ENTERPRISE RISK MANAGEMENT

Halliburton's risk-assessment process relies on a consistent, systematic, integrated approach to risk, and includes a yearly review of items that have 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.

ANNUAL ENTERPRISE RISK ASSESSMENT

Halliburton's refreshed risk-assessment process continued in 2023. We conduct this process with our partnership 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 yearly workshops that facilitate open dialogue, debate, and existent and emergent risk evaluation. This year, 79 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 for focusing risk-mitigation attention and opportunities for process optimization. We incorporate insights gained into upcoming plans and utilize them to help Halliburton minimize risks and maximize opportunities as it achieves its strategic plans.

Our Risk Management Sustainability Commitments

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

GLOBAL IT INFRASTRUCTURE

Halliburton's IT strategy includes modernized 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. We continue our efforts to 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. These efforts reduced the on-premise infrastructure required for our work. At the end of 2023, we achieved our goal to reduce our global data center footprint by 75%.

CYBERSECURITY

Halliburton takes every threat to cybersecurity seriously. Our Board receives quarterly updates about cybersecurity matters and Halliburton's Audit Committee receives an in-depth annual review on the topic.

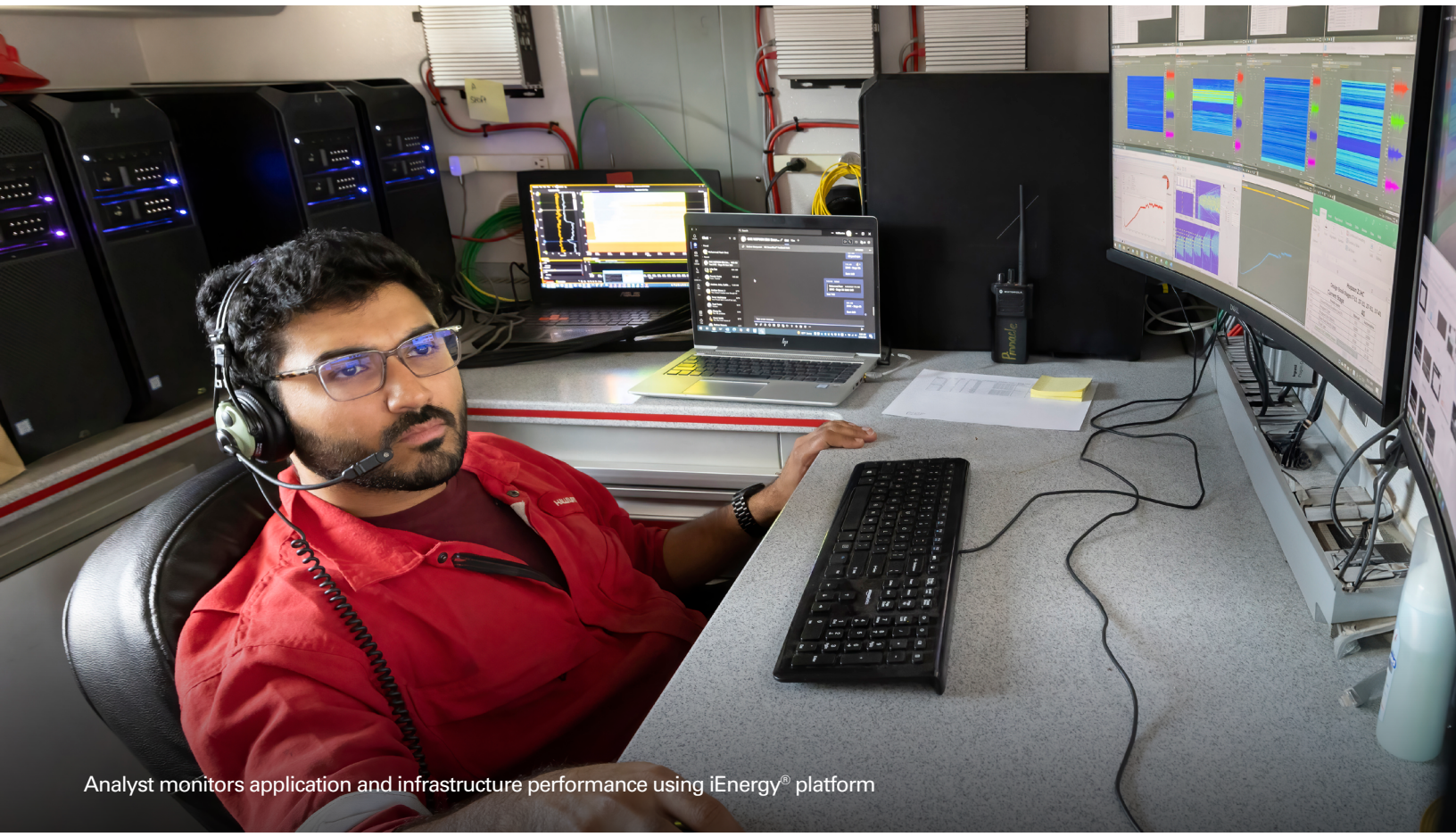
Halliburton invests significant resources to protect our systems and data. We do this in ways that align with industry standards, such as the National Institute of Standards and Technology (NIST) Cyber Security Framework, NIST 800-53, NIST 800-82, and International Electrotechnical Commission 62443.

The following are examples of measures taken to implement our Defense-in-Depth design philosophies for Information Technology (IT) and Operational Technology (OT) systems:

- Multi-factor authentication, which verifies users' identities beyond their credentials
- "Zero trust," which establishes layers of protection for users and devices
- "Least privilege," which limits the content individual users can access

Halliburton continued to perform OT security self-assessments for all of our product lines in 2023. These assessments promote proper governance of cyber controls; help us evaluate evolving cyber risks; and improve our product line network segmentation, monitoring, and endpoint security management. We regularly evaluate advanced cybersecurity technologies with potential to help Halliburton expand our portfolio of OT security solutions.

In 2023, we further enhanced our annual cybersecurity training program. We launched additional training on specific subjects, such as phishing and privileged access management, that are now required for select groups of Halliburton personnel and optional for the rest of our employees. The groups that are required to complete these new training courses do so alongside Halliburton's annual cybersecurity training course, which is required of all our employees and contractors. We also added a new OT Security training that is required for all Halliburton employees and contractors.



Analyst monitors application and infrastructure performance using iEnergy® platform

Halliburton chemical reaction plant in Saudi Arabia

PHYSICAL SECURITY

Halliburton takes active steps to protect the physical safety of employees. Where employees' work responsibilities might cause risks to their physical safety, we have established safety procedures and infrastructure to minimize those risks.

Our security team monitors and assesses current and developing global security risks where Halliburton operates. It works collaboratively with local management teams to develop and execute security plans. These efforts include controls designed to enhance the security of Halliburton's personnel and assets.

Workplace Violence Prevention

Halliburton works to maintain a secure and safe workplace environment for all of our employees. Our Code of Business Conduct (COBC) and security controls are the foundation of workplace safety at Halliburton. Through on-demand training, we communicate with employees and managers about the best ways to recognize, report, and manage threats of violence.

Global Travel Risks

Halliburton operates business on a global scale. We use our network of security specialists and our 24-hour Global Security Operation Center (GSOC) to monitor global security conditions and associated risks. Because we maintain vigilant attention to global security conditions, we can warn our employees about threats, incidents, or local developments that may affect them on business-related travel.

Autonomous Security Technology

In 2023, we continued to integrate security technologies to provide enhanced capabilities for security operations, emergency response, and autonomous access control. This included the extension of our drone program, which recorded over 1,000 miles flown and improved our overall situation awareness.