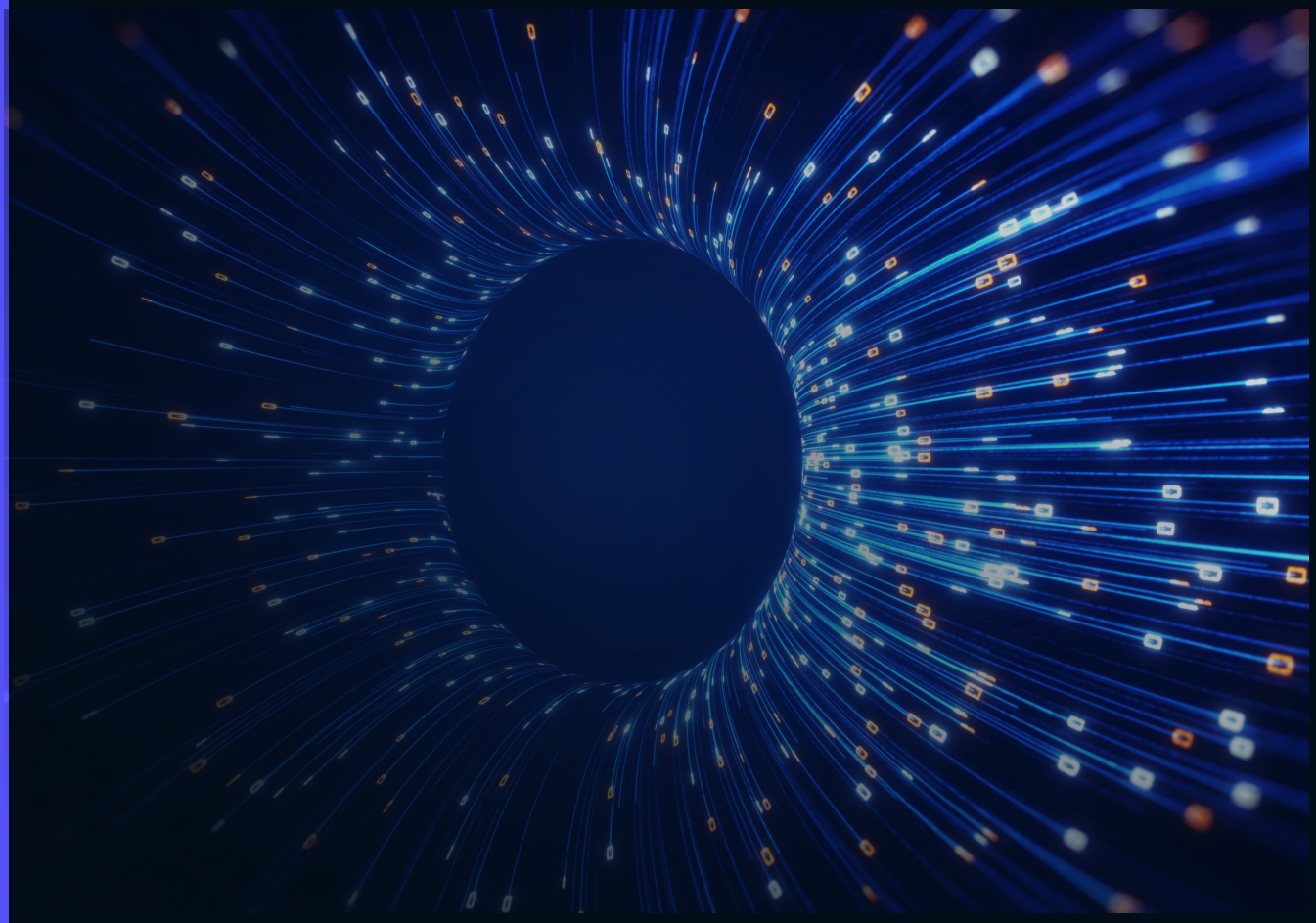
KOVRR

CASE STUDY

GG Group Establishes Risk-Based Decision-Making *with Kovrr*



www.kovrr.com

From Static Spreadsheets to a Dynamic, Centralized Cyber Risk Register

Overview of the Company

GG Group (Gebauer & Griller) is a global, family-owned manufacturer of cables, wires, and cable harnesses headquartered in Vienna, Austria. Founded in 1940, the company employs more than 4,000 people across 13 locations in EMEA, the Americas, and APAC, serving automotive and industrial markets with solutions for energy and data transmission. In its 2024/25 financial year, Gebauer & Griller reported a turnover of over €650 million.

The Problem

As a global manufacturer operating across multiple regions and business units, GG Group faced growing pressure to formalize its approach to cyber risk management. The information security team, led by Boris Orbach, Head of Global Information Security (CISO), had long recognized the need to shift from an instinct-based decision-making approach to a structured, risk-based one in which potential loss scenarios and their respective mitigation initiatives could be more easily compared and prioritized.

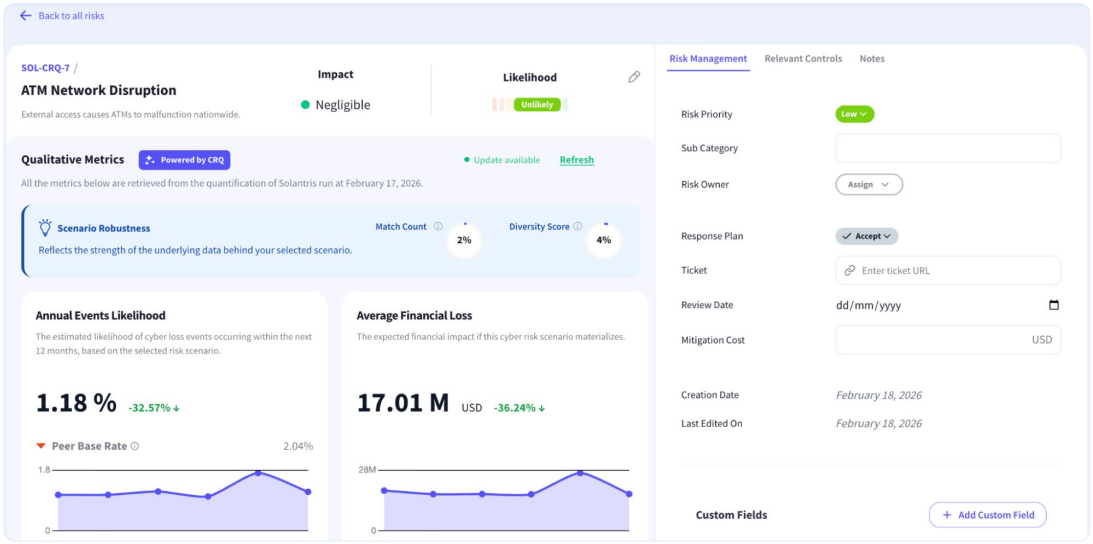
> "Our main goal was to change our decision-making to be risk-based.
> Wherever a high risk was identified, it needed to be supported by the numbers."
>
> **Boris Orbach**, Head of Global Information Security (CISO), GG Group

Without a central system capable of objectively connecting risks and measuring their financial impact, involving stakeholders outside the IT and security team, such as procurement or legal, required scheduling individual meetings, manually walking each party through the relevant risks, and often waiting weeks for any meaningful follow-through. The process was unsustainable and offered little visibility into the organization's overall risk posture.

Before turning to Kovrr, the team had evaluated several risk management tools, but found that most were either too granular to manage with a small team or amounted to little more than a digitized version of what they already had. What they needed was a solution that could provide a high-level view of their risk landscape and serve as the foundation for the risk-based decision-making culture they were working to build.

The Solution

GG Group's work with Kovrr began with a business impact analysis (BIA), through which the team identified and cataloged the organization's key systems and tools. This foundational step was critical, as the findings informed the construction of GG Group's Cyber Sphere, Kovrr's proprietary framework for modeling an organization's unique risk profile. With a quantified entity in place, cyber risk quantification (CRQ)-based scenarios could then be run across the full risk register, grounding each risk in modeled financial exposure data.



Kovrr's CRQ-powered cyber risk register translates each identified risk scenario into quantified financial exposure data, enabling security teams to assign priority levels and response plans.*

With the groundwork in place, the Kovrr team worked with GG Group to migrate their existing risk data into the platform, analyzing the team's legacy spreadsheet, mapping each risk, and generating CRQ scenarios for each entry. Initially, risks were processed in batches of 10 to 20 per session, allowing the teams to review and refine the results as they went. Once the approach was validated, a script was written to process the remaining risks at once, ultimately importing a total of 127 risks into the cyber risk register.

> "The transition of our risks into the platform was really smooth and really swift, almost effortless. I really enjoyed working with the Kovrr team throughout."
>
> **Matej Havlas**, AI & GRC Specialist, GG Group

The GG Group team also leveraged the platform to build out a priority and response plan, with the existing risk data informing which risks warranted acceptance, mitigation, or escalation. By pulling in controls from a year prior alongside current data, the platform produced a concrete visualization of how their risk management program had evolved over time, equipping them to tell a more complete story of how their security posture had measurably improved.

* Disclaimer: The figure shown is illustrative and does not reflect GG Group's actual data.

The Outcome

By migrating its existing risk data into Kovrr's platform, GG Group gained a more comprehensive, actionable view of its cyber risk landscape than its spreadsheet-based approach had previously allowed. With 127 risks quantified and organized within a single register, the team finally had a centralized system where ownership could be assigned, mitigation progress tracked, and financial exposure measured across the organization, capabilities that had not existed in any comprehensive, unified form.

> "A massive benefit of the risk register is everything around how we can manage risks. Assigning them, connecting them to controls, and defining deadlines. We didn't have that here before."
>
> **Boris Orbach**, Head of Global Information Security (CISO), GG Group

The priority and response plan gave the team a data-driven framework for determining where to focus their efforts, replacing ad-hoc judgment calls with a more deliberate, repeatable process. Reconstructing the historical trajectory of their risk posture allowed GG Group to demonstrate, with data, that they had already been actively reducing risk over time, rather than merely cataloging it. This narrative became a key component of a board-ready presentation that gave leadership a quantified picture of the organization's cyber exposure for the first time.

For GG Group, the risk register marks a meaningful shift in how the organization approaches cyber risk. With a centralized, quantified view of their risk landscape now in place, the team finally has the foundation to make security decisions that are structured, data-driven, and built to scale with the organization.