

Board-Level Cyber Reporting

The One Report Your Board of Management
Will Actually Use

Executive Summary

Boards don't want heat maps, color charts, or cybersecurity buzzwords. They want numbers they can understand. They want to see how cyber incidents would affect the company in financial terms. And they want clear options for what to do next. Most security reports don't offer this. They stay technical, vague, or disconnected from the decisions leaders need to make.

The Board of Management (BOM) Report from Squalify fills this gap. It turns the results from the Squalify platform into a simple financial view the Board of Management will actually use. It shows the worst case loss, the expected large loss, how these figures compare to key company metrics, and whether the current risk fits the defined limits. It also explains what changed since the last period and why.

A central part of the report is the simulation view. It lays out different improvement paths, the budget for each path, the expected reduction in risk, and the return on security investment. This gives leadership the information they need to choose the most suitable investment and a clear reason to justify that choice.

Put simply, the Board of Management Report gives leaders a factual, financial view of cyber risk they can act on. The value isn't only in the numbers. It's the storyline that turns strategy into action.

Why Traditional Cyber Reporting Fails in the Boardroom

The Communication Gap

Most cyber reports never reach the Board because they cannot be used for decisions. They focus on technical detail, long lists of controls, and color-coded ratings that do not show financial impact.

Boards cannot see what a major incident would cost.

They cannot see whether the company sits inside or outside its defined risk limits.

They cannot link any of this to the company's financial KPIs.

This creates a gap between how security teams communicate and how Boards make decisions.



What Boards Actually Want

Boards want direct answers to simple questions:

- How much could a major cyber event cost?
- Are we inside our risk appetite?
- What changed since the last period?
- What is driving the change?
- Which improvements reduce risk the most?
- How do we compare to peers in our industry?
- What options do we have to reach our targets?

These are basic management questions.

Most security reports cannot answer them.

Why Numbers Matter

Boards think in financial terms.

They evaluate risk, budgets, and strategy through measurable figures.

Cyber risk is no different.

It can be measured.

It can be compared across entities, regions, and years.

It can be reduced through targeted changes.

It has become a financial discipline.

Boards need cyber reporting that reflects this.

The Only Report Format That Matches How Boards Make Decisions

What It Is

The Board of Management Report is a **fully customizable dashboard** that presents cyber risk in financial terms and the individual areas the company is mostly exposed.

Every view can be adjusted to fit your company's structure, reporting style, and Board requirements.

It takes the results from the Squalify platform and organizes them in a way the Board of Management can use.

It shows the main loss figures, explains what drives them, and offers clear options for improvement.

What It Delivers

The report includes a set of views Boards need for decisions.

Each view can be reordered, expanded, or replaced based on your needs:

- Worst Case Loss
- Expected Large Loss
- Annual Expected Loss
- Loss drivers explained in plain language
- Year-over-year changes and their causes
- Peer benchmarking
- Subsidiary and entity comparisons
- Control maturity gaps
- Suggested improvement priorities
- Simulation outcomes and budget options

You decide what to show, how much detail to include, and what narrative fits the discussion. No fixed templates. No rigid layout. Everything adapts to your Board's expectations.

Why It Works

The Board of Management Report works because it aligns with how Boards make decisions:

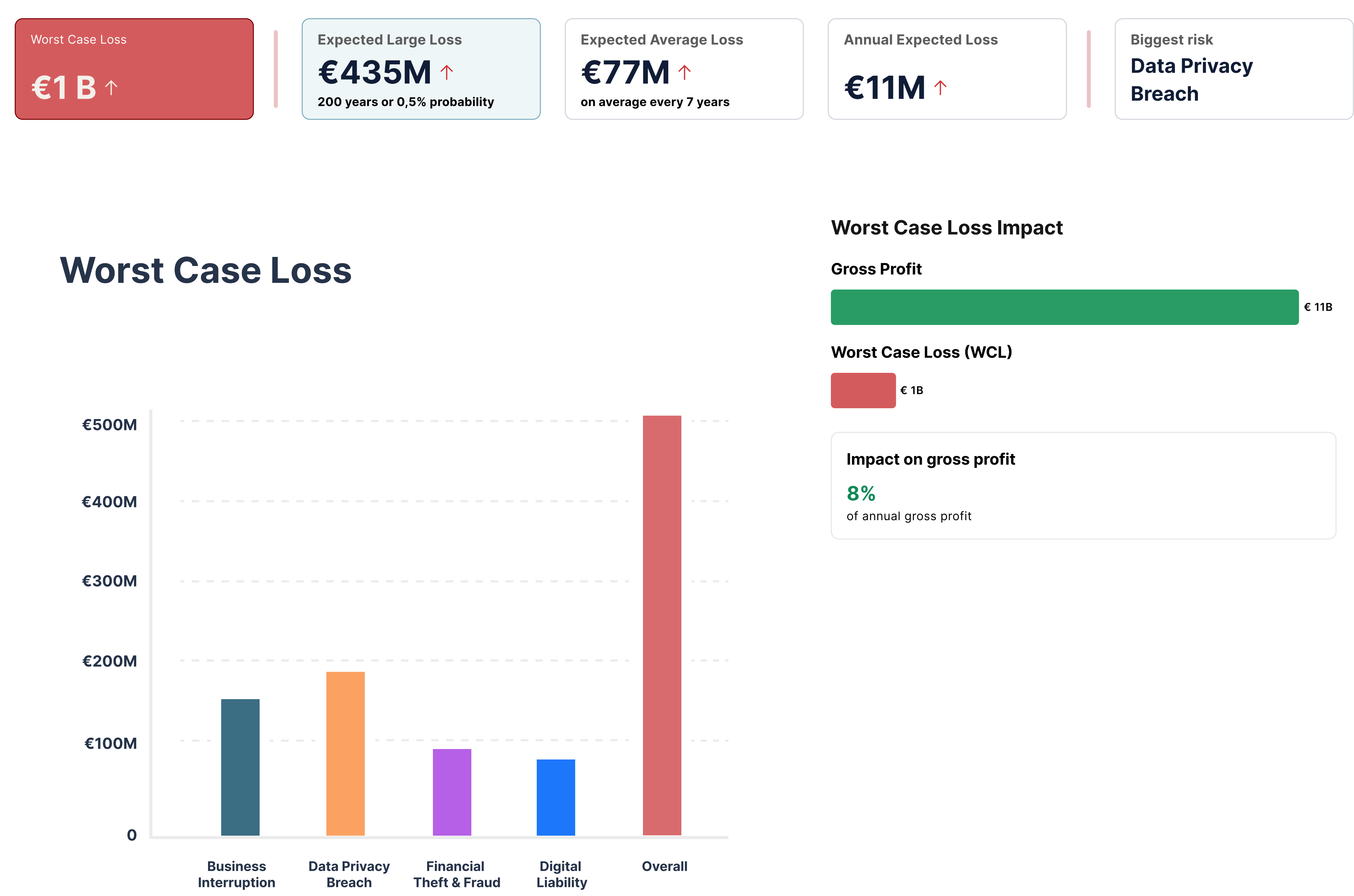
- It uses financial metrics leaders already manage
- It gives a consistent logic across the whole organization
- It replaces subjective scoring with measurable figures
- It shows what changed, why it changed, and what it means
- It supports the exact storyline leadership needs for decisions
- It adapts to each company's structure, maturity, and reporting culture

It turns cyber reporting into a focused, board-ready narrative that fits your organization instead of forcing you into a fixed format.

Core Elements of the Board of Management Report

Worst Case Loss

The Worst Case Loss shows the **financial upper boundary of a severe cyber incident**. It translates cyber exposure into figures the Board can compare with core company metrics. This view links the potential loss to items such as gross profit, cash flow, or dividend payout. It shows whether a single event could strain the company’s financial position.



Expected Large Loss

The Expected Large Loss **links cyber exposure to the company’s risk appetite limits** for recurrence periods of 100 years (1%), 200 years (0.5%), 500 years (0.2%) and 1000 years (0.1%). It shows whether the organization sits inside or outside its defined thresholds. This view creates clarity for escalation, reporting, and accountability.

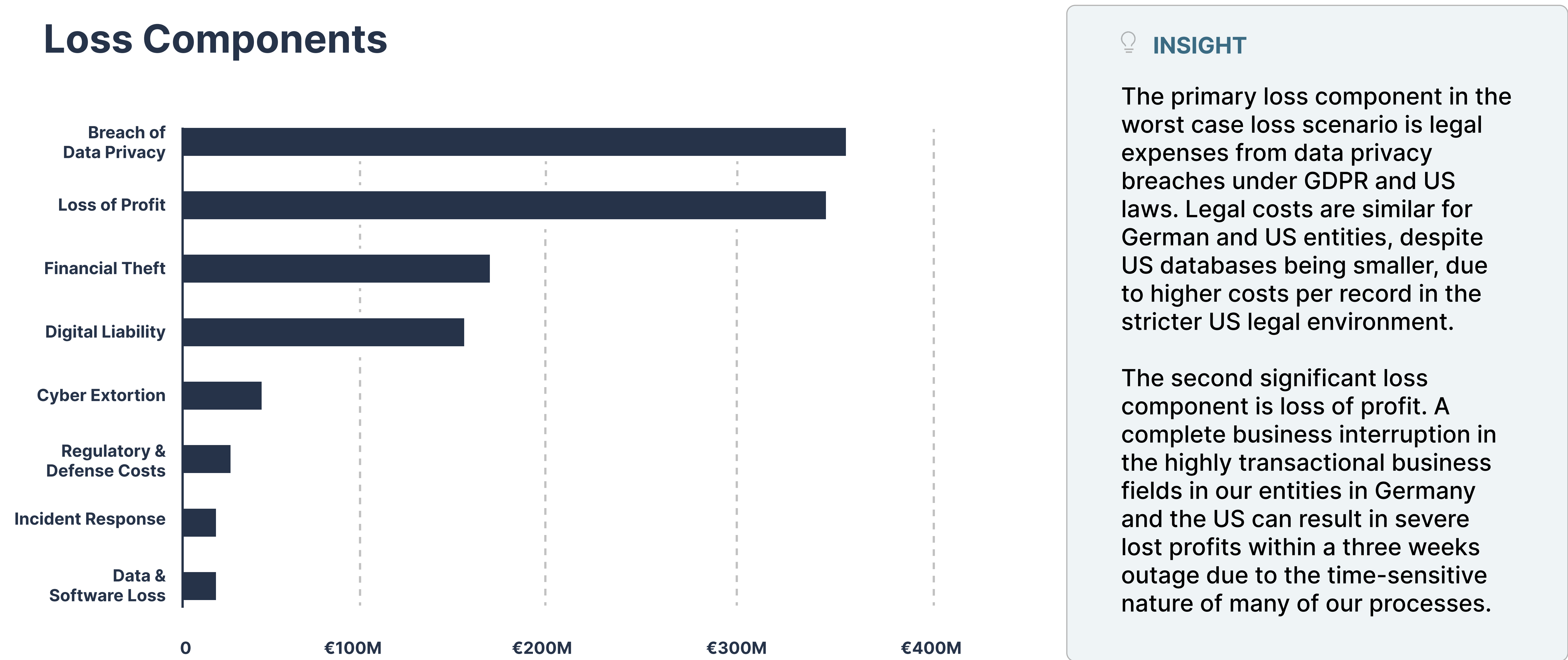
Annual Expected Loss

The Annual Expected Loss is the **baseline indicator for budget planning**. It shows the average expected cost of cyber incidents within a year and supports discussions about funding levels and priorities.

Loss Components

This view breaks down the **main cost drivers behind a loss figure**:

- Breach of Data Privacy
- Loss of Profit
- Financial Theft
- Digital Liability
- Cyber Extortion
- Regulatory & Defense Costs
- Incident Response
- Data & Software Loss



It explains where costs come from and how each driver contributes to the total. This narrative helps leaders understand the story behind the number instead of only seeing a headline value.

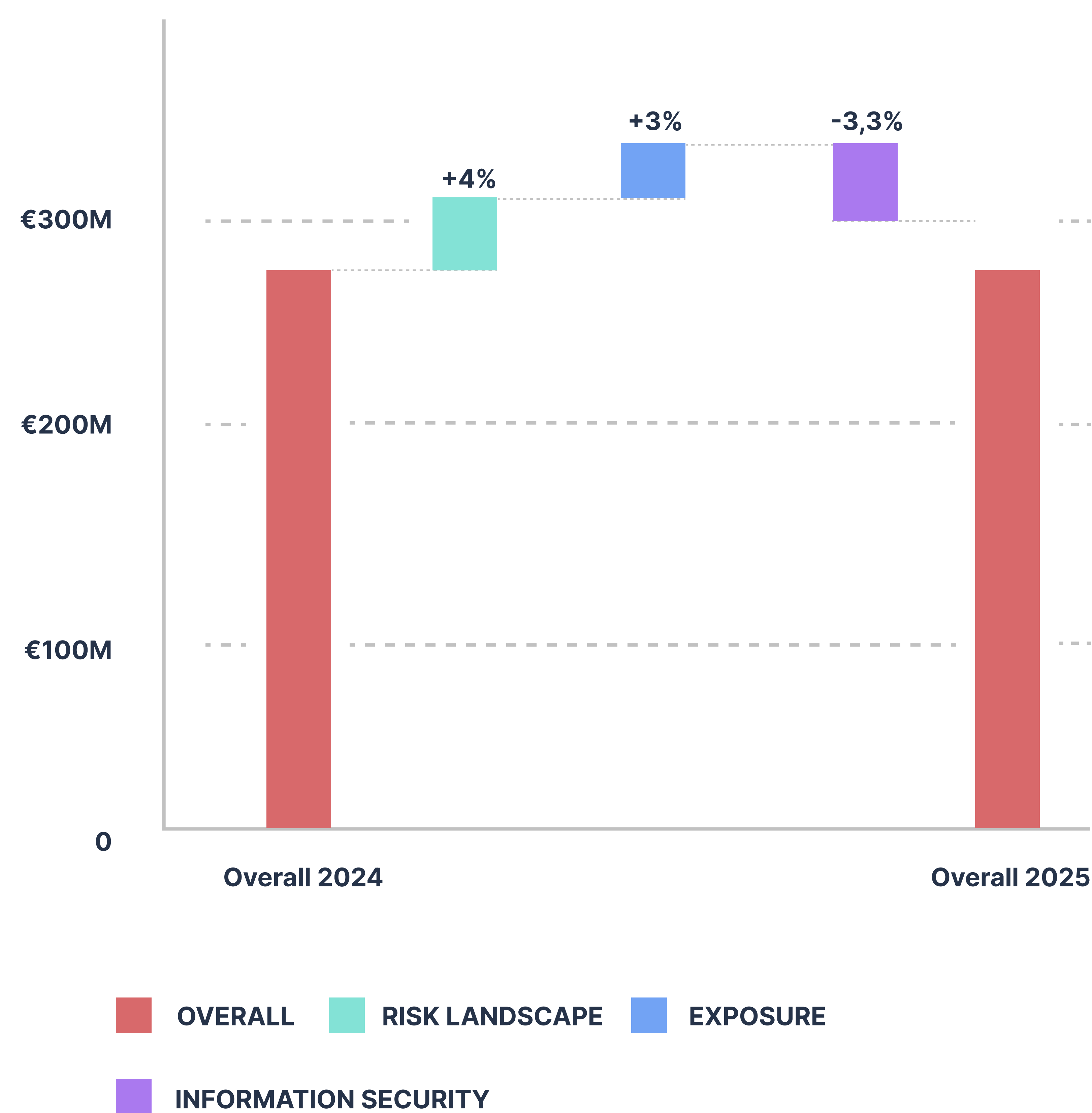
Year-over-Year Development

The delta analysis shows **how risk changed since the last reporting period**. It separates the drivers into three categories:

- Changes in the external risk landscape
- Changes in the company’s exposure
- Changes in information security maturity

This helps leadership see what is driving the movement and where action is needed.

Delta Analysis Year-over-Year

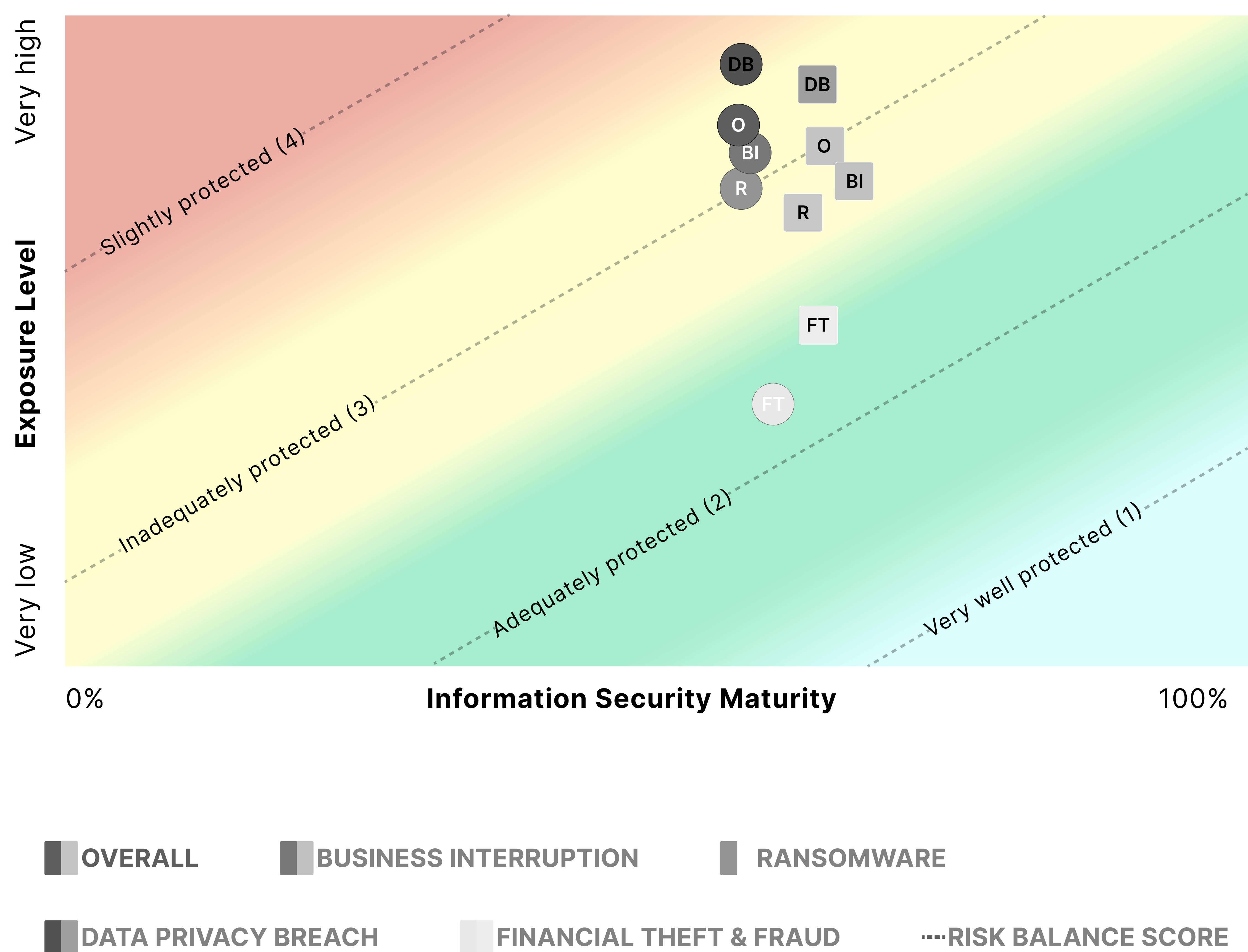


Benchmarking

Benchmarking compares the company cyber risk profile (inherent exposure based on what the company is doing vs InfoSec maturity) to either:

a. Overall Industry average

Risk Balance Banking Group vs Industry Average

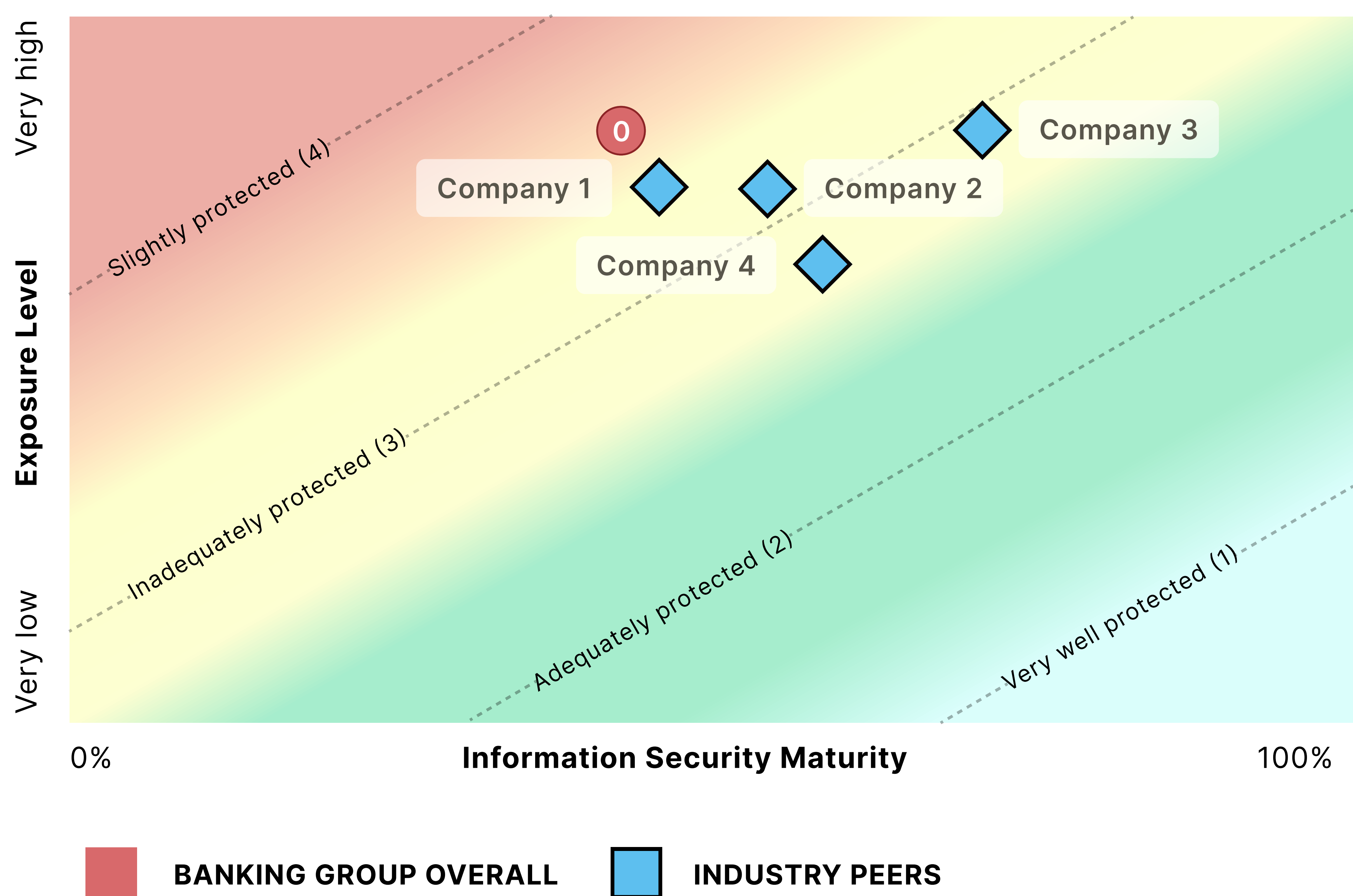


b. Similar organizations for

- Industry peers
- Comparable revenue groups
- Comparable employee groups

It shows whether the company is ahead, behind, or in line with others facing similar risks.

Risk Balance Banking Group vs Industry Peers



INSIGHT

Most of the industry peers show a similar range of exposures with on average "high" exposure scores.

But in respect of the information security maturity, Banking Group is behind its peers.

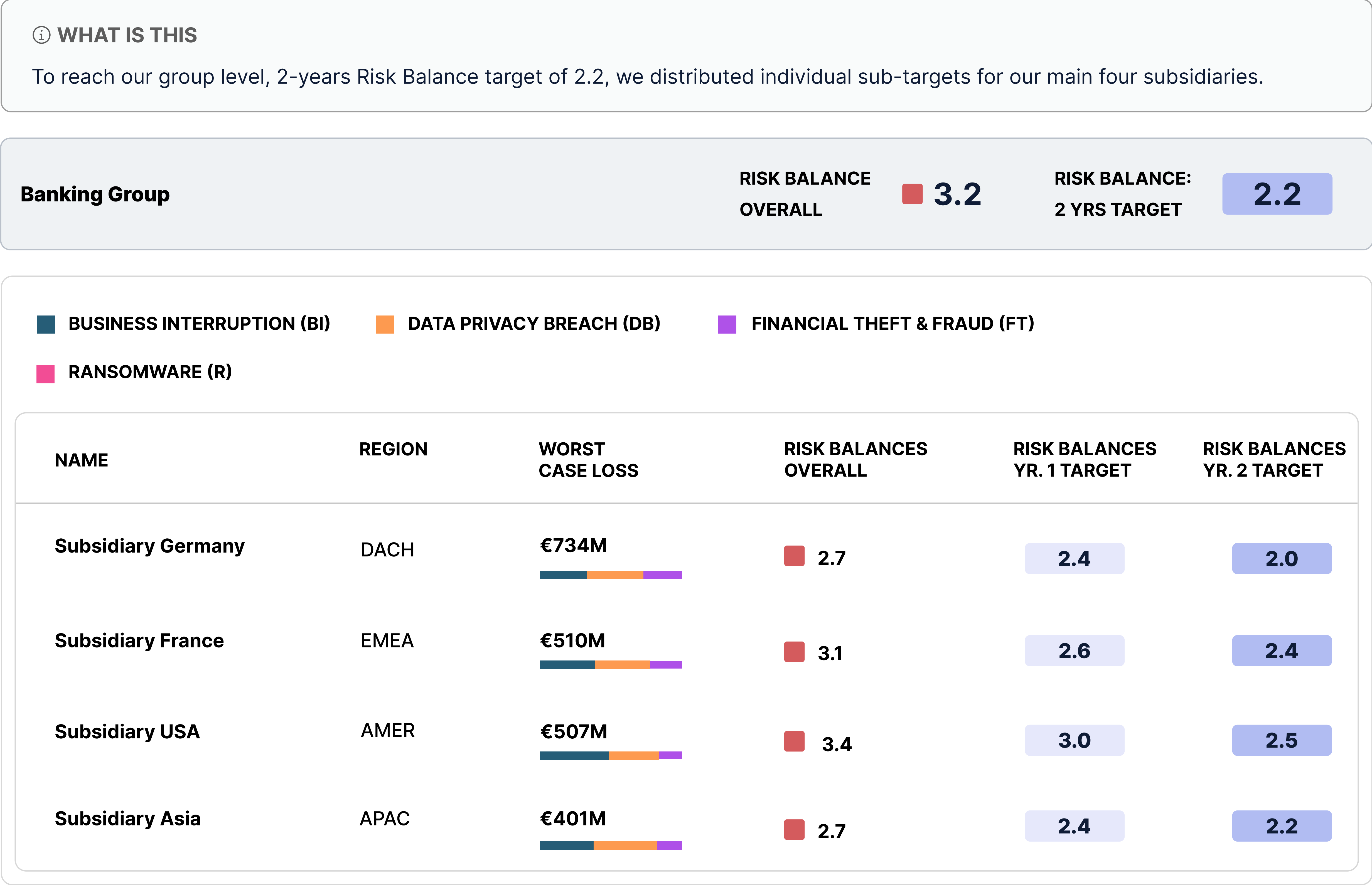
Within this peer group only Company 4 has a nearly adequate Risk Balance close to a score of 2. Also most of our other peers need to invest in higher information security as well to achieve a balanced risk score of around 2.

Subsidiary / Entity View

This view shows **how cyber risk is distributed across the full enterprise**. It highlights which entities carry the highest exposure or the lowest maturity, and whether current investments match their actual risk.

It helps determine how each subsidiary should contribute to the group’s improvement goals. Entities with higher exposure or lower maturity receive more ambitious targets, ensuring resources are directed where they are needed most and timelines remain realistic.

It gives Group CISOs a clear way to identify outliers, set priorities, and steer global programs with improvement targets that match the group-level strategy.



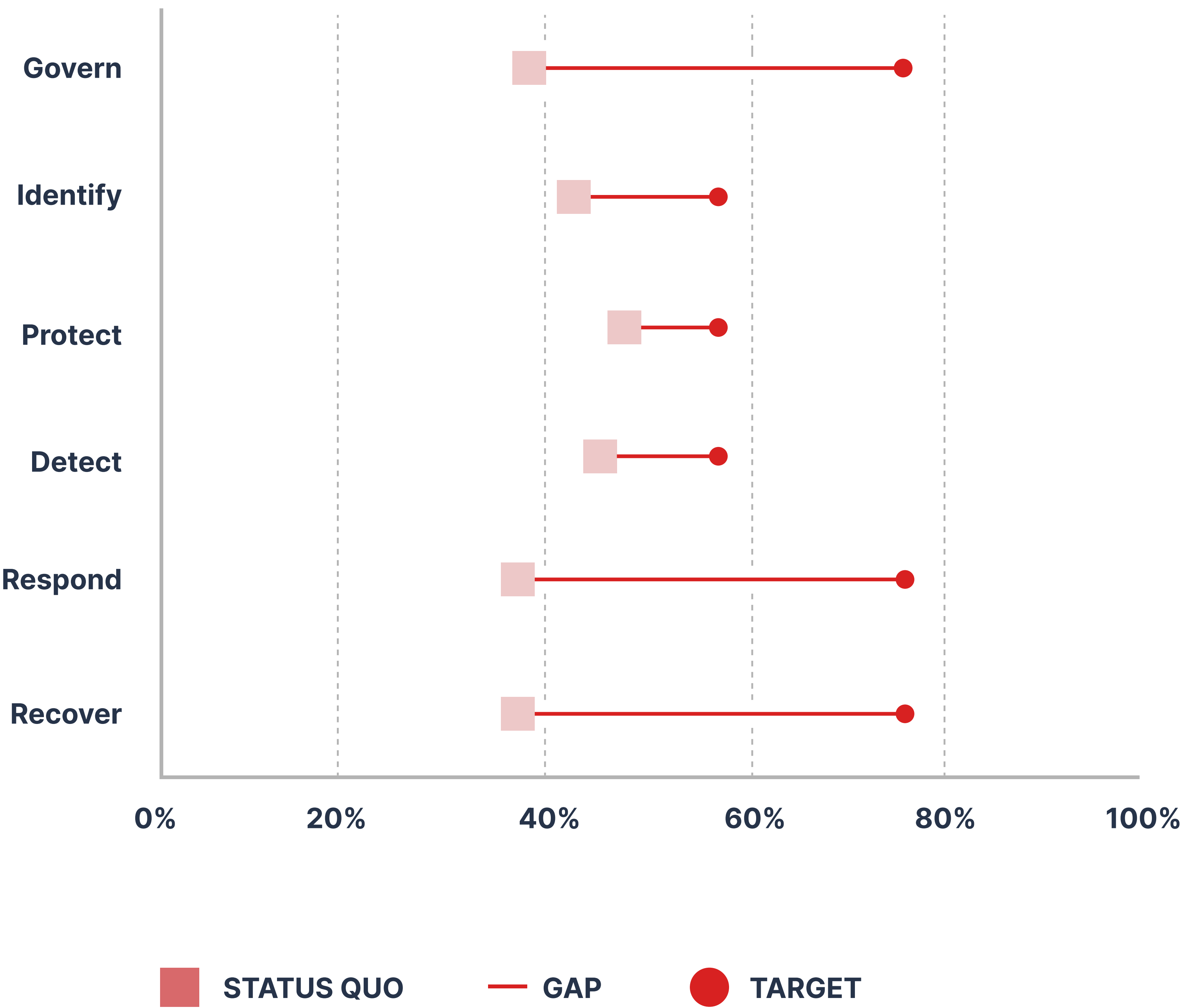
Control Maturity

This view shows **which information security control areas need improvement at a company level**, rather than individual system performance.

It highlights gaps against target levels and supports planning for the next improvement cycle.

It connects the cybersecurity strategy to measurable and trackable progress. Squalify uses the NIST CSF by default but can also map to your custom cybersecurity framework (like ISO 27001 or NIST2).

Average Information Security Maturity by Control Chapter

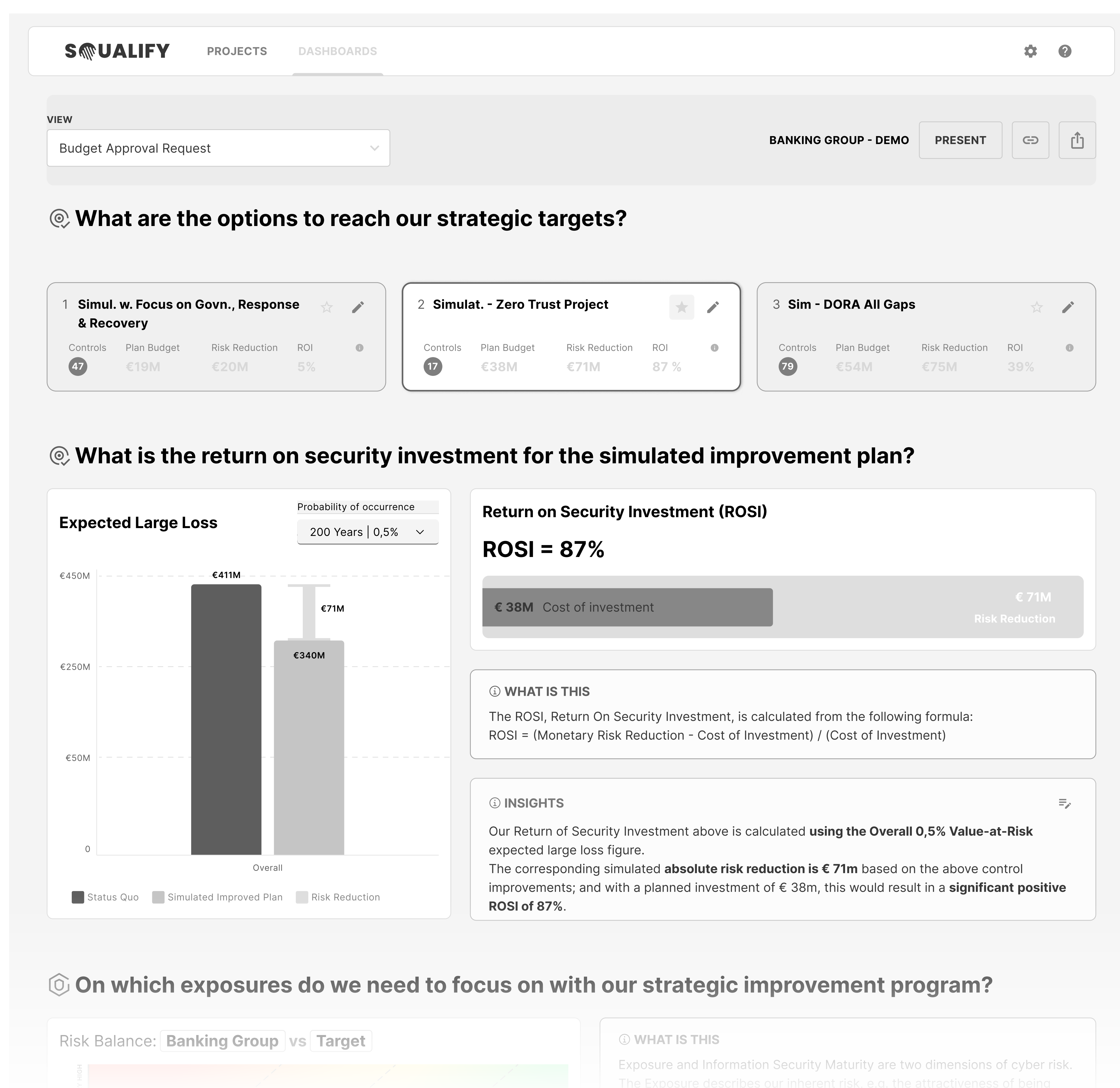


What the Board Can Actually Decide On

Why Boards Need This View

Boards don't want long explanations. They want clear options, with numbers that show what each option costs and what it delivers.

The **Budget Approval Report** provides this in a simple, comparable format.



Prioritizing Exposures

This view shows where the biggest gaps are and which areas deserve attention. It helps the Board see:

- Which risk scenarios sit furthest from target
- Where improvements would have the strongest effect
- How these choices support the company's wider plans

Simulations: The Decision Engine

Simulations **show different improvement paths side by side.**

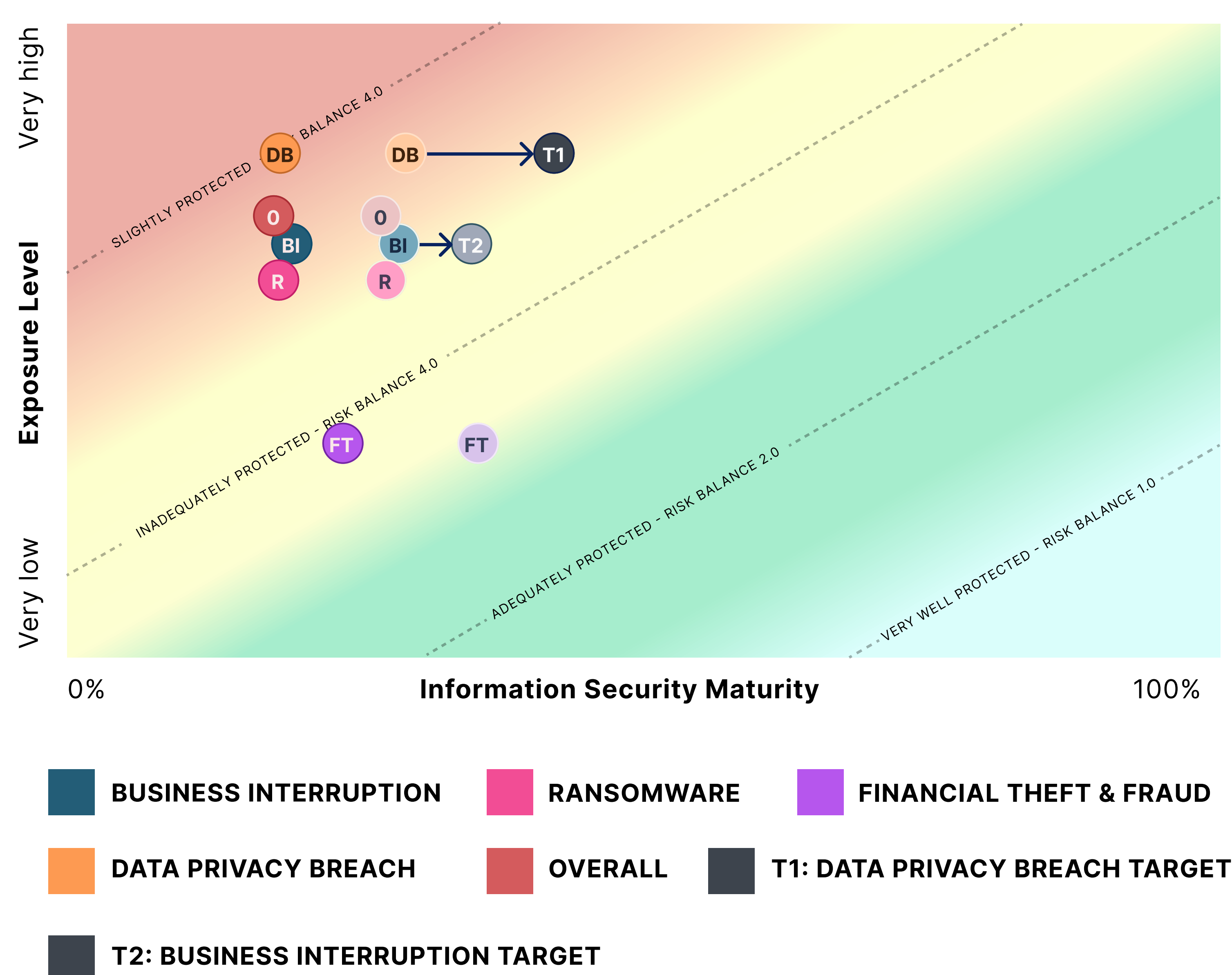
They model the effect of control changes before any budget is committed.

They quantify how much each option reduces financial risk and how it balances cost, exposure, and business goals.

This helps identify the measures that deliver the strongest impact.

It gives leadership a simple way to compare strategic options and understand the trade-offs.

Risk Balance Banking Group vs Simulation



INSIGHT

The focused improvements in the Protect and Detect controls have improved the Risk Balance score for Data Privacy Breach, Business Interruption and Ransomware scenario most, moving it a significant step closer to the target score of 2.2. The overall control improvements would also benefit the Risk Balance for the remaining scenarios.

How CISOs Use This

CISOs use the Budget Approval Report to support decisions with clear facts. It helps them:

- Build a defensible security strategy
- Justify budget requests with transparent numbers
- Align business, finance, and IT on the same plan

How Boards Should Use the BOM Report

Quarterly Oversight

The BOM Report gives the Board a consistent quarterly view of the company's cyber exposure. It shows what changed and whether current risks remain within defined limits.

Evaluating Risk Appetite

Boards can use the Expected Large Loss view to see if the company sits inside or outside its risk appetite. If thresholds are exceeded, the report makes the reason clear and shows what actions are available.

Guiding Investment Decisions

The simulation view helps Boards compare different improvement paths. It links each option to its cost, its expected reduction in risk, and its return on security investment. This gives Boards a transparent basis for choosing the most suitable investment.

Assessing Security Program Performance

Boards can track progress by comparing current figures to the previous period. The delta analysis shows whether improvements come from stronger controls, lower exposure, or changes in the external landscape.

Steering Subsidiaries and Entities

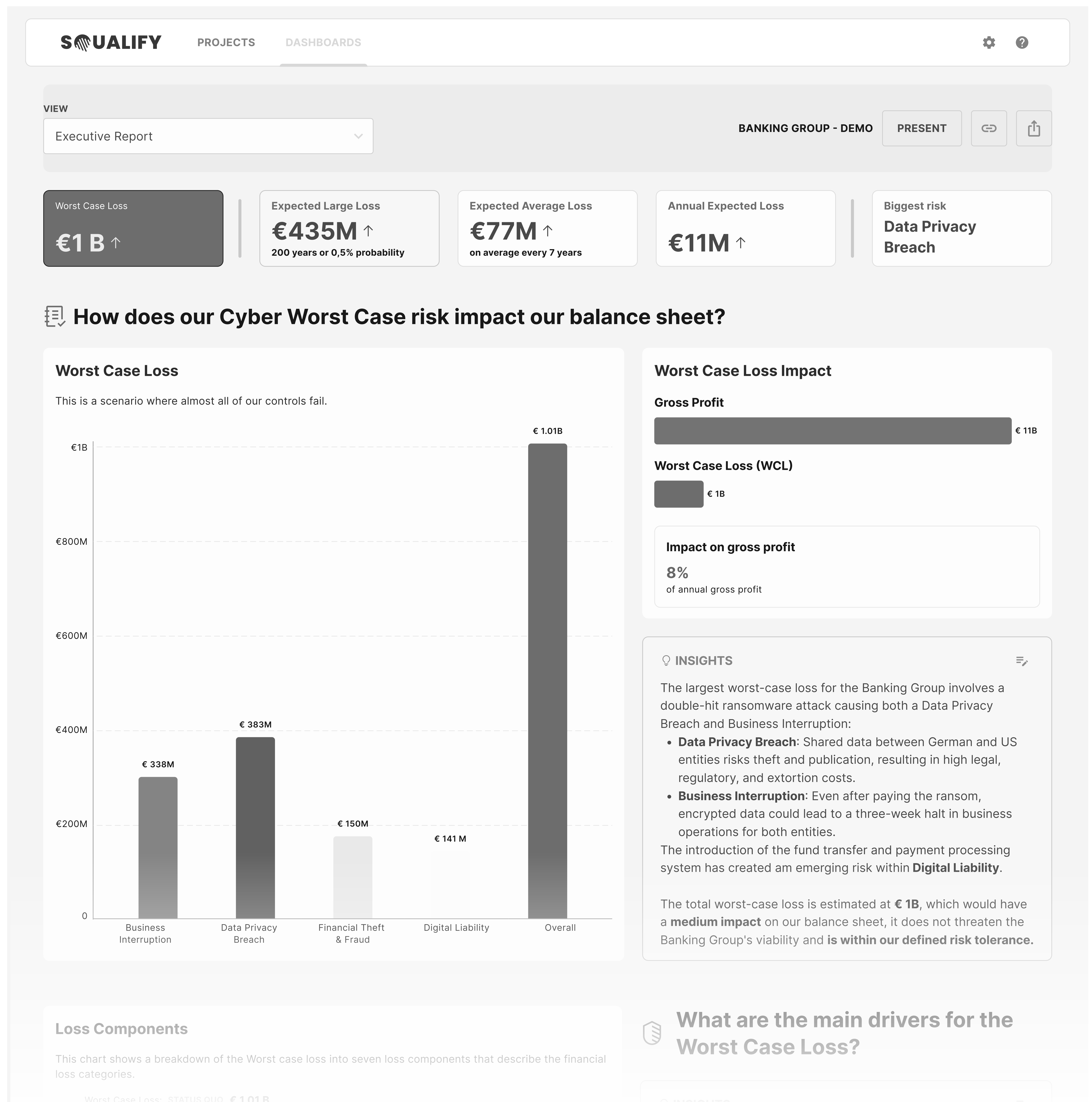
The entity view highlights which parts of the organization carry the highest exposure or lowest maturity. This helps Boards understand where oversight is most needed and where local leadership should focus.

Supporting Executive Accountability

The BOM Report makes responsibilities clear. It shows which risk movements come from business growth, which from external changes, and which from the security program. This allows Boards to hold executives accountable based on data, not assumptions.

Aligning Cyber to Business Planning

By linking cyber exposure to financial metrics, the report helps Boards integrate cyber into broader planning cycles. It supports decisions on budgeting, growth, new products, and major initiatives that change exposure.



Conclusion: A New Standard for Board-Ready Cyber Reporting

Cyber risk has become a financial discipline.

Boards need reporting that supports this: simple figures, clear explanations, and a direct link to business impact.

The Board of Management Report from Squalify gives leadership exactly that. It frames cyber exposure in financial terms, shows how current risks compare to the company's limits, and lays out practical options for reducing those risks.

This is not about replacing expertise with dashboards.

It is about giving Boards a faster and clearer way to understand the implications of cyber risk and to base their decisions on measurable facts.

The value goes beyond quantification.

It is the combination of a clear storyline and realistic simulations that helps leaders choose a direction and justify it.

This is the standard modern cyber governance requires.

Book A Meeting

If you want your Board to stop guessing and start deciding, talk to us. We'll show you how your data turns into a clear Board of Management Report and how it supports your next leadership discussion.

[Book Meeting](#)

Learn more at

www.squalify.io



Squalify - Cyber Risk Quantification for the Boardroom
www.squalify.io