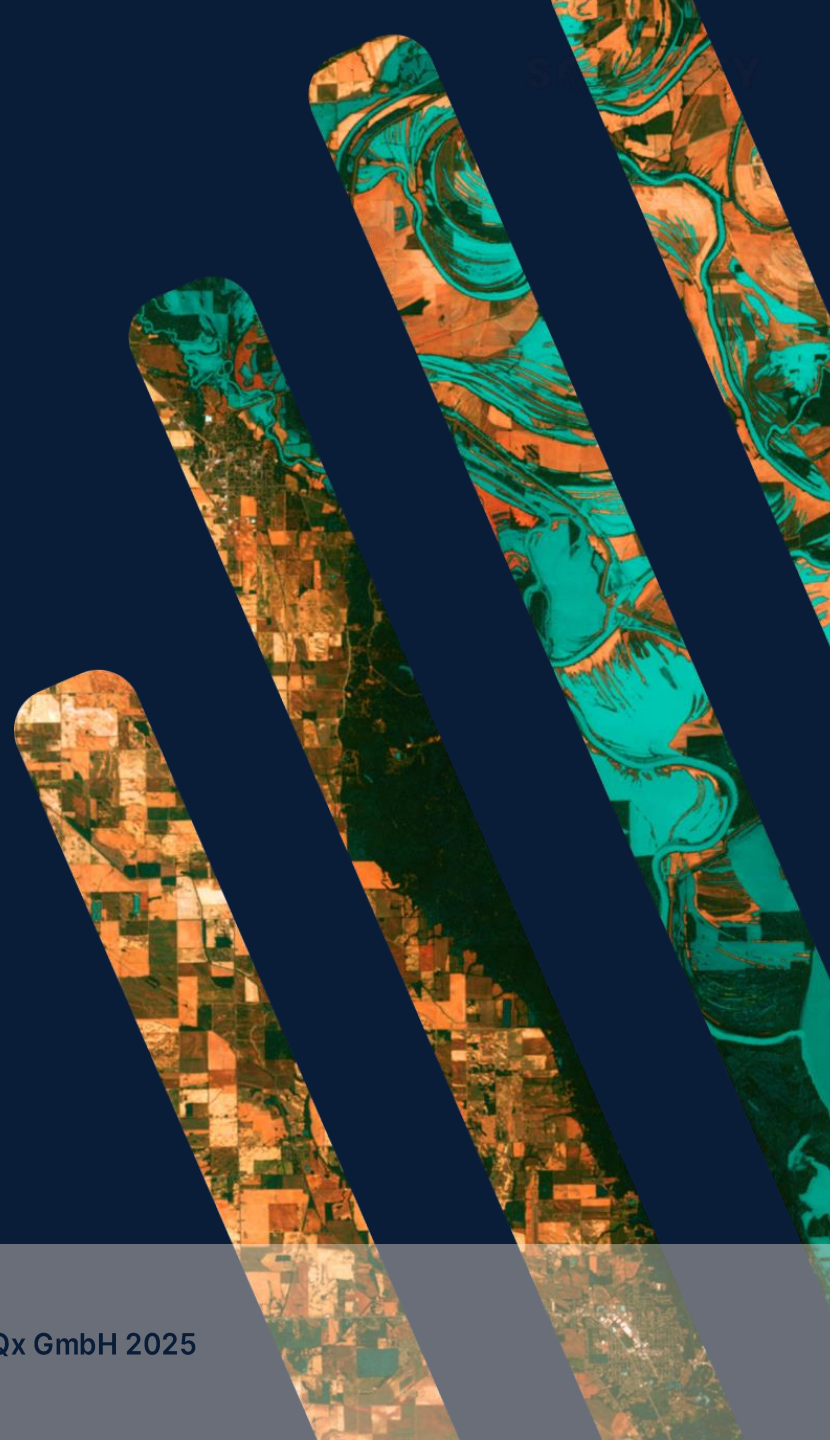
SQUALIFY

A **MUNICH RE** VENTURE

CYBER RISK QUANTIFICATION FOR THE BOARDROOM



Trusted by industry leaders like:

JUNGHEINRICH Deloitte. MTU Aero Engines

WHY CYBER RISK QUANTIFICATION?

88%

of executives agree that ”measuring cyber risk is crucial for prioritising cyber risk investments”

but only

15%

are measuring the financial impact of cyber risks to a significant extent

Source: PwC Global Digital Trust Insights, 2025

THE EXECUTIVE BOARD IS ASKING…

SQUALIFY

- ✓ Gives the board the right answers
- ✓ Makes you ready for the boardroom
- ✓ Helps you with the conversation
- ✓ Helps you speak the same business language

TOP-DOWN VS BOTTOM-UP

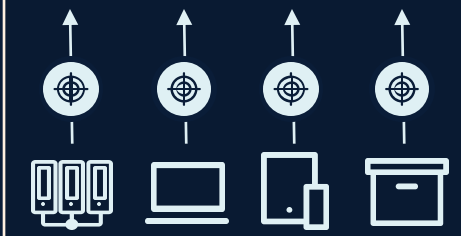
Currently two prevailing cyber risk management approaches in the market

Top-Down

Strategic decision making

- Financial impact to the company
- Business consequence driven risk scenarios
- Broad scope company-wide assessment
- Includes unknown risks
- Purely quantitative, extended with qualitative insights

SQUALIFY FOCUS



Bottom-Up

Operational decision making

- Financial impact based on company assets
- Technical cyber threat driven risk scenarios
- Narrow scope system-level assessment, difficult to aggregate at the company-wide level
- Aggregation via known threat vectors
- Mostly qualitative

SQUALIFY VALUE PROPOSITION

Enabling multiple use cases

Financial Cyber Losses

Budget Approval & Risk Reduction Simulations

Subsidiaries Steering

Supply Chain Cyber Risk

Level of Cyber Insurance

Cyber Risk Monitoring

Cyber Regulatory Compliance

Industry Benchmarking

WHY SQUALIFY?

Distinctive methodology and extensive data ensure highly accurate results, simply

Our secret sauce!

100,000+
companies included in cyber loss database

4,500+
companies quantified

1M+
small loss claims

130
industries

10K+
large loss claims

80+
countries

- Leveraging **Munich Re's** vast historic cyber insurance data and model
- **Defendable results**, in plain language, focused on business costs, with less guesswork
- Quick assessments in 24 hours and full CRQs within days

HOW DOES IT WORK?

We allow you to focus on the business context, making results more explainable

YOU WILL NEED

- **Basic company data**
- **Company-relevant scenarios**
- **Information security maturity data**

YOU WILL NOT NEED

- Guesstimate threat inputs
- Integrations
- Lots of spreadsheets

SQUALIFY PLATFORM

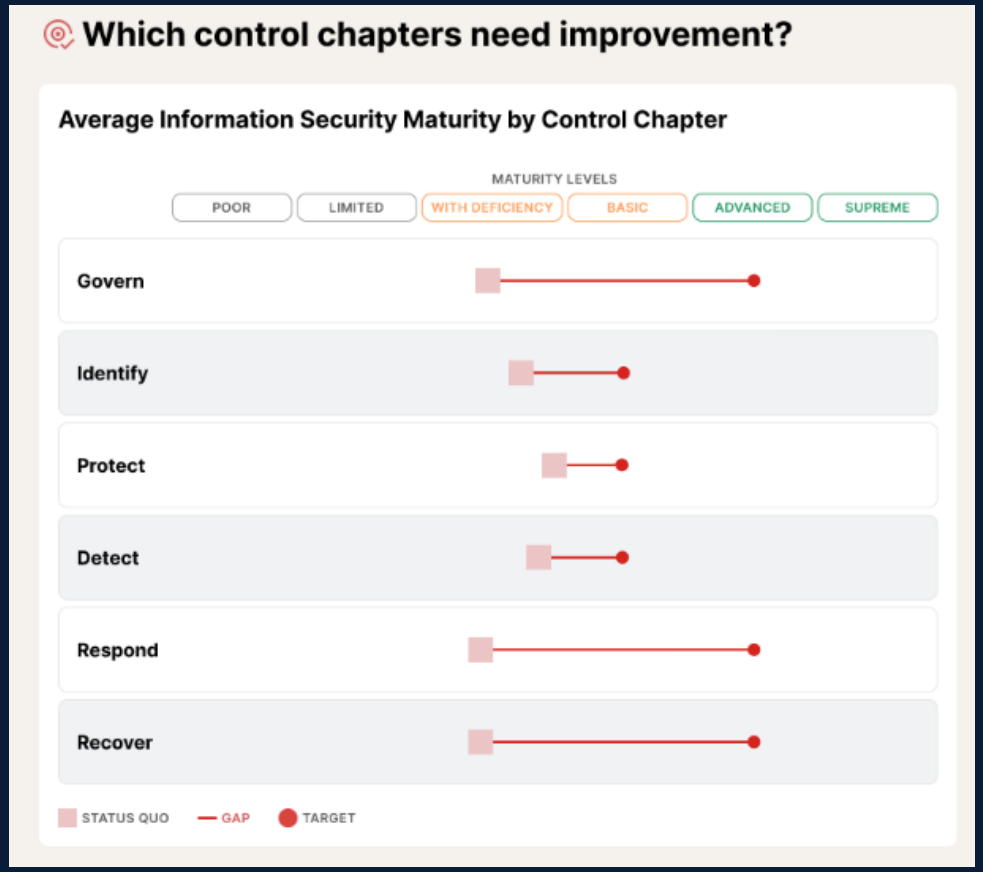
Cyber Risk Quantification Model

Historic Loss Database

Monte Carlo Simulation

WHAT YOU GET – EXAMPLE OUTPUT

Providing full transparency with clear financial figures and the right business language



WHAT YOU GET – EXAMPLE OUTPUT

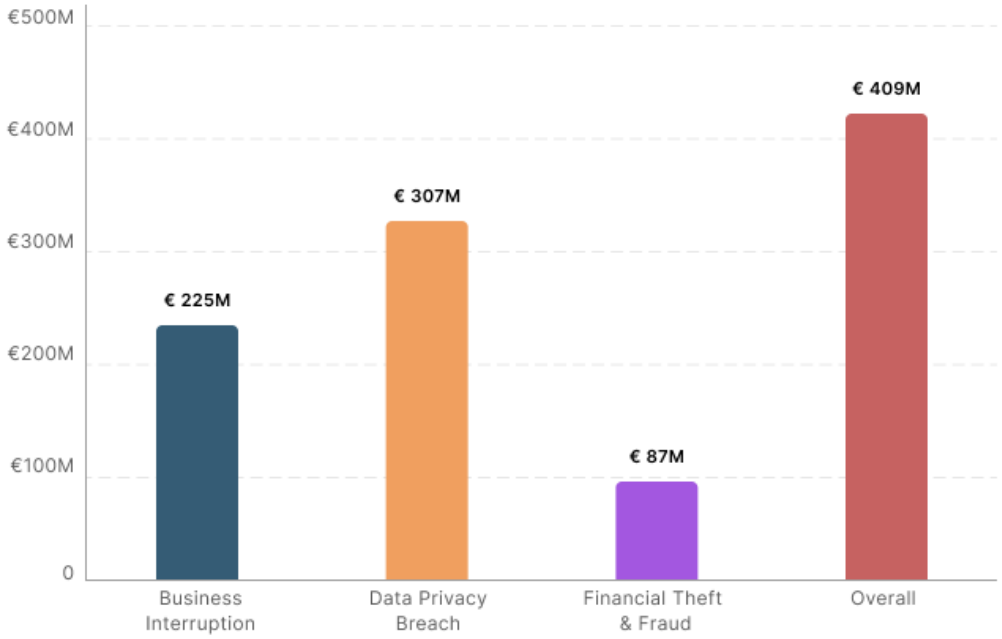
Providing full transparency with clear financial figures and the right business language

How does our current expected Cyber loss potential fit to our risk appetite?

Expected Large Losses

These losses refer to significant financial losses that may incur for specific recurrence periods due to a cyber security incident.

Probability of occurrence: 200 Years | 0,5%



Risk Reporting Thresholds

Edit

INSIGHTS

The statistical overall large loss of € 409m at a probability of 0,5% is still **below our risk limit** defined by the Board of Management. From € 500m, approval from the Board of Management is required, and above € 1bn, our Supervisory Board needs to approve this exposure.

The overall expected large loss is still within our defined risk appetite, but not that far away from the risk limit for the Board of Management approval. Currently, no escalation process is needed.

WHAT YOU GET – EXAMPLE OUTPUT

Ability to steer cyber maturity of multiple subsidiaries or business entities/functions

How do our entities currently compare by different risk metrics?

Gaining an overview of different entities will give in-depth insights into the individual risk profiles of our main subsidiaries, enabling a group-wide management and risk-based steering of their cyber risk, depending on the different exposures of the subsidiaries.

Worst Case Loss × | Overall 200Years Modelled Large Loss × | Largest 200Years Modelled Large Loss × | Overall 100Years Modelled Large Loss ×

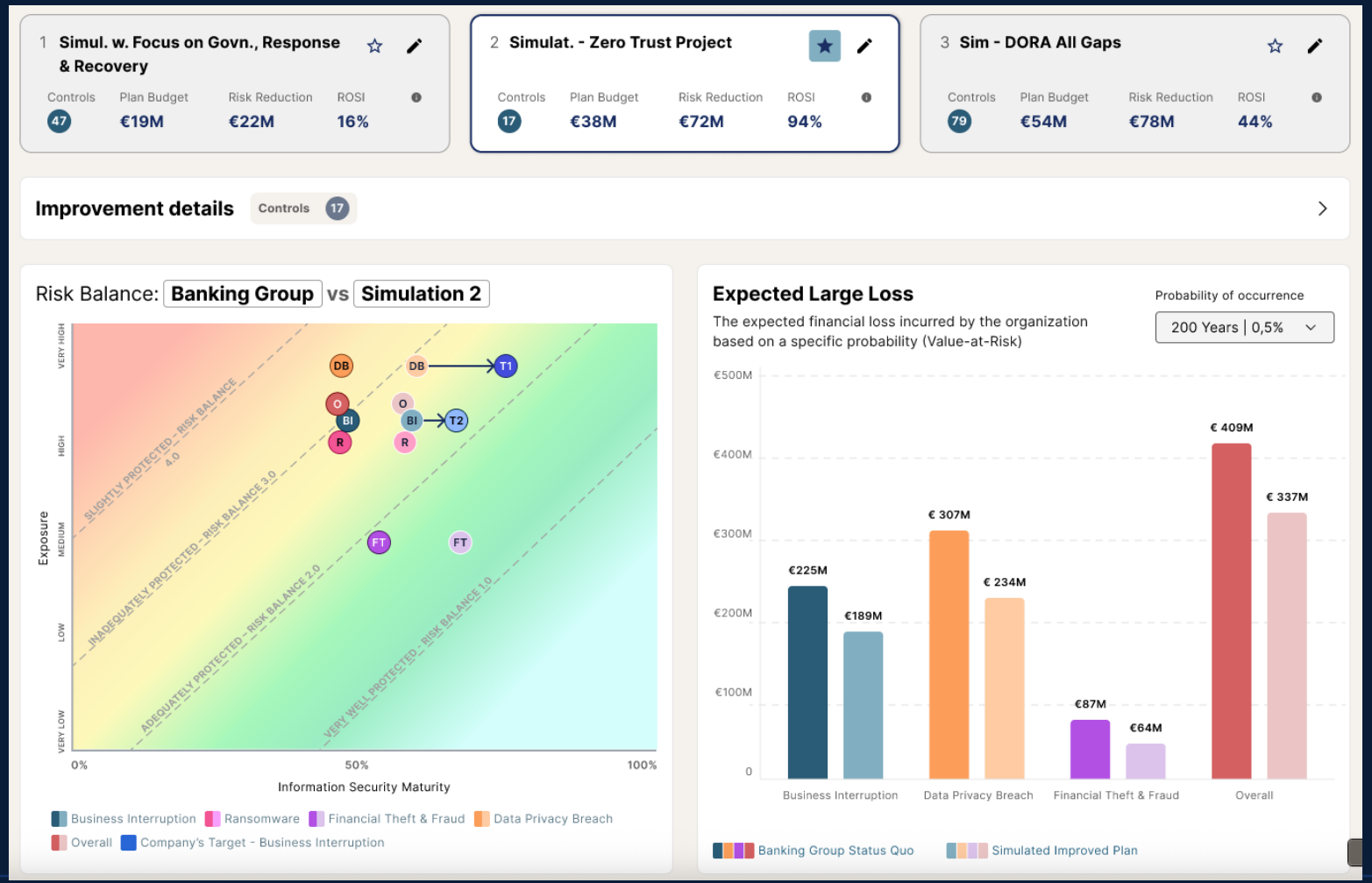
Overall Modelled Average Loss × | Add Columns +

BUSINESS INTERRUPTION (BI) DATA PRIVACY BREACH (DB) FINANCIAL THEFT & FRAUD (FT)

NAME	OVERALL EXPOSURE LEVEL	INFOSEC MATURITY	RISK BALANCE	WORST CASE LOSS	OVERALL 200Y MLL	LARGEST 200Y MLL	OVERALL 100Y MLL	OVERALL MAL	
Banking Group	High to very high	**47%**	**3.2**	**€ 865M**	**€ 409M**	**€ 307M**	**€ 279M**	**€ 77M**	7 years
Subsidiary Germany	High	**53%**	**2.7**	**€ 734M**	**€ 286M**	**€ 200M**	**€ 196M**	**€ 56M**	7 years
Subsidiary France	High to very high	**51%**	**2.9**	**€ 510M**	**€ 236M**	**€ 176M**	**€ 160M**	**€ 40M**	6 years
Subsidiary USA	High to very high	**40%**	**3.4**	**€ 507M**	**€ 288M**	**€ 262M**	**€ 194M**	**€ 49M**	6 years

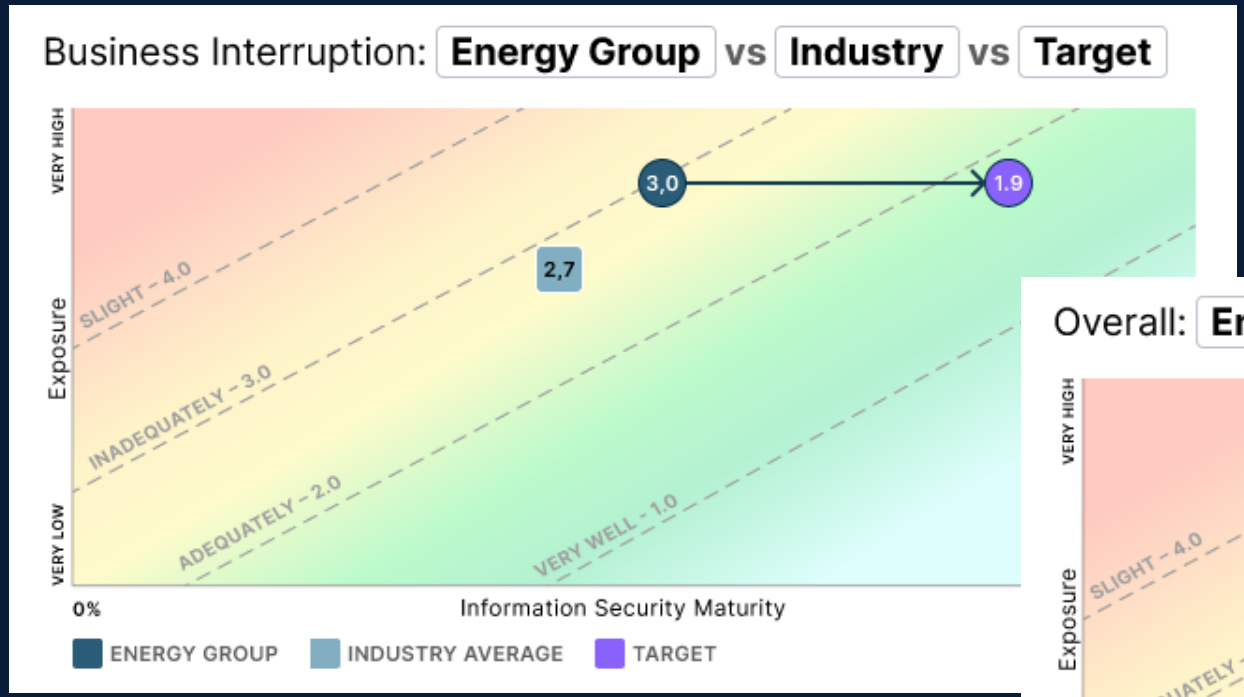
WHAT YOU GET – EXAMPLE OUTPUT

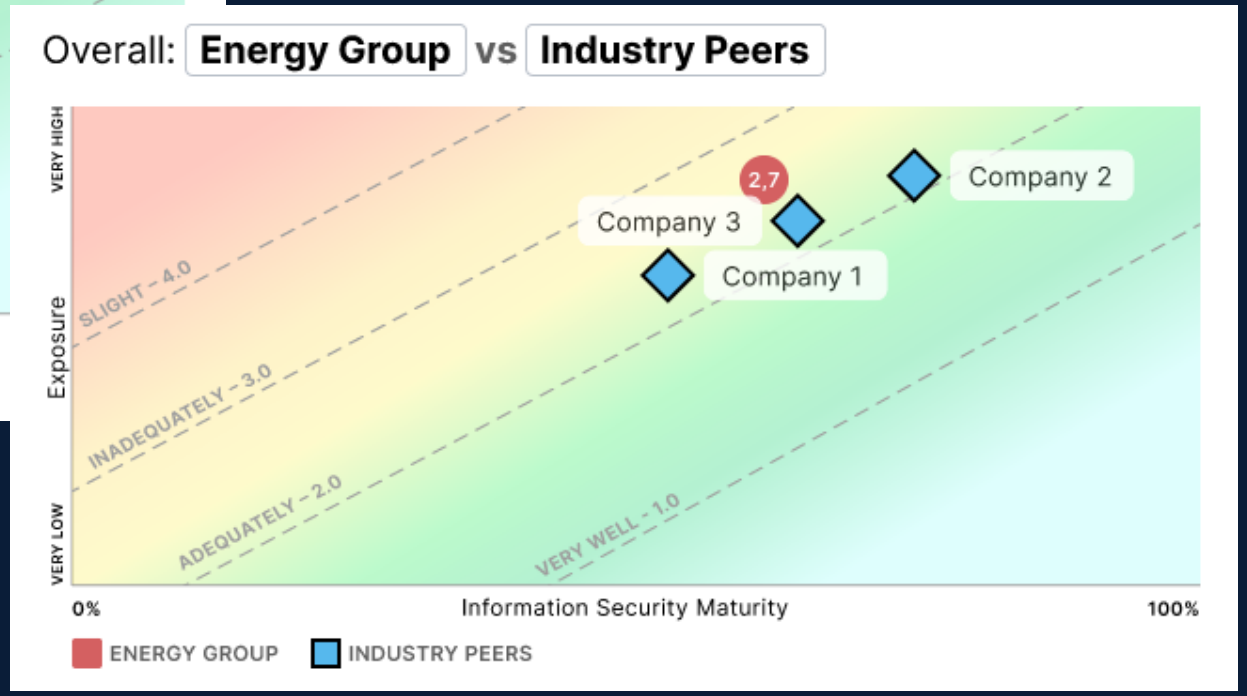
Ability to simulate investment scenarios, showing ROSI and impact of cybersecurity improvement measures



WHAT YOU GET – EXAMPLE OUTPUT

Benchmarking against industry average and similar industry peers





NEXT STEPS

Hungry for more? Let‘s talk!

Yash Bajaj

Business Development Manager

ybajaj@squalify.io

+49 170 8042072

Trusted by industry leaders like: