



## WHAT IS FAIR?

### From a Compliance-based to a Risk-based Approach to Information Security and Operational Risk

Organizations are increasingly transitioning to risk-based approaches to information security and operational risk, as compliance to regulations alone provide only a minimum layer of security and fail to adequately protect them.

- Information risk has become a business issue, not just a technology issue, as most business processes have digitalized.
- Boards of directors and business executives want to understand an organization's loss exposure in financial terms to enable effective decision-making.
- Risk and security professionals must become facilitators of the balance between protecting the organization and running the business.

**THE WALL STREET JOURNAL** | BUSINESS

JOURNAL REPORTS: LEADERSHIP

**CIOs' Top Management and Policy Priorities**

The Top Priorities of CIOs at The Wall Street Journal's 2015 CIO Network Conference

Feb. 9 2015 11:00 p.m. ET

**1. Make Security everyone's business.**

**2. Cyber risk = business risk. A primary responsibility for a CIO or CISO when talking to the CEO or board of directors is to articulate how cyber security translates into dollars and cents. Putting monetary value on security events, and tying security to real-life business cases, can show senior executives the potential impact of a cyber event in terms that make sense to them.**

# FAIR: A Methodology for Quantifying and Managing Risk in Any Organization



**Factor Analysis of Information Risk (FAIR)** is the only international standard quantitative model for information security and operational risk.

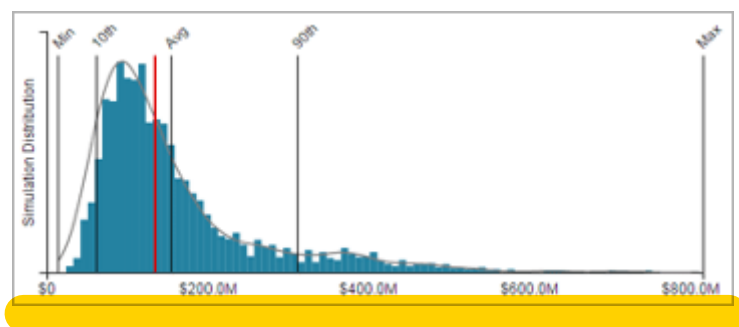
- FAIR provides a model for understanding, analyzing and quantifying information risk in financial terms.
- It is unlike risk assessment frameworks that focus their output on qualitative color charts or numerical weighted scales.
- It builds a foundation for developing a robust approach to information risk management.

GET YOUR BOOK TO LEARN ALL ABOUT FAIR

## A Common Language That All Can Understand

With **FAIR**, you can:

- Speak in one language concerning your risk;
- Take a portfolio view to organizational risk;
- Challenge and defend risk decisions using an advanced risk model; and
- Understand how time and money will impact your security profile.



SIGN UP FOR FAIR TRAINING

## An Enterprise Scalable Risk Model

FAIR's risk model components are specifically designed to support risk quantification:



- A standard taxonomy and ontology for information and operational risk.
- A framework for establishing data collection criteria.
- Measurement scales for risk factors.
- A modeling construct for analyzing complex risk scenarios.
- Integration into computational engines such as **RiskLens** for calculating risk.

**Login** on the members resources page to get your FREE copy of the FAIR Book chapter on the FAIR risk ontology.

Also free - a full-size version of the FAIR risk model, available [here](#) for download.

The FAIR methodology was conceived as a way to provide meaningful measurements so that it could satisfy management's desire to make effective comparisons and well-informed decisions. FAIR has become the only international standard Value at Risk (VaR) model for cybersecurity and operational risk.

LEARN MORE ABOUT BUILDING A RISK MANAGEMENT PROGRAM WITH FAIR

## An International Standard by The Open Group



The Open Group has chosen FAIR as the international standard information risk management model. The Open Group has published two standards, O-RT, Risk Taxonomy Standard, and O-RA, Risk Analysis Standard, comprising Open FAIR.

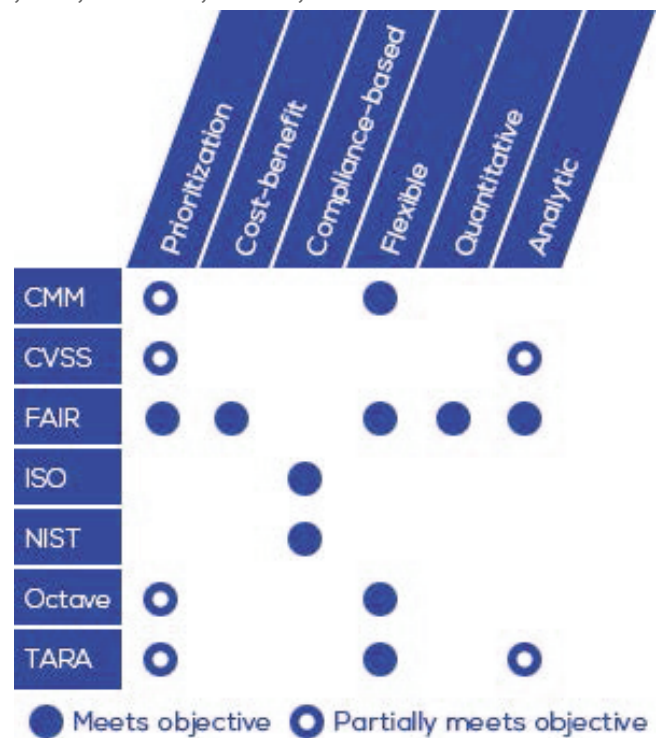
- The Open Group is a global consortium that enables the achievement of business objectives through IT standards.
- It has more than 500 member organizations including companies such as HP, IBM, Oracle, Accenture, Cap Gemini and MITRE.
- Standardization of Open FAIR was achieved following a most rigorous review and comparison with other risk methodologies, and development using an open, consensus standards process.
- The Open Group has numerous publications available on Open FAIR, which are available [here](#).
- The Open Group accredits Open FAIR training courses and certifies individuals. Details regarding Open FAIR accreditation and certification are available [here](#).

SIGN UP FOR FAIR TRAINING

## Complementary to Existing Risk Frameworks

FAIR's risk analysis capabilities complement the existing risk management frameworks.

- Risk frameworks from organizations such as **NIST, ISO, OCTAVE, ISACA**, etc. are useful for defining and assessing risk management programs.
- They all prescribe the need to quantify risk, but for the most part, they leave it up to the practitioners to figure it out.
- Some are silent on the subject of how to compute risk, while others are open in the allowance of 3rd party methods.
- Frameworks such as NIST 800-30 attempt to measure risk, but fall short as they rely on qualitative scales and flawed definitions.
- FAIR helps fill that gap by providing a proven and standard risk quantification methodology that can be leveraged on top of those frameworks.



LEARN MORE IN THE FAIR BOOK

**HOME**

**ABOUT**

**GET INVOLVED**

**LEARN FAIR**

**EVENTS**

**AWARDS**

**ADVISORS**

---

© 2019 FAIR INSTITUTE

[TERMS OF USE](#) | [PRIVACY](#) | [GENERAL MEMBER AGREEMENT](#) | [SITE MAP](#)