



Cyber Risk Quantification for the *World of Cyber Insurance*

An insurer relies on various data points to evaluate cyber risk when considering potential policyholders :

1. **Company Information:** Details such as the organization's size, industry sector, revenue, and geographic location provide insights into its risk profile.
2. **Cybersecurity Practices:** The effectiveness of the company's security measures, including firewalls, encryption protocols, regular audits, employee training, and incident response plans, is assessed.
3. **Historical Cyber Incidents:** Previous breaches or cyber events within the company's history offer valuable context for understanding its vulnerability to future attacks.
4. **IT Infrastructure Analysis:** Examination of the organization's network setup, software and hardware systems, and relationships with third-party vendors helps identify potential weak points.
5. **Data Protection Measures:** Compliance with data protection regulations like GDPR or HIPAA, as well as the company's data handling and encryption practices, are scrutinized.
6. **Risk Assessment Tools Usage:** Questionnaires and assessments are employed to gauge the company's overall risk posture and tailor coverage accordingly.
7. **Financial Evaluation:** Financial data analysis aids in estimating the potential financial impact of a cyber incident and determining appropriate coverage limits.
8. **Industry Benchmarking:** Comparing the company's cybersecurity practices with industry standards helps assess its risk relative to similar organizations.
9. **External Threat Intelligence Utilization:** External threat intelligence sources are leveraged to stay informed about emerging cyber threats and evaluate the likelihood of targeted attacks.
10. **Compliance Monitoring:** Ensuring adherence to cybersecurity regulations and standards is integral to evaluating the company's overall risk exposure.

By considering these data points, an insurer can effectively assess cyber risk and offer customized coverage solutions tailored to each policyholder's needs.

Citalid uses Gartner's Minimum Effective approach to deliver the best outputs for each insurer.

Solutions for enterprises and portfolios.

Cyber Risk Management for enterprises

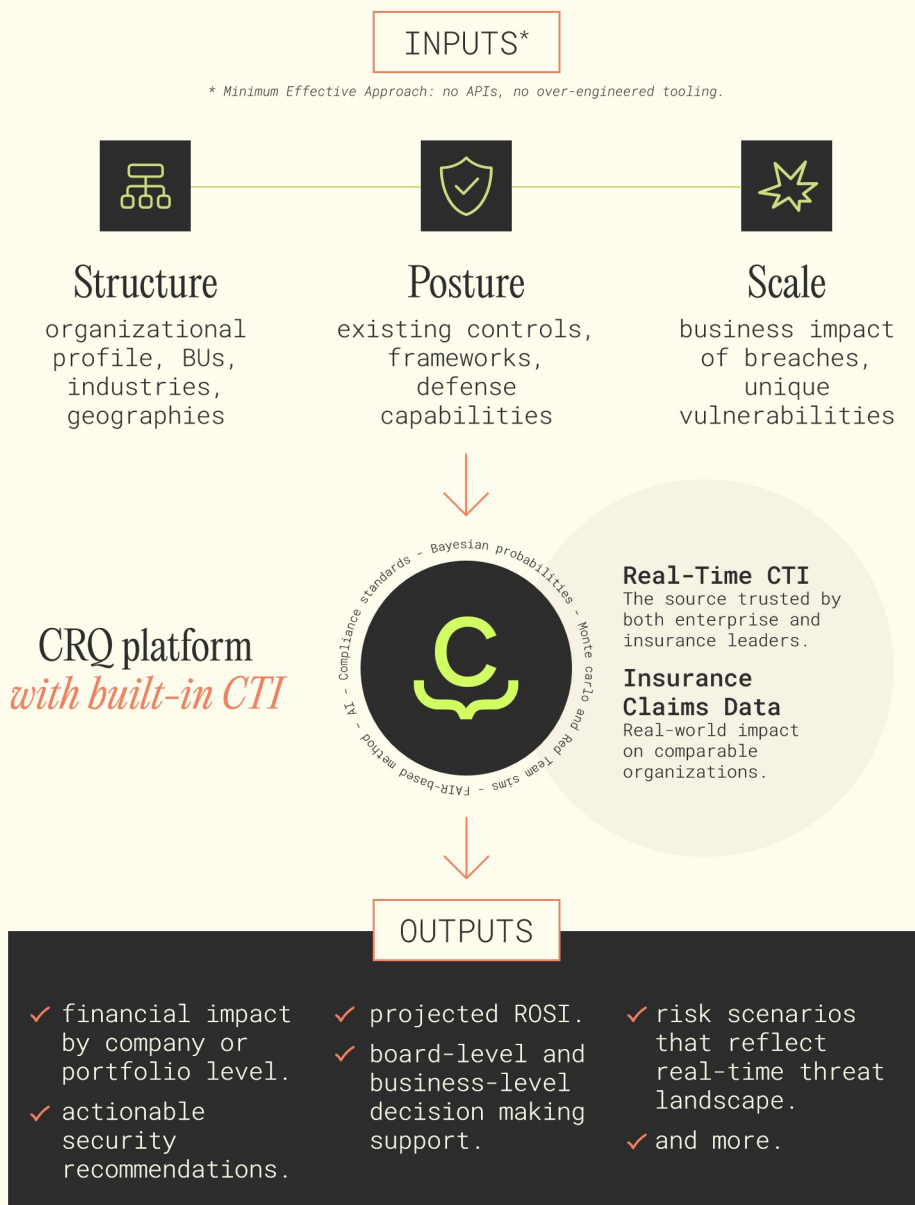
CISOs use Citalid to know which security programs and risk management strategies make the most sense for their unique organizational profile (business and threat landscape related) – and the ROSI of each effort.

Cyber Risk Portfolio Management for insurers and financial institutions

Insurers use Citalid to see the full value at risk for a prospect, a client, or portfolio-wide. They trust our advanced probabilities based on real-time CTI to offer more value through insurance products.

Simple inputs. Illuminating outputs.

Security leaders and insurers prefer our market-proofed CRQ+CTI model for its accuracy, transparency and actionable insights.



TRUSTED BY
100+ CLIENTS

- Allianz 
- ALSTOM
- Capgemini 
- Lagardère
- relyens 
- lneo 

“We manage our security roadmap much more effectively with Citalid.”

CISO, luxury brand group

“This quantitative, transparent approach builds trust with our clients.”

VP, insurance brokerage

For maximum clarity in a hazy cyber risk reality, Citalid is the most practical and prescriptive CRQ choice. See it for yourself:

