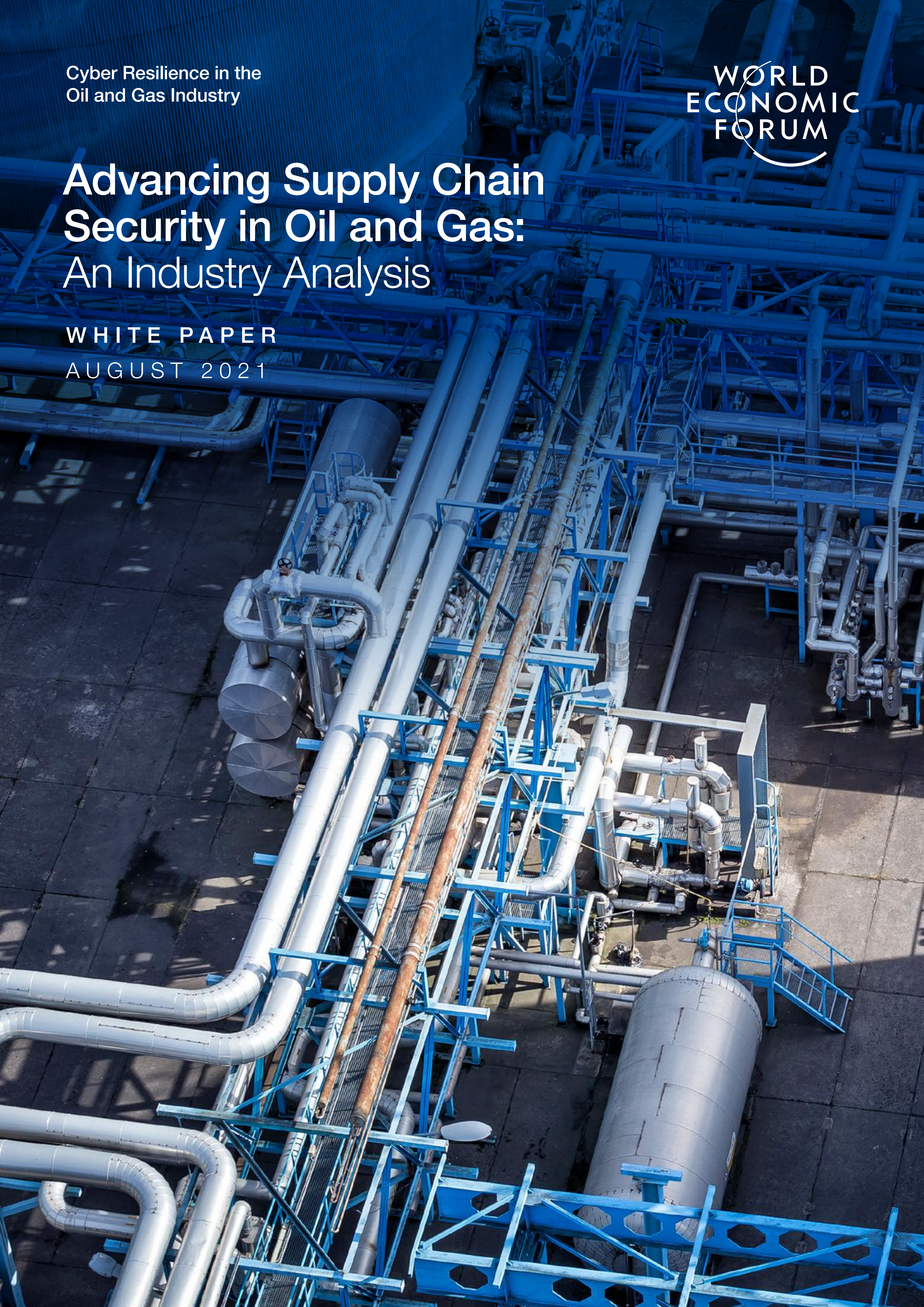
Cyber Resilience in the
Oil and Gas Industry

Advancing Supply Chain Security in Oil and Gas: An Industry Analysis

WHITE PAPER

AUGUST 2021



Images: Getty Images

Contents

Disclaimer
This document is published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

Foreword

Basim Ruwaii
Chief Information Security Officer, Saudi Aramco

Christophe Blassiau
Cybersecurity Senior Vice-President and Chief Information Security Officer, Schneider Electric

Harshul Joshi
Principal, PwC

Georges de Moura
Head of Industry Solutions, World Economic Forum

Today, the world faces an unprecedented set of global challenges ranging from climate change to recovery from the COVID-19 pandemic. The pandemic has highlighted our reliance on both a global supply chain and the internet and on accelerated industry ecosystems to achieve greater digitalization and increased connectivity between systems and people.

This reliance has also redefined the relationship between businesses and their suppliers, bringing them closer together than ever before. Seeking efficiencies amid global supply shortages, businesses and third-party suppliers have increased their collaboration and digital connectedness. While improving efficiencies, this has also expanded the vulnerabilities for malicious cyber actors to exploit.

Furthermore, the transformation of many oil and gas companies from a state of isolated operational systems and environments to fully integrated businesses has resulted in a complex supply chain and increased interdependencies between upstream, midstream and downstream.

However, the gains made possible by third parties are not without risks. Such digital interdependence has expanded the impact of potential cyberattacks as an attack on one can result in an attack on many. In the aftermath of recent supply-chain cyberattacks affecting thousands of companies globally, it is imperative that organizations take measures to protect not only their own networks, but also those of their interconnected third parties.

This implies that each exchange of information within any digital workflow in the oil and gas industry needs to be secure and resilient to threats that have consequences on the availability, reliability and safety of critical business functions and industrial systems.

As the world grows ever more complex, stakeholders in the oil and gas industry must guard against the growing numbers and varieties of threats by embracing a risk-informed cybersecurity approach to ensure its long-term sustainability and resilience.

With this in mind, the World Economic Forum authored this report with Saudi Aramco, Schneider Electric, PwC and a multistakeholder community to help identify, measure and shape approaches to mitigate supply-chain cyber risks that are endemic in the oil and gas industry. This body of work has served as a springboard for continued collaboration within the oil and gas community but also as a model for other industries and ecosystems to build upon. This blueprint will ensure that third-party risk management becomes a critical part of any organization’s overall risk management strategy. It is through this holistic and shared approach that all actors in the digital ecosystem will address the threats of today and tomorrow.

Collaboration is our greatest protective measure and we hope that this report will trigger the necessary discussions and actions needed to build cyber resilience in this evolving technological ecosystem.

Facilitating an open dialogue on cybersecurity threats and protections is a critical step in raising the bar for our global supply chain. It is through such dialogue that the industry will foster increased vigilance across the ecosystem while establishing mutual trust and understanding.

Executive summary

Cyber risks rise with hyperconnectivity and a diverse and complex supply chain of third parties.

The oil and gas industry's digital transformation and hyperconnectivity have increased the digital footprint of third parties and transformed business models quickly, mainly through an increased focus on innovation and efficiency. Today, companies around the world rely on more than 1,000 third parties[1] to support this transformation in order to gain a variety of business benefits such as cost savings, operational efficiencies, scaling of capabilities and resources, and value generation.

Such third-party expansion introduces significant cyber and operational risks, including the mishandling of confidential data, failure to meet business operational and compliance needs, and a lack of adequate safeguards against cyber threats. These risks may generate important consequences for an organization's operations, reputation and, ultimately, its bottom line. PwC's *Third Party Risk Management Digital Trust Survey Snapshot* demonstrates that one-third of surveyed organizations experienced significant disruptions due to third parties, including software supply chain disruptions (47%), cloud breaches (45%), third-party platform exposures, and outages and downtime (41%).[2] The Colonial Pipeline ransomware attack represents the most recent example; the pipeline was shut down for several days, which had a significant impact on organizations that rely on critical third parties within their supply chain, leading to gas shortages in several US states. Colonial paid the ransom demand of approximately $4.4 million to reopen the pipeline.[3] A more recent example is the compromising of Kaseya, a managed technology services provider to many small and medium-size companies: the company's safety features were subverted to push out malicious software to customers' systems (around 1,500 companies).[4] These examples underscore the need for a harmonized and holistic third-party risk management approach to effectively identify, remediate and monitor cybersecurity risks across the third parties' life cycle.

To address these challenges, organizations must establish adequate mechanisms for risk assurance throughout the third-party life cycle in adherence with internal standards and regulatory requirements. In practice, to evaluate these requirements, companies use conventional and resource-intensive methods that are not capable of keeping up with the scale and speed of change, leading to increased operational overheads or blind spots.

The lack of an aligned cyber-risk management approach causes inefficiencies (thousands of questionnaires filled out by third parties and not analysed by senders due to lack of time and resources) and redundancies (the same third party will be assessed several times by various customers against more or less the same requirements) as companies assess cyber risks using different sets of requirements from a large number of partners.[5]

A harmonized and streamlined approach would help to ensure that essential cybersecurity standards are met. To this end, the Cyber Resilience in Oil and Gas community defined a holistic approach for managing third-party cyber risks with the aim of:

- **Accelerating and streamlining** third-party risk management practices by developing a unified industry approach to identify, mitigate, monitor and communicate third-party risk

- **Improving accuracy and consistency of third-party assessments** by establishing a baseline set of requirements to assess the risk associated with third-party relationships

- **Increasing the industry's cyber resilience** by continuously adapting baseline cybersecurity standards and risk management methodologies to keep up with the pace of change in the digital and threat landscapes

This report was developed and led by the World Economic Forum, Saudi Aramco, Schneider Electric and PwC in collaboration with the Cyber Resilience in Oil and Gas community through multiple workshops and working group sessions.

The paper is intended as a practical guide for cybersecurity leaders managing third-party cyber risks within oil and gas supply chains. It includes actionable guidance, methodologies and examples to improve the oversight of third-party risks by accelerating and streamlining a holistic approach, improving the accuracy and consistency of common requirements and best practices, and ultimately improving cyber resilience across the oil and gas business environment. This report bridges information from multiple existing frameworks on third-party risk management.[6,7,8]

1 Key benefits and guiding principles

Optimize cost and time effectiveness while increasing oversight and transparency of cyber risk from third parties across the oil and gas industry.

Adopting a common approach to third-party risk management provides three key benefits to both consumer and third-party organizations supplying products and services.

FIGURE 1 **Key benefits of adopting a holistic approach to third-party risk management**

Cost and time efficiencies

- Boosts efficiency in information-gathering for due diligence with a common cybersecurity baseline
- Reduces time needed to assess and evaluate documentation, yielding significant operational savings
- Expedites readiness and onboarding and engagement cycles for both consumer and third-party organizations

Multidimensional risk coverage

- Increases security by ensuring consistent cybersecurity requirements, driven by industry experiences
- Aligns to industry frameworks and regulations, using independent control attestations
- Ensures multidimensional risk coverage from deep experience and insights from participant organizations

Transparency

- Demonstrates third parties' and consumers' attitude and investment in cybersecurity controls
- Raises both client and third-party confidence and reputation, increasing trust when doing business
- Establishes visibility of baseline cybersecurity practices adopted throughout the supply chain

10 key principles for organizations in establishing a common cybersecurity baseline

1. **Govern third parties' risk** by establishing clear roles and responsibilities within the organization as well as ownership of risks. Strong cross-functional collaboration of security, procurement, legal and business departments is vital for success.

2. **Develop the cyber literacy and education of employees handling third parties** by providing cybersecurity education and guidance on performing duties and responsibilities consistent with related policies, procedures and agreements.

3. **Establish access controls and management of critical assets** based on "need-to-know" and "need-to-operate" access to assets, information and facilities by both employees and third-party contractors.

4. **Implement change and configuration management** specifically on the assets, information and facilities falling under the third party's scope of engagement.

5. **Require secure-by-design and by-default systems, services and interfaces** by embedding adequate layers of security and privacy safeguards according to the asset criticality.

6. **Maintain response and recovery mechanisms by ensuring incident management, business continuity management (BCM) and disaster recovery planning (DRP)** are in place, up-to-date with emerging threats and risks, and tested regularly following scenarios derived from intelligence and consequence-driven analysis.

7. **Protect critical information while aligning with relevant regulations and policies** by implementing appropriate regulatory monitoring, preventive and detective, response and recovery controls.

8. **Secure operational and physical environments by using leading safety practices** to ensure policies and regulations are incorporated into physical environments.

9. **Implement a secure development life cycle of products, systems and tools** that provide reasonable assurance that third parties apply security controls and secure coding techniques to system development life cycles, authenticity validation procedures and integrity of source code.

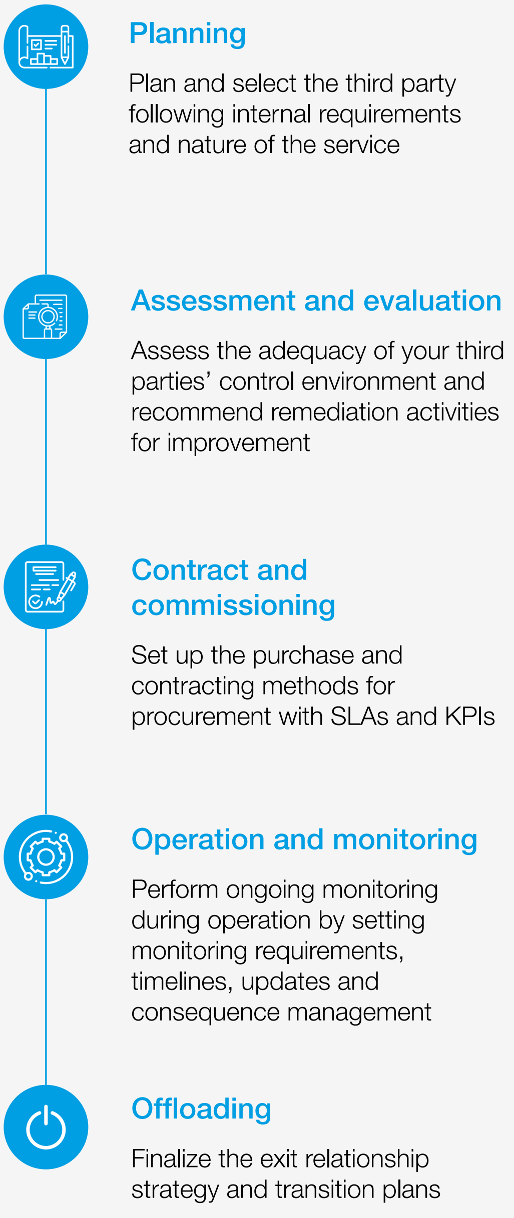
10. **Provide support for vulnerability management and patching** of products and services by demonstrating capabilities are in place to detect vulnerabilities or malware in the third party's environment and products.

2 Holistic approach to managing third-party risks

Alignment on a streamlined approach for third-party risk management increases cyber resilience across the industry.

This comprehensive approach provides a common model and taxonomy across the third-party life cycle in five important phases.

FIGURE 2 **First proposal for a holistic approach to third-party risk governance**



Planning

Plan and select the third party following internal requirements and nature of the service

Assessment and evaluation

Assess the adequacy of your third parties' control environment and recommend remediation activities for improvement

Contract and commissioning

Set up the purchase and contracting methods for procurement with SLAs and KPIs

Operation and monitoring

Perform ongoing monitoring during operation by setting monitoring requirements, timelines, updates and consequence management

Offloading

Finalize the exit relationship strategy and transition plans

1. The **planning** phase focuses on the organization's plans, and preselects third parties depending on the nature of the service provided. During this phase, the businesses determine the need for a third party and strive to understand the associated risks inherent in the scope of engagement. In addition, it is important to start engaging from the outset with the procurement department, which will oversee the selection of new vendors.[9]

2. The **assessment and evaluation** phase evaluates a third party's cyber posture and environment against an established set of common requirements based on the product and service provided. These assessment activities may involve the use of multiple assessment and evaluation methods to assess control effectiveness. The assessment methodology relies on criteria that are used to identify a third party's criticality and associated requirements and define the residual risks.[10]

3. The **contract and commissioning** phase defines the contractual terms and conditions with a third party in alignment with the scope of engagement, associated risk, roles and responsibilities etc. Organizations often have predefined contractual language set forth by their legal departments, which can be tailored based on the third party's risk profile.

4. The **operation and monitoring** phase initiates the continuous processes of evaluating the performance of third parties and monitoring the changes in risk associated with the product or service. These activities are usually driven by the residual risk review and reassessment using similar evaluation methods to those used in the assessment and evaluation phase, and ad-hoc activities triggered by events or recent incidents. Setting monitoring requirements, an operating model of collaboration, the periodicity of touchpoints, timelines, updates and consequence management are essential aspects of this phase.

5. The **offloading** phase includes the steps taken to terminate a relationship with a third party in an effective and secure manner. Offloading may take place for various reasons such as underperformance, significant quality issues, transition to another third party, insourcing etc. Organizations will often have exit strategies and/or termination checklists to complete as a part of this offloading process.

CASE STUDY

Tackling third-party risk management at Shell

Supply-chain cyberattacks have become more prevalent in 2021. With the ever-growing sophistication of attacks combined with the wide variety of new techniques in use, third-party risk management needs to be addressed as a top priority, at the same level as other enterprise strategic risks. The conventional third-party risk management approach is no longer effective in enabling a proactive response to emerging supply-chain risks. Supply-chain risk requires a new, multifaceted approach.

Third-party risk management at Shell is fully integrated across sourcing, assurance and IT. Sourcing plays a pivotal role in robust supply-chain management. The initial screening of third parties is considered equally as important as imposing strong contractual obligations and managing a contract after it has been awarded. Shell's assurance process aims to validate the ability of third parties to adhere to contractually agreed terms in ensuring security across the business environment. Shell uses data analytics across its vendor risk-management platform, security ratings and sourcing engine.

This integrated approach to supply-chain risk management helps Shell to ensure a robust and comprehensive view of constantly changing supply-chain risk vectors. In case these evolving risks are not within Shell's risk appetite, preventive measures can be implemented to safeguard information assets. When coordinated action is required across the business environment, an established communication protocol enables timely cooperation with individual service organizations. Only when acting in a fully aligned manner with suppliers can Shell successfully tackle the ever-growing challenge of keeping its business systems healthy and resilient against emerging supply-chain attacks.

CASE STUDY

Adopting a third-party risk management programme - Galp Energia

Galp has implemented a third-party cyber-risk management process based on questionnaires aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and using a risk-based approach through three service tiers based on the potential cyber risks. These questionnaires are evaluated in parallel with a technical assessment of the proposals, considering both the answers given and the risk vectors observed using a cybersecurity-rating tool.

In addition, awareness sessions are conducted regularly to ensure that internal stakeholders have a clear understanding of the process and of service-level agreements (SLAs), by providing access to a dashboard that presents the cyber-risk evaluation stage in near real time. Awareness materials are also developed and distributed to the suppliers.

As a result of the evaluation, when relevant risks are identified following the standard enterprise risk management process, the business unit can accept the risks and endorse the service if its benefits outweigh the potential impacts. However, it is also possible to reduce the identified risks through the mitigation and remediation plans developed between Galp's cyber-risk team and suppliers.

Despite some expected initial internal resistance, Galp's business units have quickly understood the value of this approach. The key to this success has been to follow a risk-based approach and not be compliance-driven – working side-by-side with businesses both to give them visibility on supplier risks and to help them work with the supplier they want. The real surprise of this programme has been the buy-in from suppliers, which perceived the process as a means of improvement and provided little resistance to implementing the agreed mitigation measures. This has also led to an improvement in Galp's overall portfolio cybersecurity rating.

3 Implementation guidelines

Essential guidelines for implementing cybersecurity baseline requirements increases the effectiveness of cybersecurity across the industry.

Effective implementation of third-party risk management requires a strong alignment across three main phases:

- **Assessment and evaluation**: Develop common cybersecurity requirements across the industry in this phase to establish a common baseline of cybersecurity requirements for third-party risk assurance across the supply chains of third parties.
- **Contract and commissioning:** Establish a consistent contractual taxonomy during this phase by aligning procurement and cybersecurity needs with specific terms and conditions, to avoid gaps between organizations and third-party expectations.
- **Operation and monitoring**: Share best practices and common minimum requirements in this phase to ensure continuous monitoring of third parties' performance and changes in their risk profiles.

3.1 Assessment and evaluation in depth

The assessment and evaluation of third parties enables organizations to better understand and rate the third parties' environment while identifying significant issues that need to be addressed in a timeline commensurate with the risk. For an effective assessment and evaluation of a third party, organizations need to:

1. Select the appropriate assessment depth and in-scope requirements to calculate the residual risk of the product/service provided in alignment with an established industry framework and/or standards. Organizations should employ additional requirements based on their internal priorities and regulatory needs.
2. Assess and evaluate the third party's cybersecurity requirements to gain insights and reasonable assurance of the existing controls to effectively calculate the residual risk.

1. How to select the appropriate requirements

The selected requirements depend on the scope of engagement and risk rating associated with the third party's product and service. The following four questions help to define the inherent risk rating of the third-party product/service.

Would the third party have logical and physical access to critical[11] IT systems? This includes third parties that will have system access privileges and can control critical IT systems, including account software providers that connect to critical IT systems (e.g. enterprise resource planning [ERP] or customer relationship management [CRM]), cloud providers that host and provide critical IT systems, remote work applications etc.

Would the third party have logical and physical access to critical OT systems? This includes all third parties that will provide, install or integrate components, products and systems in the industrial environment.

Would the third party have access to sensitive information? This includes all third parties that access, process and control sensitive business and personal information.

Would any critical business process depend on outsourcing to the third party? This includes all third parties that provide services required for critical business operations.

TABLE 1 Third-party inherent risk rating scoring example

Inherent risk rating	Scoring
Critical	All segmentation criteria = Yes
High	3 of 4 segmentation criteria = Yes
Moderate	2 of 4 segmentation criteria = Yes
Low	0–1 of 4 segmentation criteria = Yes

CASE STUDY Maintaining a third-party risk classification based on scope – Schneider Electric

Before 2020, isolated initiatives alone addressed third-party cybersecurity risks stemming from suppliers at Schneider Electric. To manage cybersecurity risks from third parties consistently and efficiently, the company set up a cross-functional programme and enforced a new policy, targeting a large range of suppliers, from product component producers such as original equipment manufacturers (OEMs) to technology providers such as cloud and infrastructure hosting services.

A risk-based approach classifies suppliers into four categories (critical, high, moderate and low) and introduces security requirements and consequence management for noncompliance. The policy tailors the requirements and mitigation measures based on supplier risk profile.

The benefits include:

Making cybersecurity "top-of-mind" in supplier interactions and for high-ranking executives up to C level; systematically embedding cybersecurity provisions in supplier agreements

Enforcing collaborative and continuous monitoring, threat and risk vectors identification with critical suppliers (using cyber-scoring platforms, cyberthreat intelligence platforms)

Performing security and privacy checks on delivered platforms within the frame of an internal security certification process; systematically enforcing internal and external cyber assessments (e.g. shared assessments platforms) using a risk-based approach

Enabling a transparency mindset to ensure supplier vulnerabilities and incidents are known by the company before they are publicly known; documenting supplier incidents to capture and respond to any other incidents in a structured and collaborative way across the company

FIGURE 3 Definition and scope – Schneider Electric example

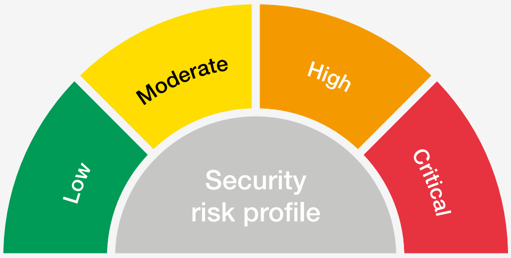
Key figures

50,000+ vendors

80 commodities

€12 billion total spent

Classification



Critical	Partners, co-innovation ("crown-jewel" vendors)
High	Critical business impact, access to confidential and restricted (strategic, personal) data
Moderate	Regulatory impact and important business
Low	Procurement categories with low-risk purchases and data

The segmentation criteria are complemented by 39 cybersecurity baseline requirements that follow 10 principles.[12] The working group laid down this set of requirements to help the oil and gas industry establish a common baseline that, used with a practical assessment questionnaire, drives a consistent approach for assessing and evaluating third-party control environments.[13,14]

2. How to perform the assessment

The choice of method will depend on the third-party product and service criticality, as defined by each organization. Having a range of methods available facilitates risk assessment, increases the scaleability and improves the efficient use of resources as the volume of assessment increases. Many organizations perform a series of third-party assessments based on internal requirements that align with common frameworks such as NIST CSF[15] or ISO 27001/2.[16] While these assessments ensure that a service provider adheres to the best practices, they are often time-consuming and onerous for the organization. In addition, the third-party provider frequently has to respond to a large number of very similar requests. The cybersecurity requirements set forth by the working group aim to streamline the third-party due diligence process. In addition, the approach can be taken a step further to include a shared model across the industry, with a general agreement among parties that a more rigorous assessment can be performed once and shared across multiple contracting organizations, benefitting both the third party and the contracting organization. Such a model usually requires a partnership with private organizations for the enabling technology and execution of assessments.

FIGURE 4 **Assessment evaluation model**

	Scoring ratings	Shared assessments	Internal assessments	Industry certifications
	Cybersecurity ratings are a data-driven, objective and dynamic measurement, demonstrating the cybersecurity posture level of organizations	Third-party risk programmes give organizations a detailed report on the cybersecurity maturity of third parties (people, process and procedures)	Internal assessments are based on an organization's specific cybersecurity requirements following the criticality of the service provided by third parties	Cybersecurity industry certifications provide a form of attestation on the level of security controls of organizations based on external audit exercises
Scaleability	High to rapid	High but dependent on the business environment	Low	Low
Scope	Partial	Variable	Variable	Variable (depending on certification)
Frequency	Continuous	On demand	Event-driven	Annual
Methodology	Scan of external-facing assets	Proprietary security assessment	Proprietary security assessment and organization-based accreditation	Audit, proprietary security assessment
Intrusiveness	Low, public data from internet/market	High, needs nondisclosure agreement (NDA)	Variable, may need NDA	High, needs NDA
Supplier cost/effort	None	Vendor (also) pays but sponsoring is possible	Variable	Moderate to high
Consumer cost/effort	Moderate	High	Moderate to high	None for organization

Scaleability →

← Coverage of assessments

Source: Working group inputs

CASE STUDY

Instituting a holistic third-party cybersecurity framework and certification model – Saudi Aramco

Saudi Aramco initiated its supply-chain cybersecurity programme in 2016 to combat third-party risk by embedding cybersecurity into its third-party engagement life cycle. The programme aimed to identify the necessary elements to ensure the security of Saudi Aramco data and assets entrusted to third parties by improving critical third parties' cybersecurity readiness as well as minimizing potential disruption in the event of a cyberattack.

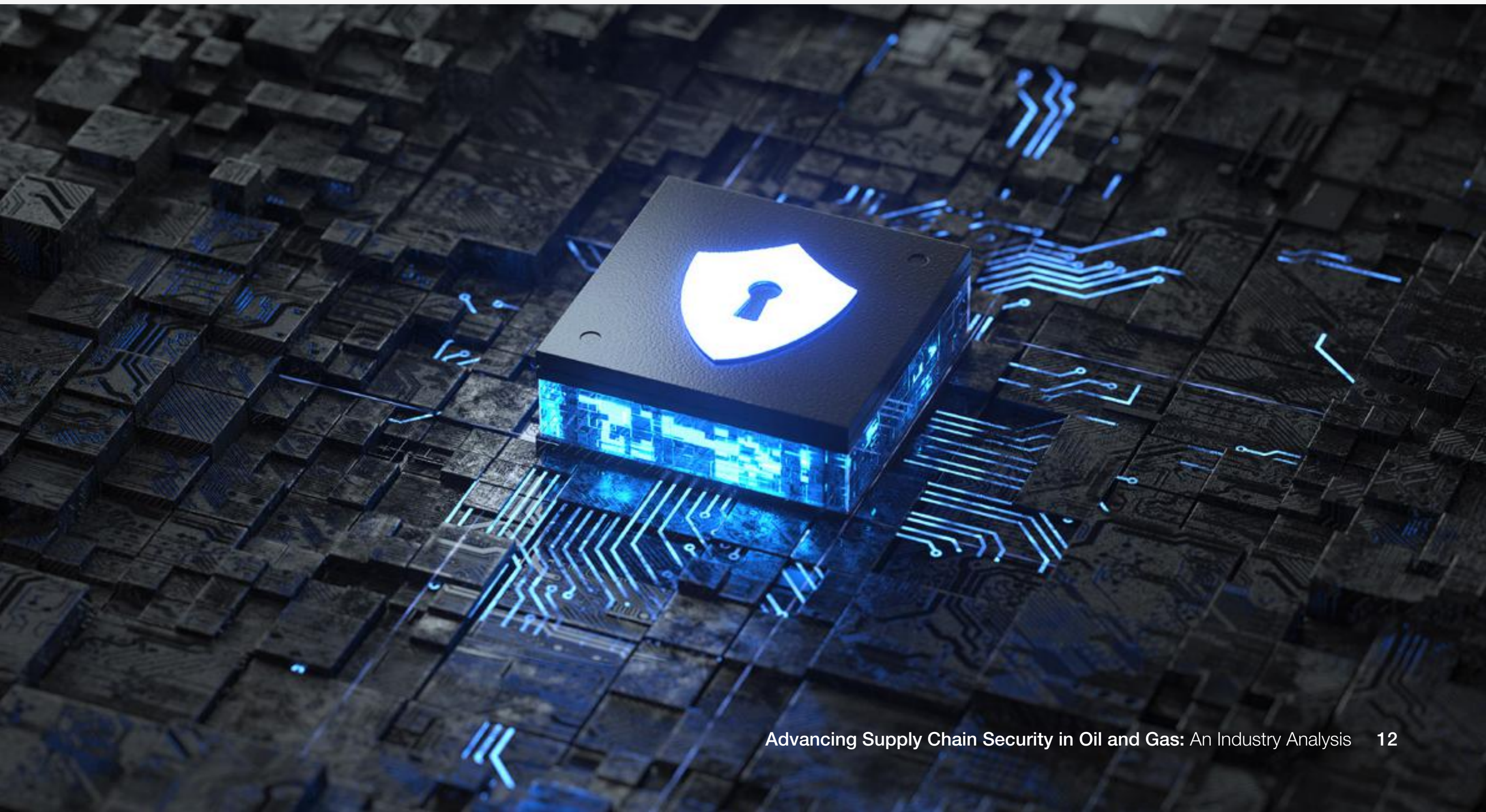
The programme made sure cybersecurity would no longer be an afterthought when engaging with third parties by embedding cybersecurity requirements in the third-party engagement process. Nonetheless, continuous collaboration among cybersecurity, legal, procurement and business is important to ensure success in implementing such a programme.

Through this effort, the company established crucial cybersecurity elements, including cybersecurity contractual terms, third-party cybersecurity policy and standards, cyber incident reporting and third-party risk-based classification. To sustain the programme efforts, third-party cybersecurity functions and processes were formalized. This included formalization of the Saudi Aramco Cybersecurity Compliance Certificate (CCC) with nine audit firms as authorized entities to assess and issue the CCC independently, based on the organization's compliance with Saudi Aramco's third-party cybersecurity standard.

FIGURE 5

Saudi Aramco framework elements: holistic view

Risk management	Contracting	Governance	Compliance	Security operations	Incident management
Risk-based classification criteria	Terms and conditions	Third-party cybersecurity policies	Compliance assessment and certificate	24/7 monitoring	Incident response
Risk assessment	Pre-engagement assessment	Awareness and outreach	Compliance and monitoring	Threat management	Disaster recovery



3.2 Contract and commissioning in depth

The contract and commissioning phase aims to define baseline contractual terms and conditions according to the product/service and associated risk, and to update the contractual terms based on identified issues (if applicable). The outcome of the assessment and evaluation phase determines whether there is a need for additional and more stringent contract clauses on the control environment.

Key recommendations for streamlining the contract and commissioning phase

- Agree on organizational-level standard cybersecurity contractual terms and conditions, using existing industry baseline language[17] (e.g. minimum cyber requirements for all third parties) where possible.

- On top of the *standard* contractual terms and conditions defined above, institute more elaborate *enhanced* contractual terms based on the product/service type and criticality (e.g. for IT and cloud vendors, operational technology [OT] organizations, marketing etc.).

- Use segmentation criteria or the internal inherent risk questionnaire to assess the risks and determine the level of enhanced terms and conditions needed (e.g. an IT vendor processing personal data in Europe will also sign a data protection addendum on top of cyber terms and conditions).

- Consider the issues identified during the assessment process before executing the contract in order to adjust the terms and conditions for any changes in risk.

- Engage with risk subject matter experts (SMEs) and the legal department throughout the negotiation process as an escalation path for clause negotiation.

Typically, operators define their own contractual language that is specific to their organizational and business requirements. The World Economic Forum Cyber Resilience in Oil and Gas community identified a list of 12 common cybersecurity-related contractual term topics for more efficient and streamlined third-party contract development:

1. Cybersecurity policy and governance

2. Cybersecurity risk management and assessments

3. Incident response and collaboration

4. Identity and access management

5. Network and cloud security

6. Asset management

7. Endpoint security

8. Physical security

9. Human resources

10. Confidentiality

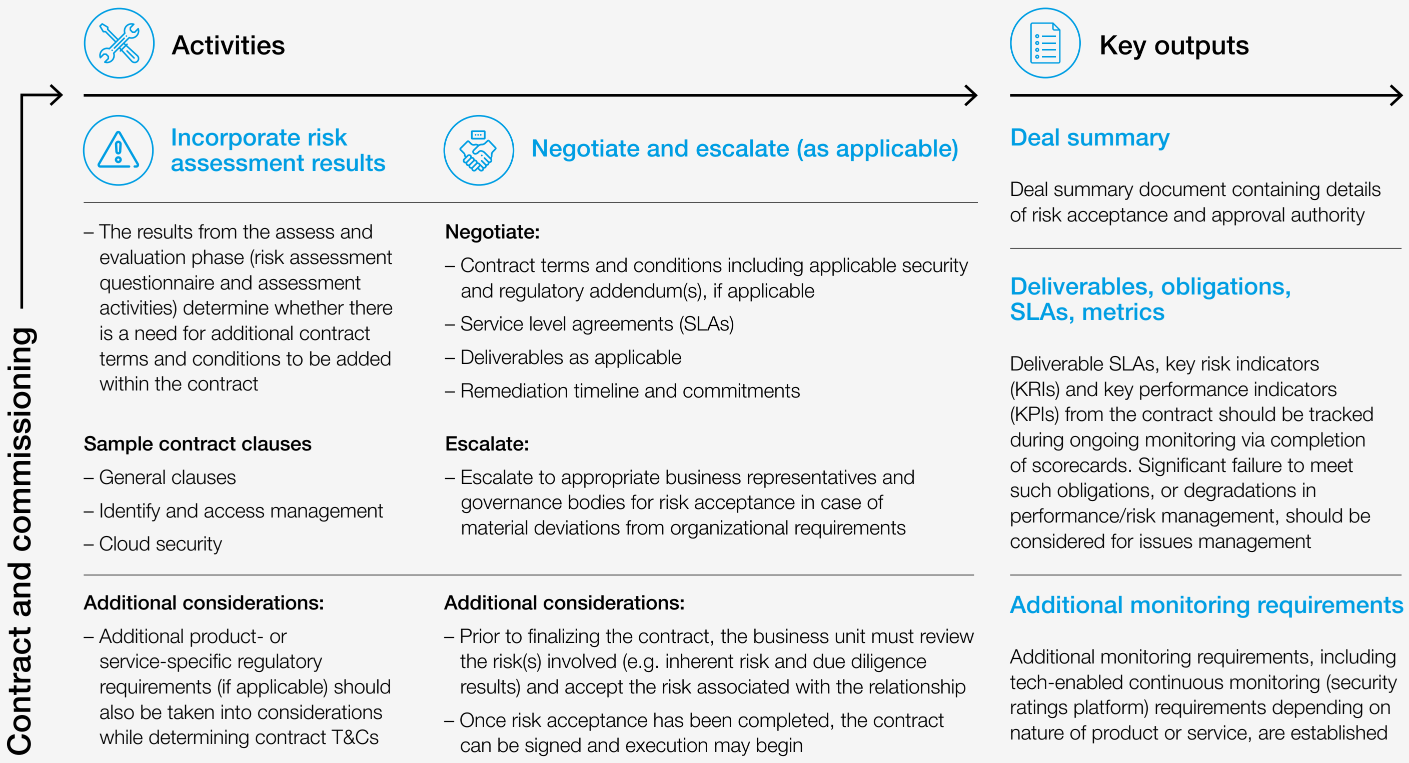
11. Business continuity and disaster recovery planning

12. Secure development and source code protection

A combination of the segmentation criteria and the residual risk rating will determine whether standard or enhanced terms and conditions are used.

General contract clauses should be included, and may be adapted based on the risks and criticality. Standard model procurement contract language addressing cybersecurity risk from third parties exists and should be included to facilitate the process.[18]

FIGURE 6 | Contract and commissioning: essential activities and outputs



Contract and commissioning

Activities

Incorporate risk assessment results

- The results from the assess and evaluation phase (risk assessment questionnaire and assessment activities) determine whether there is a need for additional contract terms and conditions to be added within the contract

Sample contract clauses

- General clauses
- Identify and access management
- Cloud security

Additional considerations:

- Additional product- or service-specific regulatory requirements (if applicable) should also be taken into considerations while determining contract T&Cs

Negotiate and escalate (as applicable)

Negotiate:

- Contract terms and conditions including applicable security and regulatory addendum(s), if applicable
- Service level agreements (SLAs)
- Deliverables as applicable
- Remediation timeline and commitments

Escalate:

- Escalate to appropriate business representatives and governance bodies for risk acceptance in case of material deviations from organizational requirements

Additional considerations:

- Prior to finalizing the contract, the business unit must review the risk(s) involved (e.g. inherent risk and due diligence results) and accept the risk associated with the relationship
- Once risk acceptance has been completed, the contract can be signed and execution may begin

Key outputs

Deal summary

Deal summary document containing details of risk acceptance and approval authority

Deliverables, obligations, SLAs, metrics

Deliverable SLAs, key risk indicators (KRIs) and key performance indicators (KPIs) from the contract should be tracked during ongoing monitoring via completion of scorecards. Significant failure to meet such obligations, or degradations in performance/risk management, should be considered for issues management

Additional monitoring requirements

Additional monitoring requirements, including tech-enabled continuous monitoring (security ratings platform) requirements depending on nature of product or service, are established

3.3 Operation and monitoring in depth

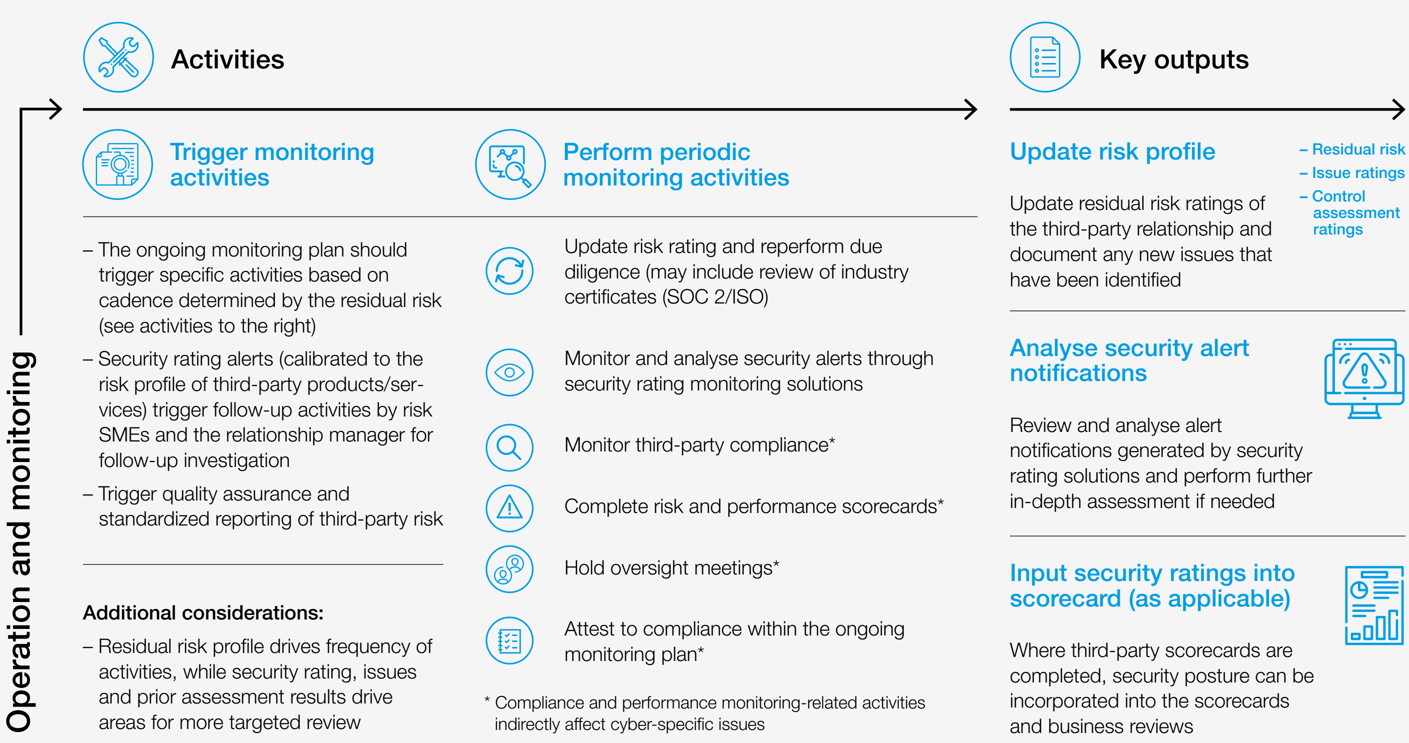
Operation and monitoring activities take place for as long as the third-party relationship is active, to ensure that third parties deliver the expected value securely, while monitoring and addressing any changes in risk profile and overall security performance. Reassessment and monitoring activities are time-consuming, costly and labour-intensive, but a risk-based approach enables a focus on high-risk relationships while driving efficiency.

Key recommendations for streamlining the contract and commissioning phase

- Set a cadence to review the risk rating of the third party in order to capture any change in the risk profile of the third party and scope of engagement (e.g. solution moved from on-premises to cloud).
- Perform a continuous and risk-based review of the nature, timing and extent of continuous monitoring activities (reassessment, monitoring through security rating platforms etc.).
- Define criteria that would trigger ad-hoc assessment and audit activities (e.g. negative news, change in security service rating, a security incident etc.).
- Embed cybersecurity in business reviews with third parties and continuously communicate on the evolving risks and threat landscape (e.g. chief information security officer [CISO] to CISO, security operations centre [SOC] to SOC connections) .
- Define reporting mechanisms to raise awareness and ensure timely and informed decisions by board and senior leadership (oversight meetings, performance scorecard etc.).

Traditionally, operations and monitoring activities include a review of the inherent risk rating to capture any change in service, reassessment of the third party's control environment, and use of security rating platforms to guide targeted assessments or trigger full ad-hoc assessments.

FIGURE 7 Operation and monitoring: essential activities and outputs



Operation and monitoring

Activities

Trigger monitoring activities

– The ongoing monitoring plan should trigger specific activities based on cadence determined by the residual risk (see activities to the right)

– Security rating alerts (calibrated to the risk profile of third-party products/services) trigger follow-up activities by risk SMEs and the relationship manager for follow-up investigation

– Trigger quality assurance and standardized reporting of third-party risk

Additional considerations:

– Residual risk profile drives frequency of activities, while security rating, issues and prior assessment results drive areas for more targeted review

Perform periodic monitoring activities

Update risk rating and reperform due diligence (may include review of industry certificates (SOC 2/ISO)

Monitor and analyse security alerts through security rating monitoring solutions

Monitor third-party compliance*

Complete risk and performance scorecards*

Hold oversight meetings*

Attest to compliance within the ongoing monitoring plan*

* Compliance and performance monitoring-related activities indirectly affect cyber-specific issues

Key outputs

Update risk profile

– Residual risk
– Issue ratings
– Control assessment ratings

Update residual risk ratings of the third-party relationship and document any new issues that have been identified

Analyse security alert notifications

Review and analyse alert notifications generated by security rating solutions and perform further in-depth assessment if needed

Input security ratings into scorecard (as applicable)

Where third-party scorecards are completed, security posture can be incorporated into the scorecards and business reviews

To understand the nature, timing and extent of these activities, organizations use a reassessment matrix, as shown below. This matrix represents an illustrative example on how to perform the assessment. Organizations may consider applying different timing and mechanisms at different scores of residual risk.

TABLE 2 Ongoing monitoring overview: reassessment schedule

		Inherent risk rating											
		Critical			High			Medium			Low		
		Nature	Timing	Extent	Nature	Timing	Extent	Nature	Timing	Extent	Nature	Timing	Extent
Residual risk rating	Critical	Onsite	Annual	Scoped testing	Onsite	18 months	Scoped testing	Remote	24 months	Scoped testing	Remote	36 months/ as needed	Scoped enquiry
	High	Onsite	Annual	Scoped testing	Onsite	18 months	Scoped testing	Remote	24 months	Scoped testing	Remote	36 months/ as needed	Scoped enquiry
	Medium	Onsite	Annual	Scoped testing	Onsite	18 months	Scoped testing	Remote	24 months	Scoped testing	Self assess	36 months/ as needed	Scoped enquiry
	Low	Onsite	Annual	Scoped testing	Remote	18 months	Scoped testing	Remote	24 months	Scoped testing	Self assess	36 months/ as needed	Scoped enquiry

As outlined above, those products and services with a higher inherent risk rating may be assessed more frequently via more in-depth assessments. However, if there are strong controls in place, resulting in a lower residual risk rating, the depth of the assessments may be reduced over time. In summary, the holistic approach to third-party risk management should take a risk-based approach to enable organizations to focus on those relationships that are the most critical.

CASE STUDY

Scaling the automated security incident workflow – SecurityScorecard

With the increased connectivity of supply chains, a modern and efficient third-party risk management programme is necessary to identify and remediate issues before they become an incident or breach. Proactive tools such as security ratings cannot mitigate this risk alone, but they are a necessary component of good cybersecurity programmes and governance. Creating an automated security incident workflow is common via a security, orchestration, automation and response (SOAR) solution. However, the cost of integrating and implementing this with traditional solutions for managing vulnerability to cyberattack is prohibitive because licence costs increase with the number of suppliers.

Security assessments are combined with continuous monitoring of the internet to deliver automated "event-based" evaluations. Vulnerabilities discovered by scanning then link with third-party threat feeds to enable automated rules that trigger the sending of an assessment questionnaire immediately after a potential threat is detected. This event-based approach improves on the usual method of periodically sending questionnaires by:

- Enabling immediate reassessment of a vendor with no input required by the cybersecurity team

- Scaling to thousands of continuously monitored companies instead of choosing only a select few

- Providing score-drop events, breach events and individual security vulnerabilities and exposures to trigger an assessment

- Tailoring the assessment sent based on the vendor portfolio to specific standards and frameworks

- Maintaining a small vendor risk management team while providing expanded coverage

Learning that a vendor experienced a data breach 11 months ago when reading its annual response to your questionnaire is definitely not adequate. Cybersecurity monitoring needs to follow the continuous evolution of cyber threats with the addition of automation at scale.

CASE STUDY

Setting three practices for third parties' infrastructure review – Palo Alto Networks

With a growing volume of business, acquisitions and new routes to market, businesses are constantly under threat from breaches that occur within their supply chains. It is vital to review not only the company's own internal infrastructure but also that of vendors and partners. Palo Alto Networks follows this guideline by using three practices:

1. **Review internal and external security procedures:** At Palo Alto Networks, any new vendors or partners undergo a thorough vetting process to gain network access based on the connectivity standard, which includes:

- A privacy review

- An information security review (including a questionnaire, review of certifications, attestations, external views through tools such as Xpander, Bitsight and SecurityScorecard)

- A capability rationalization review

- A full integration/implementation review based on Palo Alto's supply-chain management policy

2. **Establish written security guidelines and controls**: Palo Alto also has a Supplier Information Security Terms written agreement requiring suppliers to adhere to processes and protocols that minimize the likelihood of attacks – for example, cybercriminals using a supplier's website to host malware.

3. **Training/sharing security best practices with staff and vendors**: Human error is still by far the most significant source of data breaches, which means it is crucial for organizations to train all staff in the best security methods. Palo Alto vets vendors and also incorporates it into the Supplier Information Security Terms.

The above focuses more on the prevention side (i.e. vetting, reviewing, monitoring). On the monitoring side, Palo Alto Networks uses different tools (including third-party tools such as Xpander) that help monitor suppliers and detect supply-chain effects. Outside of technology, Zero Trust strategy is deployed across the environment to compartmentalize any potential supply-chain threat.

CASE STUDY

Securing remote connectivity across operational technology supply chains – Schneider Electric – Claroty

The expansion of remote working due to COVID-19 has triggered unintended consequences for organizations worldwide. The pandemic led to an increase in the number of connected devices and democratized remote access across supply chains and operations, including critical infrastructure. Organizations became increasingly dependent on third parties to maintain business continuity, with remote access posing risks to oil and gas pipeline operations.

These risks were particularly concerning for one pipeline operator that relies heavily on third parties to support the full spectrum of its oil and gas operations via remote access. Its operational technology personnel, including third-party service providers, must be able to command operations remotely while allowing security teams to maintain the same level of visibility, control and response within a maximum of six hours as required for onsite personnel.

To safeguard operational networks from threats introduced via third-party remote users, Claroty and Schneider Electric partnered with the pipeline operator to equip its personnel and third parties with a highly secure and unified capability for remote maintenance. Any of the operator's third-party service providers can now use this capability to access its operational network remotely – all the while upholding adequate security requirements and without posing any additional risks to pipeline operations.

With such unified remote access requirements, the operator minimized risk exposure and improved the visibility and control of the large footprint of third parties remotely accessing pipeline operations.

Conclusion

Public-private collaboration is essential to drive the alignment of cybersecurity practices between businesses and third parties.

With businesses relying on digital supply chains composed of a vast number of third parties, improving the oversight of cyber risk is more important than ever. In this report, the World Economic Forum Cyber Resilience in Oil and Gas community seeks to provide guidance to cybersecurity leaders and practitioners to streamline and harmonize approaches to managing third-party risks.

The members of the Cyber Resilience in Oil and Gas community propose a holistic approach to third-party risk management in order to strengthen overall cyber resilience throughout the oil and gas industry.

The primary driver of a unified approach is to streamline the resource-intensive and cumbersome practices used to assess third parties. The proposed baseline questionnaire and methodology in this report should serve as a blueprint to be shared and used across many organizations and would also be relevant to other critical-infrastructure industries.

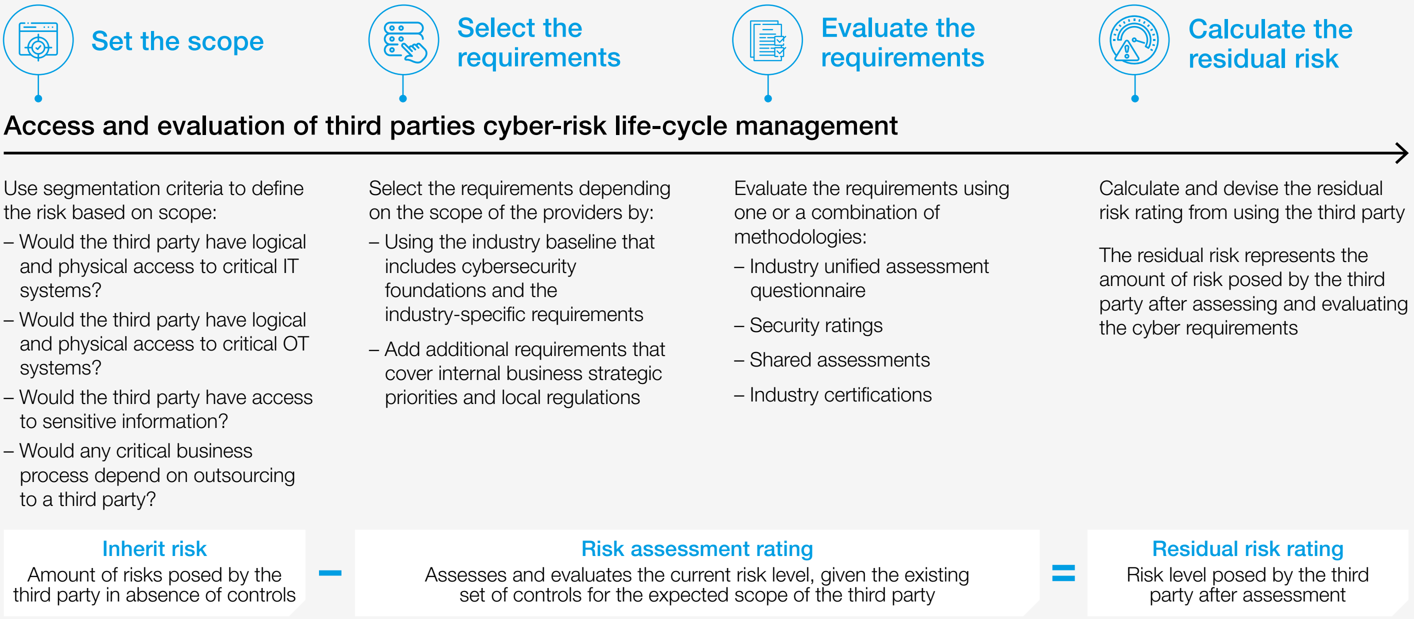
A call to action should be made to the industry to implement these guidelines, define minimum monitoring and reassessment activities and operationalize the shared assessment model throughout the third-party business environment.

The digital transformation of the oil and gas industry will continue to evolve and bring more third-party connectivity and complexity throughout supply chains. Public-private collaboration is an essential catalyst to drive the alignment of cybersecurity practices.

Appendix A: Assessment and evaluation – third parties cheat sheet

Evaluating the cyber risk posed by third parties enables organizations to take a risk-based approach when engaging with third parties. Managing risk throughout the life cycle of the relationship with a third party aids effective decision-making and increases visibility to ensure the correct level of monitoring.

FIGURE 8 **Assessment and evaluation life cycle: four key stages to calculate the residual risk posed by third parties**



Set the scope

Select the requirements

Evaluate the requirements

Calculate the residual risk

Access and evaluation of third parties cyber-risk life-cycle management

Use segmentation criteria to define the risk based on scope:

- Would the third party have logical and physical access to critical IT systems?
- Would the third party have logical and physical access to critical OT systems?
- Would the third party have access to sensitive information?
- Would any critical business process depend on outsourcing to a third party?

Select the requirements depending on the scope of the providers by:

- Using the industry baseline that includes cybersecurity foundations and the industry-specific requirements
- Add additional requirements that cover internal business strategic priorities and local regulations

Evaluate the requirements using one or a combination of methodologies:

- Industry unified assessment questionnaire
- Security ratings
- Shared assessments
- Industry certifications

Calculate and devise the residual risk rating from using the third party

The residual risk represents the amount of risk posed by the third party after assessing and evaluating the cyber requirements

Inherit risk
Amount of risks posed by the third party in absence of controls

–

Risk assessment rating
Assesses and evaluates the current risk level, given the existing set of controls for the expected scope of the third party

=

Residual risk rating
Risk level posed by the third party after assessment

TABLE 3 **Third-party cybersecurity requirements**

Residual risk matrix		Inherent risk rating			
		Low	Medium	High	Critical
Risk assessment rating	Very good	Low	Low	Medium	Critical
	Good	Low	Low	High	Critical
	Fair	Low	Medium	High	Critical
	Poor	Low	Medium	High	Critical

The combination of the inherent risk and the risk assessment provides the residual risk rating. A risk-based approach is pivotal to identify the higher-risk third parties. In order to support organizations, the following tools have been developed by the working group with the support of PricewaterhouseCoopers (PwC):

- Segmentation criteria to define the scope and calculate the inherent risk. However, it is highly recommended that each organization develops a more robust questionnaire to get a better understanding of the inherent risk and drive downstream activities.
- Unified assessment questionnaire that provides a list of questions covering the 39 industry-specific baseline requirements.[19] The unified assessment and evaluation questionnaire consists of a maximum of 194 questions that can be adjusted according to the segmentation criteria. The assessment summary generates a risk assessment rating scoring as depicted in the table below that is based on the percentage of "effective" controls out of total in-scope questions.

TABLE 4 Risk rating categorization example

Risk rating	% effective
Strong	95% +
Satisfactory	85–94%
Fair	75–84%
Unsatisfactory	Less than 75%

Appendix B: Taxonomy

Term	Definition
Cyber resilience	A dimension of cyber-risk management, representing the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources.[20]
Cyber risk	Probable loss event that materializes when a cyberthreat affects an asset of value and results in a material impact on an organization. Cyber risk can be measured as the probable frequency and the probable impact of a loss event.[21]
Information technology (IT)	Any form of technology – that is, any equipment or technique used by a company, institution or any other organization – that handles information.
Operational technology (OT)	Industrial process assets and manufacturing/industrial equipment. OT has existed for much longer than IT – ever since people started to use machinery and equipment powered by electricity in factories, buildings, transportation systems, the utility industry etc.
Residual risk	The portion of risk remaining after security measures have been applied. Residual risk is derived from the (inherent) risk posed by the third party and the result of the risk assessment.
Risk appetite/tolerance	An organization or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives. Note: risk tolerance can be influenced by legal or regulatory requirements.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk management	Coordinated activities to direct and control an organization in terms of risk.
Third party or parties	Any external entity or entities that interact with an organization. These may include service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums and investors, and may include both contractual and non-contractual parties.
Third-party risk management	The risk management process used to identify, assess and mitigate the risks associated with third parties.

Contributors

The World Economic Forum Cyber Resilience in Oil and Gas Initiative is a global, multistakeholder endeavour to strengthen cyber resilience in the oil and gas industry. The project engaged stakeholders across several oil and gas organizations, businesses, providers and governments.

Lead authors

Mansur Abilkasimov
Director Cybersecurity Governance, Schneider Electric

Dheba Al-Rashid
Head of Cybersecurity Programs Development, Saudi Aramco

Ali H. Asseri
Head of Supply Chain and Third-Party Cybersecurity Compliance, Saudi Aramco

Filipe Beato
Lead, Centre for Cybersecurity, World Economic Forum

Dennis Frio
Managing Director, PwC

Jonathan Pastore
Director, PwC

Acknowledgements

Supply chain working group co-chairs

Mansur Abilkasimov
Director Cybersecurity Governance,
Schneider Electric

Ali H. Asseri
Head of Supply Chain and Third-Party Cybersecurity Compliance, Saudi Aramco

Advisory Team

Basim Al-Ruwaii
Chief Information Security Officer, Saudi Aramco

Christophe Blassiau
Senior Vice-President, Digital Security and Global Chief Information Security Officer, Schneider Electrics

Georges de Moura
Head of Industry Solutions, Centre for Cybersecurity, World Economic Forum

Robert Lee
Chief Executive Officer, Dragos, USA

Anders Rimstad
Chief Security Officer, Aker, Norway

Leo Simonovich
Vice-President and Global Head, Industrial Cyber and Digital Security, Siemens Energy, USA

Supply chain working group members

The working group consists of senior executives from the oil and gas industry tasked with leading in-depth discussions to illuminate the industry's best practices and create new solutions to help organizations manage third-party risks.

Aker BP, Norway
Sigmund Kristiansen

American Petroleum Institute, USA
Suzanne Lemieux

bp, United Kingdom
Jason Donner, Heath Drew

Check Point Software Technologies, Israel
Rishi Muchalla

Claroty, USA
Simon Chassar

Cognite, Norway
Jakob Eide

Cyber Security Agency of Singapore, Singapore
Thian Chin Lim

Cybersecurity and Infrastructure Security Agency, USA
Gabriel Hengel, John Ransom, Robert Watson

Dragos, USA
Jason Christopher

Ecopetrol, Colombia
Alberto León Lozano

Eni, Italy
Giorgio Medina

Enquest, United Kingdom
Michael Rapley, Michael Thomson

Galp Energia, Portugal
Tiago da Cunha Oliveira

Global Resilience Federation, Singapore:
AJ Eserjose, John Lee

Halliburton, USA
Mary Rose Martinez

HCL Technologies, India
Neelakarun Asari

Institute for Security and Safety (ISS), Germany
Guido Gluschke, Swantje Westpfahl

Kuwait Oil Company (KOC), Kuwait
Reem Faraj Al-Shammari

MITRE, USA
Emily Frye

North American Transmission Forum, USA
Valerie Agnew

Occidental Petroleum, USA
Fakhry Nusiebeh

Office of Gas and Electricity Markets (Ofgem), United Kingdom
Mohammed Zumla

Palo Alto Networks, USA
Haider Pasha

Pan American Energy, Argentina
Maria del Rosario Romero

PETRONAS, Malaysia
Muhittin Hasancioglu

PwC, USA
Dean Spitzer, Harshul Joshi, Madison Hirsh, Kyle Saud

Repsol, Spain
Javier García Quintela

Royal Dutch Shell, Netherlands
Oleg Stryzhak

Royal Vopak, Netherlands
Arno Sevinga

Saudi Aramco, Saudi Arabia
Eyade Subahe, Muhanad A. Shahat

Schneider Electric, France
Elisabeth Williamson

SecurityScorecard, USA
Mike Wilkes

Suncor Energy, Canada
David Craig, John Hill

Tech Mahindra Limited, India
Dhaval Bhatt

The Forum also wishes to acknowledge contributions from Tony Eddleman from the Nebraska Public Power District, Tom Galloway and Ken Keels from the North American Transmission Forum, and Younes Dragoni from the Global Shapers Lugano Hub.

Endnotes

1. Bryan, Jordan, “A Better Way to Manage Third-Party Risk”, *Gartner*, 15 August 2019: https://blogs.gartner.com/smarterwithgartner/a-better-way-to-manage-third_party-risk/ (link as of 15/7/21).
2. Jibilian, Isabella and Katie Canales, “The US Is Readying Sanctions Against Russia over the SolarWinds Cyberattack. Here’s a Simple Explanation of How the Massive Hack Happened and Why It’s such a Big Deal”, *Insider*, 15 April 2021: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?utm_source=copy-link&utm_medium=referral&utm_content=topbar (link as of 15/7/21).
3. Bussewitz, Cathy, “Colonial Pipeline Confirms It Paid $4.4 Billion to Hackers”, *PBS*, 19 May 2021: https://www.pbs.org/newshour/economy/colonial-pipeline-confirms-it-paid-4-4-million-to-hackers (link as of 15/7/21).
4. Paul, Kari, “Who’s Behind the Kaseya Ransomware Attack – and Why Is It So Dangerous?”, *The Guardian*, 7 July 2021: https://www.theguardian.com/technology/2021/jul/06/kaseya-ransomware-attack-explained-russia-hackers (link as of 15/7/21).
5. *PwC Third Party Risk Management Digital Trust Survey Snapshot – Building Digital Trust: Trust in Third Parties*: https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/digital-trust-leadership-operations-partnership/trust-in-third-parties.html (link as of 15/7/21).
6. National Institute of Standards and Technology, “Best Practices in Cyber Supply Chain Risk Management”: https://www.nist.gov/system/files/documents/itl/csd/NIST_USRP-Boeing-Exostar-Case-Study.pdf (link as of 15/7/21).
7. ISACA, “The NIST Cybersecurity Framework – Third Parties Need Not Comply”, *Isaca Journal*, 2020: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2020/volume-1/the-nist-cybersecurity-framework-third-parties-need-not-comply_joa_eng_0220.pdf (link as of 15/7/21).
8. Cybersecurity and Infrastructure Security Agency, “NIST ICT Supply Chain Risk Management Toolkit”: https://www.cisa.gov/ict-supply-chain-toolkit (link as of 15/7/21).
9. Many organizations have developed an inherent risk questionnaire that is completed by the business unit to gather information on the product/service, generate an overall inherent risk rating (IRR) and trigger applicable due diligence assessments and contractual terms and conditions.
10. The residual risk is the risk exposure after considering the effectiveness of the third party’s control framework.
11. The definition of “critical” may differ by organization; however, in general, if an outage in the product and service would result in a significant impact to the organization, it may be considered “critical”.
12. To build the baseline requirements, the group explored the existing supply chain criteria established by the North American Transmission Forum (NATF) for the electricity industry as a precedent and example; see North American Transmission Forum, “Supply Chain Cyber Industry Coordination”: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination, combining information provided by the NIST supply chain toolkit and Dragos operational technology risk management guidelines (link as of 15/7/21).
13. World Economic Forum, “Cyber Resilience in Oil & Gas”: https://www.weforum.org/projects/cyber-resilience-in-oil-and-gas-industry (link as of 20/7/21).
14. Christopher, Jason D., “Industrial Cyber Risk Management: Guideline for Operational Technology”, *Dragos*, March 2021: https://hub.dragos.com/hubfs/Whitepaper-Downloads/Industrial-Cyber-Risk-Management-2021March.pdf (link as of 15/7/21).
15. National Institute of Standards and Technology*, Cyber Security Framework (CSF):* https://www.nist.gov/cyberframework (link as of 15/7/21).
16. International Organization for Standardization, *ISO/IEC 27001 Information Security Management Standard*: https://www.iso.org/isoiec-27001-information-security.html (link as of 15/7/21).
17. World Economic Forum, “Cyber Resilience in Oil & Gas”: https://www.weforum.org/projects/cyber-resilience-in-oil-and-gas-industry (link as of 20/7/21).
18. Edison Electric Institute, *Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk, version 2.0,* May 2020*:* https://www.eei.org/issuesandpolicy/Documents/EEI%20Law%20-%20Model%20Procurement%20Contract%20Language.pdf (link as of 15/7/21).
19. Unified assessment questionnaire available on the World Economic Forum Cyber Resilience in Oil and Gas project page: https://www.weforum.org/projects/cyber-resilience-in-oil-and-gas-industry (link as of 15/7/21).
20. Ross, Ron, Victoria Pillitteri, Richard Graubart, Deborah Bodeau and Rosalie McQuaid, “Developing Cyber Resilient Systems: A Systems Security Engineering Approach”, NIST Special Publication 800-160, Volume 2: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf (link as of 15/7/21).
21. Freund Jack and Jack Jones, *Measuring and Managing Information Risk: A FAIR Approach*, Butterworth-Heinemann, 2014.

WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org