Subsidiaries Steering: Built for Group CISOs Managing Risk at Scale

A Unified View of Cyber Risk for When You're Managing 5, 50, or 500+ Entities.

Why Most Strategies Break Down in Multi-Entity Environments

Managing cyber risk across a multinational enterprise isn't just about "more risk." It's about **more complexity**.

And yet, most risk programs still try to apply a one-size-fits-all strategy. The result? A disconnect between risk, investment, and accountability.

Group-level reports become too high-level to drive action. Subsidiaries operate in silos. And CISOs are forced to choose between oversimplified dashboards or overwhelming detail.

When your organisation spans dozens or even hundreds of subsidiaries or business units, traditional risk management models fall short.

You are dealing with:

- **Different maturity levels**
- **Varying exposures and threat landscapes**
- **Conflicting regional regulations**
- **Multiple business models under one roof**

Subsidiaries Steering: Built for Group CISOs Managing Risk at Scale

One Strategy. Multiple Entities. Full Control.

Subsidiaries Steering is built for the real-world complexity of multinational organizations. It enables CISOs and group-level cyber leaders to steer risk strategically across subsidiaries, without oversimplifying or drowning in data.

With Subsidiaries Steering, you can:

- ✓ **Different maturity levels**
- ✓ **Varying exposures and threat landscapes**
- ✓ **Conflicting regional regulations**
- ✓ **Multiple business models under one roof**

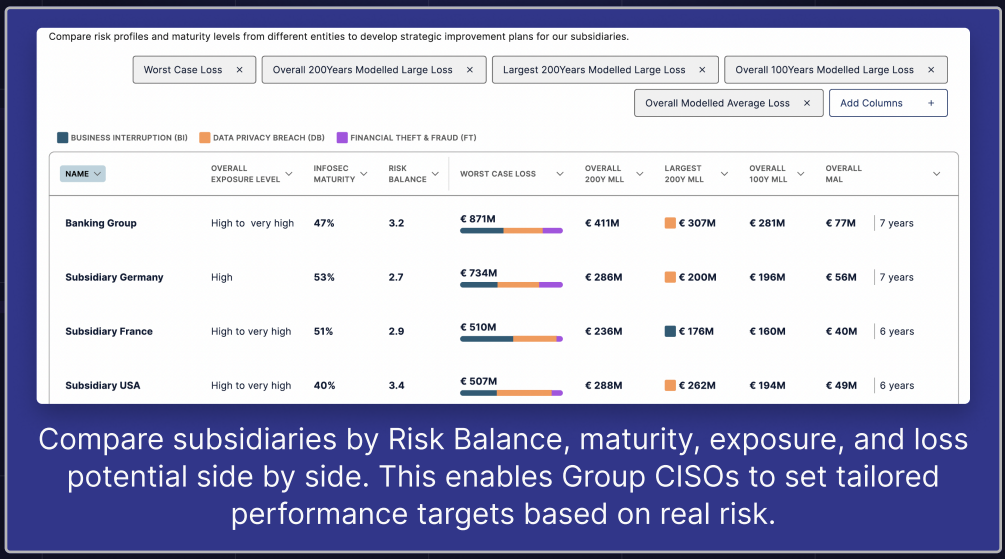
When to Use Subsidiaries Steering

- ▶ **You're managing more than 3 subsidiaries**
- ▶ **Your entities operate in different sectors or countries**
- ▶ **You need a unified view of risk, without losing local context**
- ▶ **You want to link cyber investment to performance at the entity level**
- ▶ **You have multiple business models within the group (e.g. financing, manufacturing and digital services)**

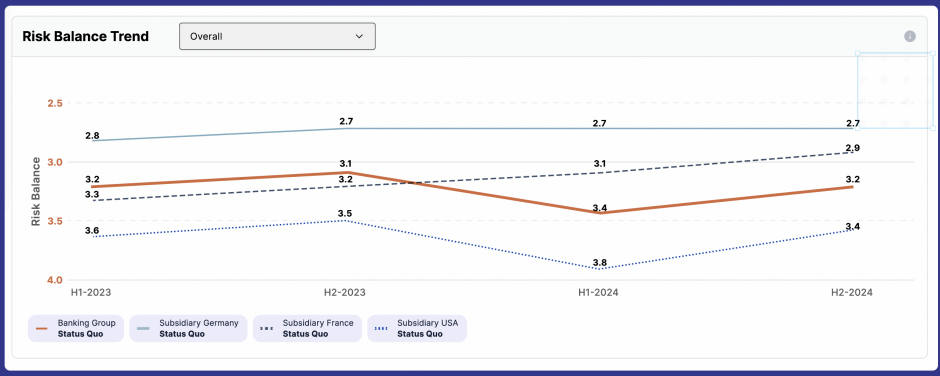
Subsidiaries Steering: Built for Group CISOs Managing Risk at Scale

What Subsidiaries Steering Looks Like in Practice

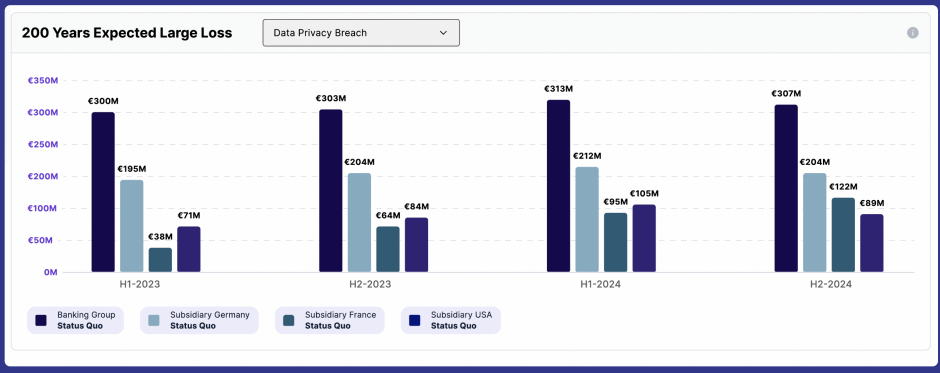
Screenshots below show how Group CISOs can compare, simulate, and steer cyber risk across subsidiaries, using real metrics like Risk Balance, Worst Case Loss, and improvement targets over time.



Compare subsidiaries by Risk Balance, maturity, exposure, and loss potential side by side. This enables Group CISOs to set tailored performance targets based on real risk.



Track how risk evolves per subsidiary and whether current security investments align with actual exposure. This supports regulatory argumentation and helps monitor strategic progress over time.



Identify which entities face the highest exposure in key loss categories. Business Interruption, Data Privacy Breach, Financial Fraud and Theft, and Ransomware. Simulate past programs to quantify risk reduction in Euors or Dollars and demonstrate ROSI with confidence.

Benchmark subsidiaries against one another to uncover gaps in maturity and risk posture. Assign risk-based 1-year and 2-year improvement targets aligned with group-level strategy.

Evaluate how each subsidiary must contribute to group-level improvement goals. Subsidiaries with greater exposure or lower maturity are given more ambitious targets, ensuring resource allocation is justified and timelines are achievable.

www.squalify.io