# Navigating Third-Party Risks in Energy & Utilities

Trends, Challenges and Solutions

# Contents

# Introduction

**The Energy & Utilities (E&U) sector plays a critical role in the global economy, providing essential services such as power generation, transmission and distribution, as well as water and gas supply.**

These services form the backbone of modern society, supporting a wide range of industries and ensuring the functioning of our day-to-day lives. Given its vital importance, this sector faces a unique set of challenges in terms of risk management, particularly when it comes to third-party relationships.

In recent years, the E&U sector has become increasingly reliant on third-party relationships to achieve cost efficiencies, access specialized expertise, and implement innovative technologies. From technology providers and contractors to suppliers and service providers, these third-party relationships have become an integral part of the sector's operations. However, this increased reliance on external partners also exposes organizations to a range of third-party risks that must be effectively managed.

This whitepaper gives insight into the growing importance of Third-Party Risk Management, the key risks for the Energy & Utilities sector, the benefits of effective Third Party Risk Management, the specific challenges and NTT DATA's approach & solution to address them.

CHAPTER 1

# The Evolving Third-Party Risk Landscape

### Growing reliance on technology and digitalization

The E&U sector has experienced rapid digitalization and technological advancements in recent years, with organizations adopting new technologies to improve efficiency, reduce costs and meet the evolving demands of consumers. These advancements include smart grids, renewable energy sources, digital twins, and the Industrial Internet of Things (IIoT). As a result, the sector's reliance on third-party technology providers has grown, increasing the potential for risks associated with data breaches, cyberattacks and technology failures.

### Increasing interconnectivity and interdependence

Modern E&U systems are characterized by a high degree of interconnectivity and interdependence, both within the sector and with other critical infrastructure. This interconnectedness enhances the efficiency and resilience of the energy grid, but it also increases the potential for cascading failures and exposes organizations to risks originating from their third-party partners.

### Evolving regulatory and compliance requirements

Regulatory requirements and compliance standards are continuously evolving to address new risks and challenges in the E&U sector. These changes may include enhanced cybersecurity requirements, more stringent environmental regulations, and increased focus on supply chain security. As a result, organizations must ensure that their third-party partners are compliant with relevant regulations, as failure to do so could lead to significant fines, reputational damage, and even operational disruptions.

### EU initiatives: NIS-2 and Corporate Sustainability Due Diligence

The NIS-2 directive and the Corporate Sustainability Due Diligence directive are two regulatory frameworks that have significant implications for third-party risk management in the E&U sector. The NIS-2 directive, which is the revised version of the EU Network and Information Systems Directive, aims to strengthen the cybersecurity and resilience of critical infrastructure across the European Union (EU). The directive requires operators of essential services, including those in the E&U sector, to take measures to identify and mitigate the risks posed by their supply chains. The directive entered into force in January '23 and needs to be adopted by member states in national laws before October '24.

In the beginning of 2022, the Commission adopted a proposal for a Directive on Corporate Sustainability Due Diligence. The aim of this Directive is to foster sustainable and responsible corporate behaviour and to anchor human rights and environmental considerations in companies' operations and corporate governance. The new rules will ensure that businesses address adverse impacts of their actions, including in their value chains inside and outside Europe.

### Climate change and environmental risks

Climate change and environmental risks are increasingly impacting the E&U sector. These risks include the physical effects of climate change, such as extreme weather events, as well as the transition risks associated with the shift towards a low-carbon economy. Organizations must be proactive in managing these risks and ensuring that their third-party partners are taking appropriate steps to mitigate their environmental impact and adapt to the changing climate.

### Geopolitical risks and supply chain disruptions

Geopolitical risks, such as trade disputes, regional conflicts, and political instability, can have significant implications for the E&U sector. These risks can disrupt supply chains, impact the availability and cost of critical resources, and hinder the sector's ability to deliver essential services. As organizations increasingly rely on third-party suppliers and partners across the globe, they must be prepared to manage the potential risks that may arise from geopolitical events and supply chain disruptions.

In summary, the third-party risk landscape in the E&U sector is becoming increasingly complex and challenging. The growing reliance on technology and digitalization, increasing interconnectivity and interdependence, evolving regulatory requirements, climate change, and geopolitical risks all contribute to the need for robust third-party risk management strategies. By proactively addressing these risks, organizations can better protect their operations, reputation, and bottom line.

CHAPTER 2

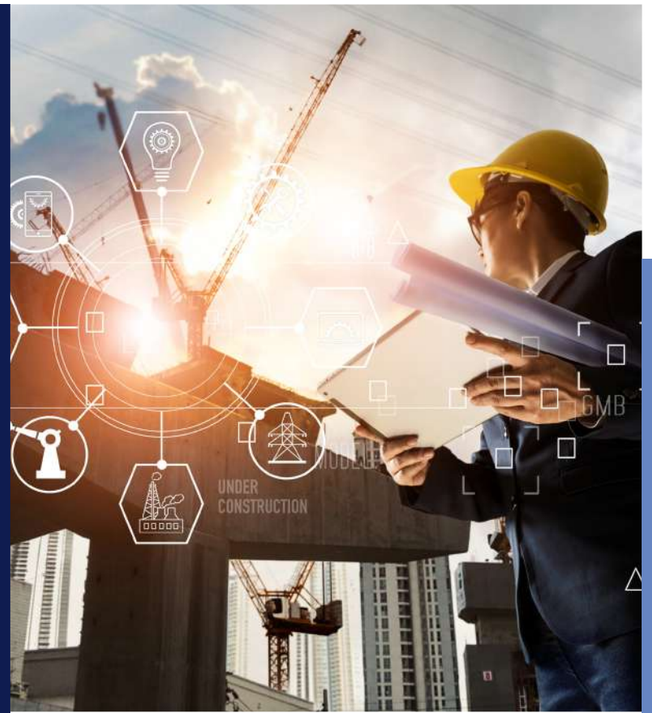
# Key Third-Party Risks in the E&U Sector

### Cybersecurity risks

As the E&U sector becomes more digitally interconnected, cybersecurity risks have emerged as a significant concern. Third-party technology providers and vendors may inadvertently introduce vulnerabilities into an organization's systems, making them susceptible to data breaches, cyberattacks, and unauthorized access. Cybersecurity risks can lead to disruptions in critical infrastructure, loss of sensitive data, financial losses, and reputational damage. Organizations must carefully assess the cybersecurity practices and capabilities of their third-party partners to minimize these risks.

**In 2020, a cyber attack on a third-party provider of services to the Portuguese utilities company, EDP - Energias de Portugal, resulted in the exposure of sensitive data of EDP's customers and employees. The breach was caused by a vulnerability in the IT systems of the third-party provider, which allowed hackers to gain access to EDP's network.**

RagnarLocker ransomware hits EDP energy giant, asks for €10M (bleepingcomputer.com)




### Operational risks

Operational risks refer to the potential disruptions or failures in an organization its processes, systems or infrastructure, often resulting from third-party involvement. These risks can stem from inadequate maintenance, poor integration of new technologies, or insufficient oversight of subcontractors and service providers. Operational risks can lead to service outages, equipment failures, and even accidents, affecting the reliability and safety of the services provided by energy and utilities organizations.

**In March 2019, Norsk Hydro, a Norwegian aluminium and renewable energy company, suffered a ransomware attack by the LockerGoga group. The cyberattack disrupted the company's operations across Europe and the United States, forcing it to switch to manual operations at some of its facilities. The company decided not to pay the ransom and instead focused on restoring its systems from backups. The attack resulted in financial losses estimated at around $40 million.**

Norsk Hydro's initial loss from cyber attack may exceed $40 million | Reuters

### Regulatory and compliance risks

The E&U sector is subject to a wide range of regulatory requirements and compliance standards, which vary across different jurisdictions and are constantly evolving. Third-party partners must adhere to these requirements to ensure the organization remains compliant. Failure to do so can result in fines, sanctions, legal actions, and reputational damage. Organizations must monitor their third-party partners' compliance with relevant regulations, standards, and industry best practices to mitigate regulatory and compliance risks.

**In 2021, Petrofac, a UK based oilfield service company, was fined €77 million by the UK regulator for failing to prevent corruption in its contracts with third-party intermediaries. The company had failed to conduct adequate due diligence on its third-party intermediaries, leading to the payment of bribes to foreign officials.**

Serious Fraud Office secures third set of Petrofac bribery convictions - Serious Fraud Office (sfo.gov.uk)

### Environmental, social, and governance (ESG) risks

ESG risks are increasingly relevant for the E&U sector, as stakeholders and regulators demand greater accountability and transparency in managing environmental impacts, social responsibilities, and governance practices. Third-party partners can introduce ESG risks into an organization's operations, such as poor environmental management, labor rights violations, or unethical business practices. Organizations must conduct thorough due diligence on their third-party partners to ensure they meet ESG standards and implement robust monitoring and reporting mechanisms to track their performance.

**In 2021, TotalEnergies (formerly known as Total), a French multinational oil and gas company, faced criticism over its operations in Myanmar. The company was accused of indirectly financing the military junta by paying taxes to the government for its gas project, the Yadana gas field, which was operated in partnership with other international companies. The Myanmar military was alleged to have been involved in human rights abuses, including violence against protesters following the coup in February 2021.**

Total, Chevron suspend payments to Myanmar junta from gas project | Reuters

### Financial risks

Third-party financial risks are a significant concern for companies in the E&U sector. These risks can arise when a company relies on a third-party supplier or partner for critical goods or services, and that third party experiences financial difficulties or goes bankrupt. Such situations can have severe consequences for companies, including supply chain disruptions, delayed projects, and financial losses.

**In January 2018, Carillion, a major UK construction and facilities management company, went into liquidation due to significant debt and a series of unprofitable contracts. EDF Energy, a UK-based energy supplier and part of the French state-owned utility EDF, had contracted Carillion for facilities management services at its nuclear power stations in the UK. The collapse of Carillion left EDF Energy scrambling to find alternative providers for the critical services that Carillion had been contracted to deliver..**

Britain investigates Carillion directors after collapse | Reuters

CHAPTER 3

# Benefits of Effective Third-Party Risk Management

### Enhanced business resilience

Implementing a robust third-party risk management strategy enables organizations to identify, assess, and mitigate risks associated with their external partners. By addressing potential vulnerabilities and threats proactively, organizations can build greater resilience in their operations, ensuring the continuity of essential services even in the face of disruptions. This resilience is crucial for maintaining the trust and confidence of customers, stakeholders, and regulators in the E&U sector.

### Improved regulatory compliance

Effective third-party risk management helps organizations ensure that their partners adhere to relevant regulatory requirements and compliance standards. By monitoring and evaluating the compliance of third-party partners, organizations can avoid fines, sanctions, legal actions, and reputational damage that may result from non-compliance. In addition, a strong risk management approach can demonstrate to regulators that the organization is committed to maintaining high standards and prioritizing the safety and security of its operations.

### Reduced operational and financial losses

Proactively managing third-party risks can help organizations prevent or mitigate disruptions, failures, and incidents that could lead to significant operational and financial losses.



By addressing potential risks before they materialize, organizations can avoid costly downtime, equipment failures, and service outages. Moreover, a comprehensive risk management strategy can help organizations identify and address inefficiencies and vulnerabilities in their supply chain, leading to cost savings and improved operational performance.

### Strengthened reputation and stakeholder trust

An organization's reputation is heavily influenced by the actions and performance of its third-party partners. By effectively managing third-party risks, organizations can ensure that their partners uphold high standards in areas such as cybersecurity, environmental management, and social responsibility. This commitment to risk management can help organizations build and maintain trust with their stakeholders, including customers, investors, regulators, and the broader community.

### Competitive advantage

Organizations that invest in robust third-party risk management can gain a competitive advantage in the E&U sector. A strong risk management approach demonstrates to stakeholders that the organization is proactive, responsible, and committed to delivering reliable services. Furthermore, organizations that effectively manage third-party risks can more easily adapt to changing market conditions, regulatory requirements, and emerging threats, positioning them for long-term success in the sector.

### Increased operational efficiency

A well-designed third-party risk management program can help organizations streamline their processes, reduce manual effort, and increase productivity.

In conclusion, effective third-party risk management can provide significant benefits for organizations in the E&U sector, from enhanced resilience and regulatory compliance to reduced losses and improved reputation. By proactively addressing the risks associated with third-party relationships, organizations can protect their operations, stakeholders, and bottom line, ultimately gaining a competitive edge in the market.

CHAPTER 4

# Challenges of Managing Third-Party Risk in the Energy and Utilities Sector

### Lack of fit-for-purpose technology

Organizations often rely on spreadsheets to manage third-party risks, but this approach has significant limitations. Spreadsheets can be time-consuming to maintain, prone to human error, and difficult to scale as the number of third-party relationships grows. Moreover, they offer limited capabilities for real-time monitoring, analytics, and reporting, making it challenging for organizations to identify and address emerging risks and trends effectively.

### Labour-intensive processes

Managing third-party risks often involves collecting, analysing, and updating vast amounts of data from various sources, which can be a labour-intensive and time-consuming process. This manual approach is expensive and can divert valuable resources away from strategic risk management activities and decision-making, and may lead to incomplete or outdated risk assessments.

### Inefficient collaboration and communication

Traditional 'siloed' approaches to third-party risk management can result in inefficient collaboration and communication between different departments and stakeholders within an organization. This lack of coordination can lead to gaps in risk management efforts, delays in decision-making, and inconsistencies in risk mitigation strategies and controls.

### Lack of qualified risk management personnel

The E&U sector faces a shortage of qualified risk management personnel, making it difficult for organizations to recruit and retain the expertise needed to manage third-party risks effectively. This talent gap can hinder organizations' ability to identify, assess, and mitigate risks, ultimately affecting their overall risk management capabilities and resilience.

### Increased reliance on third-party partnerships

With the sector's increasing reliance on external partners, organizations face a higher risk of exposure to a range of third-party risks.

CHAPTER 5

# Overcoming the Challenges with Smart Technology

### Tooling for Multidisciplinary Third-Party Risk Management

Effective third-party risk management in the E&U sector requires a multidisciplinary approach, combining the expertise and data of various stakeholders such as procurement, legal, risk management, and information security. To enhance the effectiveness of this approach, companies need to leverage technology solutions that can automate due diligence assessment process and provide real-time monitoring capabilities.

### Smart Due Diligence Automation

One of the most critical aspects of third-party risk management is due diligence assessments. Companies need to ensure that their suppliers, contractors, and other partners meet their standards for security, compliance, sustainability, financial stability and so on. Due diligence assessments traditionally involve a significant amount of manual work, which can be time-consuming and error-prone. However, companies can leverage automation tools to streamline this process, reduce labor and improve its accuracy.

### Real-time Monitoring to Timely Identify Imminent Threats

Real-time monitoring capabilities are another critical aspect of effective third-party risk management. Companies need to be able to monitor their third-party risks continuously and respond quickly to any changes in risk levels.



To do this, companies can leverage real-time monitoring solutions that use automation and machine learning to monitor their suppliers and partners' risk posture continuously.

### NTT DATA's Fit-for-Purpose Solution: 3rdRisk

3rdRisk is a state-of-the-art technology solution designed to address the unique challenges of third-party risk management in the E&U industry. With a robust set of features and capabilities, the 3rdRisk platform empowers organizations to manage and mitigate third-party risks effectively. Key features NTT DATA's 3rdRisk solution include:

- Usage of Industry-specific risk assessment framework: the NTT DATA's and 3rdRisk third-party risk assessment methodology is tailored to the E&U sector, providing a comprehensive understanding of the risks associated with third-party relationships.
- Real-time monitoring and alerts: the 3rdRisk platform enables continuous monitoring of third-party risks, with automated alerts to notify risk, security and sustainability managers of potential issues or changes in the risk landscape.
- Advanced analytics and reporting: 3rdRisk's analytics capabilities allow companies in the E&U sector to gain valuable insights into their third-party risk exposure, enabling informed decision-making and risk mitigation strategies.
- Integration with existing systems: 3rdRisk can seamlessly integrate with a company's existing procurement systems and risk management infrastructure, enhancing its effectiveness and providing a unified view of third-party risks.
- Content integrations: 3rdRisk partners with leading risk content providers, including BitSight, SecurityScorecard, Altares – Dun & Bradstreet, EcoVadis, Refinitiv and others. These allow organizations to access and leverage valuable external data and insights, enhancing their third-party risk assessments and decision-making capabilities.

# Conclusion and Recommendations

In today's complex and interconnected business environment, third-party risk management is an essential component of an organization's overall risk management strategy, particularly in the E&U sector. As organizations increasingly rely on external partners for essential services, technology, and supplies, they must be proactive in addressing the various risks associated with these relationships, including cybersecurity, operational, regulatory and compliance, ESG, and supply chain/vendor risks.

NTT DATA's 3rdRisk platform provides a comprehensive solution for organizations in the E&U sector, offering advanced tools and capabilities for identifying, assessing, monitoring, and managing third-party risks. By leveraging 3rdRisk, organizations can build greater resilience, enhance regulatory compliance, and improve their overall risk management capabilities, positioning themselves for continuous success in a competitive and rapidly evolving market.

To effectively manage third-party risks in the E&U sector, organizations are recommended to take the following steps:

1. Develop a comprehensive third-party risk management strategy that aligns with the organization's overall risk appetite and objectives.

2. Implement a robust due diligence process to assess potential third-party partners' risk profiles, including financial stability, regulatory compliance, cybersecurity capabilities, and ESG performance.

3. Establish ongoing monitoring and reporting mechanisms to track the performance of third-party partners and identify emerging risks and vulnerabilities.

4. Implement risk mitigation strategies and controls to address identified risks and minimize their impact on the organization's operations and reputation.

5. Foster a risk-aware culture throughout the organization, ensuring that employees at all levels understand the importance of third-party risk management and their role in supporting the organization's risk management efforts.

By taking a proactive approach to third-party risk management and leveraging the capabilities of the 3rdRisk platform, organizations in the E&U sector can protect their operations, stakeholders, and bottom line, ultimately gaining a competitive edge in the market.

NTT DATA

## About NTT DATA

NTT DATA, part of the NTT Group, is an innovative global IT and business services company headquartered in Tokyo. The company assists clients in their transformation process through consulting, industry solutions, business process services, digital and IT modernization and managed services. NTT DATA enables them, but also society, to face the digital future with confidence. The company demonstrates its commitment to the long-term success of its customers by combining global reach with local focus, working with them in more than 50 countries around the world.

## Key contact

**Michiel Donders**
Director Energy & Utilities
NTT DATA Netherlands

**David Gomez Sanchez**
Governance, Risk & Compliance Lead
NTT DATA

**Visit us at benelux.nttdata.com**