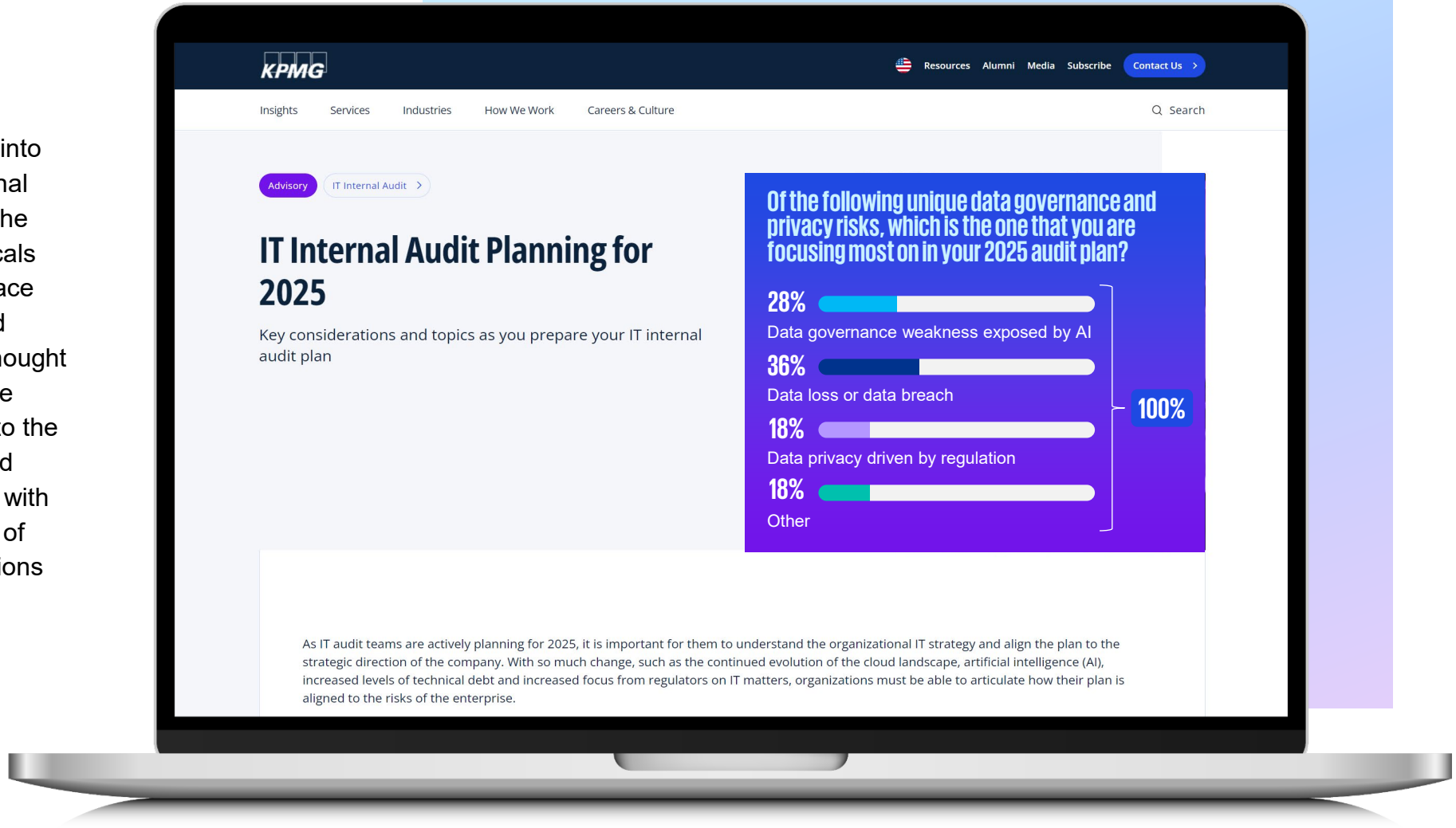
KPMG

Advanced IT internal audit planning for 2025 and beyond

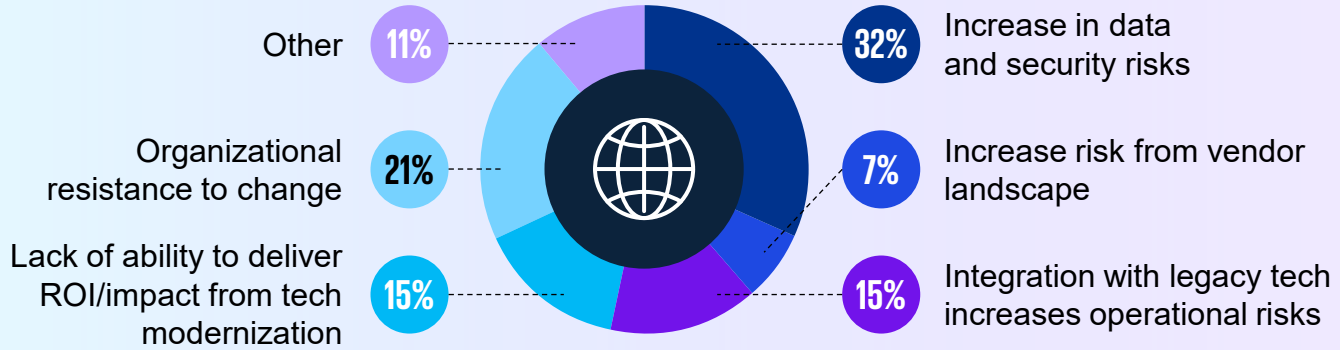
A focus on the energy, natural resources, and chemicals sectors

Introduction

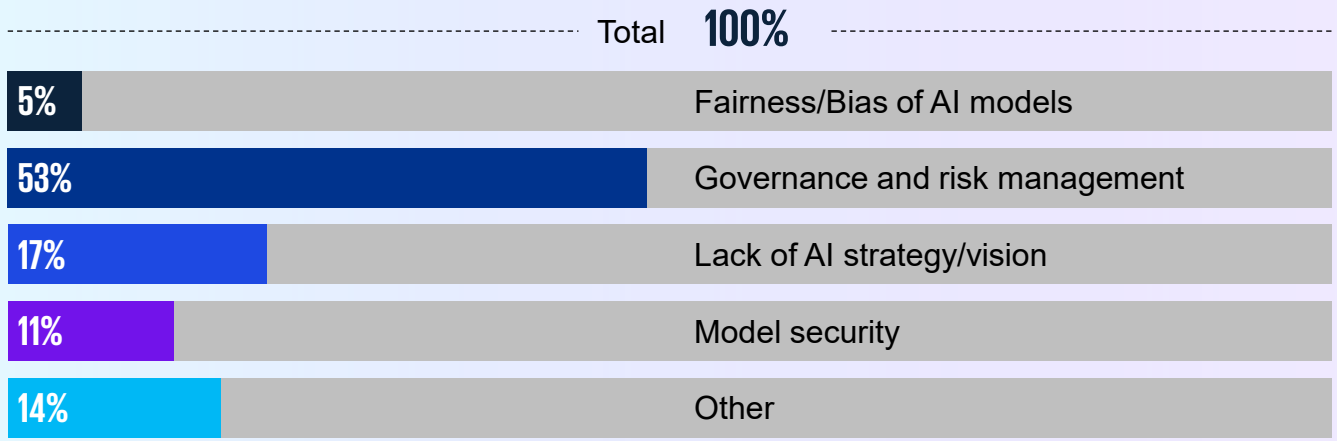
In this latest publication, we will delve into the transformative potential of IT internal audits in guiding organizations within the energy, natural resources, and chemicals (ENRC) industries. As these sectors face rapid technological advancements and evolving regulatory landscapes, this thought leadership piece focuses on the unique challenges and opportunities specific to the ENRC industry. Here, we offer targeted audit considerations designed to align with the strategic goals and specific needs of this dynamic sector, helping organizations navigate the future with confidence.



Of the following unique technology modernization risks, which is the one that you are focusing most on in your 2025 audit plan?



Of the following unique AI risks, which is the one that you are focusing most on in your 2025 audit plan?



Strategic alignment and industry-specific value creation

For IT internal audit to genuinely serve as a strategic partner within the ENRC industries, the audit planning process must address the industries' unique challenges, such as managing complex global supply chains and ensuring the security of sensitive data amid increasing digitalization and regulatory scrutiny. The objective is to create a value-driven audit plan that not only mitigates risks but also fosters growth and innovation within the sectors.

Industry-specific audit considerations

In our published paper, we explore the "Top Risks" areas of focus for 2025, and here we expand to drill down on how they manifest for the power and utilities sector. This industry-specific lens underscores the importance of tailoring audit strategies to address the nuanced needs and challenges of the industry.

Power and utilities

1. **Physical security and cybersecurity convergence**: As physical and cybersecurity risks converge, particularly at critical infrastructure sites, audits must evaluate the integration of physical security measures with cybersecurity practices to prevent both physical and cyber intrusions.

2. **Supply Chain cybersecurity**: The security of a utility's supply chain is crucial, especially with increased reliance on third-party vendors for critical software and hardware. Audits need to ensure comprehensive risk assessments are performed on all suppliers and that continuous monitoring systems/processes are in place.

3. **Business continuity and disaster recovery**: Ensuring continuity of operations during and after major disruptions is essential. Audits should test the effectiveness of disaster recovery plans and business continuity procedures, focusing on IT systems and operational technology.

4. **Legacy technology and system obsolescence**: Legacy systems used by utilities pose significant risks due to potential incompatibilities and outdated security measures. Audits should assess the risks associated with maintaining these systems and should evaluate the strategic plans for technology upgrades or transitioned

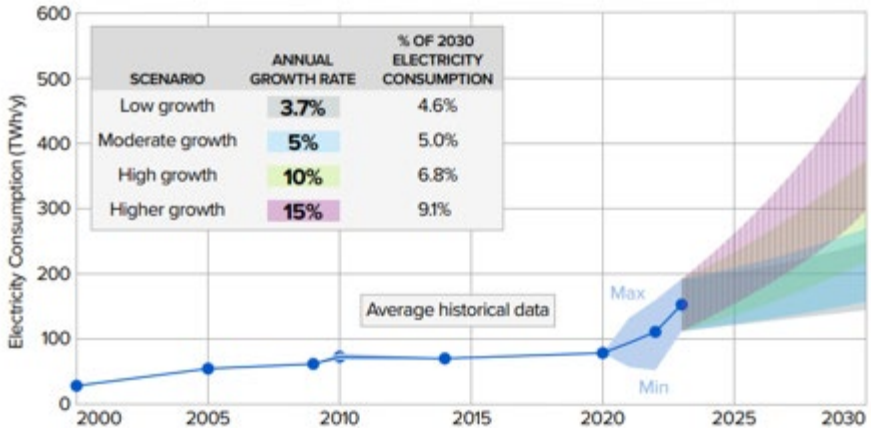
5. **Endpoint security management**: The increase in remote work, the variety of endpoint types existing in technology environments, and mobile device usage extends the utility's attack surface. Risks also exist around configuration drift as similar technologies may be deployed with different levels of protection/software. Audits must evaluate endpoint security strategies, including device management, encryption practices, monitoring capabilities, and access controls.

Risk Spotlight – Hyperscaler energy needs to serve AI demand

The rapid expansion of data centers driven by the growing demand for AI and cloud computing is presenting significant challenges for utilities and generation companies. This unprecedented growth places immense pressure on the existing energy infrastructure, leading to a variety of risks. These include the concentration of data centers in specific regions causing localized grid stress, increased environmental impact and carbon footprint of high energy consumption, the mismatch between energy supply and increasing demand, the substantial financial investments and regulatory hurdles in upgrading infrastructure, and the heightened cybersecurity threats to critical energy systems. Addressing these risks is essential to ensuring the stability, reliability, and sustainability of our energy supply.

Key risks for internal auditors to consider:

1. **Geographic concentration risks:** The concentration of data centers in specific regions may lead to localized grid stress and potential failures.
2. **Sustainability and environmental risks:** High energy consumption increases the carbon footprint and poses environmental challenges. While data center providers strive to use sustainable energy sources, with a trending preference to use persistent and reliable ones such as nuclear power, increasing demand is primarily being met through natural gas consumption.
3. **Energy supply and demand mismatch:** Rapid growth in data center energy demand may outpace power companies' ability to supply electricity reliably, leading to potential capacity strain, increased costs being passed to local residents, and peak load management issues.
4. **Infrastructure investment and upgrade risks:** Significant investments in grid infrastructure (including generation assets) to accommodate new data center loads present financial and operational challenges, including high up-front costs and regulatory delays.
5. **Cybersecurity risks:** Data centers' high energy demands make critical infrastructure attractive for ransomware and malware attacks, threatening operational continuity.
6. **Technology integration risks:** Integrating new technologies to manage increased power consumption efficiently in data centers can be complex and affect overall system performance.
7. **System reliability and downtime risks:** The increased reliance on IT systems for managing the higher energy loads of data centers can lead to operational disruptions if these systems experience failures or require maintenance.



Source: *Electric Power Research Institute, Figure ES-1: Projections of potential electricity consumption by U.S. data centers: 2023–2030, Analyzing Artificial Intelligence and Data Center Energy Consumption, May 2024*

Industry-specific audit considerations

In our published paper, we explore the "Top Risks" areas of focus for 2025, and here we expand to drill down on how they manifest for upstream services sector. This industry-specific lens underscores the importance of tailoring audit strategies to address the nuanced needs and challenges of the industry.

Upstream oil & gas

1. **Assets and operations:** The reliance on legacy systems and aging physical assets in utilities'upstream infrastructure presents risks due to potential incompatibilities and outdated maintenance. Comprehensive audits are necessary to assess these risks and evaluate strategic plans for upgrades or transitions to more efficient solutions. This proactive approach ensures the continued reliability, efficiency, and safety of utility services amid evolving operational demands.

2. **Operating model:** In the ever-evolving landscape of the upstream energy sector, a robust IT operating model is essential for driving operational efficiency, streamlining processes, and enhancing data management. With ongoing digital transformations, it is critical to have a coherent IT strategy that aligns with business goals.

3. **Cyber and third parties:** Audits are crucial for assessing the integrity and security of IT systems managing supplier relationships, data exchange, and procurement processes. By identifying vulnerabilities and ensuring robust cybersecurity measures, these audits help mitigate risks related to data breaches, compliance issues, and operational disruptions. This proactive approach ensures a secure and resilient supply chain, supporting the efficiency and reliability of upstream services.

4. **Technology and data:** AI technologies are being used in upstream operations to improve efficiency and decision-making in areas such as predictive maintenance and reservoir management. This integration requires robust ethical, regulatory, governance, security, and data management practices. Audits should assess the development, deployment, and impact of AI systems to ensure responsible use and establish strong governance and security measures.

Industry-specific audit considerations

In our published paper, we explore the "Top Risks" areas of focus for 2025, and here we expand to drill down on how they manifest for midstream services sector. This industry-specific lens underscores the importance of tailoring audit strategies to address the nuanced needs and challenges of the industry.

Midstream oil & gas

1. **Cybersecurity:** Cyberattacks (including ransomware, phishing, and other malicious activities) pose a substantial risk to midstream companies. These attacks can target critical infrastructure, resulting in operational disruptions, data breaches, financial losses, and damage to reputation.

2. **Legacy systems and integration:** Many midstream companies still rely on legacy IT systems that may not integrate well with newer technologies. This can lead to inefficiencies, data silos, and an increased risk of system failures.

3. **Data management and integrity:** Midstream operations generate vast amounts of data, from sensor data to transactional information. Ensuring the accuracy, security, and integrity of this data is critical. Poor data management can lead to operational inefficiencies, regulatory compliance issues, and decision-making based on inaccurate information.

4. **Supply chain and third-party risks:** Increasing reliance on third-party vendors and service providers, including cloud service providers and other IT partners, introduces risks related to the security and reliability of those third parties. A security breach or failure in a third-party system can propagate and affect midstream operations.

5. **Regulatory compliance and legal risks:** As regulations concerning data privacy, cybersecurity, and digital operations evolve, midstream companies must ensure ongoing compliance with a complex and changing regulatory landscape. Noncompliance can result in financial penalties, legal action, and reputational harm.

Industry-specific audit considerations

In our published paper, we explore the "Top Risks" areas of focus for 2025, and here we expand to drill down on how they manifest for the chemicals sector. This industry-specific lens underscores the importance of tailoring audit strategies to address the nuanced needs and challenges of the industry.

Oil & gas refining, chemicals

1. **Cybersecurity:** Cyberattacks, including ransomware, phishing, and advanced persistent threats (APTs), are a significant concern. Attackers may target critical infrastructure to cause operational disruptions, steal intellectual property, or demand ransom payments.

2. **Operational technology (OT) security:** The integration of IT and operational technology (OT) systems in refining and chemical plants increases the risk of cyberattacks on operational technology. OT systems control critical processes, and any compromise could lead to catastrophic safety incidents and significant financial loss.

3. **Regulatory compliance and data privacy:** Compliance with environmental, safety, and data protection regulations is crucial. Noncompliance can result in significant legal penalties, shutdowns, and reputational damage. Regulations such as the General Data Protection Regulation (GDPR) and industry-specific standards must be adhered to.

4. **Supply chain and third-party risks:** The refining and chemicals sector relies on a complex supply chain and third-party vendors for IT services, raw materials, and logistics. Any disruption or security breach within the supply chain can have a ripple effect, affecting the entire operation.

5. **Legacy systems and infrastructure:** Many refining and chemical companies operate with legacy IT and OT systems that may be outdated and vulnerable to cyber threats. These systems often lack modern security features and may not integrate well with new technologies.

Industry-specific audit considerations

In our published paper, we explore the "Top Risk" areas of focus for 2025, and here we expand to drill down on how they manifest for the energy services sector. This industry-specific lens underscores the importance of tailoring audit strategies to address the nuanced needs and challenges of the industry.

Services & equipment

1. **Remote operations and field technician security:** The use of remote monitoring, control systems, and connectivity for field operations and engineering services introduces unique cybersecurity challenges. Audits should assess security measures around remote access, communication protocols, and device management.

2. **Data governance and privacy in service operations:** Managing sensitive project and operation data requires stringent governance and privacy practices. Audits should evaluate data governance frameworks, ensuring that privacy practices comply with industry regulations and standards.

3. **Cybersecurity implications of emerging technologies used by service providers:** The adoption of emerging technologies such as AI, the Internet of Things (IoT), and blockchain introduces new cyber risks. Audits should evaluate the cybersecurity measures in place for these technologies, ensuring vulnerabilities are adequately addressed.

4. **Control system segmentation and isolation:** Segregating control systems from corporate networks reduces risks of breach propagation. Audits should assess the segmentation and isolation practices in place to protect sensitive control systems from broader network threats.

5. **Cloud and data center security:** As energy service providers increasingly leverage cloud technologies and data centers for operational efficiencies, audits must examine the security of these environments, focusing on data encryption, access controls, and compliance with industry standards.

Industry-specific audit considerations

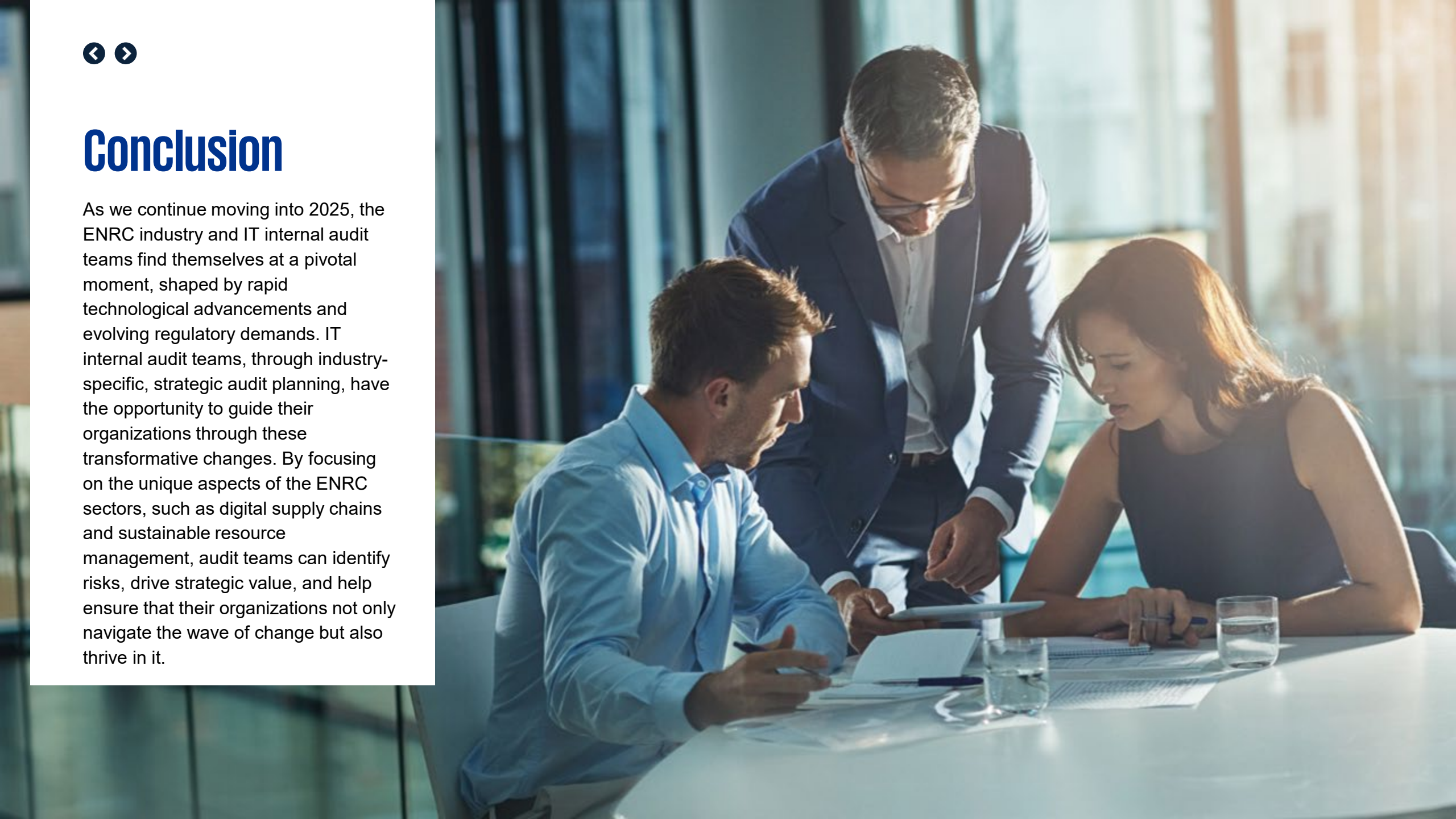
In our published paper, we explore the "Top Risks" areas of focus for 2025, and here we expand to drill down on how they manifest for the mining sector. This industry-specific lens underscores the importance of tailoring audit strategies to address the nuanced needs and challenges of the industry.

Mining

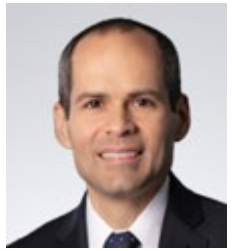
1. **Industrial control system (ICS) security:** Given the critical role of the industrial control system (ICS) in mining operations, audits must evaluate the security and resilience of ICS against cyber threats, assessing both network protections and physical access controls to prevent sabotage or unauthorized manipulation.
2. **IoT and sensor network security:** With the growing use of IoT devices and sensors in mining operations for real-time monitoring and automation, audits need to focus on the security measures in place to protect these devices from cyberattacks and ensure the integrity and reliability of collected data.
3. **Remote and autonomous operations security:** The advancement of remote and autonomous mining operations introduces new cybersecurity risks. Audits need to assess the security of remote operation centers, communication channels, and autonomous systems to safeguard against cyber intrusions and disruptions.
4. **Cyber-physical risk management:** The integration of digital and physical systems in mining necessitates robust risk management practices. Audits should examine the protocols for identifying, assessing, and mitigating cyber-physical risks to ensure the safety and security of mining operations.
5. **Employee awareness and training programs:** Human factors remain a significant vulnerability in cybersecurity. Audits should evaluate the adequacy and effectiveness of cybersecurity awareness and training programs for employees at all levels, ensuring they are equipped to recognize and respond to potential security threats.

Conclusion

As we continue moving into 2025, the ENRC industry and IT internal audit teams find themselves at a pivotal moment, shaped by rapid technological advancements and evolving regulatory demands. IT internal audit teams, through industry-specific, strategic audit planning, have the opportunity to guide their organizations through these transformative changes. By focusing on the unique aspects of the ENRC sectors, such as digital supply chains and sustainable resource management, audit teams can identify risks, drive strategic value, and help ensure that their organizations not only navigate the wave of change but also thrive in it.



Contact us



Joshua Galvan

Principal, ENRC IA Lead
M: 713-492-8259
E: jgalvan@kpmg.com

Lavin Chainani

Managing Director, ENRC IA Lead
M: 443-825-0751
E: lchainani@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**