users. A key initiative to further strengthen our security posture and improve user experience and productivity is upgrading our Enterprise Identity and Access Management solution.

In addition to our own asset protection, we work with our customers to provide assurance of adequate operational technology (OT) security by participating in International Electrotechnical Commission (IEC) 62443-based assessments.

Physical Security

Workplace Violence Prevention

Our employees' safety is paramount at Halliburton, and the maintenance of a secure and safe workplace is one of our key priorities. Fundamental to our workplace safety is commitment to our Code of Business Conduct (COBC) and established security controls. Additionally, we regularly communicate with employees and managers on how to recognize, report, and manage threats of violence. In 2021, our Corporate Security team developed and delivered targeted training modules for key staff members to enhance our ability to respond to threats of violence. We recognize that early identification and pragmatic management of these incidents are crucial factors to reduce and mitigate the risk of violence occurring in the workplace.