SAFE

# Make **FAIR** practical for your business

Factor Analysis of Information Risk (FAIR ™) (www.fairinstitute.org), is a framework to understand, measure, and analyze cybersecurity risk. Established in 2004, FAIR was designed to drive informed decision-making and it balances structural robustness with adequate flexibility. However, its implementations have often been a source of frustration for practitioners.

> **CRQ methods like FAIR lack practical implementation-level guidance for correctly scoping a FAIR analysis** - Forrester, January 2022

## A FAIR implementation can become practical and actionable when:

- **The quality of data input feed is high**. Input data should be objective and comprehensive covering the entire attack surface, and automatically updated. The input should also reflect the right business context and external threat landscape.
- **The output is reliable to make decisions on specific use cases**. An output is considered reliable if it captures the dependencies among individual risk elements and also calculating the overall organizational risk.
- **The time-to-value is quick, and the cost-to-maintain can be justified**. The time to derive value and the resources (time, budget, employees) required to maintain CRQ solutions, such as FAIR, need to be minimal.

Safe Security has built an approach to Cyber Risk Quantification that is consistent with the FAIR principles. Our approach implements the three requirements above to enable practical decision-making. **It removes the most time-consuming and inaccurate features of other CRQ models by ingesting cyber control feeds directly from your cyber tools - all in real-time.**

> While FAIR derives its status from the wider applicability and its status as an open standard adopted by the Open Group, **it is not the only approach to CRQ**
> - Forrester, January 2022

## How is SAFE consistent with FAIR principles?

Safe Security's CRQ platform - SAFE - enables you to measure, manage, and mitigate cyber risk in real-time. At its core, **SAFE's algorithm is consistent with the FAIR methodology**, and is **co-developed with Massachusetts Institute of Technology (MIT) plus CRQ pioneers such as Douglas Hubbard**, the inventor of the Applied Information Economics method.

SAFE calculates risk from the bottom up, by considering each risk element (technology assets, policy controls, people, third parties). It estimates the **probability at an 'asset' level,** then aggregates these to calculate the **probability of overall organization-level attacks**.

SAFE uses a mathematical **Bayesian Network-based** model to calculate the impact of a series of events in succession - which is how cyber attacks happen.

### SAFE Risk Model Architecture

SAFE estimates your financial risk exposure. It defines financial risk exposure as the potential primary and/or secondary losses associated with specific attack types aligned with mitigating controls.
To calculate the **primary loss**, SAFE includes the following:

1. Incident response
2. Business interruption
3. Data restoration
4. Customer support
5. Reputation damage

**Secondary loss** calculation includes:

1. Contract breach
2. Regulatory fines and consent orders
3. Litigation settlements and consent orders

> **The true value of CRQ lies not in the output of the models, but in the decisions it enables organizations to make, especially around digital strategies**
>
> - Forrester, January 2022

## How does SAFE make implementing FAIR practical?

SAFE overcomes the challenges of implementing FAIR. It enables the CISO and their security team to drive data-backed decisions using Cyber Risk Quantification.

**SAFE ensures a high quality of input data**

- Leverages API integrations to get automated and real-time data from the attack surface.
- Removes subjectivity by reducing the possibility of human errors.
- Removes the need for agent installation in most cases.

**SAFE's output is actionable**

- The question of 'So, what?' is answered by providing business context.
- Provides prioritized action plan to security and risk management leaders.
- Gives the potential $ value of cybersecurity risks to the C-Suite and Board members.
- Empowers the CFO to make data-backed decisions on cyber insurance limit, premium, and coverage.
- Justifies the ROI of cybersecurity initiatives undertaken to reduce cyber risk.

**SAFE's enables a quick time-to-value and scalable implementation**

- SAFE's cloud-based architecture covers 360° of enterprise attack surface across people, processes, technology, and third parties.
- Includes external threat intelligence indicators identified by our own cyber intelligence research team, plus the National Vulnerability Database, MITRE ATT&CK, and more.
- Incorporates multiple globally accepted compliance frameworks such as NIST CSF, PCI DSS, and CIS.

**To learn more, reach out to us at getintouch@safe.security, or visit www.safe.security**

Palo Alto
3000, El Camino Real
Building 4, Suite 200, CA
94306

SAFE