

Quantitative Risk Assessment for Cyber Security



Risk visibility



Rapid deployment



Customisable



On-premise or SaaS



Intuitive



Value for money

Cyber-attacks are now the top risk for doing business in North America, Europe, East Asia and the Pacific (World Economic Forum, 2018). This is prompting hard questions from business leaders on the level of cyber risks that they are facing, how much could be lost and the priorities for action.

With strategic and investment decisions requiring financial analysis there is an increasing demand for cyber risk to be measured in financial terms. Up to now, the application of quantitative techniques to cyber security has been difficult due to the complex range of factors to consider, each with varying degrees of uncertainty and the lack of relevant, contextual data on cyber breaches. Of particular difficulty, has been the Enterprise-wide scaling and aggregation of quantitative assessments.

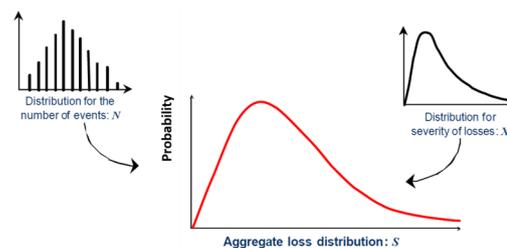
Acuity's STREAM cyber risk management platform provides both quantitative and qualitative risk assessment options which scale seamlessly across the Enterprise.

Qualitative vs Quantitative

Qualitative methods determine a risk value by using ordinal scales such as Low, Medium and High. This can be subjective, prone to bias and doesn't measure risk in financial terms.

To assess risk quantitatively we need to recognize that there are range of potential outcomes and apply statistical techniques.

	5	Medium	High	Very High	Very High	Very High
	4	Medium	Medium	High	Very High	Very High
	3	Low	Medium	Medium	High	Very High
	2	Low	Low	Medium	Medium	High
	1	Low	Low	Low	Medium	Medium
		A	B	C	D	E
		LIKELIHOOD				



By using distributions, such as Lognormal for severity of impact and Poisson for frequency of events we can use Monte Carlo simulations to estimate the probability that losses will exceed a particular level over the next 12 months and compare this with our risk tolerance.

Quantitative risk assessment in STREAM

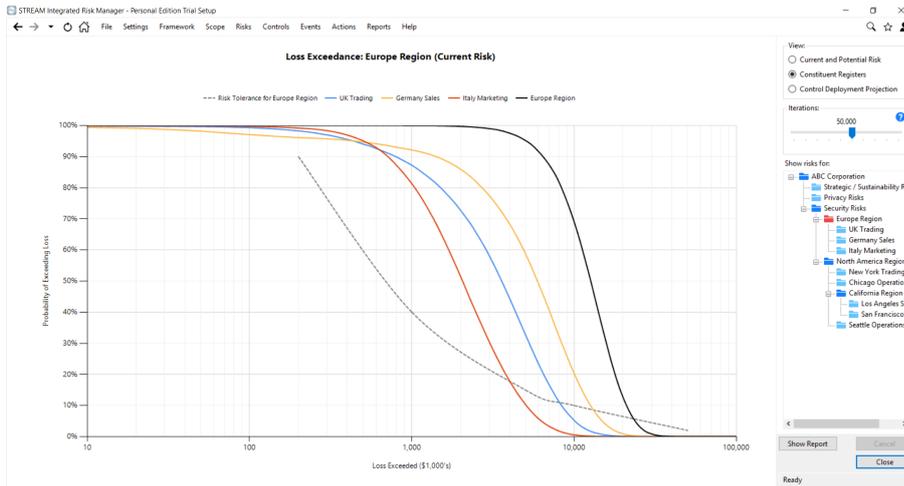
STREAM Integrated Risk Manager is a fast, flexible and easy to use risk management platform which automates the processes and reporting for a risk-based approach to cyber security.

The platform supports Enterprise-wide quantitative and qualitative risk assessment integrated with: threat and vulnerability management; incident and event management; and, action management, enabling business risk-based decision making.



Flexible configuration

Through simple settings, STREAM can be configured for quantitative, qualitative or combined quantitative and qualitative assessments, providing full flexibility for the range of risk categories and assessment approaches required across the Enterprise.



Example Loss Exceedance report in STREAM

Features

- Calculation of estimated 'Expected Loss'
- Aggregation of 'Expected Loss' across the Enterprise
- Loss exceedance report showing probability of losses exceeding certain levels in the next 12 months, compared to risk tolerance
- Control Improvement Priority report showing the control improvements which will have the greatest effect in reducing expected losses
- What-if simulation to model the effect of new or improved controls on expected losses
- Extensive reporting, including Top 10 risks by expected loss for each part of the business and across the entire Enterprise
- Integrated incident and event management, compliance management and action management with alerting, workflow and history

Benefits

- Understand potential financial losses from cyber-attacks and make financial appraisals of mitigating options
- Understand, evaluate and prioritize cyber risks using the same language as other business critical risks and opportunities
- Evaluate cyber security investment proposals and calculate 'return on security investment'
- Make better informed decisions on the requirements for cyber insurance and the levels of cover required



Contact Us

Info@acuityrm.com

www.acuityrm.com

+44 (0) 20 7297 2086

@AcuityRM

Acuity Risk Management

