KOVRR
Cyber Decisions. Financially Quantified.

Leveraging *Cyber Risk Quantification* for NIS 2 Compliance

www.kovrr.com

Table of Contents

A More Unified, Robust Approach to Cyber Risk Management

In response to the growing number of disparate cyber regulations across its member states, resulting in inconsistent cybersecurity practices, the EU drafted Directive 2022/2555, more commonly known as NIS 2. This sweeping directive, officially in effect in October 2024, aims to ensure a more uniform, proactive approach to cyber risk management across the union in the face of an interdependent market and increasingly costly risk landscape.

The European Parliament, recognizing the influence cyber activity has on EU stability, both economic and social, likewise expanded the scope of the first iteration of NIS to encompass new industries, such as public administration, postal services, waste management, and manufacturing. In an age when large-scale cyber events are inevitable, achieving a state of cyber resilience becomes significantly more feasible through collective responsibility and a shared commitment to cybersecurity.

The Importance of Complying With NIS 2

While compliance with the NIS 2 Directive is mandatory for all organizations operating within the specified industries throughout EU member states, it is similarly a strategic move that can bolster a company's competitive edge. The directive helps to ensure that businesses are well-equipped with the necessary protocols and security measures to safeguard critical operations and reduce both the likelihood of an event as well as overall financial exposure.

By proactively investing in cyber risk management, organizations enhance their resilience, making them a much more attractive option in a market where customers are increasingly aware of how vulnerable their personal information has become. Moreover, adhering to the directive's stringent requirements reduces cybersecurity costs in the long term. On average, pre-planned mitigation efforts are much less expensive than reactive responses, freeing up unforeseen resources for innovative initiatives.

That said, non-compliance also comes at a cost. Businesses that fail to meet NIS 2 standards might incur substantial financial repercussions, with "essential" entities facing monetary fines of, at minimum, €10,000,000 or 2% of their global revenue and "important" entities facing a minimum fine of €7,000,000 or 1.4% of their global revenue. Beyond these penalties, NIS 2 also introduces personal liability for executive management, such as suspension, disbarment, or other reputational consequences should their businesses not meet the regulatory guidelines.

Streamlining Compliance With New Solutions and Practices

Organizations now subject to the EU's updated NIS 2 legislation will inevitably need to explore new solutions and methodologies to accelerate compliance processes while si-

multaneously managing their existing obligations and tasks. Although challenging, this regulatory shift also presents a valuable opportunity to enhance existing cyber risk management practices, leading to the identification and resolution of previously overlooked vulnerabilities and, ultimately, fortifying resilience.

Incorporating an on-demand cyber risk quantification (CRQ) platform into the organization's toolkit can be particularly advantageous in this context. These platforms enable chief information security officers (CISOs) and other cybersecurity leaders to articulate complex cybersecurity risks and concepts in financial terms, making it easier for senior stakeholders to grasp the business impact cyber vulnerabilities can have.

With the clear, tangible insights they provide, CRQ solutions help organizational leaders align cyber risk management initiatives with organizational goals, ensuring that compliance with NIS 2 standards, such as the need to perform in-depth risk analyses and design effective incident response plans, is not only a legal obligation but also a business enabler.

On-Demand Cyber Risk Quantification for NIS 2

CRQ platforms, such as Kovrr's, come equipped with a slew of practicable features that can significantly aid organizations in their compliance efforts and enhance their overall cybersecurity posture.

Governance: Management-Level Cybersecurity Accountability

NIS 2: Article 20.1	Kovrr's CRQ
Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures.	Leverage key financial metrics, including those insights found within the **Security Control upgrade feature**, to ensure upper management tangibly understands strategies.

In Article 20, the NIS 2 Directive directly places the onus of compliance on the management bodies of both the "essential" and "important" entities. These high-level stakeholders are charged with approving cybersecurity risk management strategies and are, therefore, liable for any instances of noncompliance. Unlike the US SEC's cyber regulations, this EU legislation underscores the crucial role upper management plays in ensuring cyber resilience.

However, in order for these executives to approve any risk management strategies or programs, they must first have a tangible understanding of what they are endorsing. Kovrr's CRQ platform plays a pivotal role in this regard by transforming complex technical cybersecurity concepts into clear financial metrics. For instance, Kovrr's models can quantify the maturity levels of an organization's cybersecurity framework, be it CIS, NIST, or ISO. With these insights, it becomes much easier for stakeholders to understand the value of various initiatives.

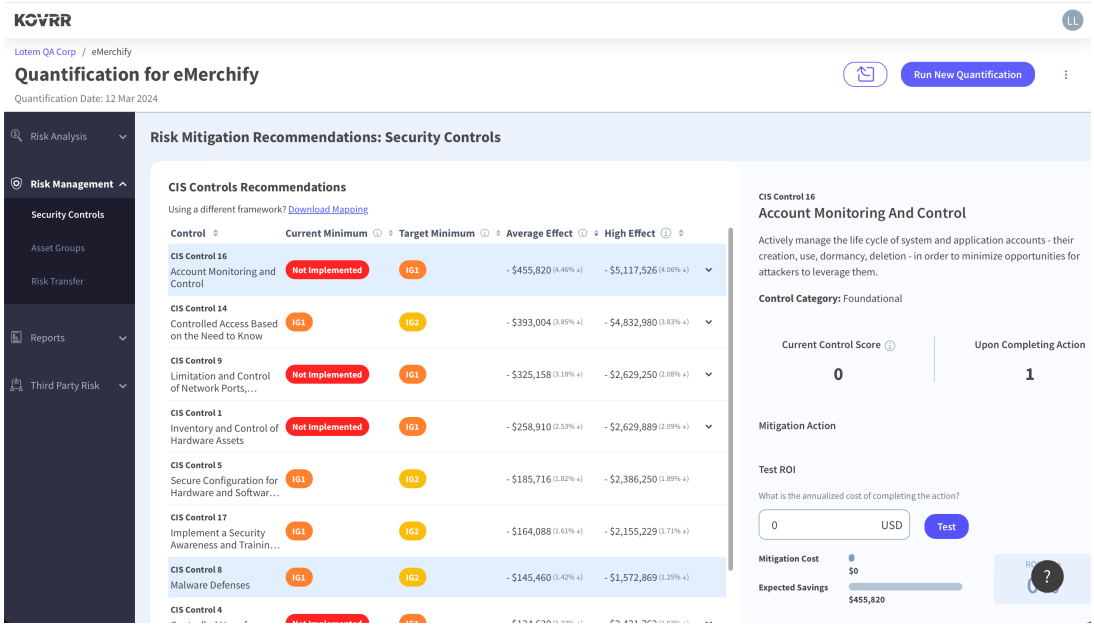

Figure 1: Kovrr's CRQ offers financial insights regarding various mitigation initiatives, communicable to all stakeholders.

In Figure 1, eMerchify has used Kovrr's CRQ solution to quantify their CIS maturity levels. Management bodies can see that, by investing in CIS Control 16, Account Monitoring and Control, they can reduce the organization's overall exposure by, on average, roughly $455 thousand. Then, armed with the monetary information, it also becomes a straightforward process to calculate the ROI, offering these stakeholders even more of an understanding of whether approving the initiative is a decision that results in greater resiliency.

This concrete translation from technical jargon into a more familiar business language ensures that management is fully equipped to evaluate cybersecurity programs, understand them, and take ownership. Beyond facilitating compliance, this capability aligns cybersecurity strategies more closely with the organization's overall objectives, integrating them into broader operational workflows rather than allowing them to remain isolated processes.

Cybersecurity Risk Management Measures: Risk Analysis Policies

NIS 2: Article 21.2a	Kovrr's CRQ
Member States...shall ensure that essential and important entities take... measures [that include] policies on risk analysis and information system security.	Adopt Kovrr's unique CRQ methodology, which incorporates **continuously updated datasets and threat intelligence**, to ensure accurate, precise assessments.

In Article 21, the NIS 2 regulations become more direct about what Member States should require from both essential and important entities in terms of developing and maintaining robust cyber risk management measures. In Section 2a, the legislation mandates that these Member States ensure that these entities develop comprehensive risk analysis policies that are designed to safeguard network and information systems by instituting standardized methods for identifying, assessing, and managing risks.

At the heart of any effective risk analysis policy is a reliable risk assessment methodology, which serves as the foundation on which every subsequent risk mitigation choice will be based. Indeed, without having an accurate, data-driven understanding of organizational cyber risks, cyber risk managers face the likelihood that programs and initiatives are improperly structured, resources are unoptimized, and systems remain vulnerable to potentially high-impact events.

With Kovrr's proprietary Cyber-Sphere (Figure 2), along with our dual top-down and bottom-up modeling approach, companies are equipped to systematically identify and assess their digital assets on-demand. After key business units and their respective data components and technological profiles have been mapped, whether segmented based on department, location, or other granularity, our models will automatically generate a bespoke event catalog of the cyber loss scenarios the organization is most likely to face due to its unique characteristics.

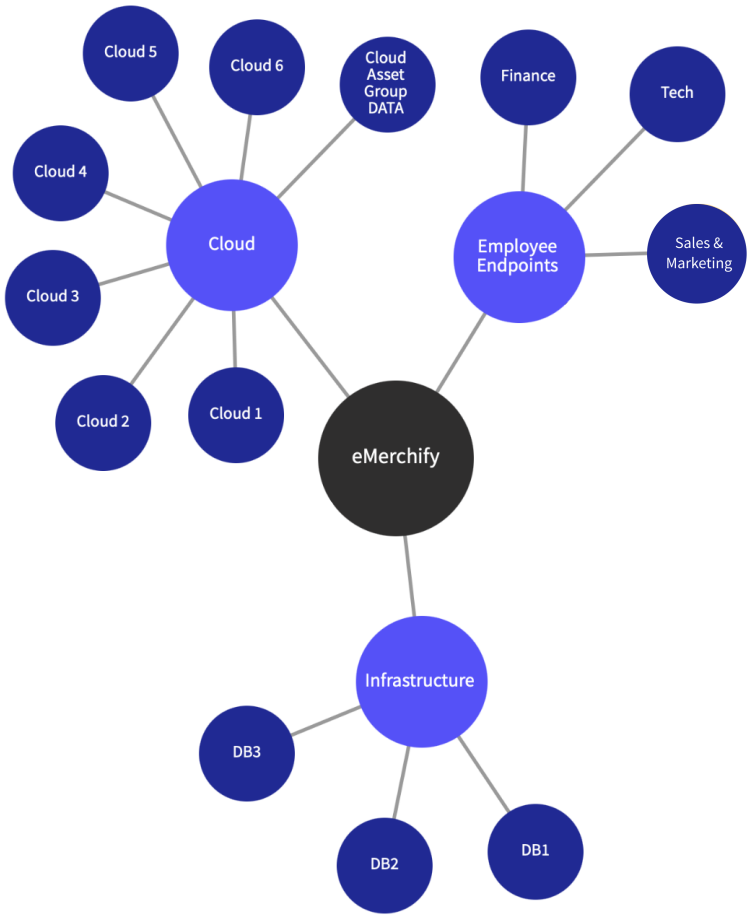

Figure 2: Kovrr's proprietary Cyber-Sphere methodology equips entities to map assets and identify the most significant cyber risks.

Then, by harnessing global loss intelligence from more than 100 continuously updated data sources, including privileged insurance loss datasets, Kovrr's CRQ produces an accurate risk assessment based on real-market financial impact data that illuminates not only the organization's exposure due to cyber activities but also the underlying factors which most significantly contribute to this exposure.

The ongoing, real-time evaluation enables entities to assess and reassess their unique cyber risk landscapes in real-time, arming those responsible with the data-driven insights necessary for crafting comprehensive policies that meet NIS 2 compliance standards.

Cybersecurity Risk Management Measures: Supply Chain Security

NIS 2: Article 21.2d	Kovrr's CRQ
Member States…shall ensure that essential and important entities take…measures [that include] supply chain security…and relationships between each entity and its direct suppliers or service providers.	Engage with Kovrr's **Third-Party Risk analysis** to explore the financial exposure various third-party service providers add to overall exposure levels. View exposure in aggregate or according to vendor or technology.

As events such as the MOVEit Data Breach and CrowdStrike faulty software update highlighted, a crucial component of cyber resilience involves assessing and accounting for third-party service provider risk. Article 21, Section 2d addresses this, directing Member States to craft national cybersecurity policies that include regulations for the way entities, both essential and important, manage the risks of their supply chains.

Entities should have robust processes in place for assessing and mitigating the added cyber exposure they face due to direct supplier or service provider relationships. To help their organizations comply with this specific line item, cyber risk managers and managerial bodies can utilize Kovrr's CRQ platform's Third Party analysis feature. This valuable feature first breaks down third-party service provider risk according to financial exposure.

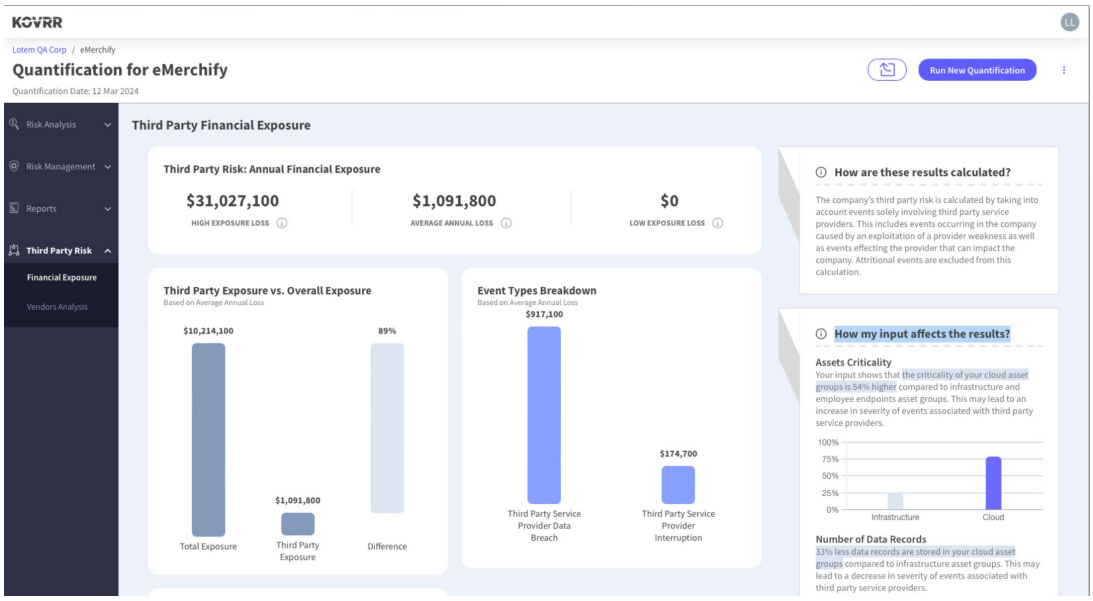

Figure 3: Kovrr's Third-Party Risk analysis offers entities a breakdown of their financial exposure due to the third-party supply chain.

For instance, in Figure 3, eMerchify stakeholders could determine that, on an average year, their entity is likely to lose approximately $31 million because of their supply chain relationships. They can also view this exposure compared to their organization's overall financial exposure, highlighting how much of their risk is driven by these external relationships. The financial exposure feature also demonstrates the type of event most likely to occur within the third-party supply chain, offering further insights into how to optimize mitigation strategies.

Kovrr's Third-Party Risk analysis similarly deconstructs these exposures by vendor and technology type. In Figure 4, for example, eMerchify faces an exposure of nearly $100 thousand due to their usage of WordPress's CMS solution. At the same time, their utilization of one of Microsoft's PAAS tools only exposes them to $4 of potential loss, which is most likely well within their risk appetite.

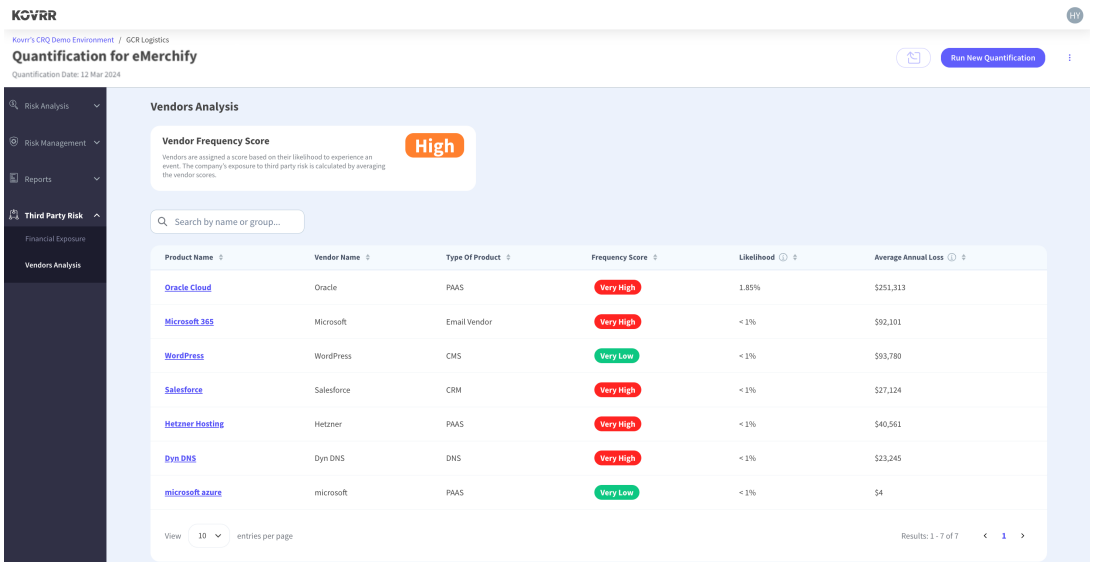

Figure 4: Kovrr's Third-Party Risk Vendor Analysis quantifies financial exposure according to specific vendors and technology types.

By offering financially quantified insights into the cyber risks associated with specific third-party service providers, the platform enables organizations to easily assess the potential impact these vendors may have on their overall exposure and resilience efforts.

Kovrr's CRQ models go well beyond merely adding up individual risks; they account for the interconnections and systemic threats, providing an even more accurate picture of the entities' aggregated third-party risk.

Cybersecurity Risk Management Measures: Quantifying Effectiveness

NIS 2: Article 21.2f	Kovrr's CRQ
Member States...shall ensure that essential and important entities take...measures [that include] policies and procedures to assess the effectiveness of cybersecurity risk-management measures.	Utilize the **Risk Progression feature**, equipped with the Risk Position Analysis and Risk Position Score. Quantify cybersecurity framework maturity levels on-demand to gain actionable insights vis-a-vis control upgrades.

Section 2f of Article 21 also requires that Member States ensure that entities within their jurisdiction develop risk management policies that include the regular assessment and subsequent optimization of cybersecurity program measures. This ongoing evaluation process is crucial to maintaining a robust defense against evolving cyber threats and underscores the notion that achieving a state of cyber resilience is a never-ending journey.

Kovrr's CRQ platform offers practical support in this area. Not only can organizations evaluate their overall financial exposure levels in the aggregate or according to various loss scenarios, but they can leverage the Risk Progression feature specifically to gauge their cyber programs' relative effectiveness against the given risk environment.

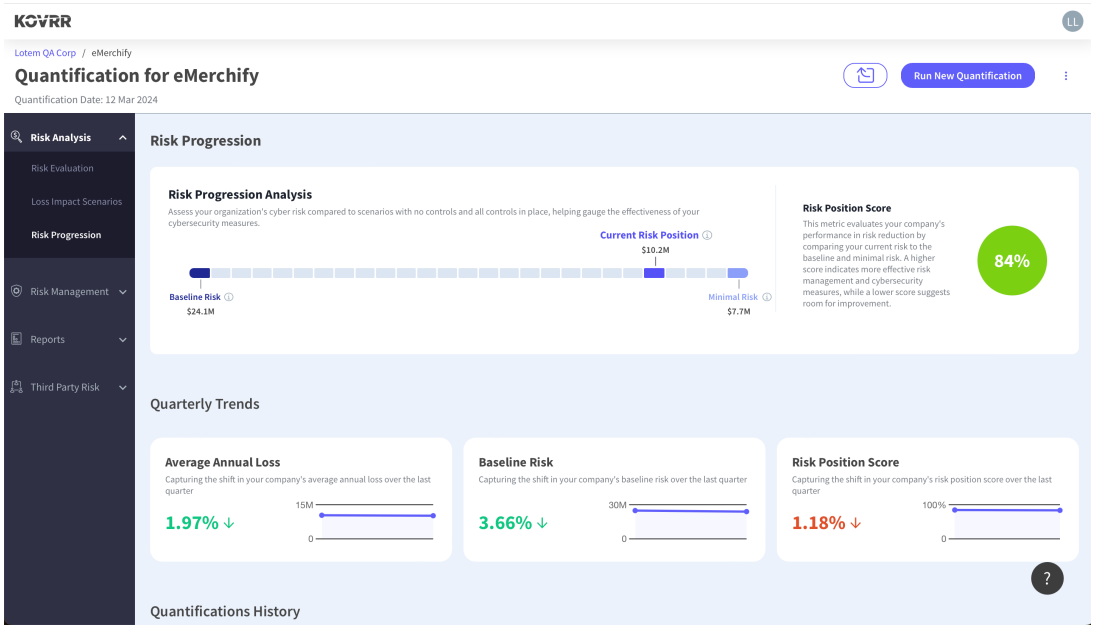

Figure 5: Kovrr's Risk Progression feature provides the KPIs necessary for optimizing cybersecurity programs on-demand.

For example, with the Risk Position Analysis pictured in Figure 5, cyber risk managers can easily determine their organization's cyber risk posture, or average annual loss (AAL), in relationship to both the baseline risk (the expected loss of an organization with the same characteristics - assets, structure, industry, revenue size, location - but without any security controls in place) and the minimal risk (the expected loss of an organization with the same characteristics, but with the most robust security systems in place).

Risk managers can similarly keep track of their Risk Position Scores over time, which is a single value quantification of the organization's risk posture in relation to the baseline and minimal risk scenarios. Ideally, this score will improve over time, even if the baseline (or the external risk environment) becomes worse, offering Member States a solid indication that their organizations operating within the country are harnessing the continuously updated, data-driven insights to ensure cybersecurity strategies remain aligned with evolving threats.

However, while entities may leverage Kovrr's Risk Progression analysis feature to evaluate the evolving robustness of their cybersecurity strategies over time, many already adhere to well-established cybersecurity frameworks, such as NIST, CIS, and ISO, to measure progress in this area. Unfortunately, these frameworks often fall short of offering actionable insights that help cybersecurity professionals understand which initiatives will have the greatest effect on their organization's cyber risk posture and, thus, should be prioritized.

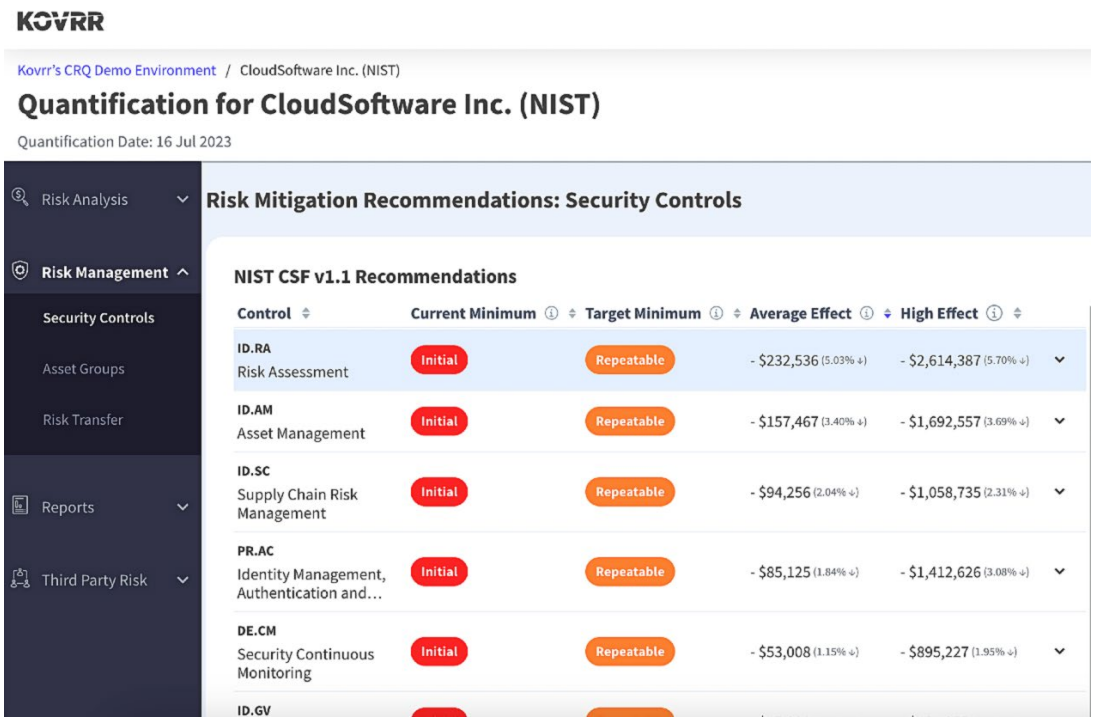

Figure 6: Kovrr's CRQ models quantify maturity levels of various cybersecurity frameworks, such as NIST, CIS, and ISO, to provide actionable enhancement insights

For example, while a security control upgrade in one category, such as Security Continuous Monitoring, may seem beneficial when using the framework in isolation, it's impossible to tell whether an enhancement in Asset Management, alternatively, may actually result in less exposure.

On the other hand, by leveraging Kovrr's CRQ models in combination with these frameworks, the details become evident (i.e., an upgrade of the Asset Management Control, as shown in Figure 6, yields the greatest benefit), allowing entities to make data-driven decisions and demonstrate a commitment to ongoing cybersecurity improvement.

Quantifying cybersecurity framework respective maturity levels with Kovrr's CRQ offers entities a more precise understanding of how their current cyber risk management measures contribute to resilience, as well as which strategies and initiatives they could prioritize to increase overall cybersecurity posture levels. With the financial figures offered both by framework quantification and the Risk Progression analysis, risk managers are equipped with communicable KPIs that can be documented in policies to signify continuous improvement and, thereby, compliance.

Reporting Obligations: Determining Significant Impact Levels

NIS 2: Articles 23.1 and 23.3	Kovrr's CRQ
Member States shall ensure that essential and important entities notify...authorities...of any incident that has had a significant impact on the provision of their services.	Employ Kovrr's **Cyber Materiality Analysis** to explore the likelihood of various loss scenarios. Use these benchmarks to create threshold-based "significant" impact decisions.

In today's cyber risk landscape, with threat actors typically evolving faster than cybersecurity protocols, it's a near inevitability that an organization will fall victim to an event, be it malicious or otherwise. With this realistic understanding in mind, the EU drafted Article 23 of NIS, requiring that Member States ensure their essential and important entities notify the competent authorities if one of these incidents has a "significant" impact on their business.

Although Section 3 of this article defines "significant" impact as one that has caused or can cause "severe" operational disruption or financial loss, the term is still ambiguous and highly dependent on the specific organization's revenue, resources, and industry. Such ambiguity presents a challenge for stakeholders who must now convene to establish clear and defensible thresholds to determine when an incident meets the criteria for mandatory reporting.

Kovrr's CRQ significantly aids in this process with its one-of-a-kind Materiality Analysis feature. This advanced tool offers three critical loss exceedance curves, each highlighting a specific aspect of potential impact, the probability of financial losses surpassing certain thresholds, the likelihood of exceeding data record compromise limits, and the chances of system outages extending beyond predefined durations. With these pre-programmed loss scenarios, entities can easily determine what may constitute a significant event, along with the likelihood of such an event occurring.

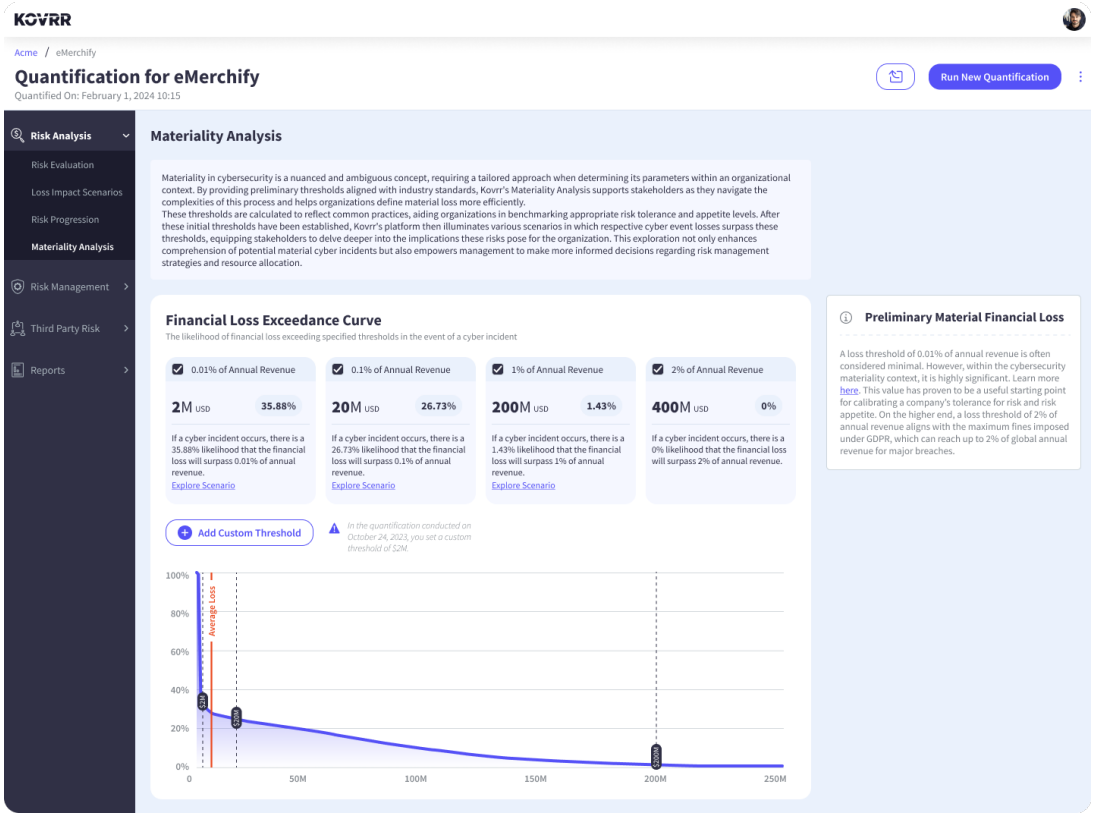

Figure 7: Kovrr's on-demand Materiality Analysis provides data-driven loss thresholds to guide NIS 2's incident reporting process.

For instance, in Figure 7, Kovrr's CRQ models determined that eMerchify has a 35.88% probability that, should they suffer from a cyber event, the financial losses will exceed 0.01% of their annual revenue, which amounts to $2 million. In many cases, this basic point of revenue would equate to a "significant" or material financial loss and would thus be the level of loss at which eMerchify should report the incident. However, Kovrr's platform also provides loss thresholds of 0.1%, 1%, and 2% of annual revenue in case entities decide they have a larger risk appetite.

By setting these quantified thresholds for financial damage, data record compromisation, or outage time duration, organizations can objectively assess whether an event's impact is significant enough to warrant reporting under Article 23. Undoubtedly, other, more qualitative factors may go into the determination process. Still, the quantitative values provide the basis for disclosure or non-disclosure decisions. Kovrr's Materiality Analysis thus offers a data-driven approach for entities to confidently navigate the complexities of reporting obligations while also aligning cybersecurity strategies with broader business objectives.

Reporting Obligations: Complying With Quick Notification Times

NIS 2: Article 23.4a and 4b	Kovrr's CRQ
Member States shall ensure that essential and important entities notify...authorities...(a) 24 hours after becoming aware of the significant incident...[and] (b) within 72 hours.	Kovrr's **Cyber Materiality Analysis** helps stakeholders determine data-driven thresholds well before an event has occurred, ensuring rapid disclosures.

Not only must Member States ensure that essential and important entities disclose "significant" events, but they also have to submit early warnings and more in-depth notifications. The early warning, as described in Article 23, must be submitted within 24 hours of "becoming aware of the significant incident," while a more detailed disclosure should be submitted 72 hours after and include an assessment of the severity and impacts.

These stringent timelines underscore the necessity of an objective process for determining "significance" benchmarks well in advance of any incident, a task with which Kovrr's Materiality Analysis likewise offers invaluable support. With thresholds already established and institutionalized, entities can quickly determine the "significance" level of any incident, eliminating the need for last-minute, anxiety-ridden discussions and likewise giving stakeholders the ability to meet tight reporting deadlines.

Creating a Safer Marketplace and Ensuring NIS 2 Compliance With CRQ

Amid increasingly stringent EU cybersecurity regulations, Kovrr's CRQ solution emerges as a critical tool for organizations that will soon need to comply with their respective Member States' national cyber policies. NIS 2 demands that, ultimately, every essential and important entity must implement robust cybersecurity programs, conduct thorough risk assessments, and continuously upgrade their strategies - which must likewise be approved by senior executives - to ensure long-term resilience.

From identifying and assessing key assets to evaluating the effectiveness of cybersecurity measures on demand, Kovrr's CRQ models provide organizations with the insights necessary to meet these new requirements. Moreover, by translating complex cyber terms into a broader business language, cyber risk management can be elevated and tangibly understood at the highest company levels, ensuring that these compliance efforts simultaneously foster growth and work towards business objectives.

Taking this proactive approach to cyber risk management indeed fuels compliance, but, more importantly, it fosters a safer, more resilient European marketplace for all.

Contact one of our cyber risk management experts or schedule a free demo today to learn more about how Kovrr's on-demand CRQ solution is invaluable to navigating the EU's NIS 2 Directive.

APPENDIX:

Kovrr's Cyber Risk Quantification for NIS 2 Compliance

NIS 2 Directive	Kovrr's CRQ Platform
Article 20.1 Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures.	**Security Control Analysis** Leverage key financial metrics, including those insights found within the Security Control upgrade feature, to ensure upper management tangibly understands strategies.
Article 21.2a Member States…shall ensure that essential and important entities take… measures [that include] policies on risk analysis and information system security.	**Full-View Models and Updated Datasets** Adopt Kovrr's unique CRQ methodology, which incorporates continuously updated datasets and threat intelligence, to ensure accurate, precise assessments.
Article 21.2d Member States…shall ensure that essential and important entities take…measures [that include] supply chain security…and relationships between each entity and its direct suppliers or service providers.	**Third-Party Exposure** Engage with Kovrr's Third-Party Risk analysis to explore the financial exposure various third-party service providers add to overall exposure levels. View exposure in aggregate or according to vendor or technology.
Article 21.2f Member States…shall ensure that essential and important entities take…measures [that include] policies and procedures to assess the effectiveness of cybersecurity risk-management measures.	**Risk Progression and Cyber Maturity** Utilize the Risk Progression feature, equipped with the Risk Position Analysis and Risk Position Score. Quantify cybersecurity framework maturity levels on-demand to gain actionable insights vis-a-vis control upgrades.

Article 23.1 and 23.3 Member States shall ensure that essential and important entities notify…authorities…of any incident that has had a significant impact on the provision of their services.	**Cyber Materiality Analysis** Employ Kovrr's Cyber Materiality Analysis to explore the likelihood of loss scenarios. Use these benchmarks to create threshold-based "significant" impact decisions.
Article 23.4a and 4b Member States shall ensure that essential and important entities notify…authorities…(a) 24 hours after becoming aware of the significant incident…[and] (b) within 72 hours.	**Cyber Materiality Analysis** Kovrr's Cyber Materiality Analysis helps stakeholders determine data-driven thresholds well before an event has occurred, ensuring rapid disclosures.