KOVRR
Cyber Decisions. Financially Quantified.

The Optimal Cyber Risk Management Tools to Streamline DORA Compliance

www.kovrr.com

Table of Contents

Over the past few decades, money has steadily transformed from a material entity to a digital one. Worldwide, people rely on the cyber realm to pay their bills, shop for food, and perform many other everyday activities. Corporations, too, particularly following the 2020 pandemic, are largely dependent on cloud-based operations, utilizing various management platforms and storing massive amounts of data online.

The financial sector is no exception, even leading the way in many regards toward total digitization. Yet, while this shift has made large and small-scale transactions alike much easier, it has also introduced significant market risks. The convenience inherently comes with the potential for a cyber attack to cause widespread market disruption and economic instability.

With such a looming catastrophic possibility in mind, the European Union (EU) decided to take preventative measures, introducing the Digital Operational Resilience Act (DORA).

What Is the Digital Operational Resilience Act (DORA)?

DORA is the EU's overarching regulation to ensure that the financial sector, which includes traditional institutions such as banks and investment firms, non-traditional entities like cryptocurrency providers, and third-party cloud service providers that offer information and communications technology (ICT) to traditional and non-traditional firms alike, remains operationally resilient in the wake of a cyber event.

This cybersecurity legislation comprises five primary pillars, each with specific articles offering further information on how to comply. EU financial organizations must strictly adhere to these provisions no later than January 17, 2025, or face penalties. These pillars are:

1. ICT risk management
2. ICT-related incident management, classification, and reporting:
3. Digital operational resilience testing
4. Management of ICT third-party risk
5. Information-sharing arrangements

Who Is Responsible for Ensuring DORA Compliance?

Within its articles, DORA grants "competent authorities" the power to evaluate an organization's observance of the ICT regulations, issue administrative penalties, and require remedial measures. In some cases, depending on the particular Member State, these authorities can impose criminal charges. For those entities that the EU has deemed "critical," however, there will be a lead overseer who has all the power of the competent authorities, plus the ability to levy fines.

The Challenges Financial Entities Face in Complying With DORA

Now confronted with a slew of new regulatory conditions, European financial institutions are compelled to gather, analyze, and report more extensive amounts of data to make highly strategic decisions. Manually handling these tasks would not only be impractical but also leave organizations with little time to do anything else. Consequently, EU business leaders are now in search of advanced cyber risk management platforms that can streamline these processes and facilitate compliance.

At the same time, amid a turbulent economy and limited budgets, companies can not afford to adopt a different tool to address each specific DORA requirement. Instead, stakeholders must carefully consider which platforms can assist with multiple aspects of regulation adherence simultaneously. While no single tool can account for all of the stringent responsibilities the EU financial sector now faces, there are certainly some that are more practical than others.

Harnessing Cyber Risk Quantification for DORA Compliance

Cyber risk quantification (CRQ) is the process of translating an organization's cyber risk into broader business terms, such as event likelihoods and financial impacts. While there are various types of quantification approaches, the one most applicable to DORA compliance is the on-demand CRQ model. This type of CRQ enables businesses to evaluate their cyber risk postures within minutes and provides data-driven insights on how to lower exposure levels.

To learn more about this process, read What Is Cyber Risk Quantification (CRQ)?

Indeed, on-demand CRQ models such as the one offered by Kovrr provide stakeholders support for the majority of DORA's core components, helping their organizations both meet compliance checkboxes and achieve a state of robust cyber resiliency.

ICT Risk Management: Defining Risk Tolerance Levels

DORA	Kovrr's CRQ Platform
ICT Risk Management, Article 5 Determination of appropriate risk tolerance level	Leverage multiple financial exposure insights and explore the top loss scenarios in the CISO Report

Among the many ways CRQ models can help organizations comply with DORA, the first use case emerges in Article 5. The provision states that the management body is entrusted with "the responsibility for setting and approving the digital operational resilience strategy...including the determination of the appropriate risk tolerance level." By quanti-

fying cyber risk, this governing body becomes equipped with the necessary, data-driven insights to do so.

Determining relevant risk appetite and tolerance thresholds is the basis of building out any cyber risk management strategy, as the majority of subsequent decisions will be based on these benchmarks. With Kovrr's CRQ platform, CISOs (chief information security officers) and other stakeholders have access to a range of possible loss scenarios they're likely to face in the upcoming year, offering the information necessary to determine these levels.

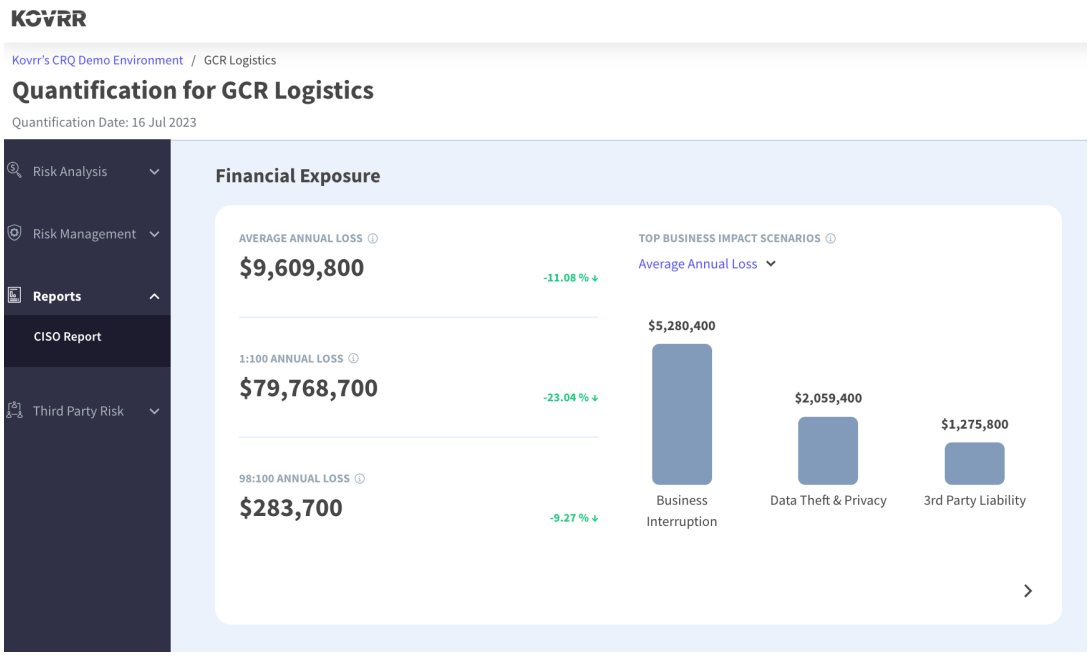

Figure 1: CRQ for GCR Logistics, Financial Exposure Statistics

For example, in Figure 1, the organization's average annual loss (AAL) expectancy is roughly $9.6 million. This figure offers a solid starting point for determining their cyber risk appetite and tolerance and allows them to make more informed decisions. On the one hand, they may decide that they are financially comfortable taking on this amount of risk and, therefore, factor it into their overall tolerance levels, ensuring there is enough capital reserve.

On the other hand, now that these stakeholders understand the potential loss they face due to ICT activities, they may opt to invest more in cybersecurity mitigation efforts or cyber insurance to reduce this exposure. Armed with the information regarding the expected costs in the upcoming year, stakeholders can accurately calculate risk tolerance levels that align with the organization's overall objectives and resources.

Additional CRQ Metrics for Determining Risk Appetite and Tolerance

DORA	Kovrr's CRQ Platform
ICT Risk Management, Article 5 Determination of appropriate risk tolerance level	Harness the Materiality Analysis for the likelihood of exceeding financial, data record, and outage time loss thresholds.

Kovrr's Materiality Analysis feature is also particularly helpful for determining appropriate risk appetite and tolerance levels, offering loss forecasts not only for financial damages but also for compromised data records and outage time hours. Indeed, agreeing upon a suitable risk tolerance involves evaluating more than the potential monetary losses an organization faces, and additional quantified metrics allow for this deeper analysis.

In Figure 2, Kovrr's Materiality Analysis highlights the likelihood of eMerchify experiencing an outage duration that exceeds the various thresholds of 8, 12, 24, and 48 hours in the case of a cyber event. Knowing these times, in combination with their exceedance likelihood, enables managerial bodies to assess the potential operational impact of prolonged outages and determine how well-aligned their current risk posture is with desired tolerance levels.

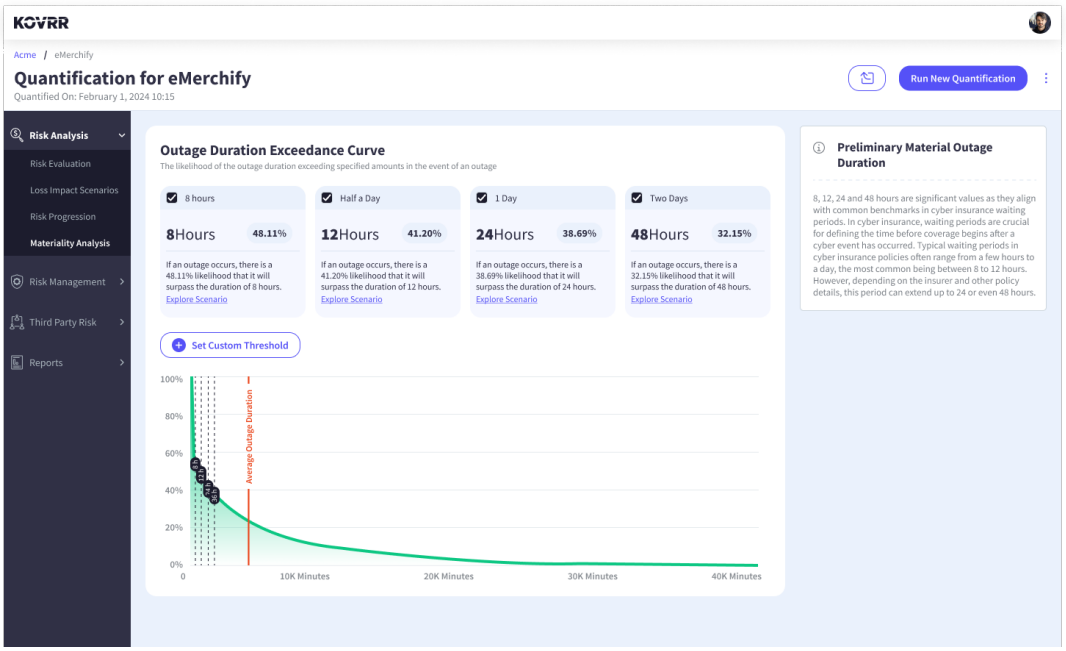

Figure 2: CRQ Materiality Analysis for eMerchify, Outage Duration Exceedance Curve

With the CRQ analysis calculations, organizational leaders may conclude, for example, that there is a higher probability than they are comfortable with of a business outage lasting more than 24 hours. With this information, they may then decide to set a lower risk tolerance and invest the resources into building a more robust cyber risk posture that minimizes this likelihood.

While risk tolerance levels vary based on the business context, having access to accurate forecasts guarantees that these decisions are realistic and justified.

ICT Risk Management: Allocate and Review the Appropriate Budget

DORA	Kovrr's CRQ Platform
ICT Risk Management, Article 5 Appropriate budget allocation and periodic review	Upgrade security controls according to financial effects within the Risk Management recommendations.

Article 5 of DORA also requires the management body to "allocate and periodically review...[the organization's] budget to fulfill the financial entity's digital operational resilience needs." On-demand cyber risk quantification's fundamental purpose is, in fact, to support any business in this endeavor, providing its financial exposure due to cyber activities. Metrics such as the average annual loss (Figure 1) give a clear indication of the level of investment required to achieve a resilient state.

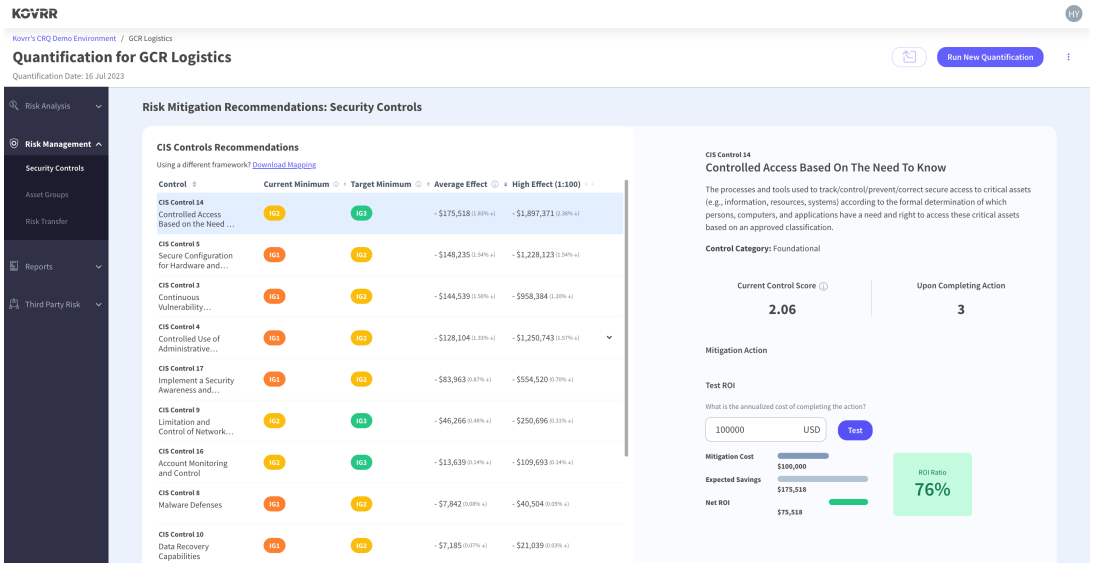

Figure 3: CRQ for GCR Logistics, CIS Control Recommendations, Upgrade Financial Effects

However, CRQ platforms like Kovrrr's also offer deeper insights into the exact security control upgrades that will yield the most significant reduction in financial exposure, assisting with more precise and effective cybersecurity budget allocation. For instance, in Figure 3, an upgrade to CIS Control 14 from level IG2 to IG3 will have the largest monetary effect, on average, reducing GCR Logistics's exposure by a little over $175 thousand.

Then, using Kovrr's cybersecurity ROI calculator, stakeholders can determine whether the required investment yields a positive return. In the case of GCR Logistics, the upgrade only costs the company $100 thousand, signifying that if resources were allocated to the particular security control, they would achieve an ROI rate of 76%. This precise

measurement results in more economic decisions, ensuring funds are effectively distributed towards resiliency.

ICT Risk Management: Maintaining Sufficient ICT Risk Knowledge

DORA	Kovrr's CRQ Platform
ICT Risk Management, Article 5 Knowledge to understand and assess ICT risk	Translate cyber and ICT risk into the broader business terms commonly used in high-level risk management meetings.

The final example, within DORA Article 5, of how CRQ assists with compliance arises from a requirement for management bodies to address one of the most common challenges organizations across industries face when it comes to integrating cyber risk management into the broader business strategy: effective communication. Indeed, these EU business leaders are now legally compelled to maintain "sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations of the financial entity."

By translating complex ICT risk management terms into monetary implications—a language these executives are particularly familiar with and comfortable conversing in—Kovrr's cyber risk quantification makes certain that all liable parties fully comprehend the financial institution's risk posture. With the broader business metrics, they can tangibly recognize what's at stake should they not invest the necessary resources into effective management programs.

ICT Risk Management: Overall Business Objective Alignment

DORA	Kovrr's CRQ Platform
ICT Risk Management, Article 6 Frameworks shall include a digital operational strategy that aligns with broader objectives	Utilize financial terminology and risk management metrics to ensure ICT mitigation strategies align with overall business aims.

Article 6 of DORA likewise lays out a number of provisions that can be more easily adhered to by harnessing an on-demand cyber risk quantification solution. Section 8 of the Article requires that European financial entities establish an ICT risk management framework that includes a digital operational resilience strategy that, in turn, explains “how [the framework] supports the entity’s business strategy and objectives” and establishes “risk tolerance levels…in accordance with the [entire entity’s] risk appetite.”

In other words, management bodies must be able to demonstrate to the competent authorities that their cyber risk management framework aligns with the broader business

goals and effectively propels it towards its targets, bearing in mind that said authorities may not have a technological background. With the financial terminology and broader business metrics Kovrr's platform provides, however, communicating this alignment becomes a fairly straightforward process.

Using Financial Terminology to Demonstrate Alignment

Metrics such as the potential reduction in exposure levels from mitigation initiatives and ROI highlight how investing in cybersecurity contributes to a financial entity's economic prosperity. A CRQ analysis provides stakeholders with the ability to showcase, for instance, that various ICT risk management measures have saved the company $1 million in potential loss in the past year. This concrete monetary figure clearly shows that cybersecurity is not a cost center but a value-adding component of the business strategy.

Using Other Business Metrics to Demonstrate Alignment

The broader business metrics (i.e., total data record loss and outage time duration) Kovrr's CRQ platform translates ICT risk into are likewise crucial for illustrating how the operational resilience strategy aligns with overall risk appetite. Should a financial entity's appetite levels require minimizing downtime due to any business risk, stakeholders can use cyber risk quantification to corroborate that they've performed the necessary calculations and taken subsequent action to reduce the likelihood of longer outage times due to cyber risk.

ICT Risk Management: Setting Clear, Long-Term Objectives

DORA	Kovrr's CRQ Platform
ICT Risk Management, Article 6 Set clear InfoSec objectives, including KPIs	Leverage the Risk Progression feature, which highlights an organization's cyber risk posture metrics over time.

Article 6, Section 8 also stipulates that operational resiliency strategies outline "clear information security objectives, including key performance indicators and key risk metrics." On top of providing organizations with a consistent, communicable structure on which to demonstrate ICT risk management success, these deliverables also make it easier to identify both the strengths and more vulnerable areas that require attention.

Figure 4: Kovrr's CRQ Risk Progression, Demonstrating Cyber Risk Posture Over Time

Moreover, by measuring the same specific metrics over time, stakeholders can highlight their cybersecurity progress and support a narrative of sustained resilience. For instance, if organizations quantify their cyber risk exposure with Kovrr's CRQ models, they'll have access to the Risk Progression feature (Figure 4), which reveals the long-term shift of change for three financial exposure KPIs: current risk, baseline risk, and minimal risk. This wider view can highlight EU stakeholders' commitment to operational resiliency, even as the risk landscape evolves.

Digital Operational Resilience Testing: A Range of Risk Assessments

DORA	Kovrr's CRQ Platform
Digital Operational Resilience Testing, Article 24 Program shall include a range of assessments, tests, and methodologies	Employ a comprehensive assessment model that illuminates a unique perspective of cyber risk exposure.

Article 24 is the first of the 64 to discuss DORA's third pillar, providing general requirements for cyber resiliency testing and instructing financial corporations to develop a program that includes "a range of assessments, tests, methodologies, practices, and tools." The passage implies that this particular ICT regulatory component is not merely a one-off activity but rather a comprehensive process that must shed light on multiple angles of the organization's resiliency levels.

Evaluating various aspects of resilience makes sense, considering the concept is inherently multifaceted. Relying solely on one assessment type, methodology, or tool can leave an organization vulnerable to blind spots. No single approach can account for all the dimensions involved in assessing overall operational resilience and its different elements, such as the efficacy of incident response plans and the reliability of backup systems. Therefore, distinct evaluation methods are necessary to provide a holistic view.

In that respect, Kovrr's cyber risk quantification solution can play a crucial role, offering stakeholders a data-driven, metric-based perspective of resiliency based on monetary exposure, outage duration potential, and data integrity vulnerabilities. By reviewing these components of digital operation resilience, financial institutions develop a better understanding of how prepared they are to withstand a cyber event and the work required to lower these forecasts to an acceptable risk value.

Integrating CRQ into a diverse testing regimen thus ensures a robust, well-rounded approach to testing digital operational resilience.

Digital Operational Resilience Testing: Evaluating Cyber Risk Scenarios

DORA	Kovrr's CRQ Platform
Digital Operational Resilience Testing, Article 25 Program shall provide scenario-based tests	Explore the Drill Down feature for a more granular view of specific cyber risk scenarios and event drivers.

Subsequent articles dive into the details necessary for digital operational resilience testing compliance, with Article 25 pronouncing that a testing program should include an evaluation of ICT risk loss scenarios. In addition to the loss exceedance curve, which illustrates a range of possible impact levels according to their likelihood (i.e., the organization has a 13% annual probability of experiencing a cyber event that costs $600 thousand but also a 2% probability of an event that costs $3 million), Kovrr's on-demand CRQ platform also has the Drill Down feature.

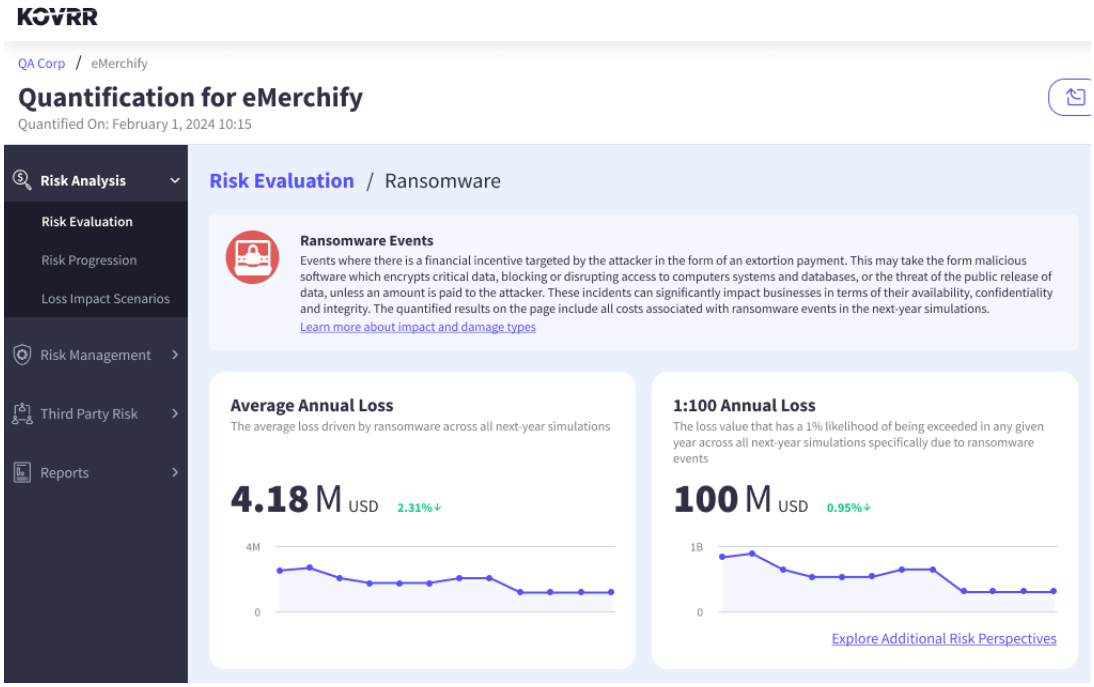

Figure 5: Kovrr's Drill Down Feature, Annual Loss Metrics for eMerchify's Ransomware Risk Landscape

This feature enables CISOs and other risk managers to explore more granular metrics regarding cyber attacks and initial attack vectors. In Figure 5, the company eMerchify has opted to drill down into a ransomware event scenario, which, on average, will cost them $4.18 million in the upcoming year (Average Annual Loss). There is also a 1% chance of losing more than $100 million due to this type of incident.

Other event statistics provided by the Drill Down feature include the likelihood of experiencing an event that results in a loss, as opposed to the likelihood across all scenarios, which included events that don't cause any financial damage. Organizations can also examine the median monetary loss, event duration, and amount of data records compromised in the case of an event that causes harm. It's also possible to evaluate which initial attack vectors are most likely to lead to a particular type of event.

With these drilled-down scenario data points, organizations have much sharper insights into the events or initial attack vectors that are most likely to threaten resiliency efforts and are, thereby, more prepared to develop targeted mitigation efforts and demonstrate due diligence for their testing programs. To learn more about all the granular scenario details found within Kovrr's CRQ, read Drill Down Feature Illuminates a Deeper View of Cyber Risk Drivers.

Analyzing ICT Risk Scenarios With Materiality Analysis

While Kovrr's CRQ platform allows risk managers to drill down to various risk scenarios according to the event type or initial attack vector, this capability is also available for the specific predefined loss thresholds offered in the Materiality Analysis feature. For instance, organizations might discover that if a cyber event occurs, they face a 1.43% likelihood of losing more than $200 million, as is the case highlighted in Figure 6.

Figure 6: ICT Risk Scenario Exploration With Kovrr's CRQ Materiality Analysis

However, stakeholders now subject to comply with DORA, Article 25, can opt to learn even more about this particular scenario, such as the likelihood of that level of loss occurring at all, the precise monetary damage they should expect, the likely total outage hours, and the number of data records compromised. A breakdown of the specific risk

drivers according to event type and initial attack vectors causing this scenario to occur is likewise provided.

This level of information is accessible for any one of the pre-generated thresholds across all three loss exceedance curves.

Management of ICT Third-Party Risk: Performing Due Diligence

DORA	Kovrr's CRQ Platform
Management of ICT Third-Party Risk, Article 28 Cost-benefit analysis of third-party services	Use the Third-Party Analysis feature to evaluate specific technology and vendor risk before adoption or engagement.

Third-party service providers significantly streamline a myriad of business activities, selling the infrastructure, platforms, and software that the majority of modern financial institutions rely on to operate. While the benefits of these information and communications technologies are immense, they do not come without their fair share of risk. Over the past few years, third-party ICT service provider breaches, such as the ones at MOVEit and SolarWinds, have caused billions of dollars worth of damage.

With this wreckage potential in mind, the EU constructed the fourth pillar of DORA, requiring that ICT third-party risk be comprehensively managed - a process that starts well before adopting the respective technology. As outlined in Article 28, prior to choosing a vendor, financial institutions must first evaluate whether the use of the selected service is worth the cost of the risk they would be taking on.

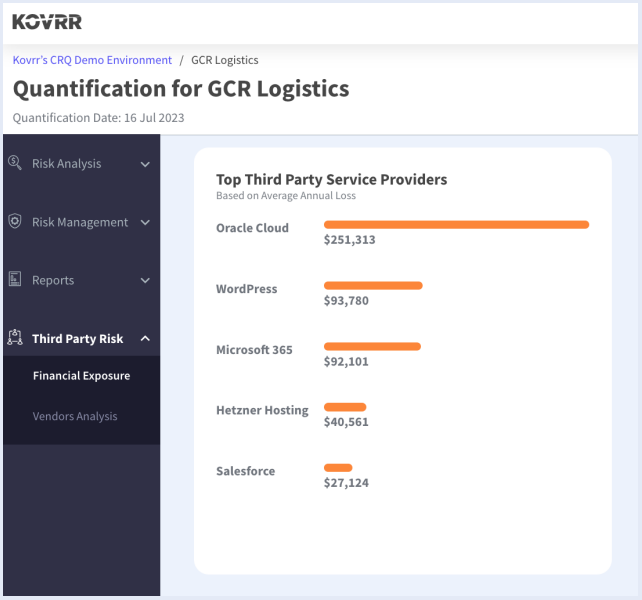

Figure 7: Third-Party Risk Analysis for GCR Logistics, Financial Exposure per Provider

Kovrr's Third-Party Risk analysis illuminates such costs, allowing stakeholders to make more informed decisions and minimize the likelihood of exceeding risk tolerance levels. For instance, in Figure 7, Kovrr's CRQ platform reveals that GCR Logistics' reliance on Oracle contributes approximately $250 thousand to their overall risk exposure, while Salesforce only adds $27 thousand. The monetary insights, which can be derived subsequent to quick updates to the CRQ platform inputs, render cost-benefit calculations relatively straightforward.

With Kovrr, financial institutions can also review the risk associated with each specific technology, offering a different perspective during the due diligence process. In Figure 8, the platform shows that GCR Logistics employs Microsoft for both email provider and platform services. In total, the ICT third-party service provider adds an extra $92 thousand of financial exposure. However, when broken down according to technology, it's easy to see that one is significantly more risky than the other. Depending on the company's risk tolerance, they may want to explore a different vendor for that same technology.

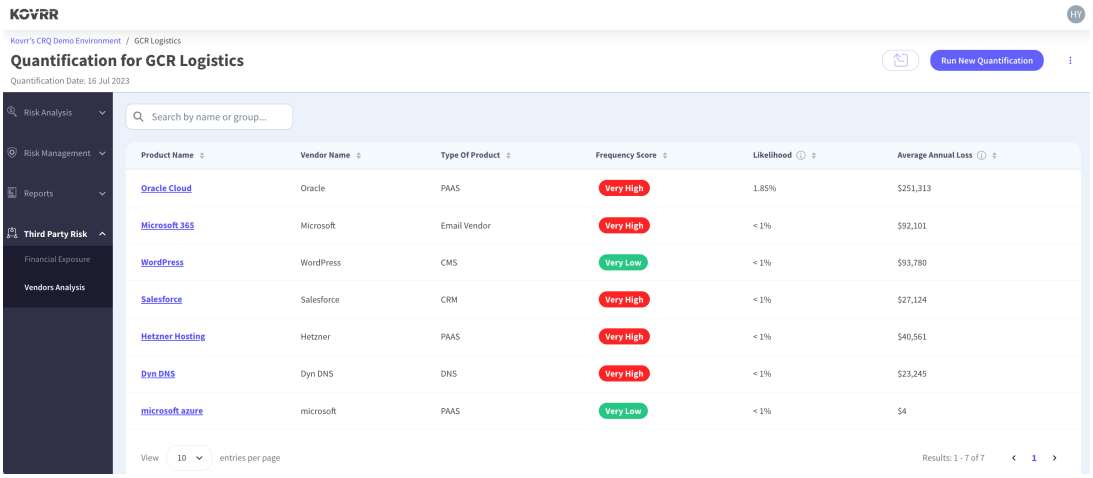

Figure 8: Third-Party Risk Analysis for GCR Logistics, ICT Risk Levels per Technology

As part of Kovrr's cyber risk quantification process, the models take into account the confidentiality, integrity, and availability of each technology and third party and use this information to generate an accurate forecast of the likelihood of a specific third-party event occurring and its respective cost. Understanding this aspect of ICT third-party services equips financial institutions to choose the optimal vendor according to their particular risk landscape and demonstrate that they've thoroughly complied with DORA.

Management of ICT Third-Party Risk: Avoiding Insolvency

DORA	Kovrr's CRQ Platform
Management of ICT Third-Party Risk, Article 29 Accounting for Potential Insolvency	Use the Third-Party Analysis feature to review the average financial exposure due to third-party relationships.

Another stipulation for managing ICT third-party risk that CRQ can assist with, found in Article 29, requires that financial institutions consider the possibility of insolvency should one of their third-party service providers experience an attack and become bankrupt. Indeed, Kovrr's CRQ platform provides the data necessary to consider this scenario.

By providing the average annual exposure based on vendor, technology, and risk type (e.g., third-party data breaches or business interruptions, Figure 9), Kovrr enables financial entities to evaluate the business risks related to over-reliance on a single provider.

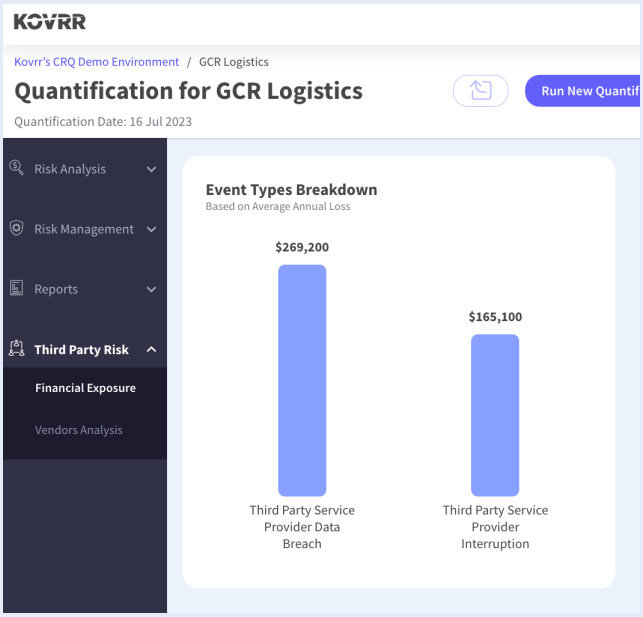

Figure 9: Third-Party Risk Analysis for GCR Logistics, Event Types Breakdown

Moreover, this quantified information provides insight into the financial stability of their ICT third-party vendors, allowing them to establish the necessary resiliency strategies or choose to work with a different provider altogether to ensure compliance with insolvency laws.

Leveraging On-Demand Cyber Risk Quantification to Comply With DORA

DORA is a much-needed regulation that will undoubtedly enhance the safety and stability of the EU financial market and, by default, the rest of the world. Nevertheless, compliance does not come without considerable challenges. Financial entities must quickly learn how to navigate this new landscape of requirements that now demand meticulous data gathering, analysis, and reporting.

Adopting an on-demand cyber risk quantification distinguishes itself as a strategic choice in this context, helping risk managers address these challenges in several key aspects. CRQ models, such as those offered by Kovrr, provide an objective, metric-based assess-

ment of various risk dimensions, including financial exposure, potential outage durations, and data integrity issues, to empower decision-makers with actionable insights that support informed decision-making and effective risk management.

Ultimately, CRQ not only facilitates compliance with DORA but also fortifies an organization's overall cyber defense strategy. This dual advantage makes it an indispensable tool for financial entities striving to navigate the complexities of DORA and achieve long-term operational resilience.

Contact one of our cyber risk management experts or schedule a free demo today to learn more about Kovrr's on-demand CRQ solution.

APPENDIX:

Cyber Risk Quantification for DORA Compliance

DORA	Kovrr's CRQ Platform
ICT Risk Management, Article 5Determination of appropriate risk tolerance level	Leverage multiple financial exposure insights and explore the top loss scenarios in the CISO Report.
ICT Risk Management, Article 5 Determination of appropriate risk tolerance level	Harness the Materiality Analysis for the likelihood of exceeding financial, data record, and outage time loss thresholds.
ICT Risk Management, Article 5 Appropriate budget allocation and periodic review	Upgrade security controls according to financial effects within the Risk Management recommendations.
ICT Risk Management, Article 5 Knowledge to understand and assess ICT risk	Translate cyber and ICT risk into the broader business terms commonly used in high-level risk management meetings.
ICT Risk Management, Article 6 Frameworks shall include a digital operational strategy that aligns with broader objectives	Utilize financial terminology and risk management metrics to ensure ICT mitigation strategies align with overall business aims.
ICT Risk Management, Article 6 Set clear InfoSec objectives, including KPIs	Leverage the Risk Progression feature, which highlights an organization's cyber risk posture metrics over time.
Digital Operational Resilience Testing, Article 24 Program shall include a range of assessments, tests, and methodologies	Employ a comprehensive assessment model that illuminates a unique perspective of cyber risk exposure.
Digital Operational Resilience Testing, Article 25 Program shall provide scenario-based tests	Explore the Drill Down feature for a more granular view of specific cyber risk scenarios and event drivers.