Platform

RiskLens' Purpose Built Platform

Designed for Cyber Risk Quantification

RiskLens is the most comprehensive suite of SaaS applications available that enables Chief Information Risk Officers (CIROs) and Chief Information Security Officers (CISOs) to quantify and manage cyber risk from the business perspective.

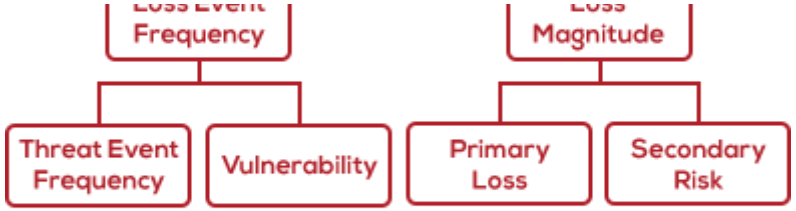
- Purpose-built on **FAIR**, the only standard quantitative model for cybersecurity and technology risk
- Integrates...

  - industry-specific loss data
  - data integration capabilities
- ...into a unified suite built specifically for business-oriented CIROs and CISOs.

How Does RiskLens Work?

1. Model your environment (assets, relevant threat communities, controls)
2. Develop risk scenarios (apply data regarding control conditions and threat activity)
3. Run simulations (calculate loss exposure with Monte Carlo simulations and run sensitivity analysis to identify areas for improvement)
4. Generate risk analytics reports (discover concentrations of risk, track loss exposure over time, and proactively manage your organization's risk)

Standards



THE Open GROUP

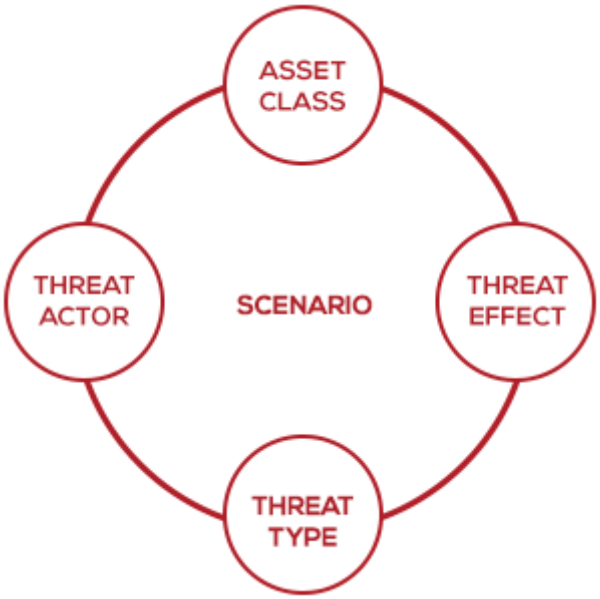
Standard

- FAIR provides a standard definition of and taxonomy for information security risk and is an international standard of the Open Group
- By applying a consistent and well defined standard that breaks the components of information risk into their individual factors, organizations are able to consistently define and manage cyber risk
- Today FAIR is used by organizations around the world, including many Fortune 500 companies

Use Distributions and Simulations with Expert Data

- RiskLens uses betaPERT distributions and Monte Carlo simulations to meaningfully quantify cyber risk, even from limited subject matter expert data
- Both methods have been in use for decades by businesses and academics to model data and drive better-informed business decisions
- Combined with FAIR and with today's available computational power, RiskLens is able to provide practical cyber risk quantification to organizations

RiskLens has tackled the complexity of effectively analyzing cyber risk across the enterprise and dramatically simplified the process of modeling risk scenarios.



Simple, Clear Scenario Modeling

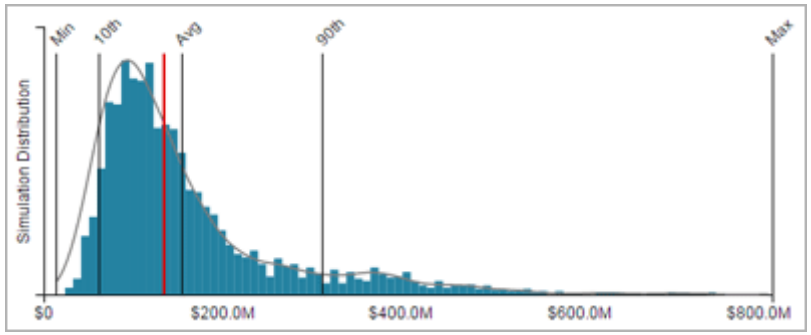
- Easy, point-and-click process for identifying which assets, threats and events to include in your analyses
- Scenario iterations streamline the process for modeling and tracking how conditions change over time
- Simple process for performing multiple "what-if" versions of an analysis to explore where points of control-leverage or fragility exist

Flexible and Adaptable

No two organizations have the exact same risk landscape, so RiskLens has been designed to enable you to describe the unique risk landscape you face

- Choose the level of granularity you need given the problems you're trying to solve, the type and quality of data you have and the resources you have to perform the analysis
- Add, subtract or refine the assets you're protecting, the threats you face and the controls you have at your disposal
- RiskLens allows you to reflect your organization's business structure by defining and focusing on specific business units and/or business

Computational Engine



Maximum	$815.5M
90th %	$312.4M
Average	$154.5M
10th %	$62.5M
Minimum	$14.8M

Risk Appetite	$135.0M

The RiskLens computational engine uses Monte-Carlo simulations to calculate the loss exposure of the modeled risk scenarios. This technique allows for highly uncertain data entered with betaPERT distributions to be used so that the full breadth of the loss impact is explored.

Multi-Scenario Aggregation

Because RiskLens uses FAIR as a foundation for individual scenarios, they can be calculated together in the computational engine allowing for the aggregation of multiple scenarios as well as the calculation of individual scenario results.

- Explore the full scope of an analysis from the executive view at 30,000 feet, to the analysts view at the individual scenario
- Aggregate loss exposure is available for the entire analysis or by department, asset category, asset class, threat community and more
- Quickly be informed of where your organization has concentrations of risk

Stress Testing with Sensitivity Analysis

Additionally, the computation engine supports Stress Testing, a sensitivity analysis which allows an organization to identify potential areas of

- By isolating each input, the computational engine is able to measure the aggregate average impact on loss exposure of the modified input
- This allows risk analysts to identify potential areas for improvement within an analysis that may contain thousands of inputs

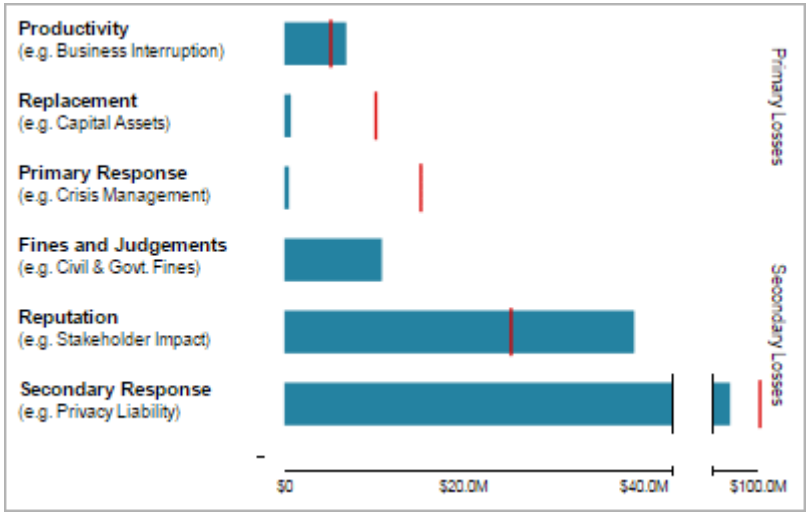
Risk Analytics

The RiskLens platform provides multiple lenses through which to view and better understand your organization's risk landscape.

Set Risk Appetite and Control Thresholds

View the results of an analysis in the context of an organization's business goals and in the language the business speaks.

- Manage the organization's risk appetite at the source of the risk components with full context
- Set risk appetite and risk thresholds for the entire enterprise or individual organizational units, forms of loss, and asset classes



Powerful Comparisons

The risk analytics components within RiskLens provide a variety of powerful comparisons for the full exploration of an analysis

- Compare loss exposure for any component within an analysis: Forms of Loss, Departments, Asset Category, Asset Class, Threat Actors, Individual Scenarios and more
- Track the enterprise's loss exposure over time for the entire organization, its departments and asset classes
- Explore all components of an analysis with the powerful Scenario Explorer; a scatter plot of the analysis' scenarios that allows for the comparison of loss exposure, loss event frequency and vulnerability

Next: Discover Our Applications

Cyber Risk Quantification

Cyber Risk Triage

Cyber Risk Maturity

Resource Center

What is FAIR?