Member Login

FAIR FAQ

What is FAIR?

FAIR stands for Factor Analysis of Information Risk. Simply stated, it is a model that describes what risk is, how it works and how to quantify it.

- FAIR is the only international standard quantitative model for cyber security and operational risk.
- Unlike risk assessment standards that focus their output on qualitative color charts or numerical weighted scales, the FAIR model specializes in financially derived results tailored for enterprise risk management.

How is FAIR different from other risk methodologies?

FAIR is an analytical risk model, whereas most information security risk methodologies in use today are Capability Maturity Models (CMM) or checklists. Analytic models attempt to describe how a problem-space works by identifying the key elements that make up the environment and the relationships between those elements — e.g., Newton's laws of the physical world described how things like gravity work. If the models are relatively accurate (no models are perfect), then analyses performed using the models should consistently align with our experience and observations. With those elements identified, measurements can be made that enable risk quantification and performance of what-if analyses, neither of which can be performed with checklist or CMM analyses.

The other methodologies answer different questions:

- Checklist methodologies (e.g., PCI, ISO, BITS, etc.) provide inventories of practices that an organization can use to evaluate and benchmark itself against. This can be useful for identifying gaps in controls and/or for comparison against other organizations. Checklists are not useful for determining how much risk exists or for understanding the effects of changes in the risk landscape (e.g., how much more or less risk will exist if…).
- CMM methodologies (e.g., SSE-CMM) provide a ordinal scale for rating the maturity of processes. This can be useful for evaluating the quality of processes, for setting goals, and for evaluating progress against those goals. CMM is not useful for quantifying risk or measuring the practical effect of changes in maturity.

FAIR provides the means to answer questions like:

- How much risk does X represent?
- How much risk do we have?
- How much more/less risk will we have if …?
- What are my most cost-effective options for managing risk?

Note that all three methodology types can be useful for most organizations, and should be complementary.

Is FAIR complicated and/or hard to use?

FAIR is conceptually very straightforward. That said, many of the risk scenarios we face in our profession are not. As a result, analyzing a complex scenario with even a simple modeling structure like FAIR can feel difficult, especially at first.

The good news is that besides being conceptually simple, FAIR is highly flexible. This allows the user to operate in "quick-and-dirty" mode or "down in the weeds", whichever is appropriate given time, resources, and the significance of the problem being analyzed. In fact, the vast majority of FAIR analyses fall into the quick-and-dirty category because that's all that is required in most instances.

As with any new skill though, there is a learning curve in how to properly scope risk scenarios. Most of that curve is spent learning how to decompose scenarios so that they can be analyzed. Once a scenario is well-defined, the analysis itself is generally quite simple.

Is FAIR an open standard or proprietary?

FAIR is an open standard by **The Open Group**. The Open Group is a standards body that has chosen FAIR as the standard information risk management model after a most rigorous review and comparison with other methodologies. The Open Group is a global consortium that enables the achievement of business objectives through IT standards with more than 450 member organizations that include companies such as HP, IBM, Oracle, Accenture, Cap Gemini and MITRE

Who uses FAIR?

FAIR is widely used by organizations in a variety of sectors, including:

- Banking

- Insurance
- Retail
- Manufacturing
- High Tech
- Health Care
- Energy
- Education
- Consultancies
- Government

Organization size has ranged from SMB to Fortune 500.

Bottom line — understanding and measuring risk can be useful for organizations of any size in any industry.

Is FAIR credible?

FAIR has been vetted at various points in its development with people who are experts in risk and quantitative analysis.

- **The Open Group** has selected FAIR as its standard model for risk management
  - The Open Group published the **FAIR-ISO/IEC 27005 Cookbook** that describes in detail how to apply the FAIR model to any selected risk management framework.
  - The Cookbook states that "FAIR is complementary to all other risk assessment models/frameworks, including COSO, ITIL, ISO/IEC 27002, COBIT, OCTAVE, etc. It provides an engine that can be used in other risk models to improve the quality of the risk assessment results.
- **NIST** recognizes FAIR as a complementary standard for quantifying and prioritizing risk in its **industry resources page**.
- The **Federal Reserve Board**, the Federal Deposit Insurance Corporation (**FDIC**), and the Office of the Comptroller of the Currency (**OCC**) seek to develop “a consistent, repeatable methodology to support the ongoing measurement of cyber risk” and are considering FAIR for that role.
- Section 3 of the **PCI Data Security Standard (PCI DSS) Risk Assessment Guidelines**, recommends compliance with standard risk methodologies such as NIST or ISO and further recommend use of FAIR as a risk framework to be used on its own or as a supplement to these standards.
- **(ISC)²** endorses FAIR as a standard taxonomy that can help our members articulate cybersecurity risk in consistent terms across their organizations and a model for assessing risk in quantifiable terms.

Is FAIR going to work well for my organization?

In order for any framework to be useful, management has to support its use. If management where you work is only interested in compliance with regulations and/or “best practice” and is not interested in understanding how much risk exists, how much risk is associated with non-compliance issues, or which risk management measures are likely to be the most cost-effective, then an analytic framework like FAIR may not be a good fit.

My executives like Red/Yellow/Green risk indicators, so why should I be interested in FAIR?

FAIR can be extremely useful for performing qualitative analysis that generates simple outputs. In fact the introductory white paper describes one way it can be used in that fashion. Also, it's simple to convert a quantitative value into a qualitative rating. For example, an organization can define parameters that match specific quantitative ranges to qualitative values — e.g., "Annualized exposure of between $100,000 and $1,000,000 risk will be considered "High Risk" (or Red on a color scale)." The advantage is that the analysis and the numbers underlying the qualitative values can be referenced to explain how the rating was arrived at.

Does FAIR use a 1-to-5 or other quantitative scale?

There are many analysis methods that use ordinal scales (e.g., 1 – 5, 1 – 10) to rate risk conditions. These frameworks are commonly mistaken to be quantitative because numbers are involved, however in each case the numeric scale could be replaced with colors or words (e.g., "High", "Medium", etc.) and be identical. In addition, common mathematical functions like addition, subtraction, multiplication, etc. can't legitimately be performed on ordinal scales (e.g., you can't multiply red times yellow).

FAIR analyses use quantitative values like frequencies, ratios, and monetary loss, which enables the use of true quantitative analysis.

How do you measure intangibles like reputation damage?

Logically, the effects of damaged reputation have to materialize in some form of loss or else we wouldn't care. These effects are tangible. For a commercial enterprise these effects materialize as reduced market share, decreased stock price (if publicly traded), and potentially the cost of capital. In the public sector, an organization's goal might be stated in terms of mission delivered and service offered and not necessarily in terms of financial goals. In these cases too, reputation damage can be assessed in financial terms through the use of subject matter estimates, expressed in ranges.

In our experience, organization executives have always been able to confidently estimate the effects of reputation damage. They understand their customers, competition, and other key business factors that would come into play from a reputation perspective. The key is to get these loss estimates from business or agency executives, as it is extremely uncommon for information security or risk analysts to estimate these effects accurately.

When would I use FAIR?

Anywhere you have a need to know how much risk exists (or could exist if...). Examples include:

- Policy exception requests
- Audit findings
- Penetration test results
- Comparing risk issues. For example, “Does data leakage or web application security represent more risk to our organization?”
- Building a business case for new security measures or for defending existing security expenditures.
- Prioritizing risk mitigation options when the budget doesn’t allow for everything. For example, “Which is likely to be more cost-effective, training my web developers or implementing an application firewall?”
- Optimizing cyber insurance coverage

Is there software for FAIR?

Yes. **RiskLens**, the technical advisor to the FAIR Institute, has developed a cyber risk quantification and management platform purpose-built on FAIR. The RiskLens platform integrates:

- maturity models
- template-based best practice workflows
- advanced VaR analytics
- industry-specific loss data
- data integration capabilities

...into a **unified suite** built specifically for business-oriented information security and operational risk officers.

I’ve heard that quantifying risk isn’t possible. Is this true?

The short answer is “No”, it’s not true.

Quantifying risk has been done for many decades in insurance and banking. Many highly-respected information risk authorities do encourage the quantification of risk, including **NIST** and **ISC(2)**.

Unfortunately, there are a lot of commonly held misconceptions about risk, particularly in the information security profession. More information about some of the most commonly expressed concerns can be found in the **FAIR Book** (*Measuring and Managing Information Risk: a FAIR approach*)

I’ve heard that there’s more to FAIR than is documented in the standards papers. What else is there?

The **Open Group standards** are intended to provide an introduction to the concepts and methods within FAIR, but does not fully cover the body of knowledge around FAIR. You can read about the most recent developments around FAIR in the award-winning **FAIR Book**.

The full model includes:

- Deeper taxonomy levels
- Models for controls analysis
- Models for analyzing an organization's ability to manage risk over time
- The use of distributions rather than scales and matrices for describing variables
- The use of Monte Carlo functions to analyze highly uncertain data
- The use of sensitivity analysis to identify especially important risk factors in scenarios
- Calibration to improve the quality and utility of estimates where data are sparse
- Means of performing risk aggregation

Despite how complex some of that sounds, platforms such as **RiskLens** simplify the process for the risk analyst and help to enable practical everyday use.

How do I become trained in FAIR?

Please see our training page **here.**

Does FAIR training count as CPE credits?

Yes. You can apply the training hours against CPE requirements for various certifications. Online video based training equates to 15 CPE credits and on-site training is 16 CPE credits.

Where can I learn more?

The FAIR Institute was created with a **mission** to provide resources to learn more about FAIR and to create opportunities to develop and exchange best practices among FAIR practitioners.

- The **'Learn FAIR' page** provides a list of good sources of additional information, including the FAIR Institute **blog** and **member resources** page.
- You can meet the FAIR experts at the annual **FAIR Conference**.
- We also encourage you to **contact us** if you have specific questions.

How can I become a member of the FAIR Institute?

You can become a member of the FAIR Institute **here**. Membership is free, courtesy of the FAIR Institute sponsors.

HOME

ABOUT

GET INVOLVED

LEARN FAIR

EVENTS

AWARDS

ADVISORS

TERMS OF USE | PRIVACY | GENERAL MEMBER AGREEMENT | SITE MAP