Calculating Risk with SAFE One

Never trust a score you cannot click!

SAFE One's approach to cyber risk quantification and management (CRQM) is purpose-built on open and defensible standards. Simplicity is a core tenet, reflected in how SAFE One calculates "risk". It is the industry's only CRQM solution that automates FAIR™ and is founded on all FAIR™ extensions (FAIR-Materiality Assessment Module, FAIR-Controls Analytics Module, FAIR-Third Party Assessment Module)

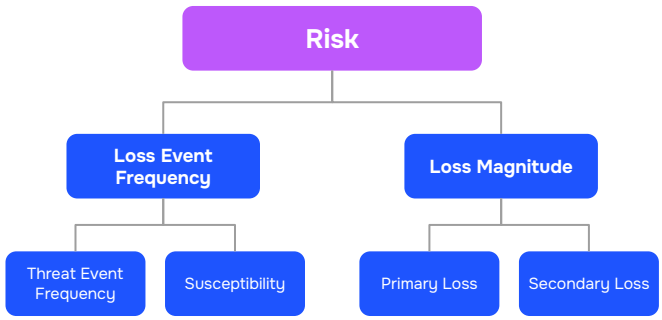
The FAIR™ Framework is the global authority and gold standard of Cyber Risk Quantification and Management (CRQM). It enables risk to be quantitatively defined, measured, managed, and communicated.

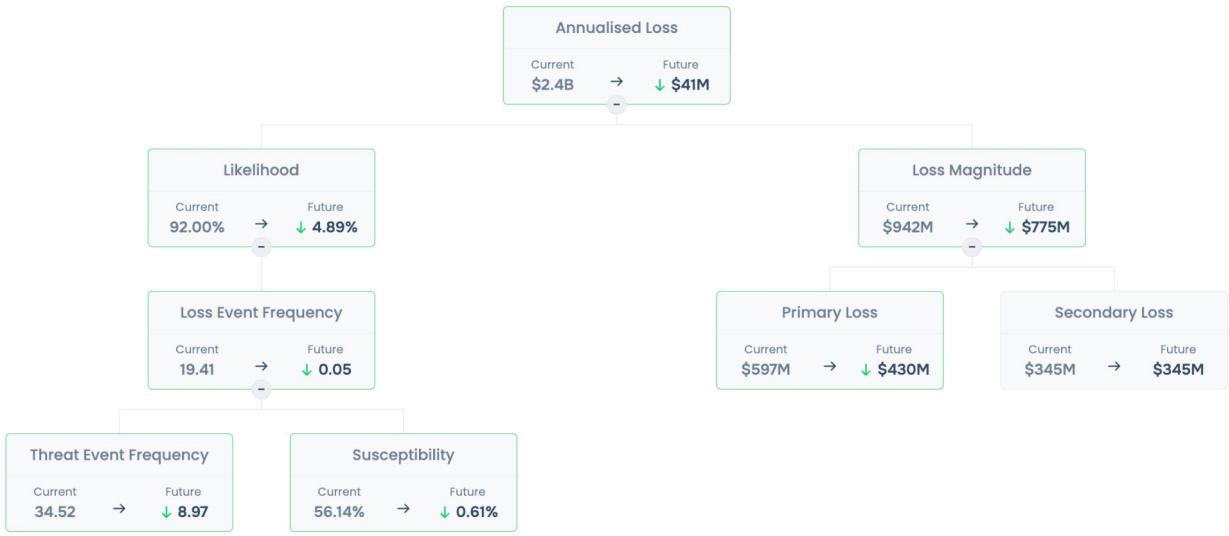
Which criteria does your cyber risk management platform meet?

- ✅ Does it enable informed business decisions?
- ✅ Is it built on robust mathematical modeling?
- ✅ Are the outcomes driven by industry standards?
- ✅ Is it defensible and transparent?
- ✅ Can it be tuned as per your enterprise's context?
- ✅ Is there a solid research foundation?

Decoding Cyber Risk and SAFE One's Engine

Risk is a factor of loss event frequency (or, breach likelihood) and loss magnitude (or, financial impact). The SAFE One scoring engine leverages extensive research-driven data points, maps to standard frameworks, and blends internal business context to provide the most actionable outputs.





The SAFE One Platform: Cyber Risk = Likelihood x Loss Magnitude

A Step-By-Step Guide To SAFE One's Scoring Method

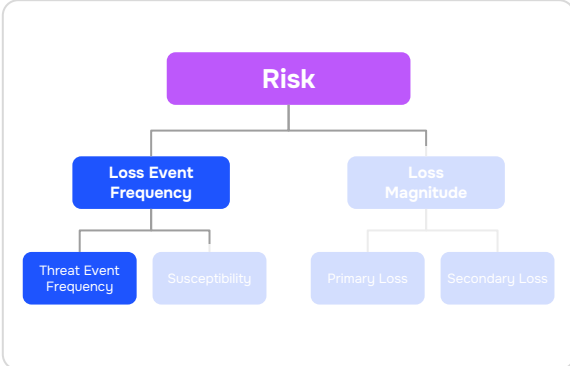
Risk has two parameters; likelihood and impact (magnitude). SAFE One leverages the FAIR Model's Controls Analytics Module to compute likelihood and the Materiality Assessment Module to derive the potential financial impact. For more details, read the research paper and datasheet.

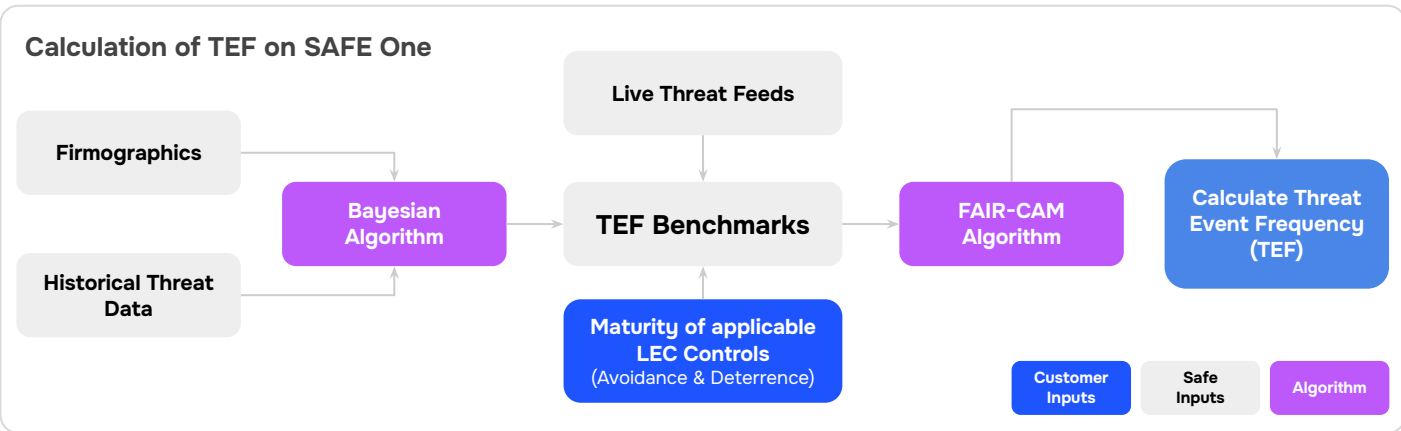
The scoring methodology in SAFE One can be decomposed into four distinct steps:

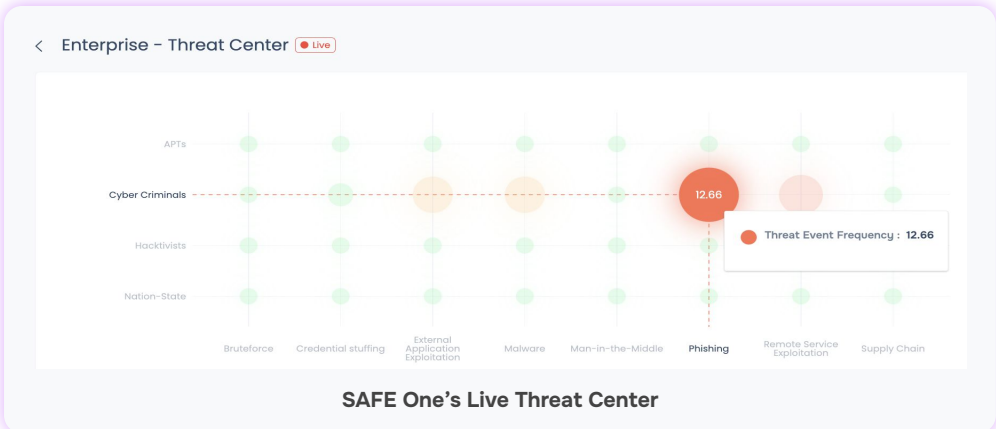
STEP 1: Calculating Threat Event Frequency
STEP 2: Calculating Susceptibility
STEP 3: Measuring Potential Financial Impact (Primary and Secondary Loss)
STEP 4: Producing Annualized Loss Exposure (ALE) via Monte-Carlo Simulation

STEP 1: Calculating Threat Event Frequency (TEF)

The goal in this step is to determine how often your organization could be a victim of a threat event. TEF is the expected frequency within 12-months a threat actor will act against asset/assets. It becomes a Loss Event if it causes material impact. SAFE One leverages historical cyber events' data of approximately 10+ years to measure TEF benchmarks. It accounts for threat actor, industry type, organization size, threat intent, initial attack method. It also leverages external threat feeds, various research-driven data sources, and avoidance controls, deterrence controls, and more to measure threat event frequency.



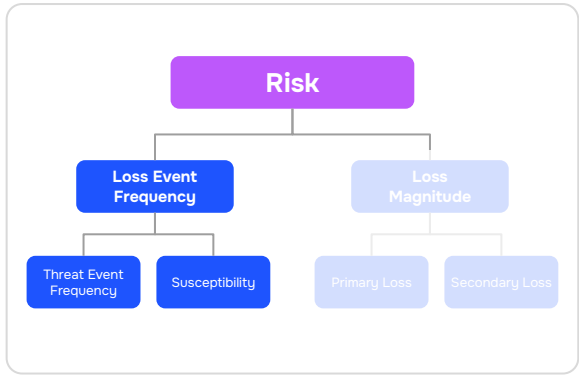




SAFE One's Live Threat Center

STEP 2: Calculating Susceptibility

SAFE One assess the extent to which an enterprise is positioned to defend against a cyberattack. Controls deployed within an environment reduce susceptibility. Susceptibility decreases as the number of effective controls increases.



Controls affect risk in three distinct ways:

1. Loss Event Controls (LEC) function by directly affecting the frequency or magnitude of loss
2. Variance Management Controls (VMC) function by affecting the reliability of controls
3. Decision Support Controls (DSC) function by affecting decisions

For example: An enterprise has 3 LEC controls, each with a control maturity of 80%, deployed as layers of resistance. This implies that an initial cyber attack attempt has a 20% chance of bypassing the first control. The second control reduces risk by another 80%, leaving a 4% chance, and the final control further reduces susceptibility to 0.8%. This demonstrates the effectiveness of a layered defense model with appropriate control maturity (coverage, capability, and reliability) in minimizing the Loss Event Frequency and susceptibility.

NOTE: Loss Event Frequency (LEF) = Susceptibility × Threat Event Frequency (TEF)

All | Threat Event Frequency | Susceptibility | Loss Magnitude

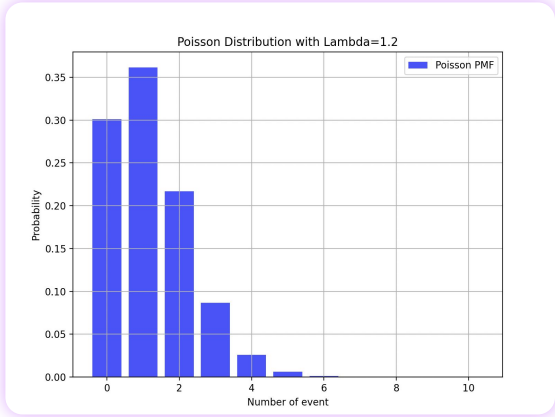
CONTROL NAME	CONTROL PARAMETER	CURRENT MATURITY	TARGET MATURITY
DLP Data Loss Prevention	Capability	M1	M2
DLP Data Loss Prevention	Coverage	M1	M2
DLP Data Loss Prevention	Reliability	M3	M3
DRE Data at Rest Encryption	Capability	M1	M2
DRE Data at Rest Encryption	Coverage	M1	M2
DRE Data at Rest Encryption	Reliability	M3	M3
EDR Endpoint Detection and Response	Capability	M2	M3
EDR Endpoint Detection and Response	Coverage	M2	M3
EDR Endpoint Detection and Response	Reliability	M1	M2

Controls Maturity Recommendations by SAFE One to Minimize Susceptibility

Deriving Breach Likelihood from Susceptibility and Loss Event Frequency

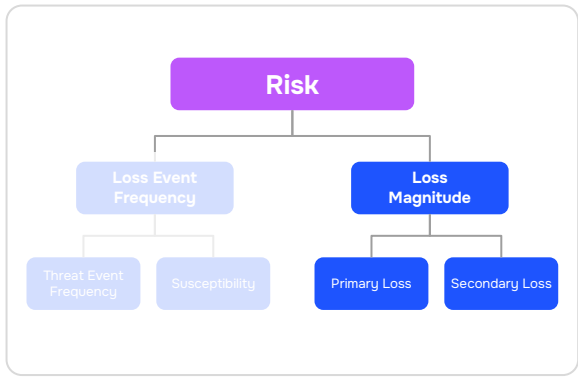
The goal of this step is to arrive at the final breach likelihood for each risk scenario. By simulating the loss event frequency using a Poisson distribution, and applying and exponential formula “Likelihood = 1 - EXP(-LEF)”, we can derive the breach likelihood.

Consider a Poisson distribution with a mean (λ) of 1.2 for LEF. When graphed, the probability of “zero-loss” years is 30%, implying that 30% of the total number of years will show zero-losses. Therefore the likelihood of at least one loss event occurring is 70%.

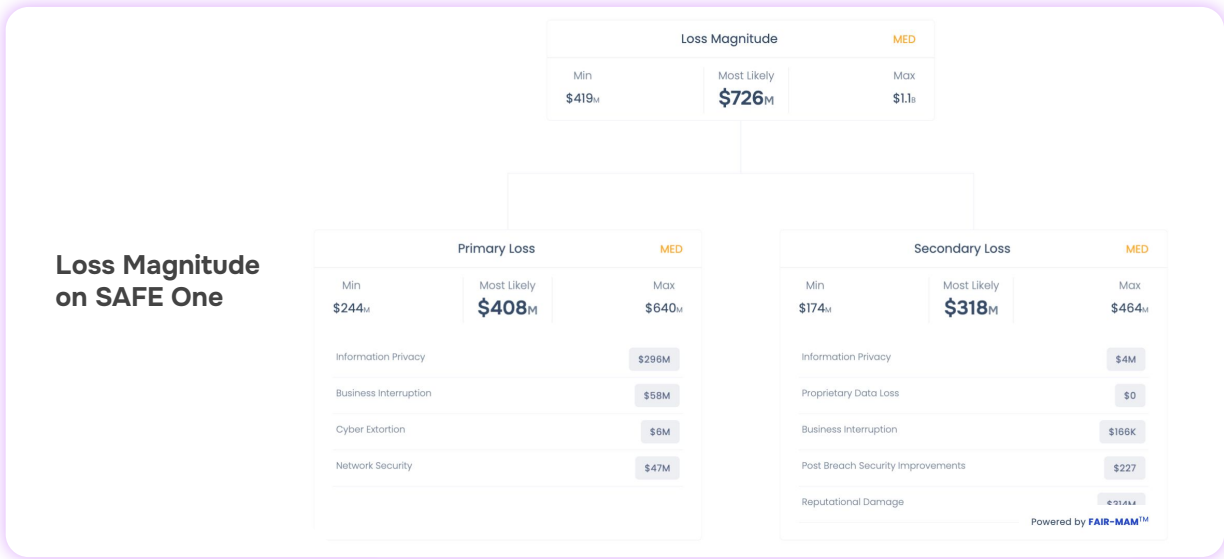


STEP 3: Measuring Loss Magnitude

In this step, the SAFE One scoring engine switches gears towards measuring the financial impact of risk scenarios. SAFE leverages algorithmic logic to generate loss magnitude from more than 6 million possible combinations of risk scenario components, FAIR-MAM benchmark driver values, group firmographic data, and Financial Impact Questionnaires. The collaboration with cyber insurance players further validates SAFE One's loss magnitude calculation. Explore real-world calculations and the backtesting of SAFE's loss magnitude on howmaterialisthathack.org



Loss Magnitude on SAFE One



STEP 4: Produce Annualized Loss Exposure (ALE) via Monte-Carlo Simulation

In the final step, the loss event frequency and severity of financial loss over 50,000 simulated years. Using lognormal distribution for each simulated loss and Poisson distribution for each simulated event, the aggregate loss for each year is derived and plotted as a Loss Exceedance Curve.

Annualized Loss Exposure Trend on SAFE One

A Worked Example from SAFE One

Industry	Retail
Revenue	$50 billion ARR
Geography	United States of America
Threat Actor	Malicious Cybercriminals
Initial Attack Method	Phishing
Intent	Data Exfiltration

Based On TEF, TEF priors, and TEF Benchmarking values, the resultant Threat Event Frequency = 0.8

Factor	Value
Applicable Controls	Based on risk scenario: Data Exfiltration
Attack Surface	10,000 assets
Control Capability	60% (Assumed common control maturity)
Control Coverage	80% of assets

We get a susceptibility of 0.4 (or 40%) based on the provided factors and SAFE's proprietary data and models. Loss Event Frequency (LEF) = 0.4 × 0.8 = 0.32 (or 32%)

Therefore, Breach Likelihood = 1 - EXP (-0.32) = 27%

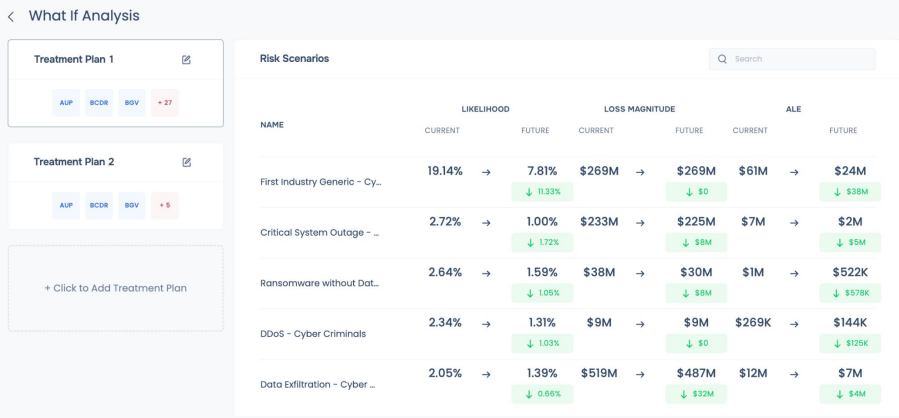
Primary Loss		Secondary Loss	
Information Privacy	$5M	Post Breach Security Improvements	$1M
Business Interruption	$4M	Reputational Damage	$3M
Cyber Extortion	$3M	Information Privacy Liability	$2M
Regulatory	$10M		

Loss Magnitude Calculation: $28 Million(MInimum: Min $588K; Maximum $54M)

Annualized Loss Calculation: The annualized loss curve represents that the organization has a 27% likelihood of experiencing a $28M loss due to a data exfiltration event.

Controls:
The only factor an enterprise can directly influence to minimize loss event frequency and susceptibility and ensure risk burndown.

It is imperative to maintain the highest possible control maturity (coverage, capability, and reliability) that is aligned to both the risk appetite of the business and the budget available.



Impact of Controls on Risk Reduction with SAFE One's "What-If?" Analysis

Accurate Quantification is Non-Negotiable in Cyber Risk Management

Cybersecurity needs to be positioned as a business enabler, and to do so, CISOs must present their findings and reports in a decision-useful manner. The SAFE One's scoring method is reliable, trustable, defensible, and can be used to drive business decisions.

Reliability is paramount for effective cyber risk quantification

An accurate scoring methodology ensures that calculated risks closely mirror potential impacts, enabling data-driven decisions. This precision prevents over or underestimation of risk, leading to optimal resource allocation, prioritized risk mitigation strategies, and safeguards against costly errors stemming from misjudged risks.

Trustworthiness is essential for the success of any risk management initiative.

Transparency in the scoring methodology and its underlying data sources integrated with the product fosters confidence among stakeholders. Clear communication based on a data-driven output builds trust, facilitating collaboration between IT and business leaders. Moreover, a transparent approach strengthens the organization's reputation for responsible risk management, encouraging stakeholder support for risk-based decisions.

Defensibility for both internal and external stakeholders with standardization

Clear communication of the risk calculation process is essential for regulatory compliance. By maintaining a standardized approach, organizations can compare risks across different business units and over time, identifying emerging risks and trends. It enables the tracking of risk mitigation strategy effectiveness, ensuring continuous improvement in the risk management process.

With trustable scoring engine built on open standards, SAFE One is truly defensible. Start or enhance your journey towards unified, data-driven cyber risk quantification and management with SAFE One.

Schedule a 1:1 demo with a SAFE cyber risk expert today!

RESEARCH SPONSOR
MITRE ATT&CK, TOP CONTRIBUTOR

PUBLISHER'S CHOICE AWARD
RISK MANAGEMENT
GLOBAL INFOSEC AWARDS - RSAC 2023

BEST NEXT GEN
CYBER INSURANCE PLATFORM
GLOBAL INFOSEC AWARDS - RSAC 2023

BEST RISK
MANAGEMENT SOLUTION
CISO CHOICE AWARDS 2022™

www.safe.security | getintouch@safe.security