

# FAIR Summary

Understanding Factor Analysis of Information Risk

## Management doesn't care about security, they care about risk.

At the end of the day, the value proposition for security depends on its ability to affect the frequency and/or magnitude of loss (i.e., risk). As a result, effectively measuring and communicating this value proposition requires a clear understanding of the factors that drive risk. Enter FAIR.

### What is FAIR?

Factor Analysis of Information Risk (FAIR) is a framework of interconnected models that describe how key elements of the risk landscape work. Unlike other “models” used widely in the industry (e.g., ISO, NIST, CMM, COBIT, etc.) FAIR models describe the underlying dynamics of the complex risk landscape -- the why and the how. This underlying description enables meaningful measurement and analysis of the landscape in ways no other models being used today can.

Initially developed in 2001 and under continual evolution since, FAIR was created by a CISO who was trying to find a practical means of answering the questions executive management was asking:

- How much risk do we have?
- How much less/more risk will we have if .....?
- What are our most significant issues?
- What are the most cost-effective ways for us to spend our risk management dollars?

### Key features of FAIR:

**Quantitative** - Whether the bottom line is measured financially, in the availability of public services, or in some other metric, the decisions executive management makes are focused on growing and/or protecting their organization's value proposition. Consequently, in order for risk analyses to be truly meaningful, they have to express risk in these same quantitative terms. FAIR allows organizations to define and analyze quantitative value/loss metrics that are meaningful to their bottom line.

**Probabilistic** - Because the future is uncertain, any statement about the likelihood and consequence of a future event is uncertain. FAIR uses widely adopted methods to account for this uncertainty in its measurements and results, which means that analysis results are far more realistic. This not only means that management decisions are based on more useful information, but also that analysis results are viewed as more credible.

**Intuitive** - This isn't rocket science. In fact, people who are trained in FAIR find the models to be extremely logical and straight-forward. In addition, a common comment from highly experienced professionals is that FAIR aligns perfectly with how they intuitively think about risk, and is “the reference they never had before”. For the new professional, FAIR becomes a shortcut to understanding risk at a much more mature level.

**Flexible** - Nobody has the time to deeply analyze every risk issue they're faced with. Fortunately, FAIR's hierarchical models can be applied at any layer of abstraction, which means you can choose the depth of your analysis based on how much time is available, the significance of the problem being analyzed, or the nature of available data. In fact, most FAIR users find that more than 95% of their analyses are performed at a simpler, higher-level of abstraction, and that it's unusual to have to “get into the weeds” to get good results.

**Compatible with widely used security/risk standards and processes** - Many of the risk management standards and processes being used today call for risk quantification. Few, however, provide any useful guidance on how to actually quantify risk. FAIR fills these gaps by providing a clear definition of the elements that need to be measured, how to measure them, and how to derive a quantified risk result. Consequently, you don't have to scrap your investment in training and experience -- you can strengthen it.

**Agnostic** - Information security risk isn't the only form of risk that management is forced to deal with. Unfortunately, the methods used to analyze risk often differ from discipline to discipline, which makes it very difficult to compare analysis results. Although born within the information security world, FAIR models are agnostic and have been used to analyze a wide variety of risk issues. This agnostic characteristic means that FAIR can be used as a standard analysis method across disciplines within an organization, or as a normalizing layer to enable comparisons of results from different disciplines.

**Familiar to management** - One of the most common complaints is that "management doesn't get it". Our experience has shown, however, that management understands risk extremely well, and that the fundamental problem boils down to communicating about security and risk in terms that are familiar and meaningful to management. FAIR provides this bridge, and can dramatically improve the quality of dialog with management.

**Vetted** - In the years since its initial development, FAIR has been used daily by organizations large and small to help improve their risk management decisions and capabilities. During this time, FAIR models and results have been used and reviewed by senior business executives, actuaries, auditors, regulators, as well as experienced risk and security subject matter experts. The models also have been reviewed by academia, where a PhD in Quantitative Analysis described FAIR as the "codification of risk".

**Sophisticated** - It may not be rocket science, but it borrows from it. Under the covers, FAIR uses various highly sophisticated principles and methods, including:

- Bayesian belief networks similar to those used in a broad range of sciences,
- Monte carlo stochastic analysis to generate useful results with uncertain data, and
- Complexity Science modeling and sensitivity analysis to perform especially powerful what-if analyses

The good news is that FAIR methods and tools shield the practitioner from the complexity of all that sophistication -- unless, of course, the practitioner chooses to look under the covers.

### How FAIR is being used:

- Prioritizing risk issues
- Identifying and comparing risk mitigation cost-benefit propositions
- Sophisticated what-if analyses
- Business case development for security and risk management initiatives
- Strategy development
- Metrics development and analysis
- Risk and security program development
- Breaking down communication barriers between management and security
- **Enabling well-informed business decisions**