RiskLens

An Adoption Guide For FAIR

ENABLING COST-EFFECTIVE DECISION MAKING

BY JACK JONES
RISKLENS CO-FOUNDER,
CHIEF RISK SCIENTIST

WWW.RISKLENS.COM
THE LEADER IN CYBER RISK QUANTIFICATION

Table of Contents

INTRODUCTION	"Good Risk Management"	1
CHAPTER 1	A Very Brief Overview of FAIR	3
CHAPTER 2	A Foundation for Adoption	7
CHAPTER 3	Dimensions of Adoption	10
CHAPTER 4	Preparation	14
CHAPTER 5	Selecting an Initial Objective & Strategy	19
CHAPTER 6	Achieving the Initial Objective	23
CHAPTER 7	Potential Adoption Challenges	29
CHAPTER 8	Long-Term Integration	33
CHAPTER 9	Wrapping Up	37

INTRODUCTION

What Does *"Good Risk Management"* Look Like?

Is it a matter of scoring well relative to some industry control framework or NIST CSF, is it the percentage of an organization's operational budget that's spent on risk management, or perhaps it's the fact that an organization hasn't experienced a significant loss event to-date? Although there may be a relationship between each of these potential indicators and the efficacy of a risk management program, they are not the drivers of good risk management. If we pause to think about the fundamentals of "good management" — be it of risk or any other organization imperative — it begins with **well-informed decision-making** and **reliable execution**.

Factor Analysis of Information Risk (FAIR) enables well-informed decisions.

This is because every decision is essentially:

- A choice between two or more options
- Every choice involves comparing and making tradeoffs between the potential benefits, costs, and downsides of each option
- Every comparison involves measurement

So measurements of some sort (whether formal or informal) are at the root of every decision. The logical inference, therefore, is that better measurements enable better business decisions, which increases the odds of better business outcomes.

If we keep this in mind as we evaluate FAIR's value proposition, or as we go about the process of leveraging FAIR, we'll find several advantages:

- It provides an effective litmus test for comparing FAIR against traditional/common risk measurement practices — i.e., evaluating which approach is more likely to result in better-informed decisions, and why
- It helps us to recognize points of leverage — i.e., identifying decisions and/or decision-making processes that can benefit from FAIR analysis
- It provides a "true north", so-to-speak, as a reminder of the fundamental value proposition behind FAIR adoption. This is especially useful when adoption challenges arise, as they often do at some point in the adoption process

> **NOTE:** FAIR is focused on evaluating, measuring, and communicating the downside aspect of the business decision landscape. This is because well-established methods already exist for evaluating potential gains (e.g., revenue increases, etc.) and costs (both implementation and cost of ownership) associated with business decisions. What has been missing in the cyber, technology, and to some degree, in the operational risk domain, has been a clear, consistent, and pragmatic means of understanding the downside dimension so that appropriate trade-offs can be made.

THIS GUIDE'S PURPOSE

This guide is intended to serve two audiences:

1. Organizations that have already decided to adopt FAIR but are unsure of how to take the next (or first) step, will find helpful information to guide those decisions.
2. Organizations that are considering adopting FAIR will find insights regarding the adoption options and challenges if they choose to begin the journey.

Regardless of your need or purpose, what you'll find here are descriptions of adoption prerequisites, keys to short and long-term success, as well as use-cases, value propositions, and challenges. This information is based on the experiences of numerous organizations — of all sizes and from various industries — that RiskLens has helped to leverage FAIR successfully. Of course, not all efforts to adopt FAIR have been completely successful, and we'll discuss those as well to reduce the odds of your organization experiencing similar challenges (or at least to reduce their effects).

CHAPTER 1

A Very Brief Overview of FAIR

Because some readers may not be familiar with FAIR, this first chapter will provide a brief description of what FAIR is.

Readers who already are familiar with FAIR should feel free to skip to the next chapter.

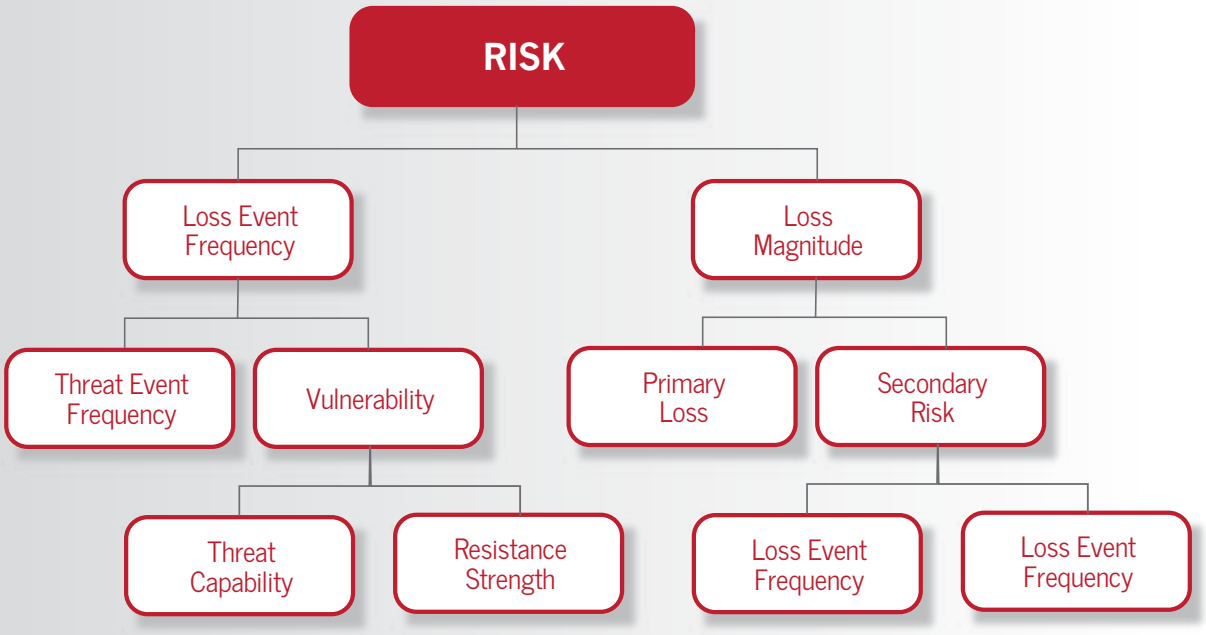
Complex Measurement

Risk is a complex measurement. By that we mean it isn't something that can be measured directly, like counting the number of chairs in a room. Instead, complex measurements involve deriving a value from two or more sub-measurements. Speed, for example, is a complex measurement in that it is derived from distance and time. Likewise, risk is derived from the probable frequency of loss and the probable magnitude of those losses.

When we have a lot of good empirical data regarding the frequency and magnitude of loss events it's relatively straightforward to derive what our likely future loss experience is going to be. This is the insurance industry's bread and butter. Unfortunately, measuring probable loss exposure becomes much more difficult when data is sparse and/or when historical data is of questionable value due to frequent changes in the risk landscape. In these instances, we're forced to derive risk by making informed and calibrated estimates of the factors that contribute to loss event frequency and magnitude. But what are those factors and, of equal importance, what are their relationships to one another so that we can derive risk effectively?

FAIR in a Nutshell: An Analytical Model

At its core, FAIR is an analytic model of the factors that drive frequency and magnitude of loss. As an analytic model, FAIR not only clearly defines the factors themselves, but also the relationship between those factors. This is analogous to the formula for measuring speed — i.e., speed = distance/time. The equation for speed identifies the factors (distance and time) as well as how they're combined (distance divided by time). Because of the complex nature of risk, however, FAIR defines several layers of sub-factors for risk (partial depth shown next).



These deeper layers are frequently necessary in fleshing-out critical assumptions and/or finding useful data to support risk analysis.

A Scoping Model

It's often not explicitly recognized, but even a measurement as simple as speed involves a second modeling component. For example, let's say we're wanting to measure the speed of cars on a racetrack. In order to end up with a measurement that others will understand, agree on, and can use, we have to first define the scope of the measurement — which car (or cars) are in scope? Are we measuring speed in a specific section of racetrack (e.g., corners versus straightaways) or over an entire lap? Are we measuring for a specific lap in the race or for the entirety of the race? Without this specificity, measurement results may not be accurate for their purpose, and someone else measuring the race is far more likely to have different results.

This specificity and clear measurement scope is particularly critical in risk measurement. Unfortunately, it's also typically missing from most risk ratings/measurements today. The FAIR model acts as a guide when fleshing out the scope of an analysis, and the analysis process used by FAIR-trained analysts places a very strong focus on ensuring that this second modeling component is well-defined.

What Happens Without FAIR?

A common question we hear is why something like FAIR is necessary. After all, cyber and technology risk professionals have been measuring/rating risk for a long time. Unfortunately, the vast majority of risk ratings/measurements that have taken place historically are based on the informal and uncalibrated mental models of the professionals. This informality and lack of rigor are largely responsible for the risk measurement problems we see repeatedly in organizations, including:

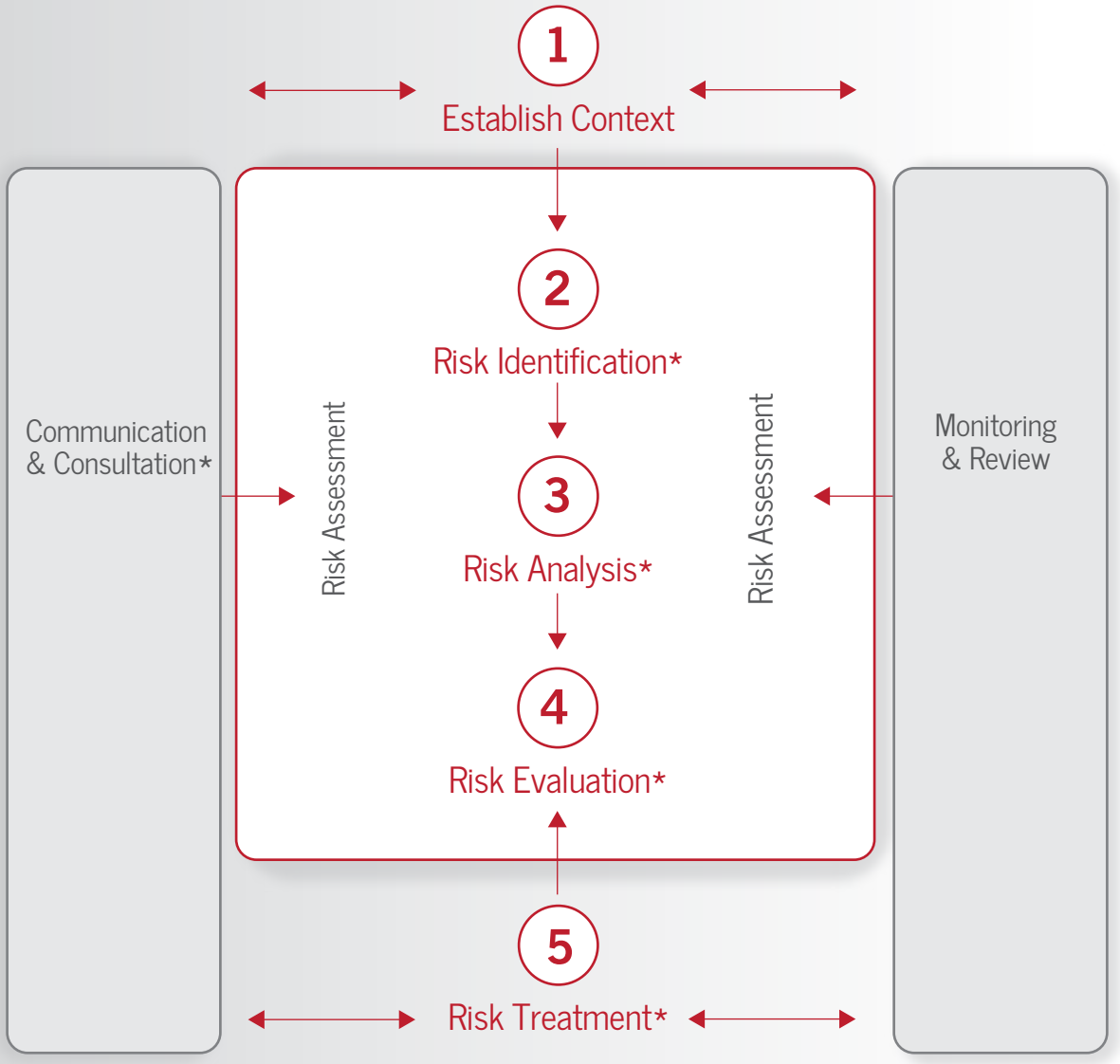
- Undefined and unexamined assumptions
- Inconsistent measurements when two or more professionals rate the same risk
- Introduction of personal bias and greater subjectivity in measurements
- Inability to express risk measurements in terms that are business-aligned or meaningful to executives
- Difficulty communicating to colleagues and management the rationale behind a risk measurement
- Inability to determine the cost-benefit proposition of risk management improvements
- Inability to effectively leverage risk-related data

The resulting unreliable and difficult to understand risk measurements prohibit organizations from identifying and focusing on their most important risks or knowing which risk management measures offer the greatest bang-for-the-buck. In other words, organizations end up making poorly informed decisions

What FAIR Isn't

FAIR is not a compliance or risk management framework, nor is it a list of controls best practices like NIST CSF, COBIT, ISO 2700x, PCI, COSO, etc. Those frameworks are useful for evaluating whether an organization is following best practices or meeting some industry standard. They do not, however, help an organization measure the loss exposure it faces from deficiencies that might be identified by using those frameworks.

FAIR is complementary to these frameworks by enabling organizations to measure the "so what" when deficiencies are identified and/or when improvements are proposed. The next image illustrates where FAIR fits into the risk management process defined by ISO 31000.



* *While FAIR is best known for helping people analyze risk, it can also be used for 1) risk identification (provides a consistent taxonomy and scoping model for defining risk); 2) risk evaluation (prioritizes top risks based on business impact); 3) risk treatment (helps people analyze the effectiveness of various treatment options); and lastly, 4) communication and consultation (provides the bases for a common reporting language, while articulating risk into monetary terms).*

CHAPTER 2

A Foundation for Adoption

"Adopting FAIR" means different things to different organizations.

This is appropriate given that organizations tend to have different needs, strengths, weaknesses, and cultures. For the purposes of this document, adoption will equate to operationalizing FAIR in some form — i.e., FAIR is baked into some aspect of how the organization manages risk. This could be relatively minimal and compartmentalized in nature, or deep and global, depending on an organization's needs, culture, and resources.

At the simplistic end of the adoption continuum are organizations that don't try to quantify risk and just leverage FAIR as a framework for understanding risk better, and as a way to normalize internal conversations about risk. At the other end of the continuum are organizations that quantify risk for all major strategic, and many tactical, decisions. Both ends of this utility continuum — and everything in-between — are legitimate examples of adoption. Because organizational needs vary, one of the objectives of this document is to help your organization identify which form/level of adoption is most appropriate, and therefore most likely to be successful.

Prerequisites for Adoption

Contrary to common beliefs (or fears), there are only two prerequisites to effectively adopting FAIR within an organization:

- At least one clear and specific value proposition for using it, and
- Critical thinking skills

We'll cover these elements in more detail below. For now simply recognize that successful adoption has absolutely nothing to do with an organization's size, industry, or "maturity." It also has nothing to do with how much data is available. Successful adoption only requires the two things listed above. Without them, an adoption effort will almost certainly fail.

A Clear And Specific Value Proposition

Newton's law of inertia applies to more than just physics. Organizations also tend to resist even relatively modest change unless there is a very clear value proposition behind it. Consequently, in order to embrace the kind of change FAIR represents, there has to be at least one clear and compelling reason. This isn't a problem for most organizations, as most organizations (if they're being honest with themselves) can identify multiple risk-related pain points that FAIR can help resolve. Examples might include:

- Inability to confidently identify their top risks
- An inability to measure and clearly communicate the cost/benefit proposition of cyber security and technology risk management efforts
- Difficulty communicating about risk with executive stakeholders
- Unproductive religious debates (internally, and perhaps with external stakeholders) about whether something represents high/medium/low risk

However, even when an organization recognizes high-level pain points such as these, it often isn't enough. In order to provide the necessary focus and support for change, organizations usually need a more down-to-earth and concise problem to solve. Before picking a problem to solve however, you'll want to gauge the organization's political and cultural landscape. Otherwise, you might choose a value proposition that, at least initially, isn't a good fit. We'll discuss this further in the next chapter.

Critical Thinking Skills

The cyber and technology risk landscape is complex and dynamic, with a lot of interdependencies and uncertainty. As a result, high quality risk analysis and measurement requires personnel who are able to decompose complex conditions into bite-sized chunks, view a problem from multiple perspectives, honestly question themselves, and accept the fact that uncertainty is always present. These are all characteristics of what's commonly referred to as critical thinking.

The good news is that the risk management and security professions are chock-full of incredibly intelligent people. The bad news is that intelligence doesn't necessarily equate to good critical thinking skills. Furthermore, many current practices in the security and risk management field (e.g., focus on compliance, superficial risk assessment and measurement methods, etc.) tend to atrophy the capabilities of people who might otherwise be strong critical thinkers.

The point is, strong critical thinking skills are far less common than you might imagine, and just because someone is a brilliant auditor, security architect, etc., they may not be well-suited or qualified to analyze and measure risk.

In order for an organization to effectively adopt FAIR, they have to ensure that personnel involved in risk measurement are strong critical thinkers. We have witnessed organizations fail at FAIR simply because they assigned people to the FAIR effort who weren't qualified in this regard.

Beyond the two prerequisites above, there are other factors that can strongly affect the level of effort and ultimate success of an adoption effort. Getting these wrong may not doom an adoption effort, but they can certainly prolong the effort, increase the levels of frustration experienced by those involved, and reduce the odds or degree of success. We'll discuss these additional factors throughout the remainder of this document.

CHAPTER 3

Dimensions of Adoption

You can characterize adoption as having three dimensions: **Scope, Depth, and Speed.**

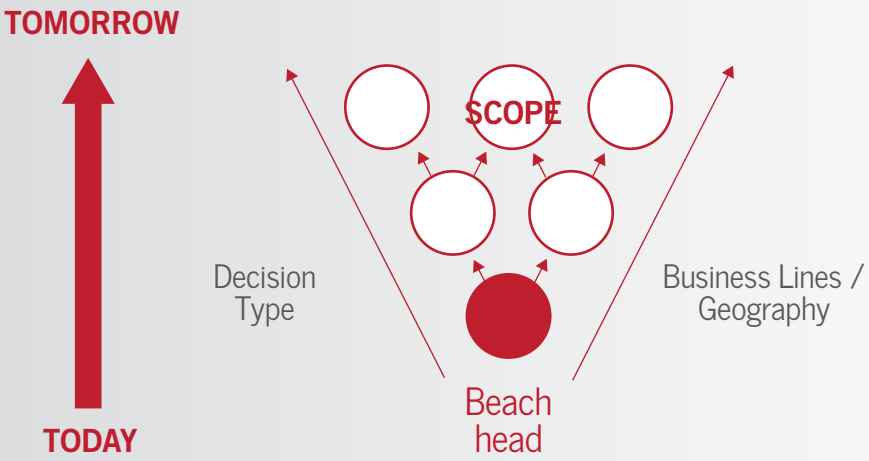
Within the context of FAIR, scope refers to how broadly FAIR is applied, depth refers to level of sophistication you apply when using FAIR, and speed is simply the pace of adoption. Understanding these dimensions within the context of your organization will allow you to define an adoption path that provides the best results at the least cost — both from a resource and a political/cultural perspective.

A rule of thumb to keep in mind is that broader and deeper adoption efforts typically introduce more cultural and political challenges. The trade-off, of course, is that the organization also realizes greater risk management benefits.

Scope

You may see FAIR as potentially forming the bedrock for risk decision-making throughout your enterprise. That said, organizational realities might make a more limited scope the right place to start. We'll get into more detail later about the cultural and political landscape around adoption, but for now simply recognize that success at a small scale can be a very powerful starting point for eventual "world domination" within your enterprise's risk management program.

This more localized starting point might take the form of just having your own team use FAIR, or it might mean using it throughout the enterprise but only on a single type of use-case (e.g., policy exception requests or cost-benefit analysis of risk management investments). If early adoption efforts within your organization are successful, the use of FAIR will grow over time.



> **NOTE:** Many RiskLens customers have found it useful to do a quick proof of concept or "pilot" FAIR analysis as a way to kick-start the adoption effort and demonstrate to internal stakeholders that high quality risk measurement is pragmatic and achievable.

Depth

You can define adoption depth as having five levels, which relate to how FAIR is used and the kinds of problems it helps solve.

Foundational

As you set (or reset) your risk management program with FAIR, your organization will begin to realize value even before you begin performing risk analyses. To begin with, having personnel trained in the FAIR model and principles will reduce risk-related confusion and noise related to imprecise terminology and uncalibrated mental models. Personnel are able to think and communicate more clearly about risk.

The advantage to this level of adoption is that it usually requires the least amount of up-front socialization and stakeholder support. The downside is that its benefits are not as strategic or profound, at least within the eyes of senior stakeholders.

Basic Triage

Although it is possible to quantify all of your organization's risk analyses with the aid of an enterprise-class software solution, many organizations can find great value in using FAIR to perform quick-and-dirty qualitative risk analyses. By using FAIR as the underlying framework for thinking through risk analyses, the odds of gross analytic error decreases significantly. One of the keys to being effective with this however, is to very clearly define the qualitative scales being used to measure the various risk factors.

Strong Triage

There's a tendency by those who are new to FAIR, to spend an inordinate amount of time trying to find hard data. The misperception being that without significant amounts of empirical data, quantification won't stand up. Fortunately, by leveraging well-established methods like calibrated estimation and Monte Carlo functions, you can do very effective and reliable quantitative risk analyses, very quickly. Even without empirical data, the results will be higher fidelity and more useful than qualitative values.

Quantitative Tactical Analyses

The scenarios you analyze at this level are for the most part the same as with Strong Triage. How much risk does this audit finding, that zero-day exploit, or that policy exception represent? How much less risk will we have if...? The primary difference between this level and Strong Triage is that at this level you more effectively leverage empirical data and security telemetry, and your analytic platform is much more powerful and efficient (i.e., Excel tools are no longer a realistic option). This greater analytic power and efficiency further improve the cost-benefit ratio of quantification.

Quantitative Strategic Analyses

Risk is a strategic concern for most organizations today, so the ability to measure and manage it well at that level can be a significant benefit. Examples of where risk quantification can make a strategic difference include, but aren't limited to:

- Defining and leveraging an economically defined risk appetite
- Identifying an organization's top risks

- Risk portfolio analysis
- Trend analysis
- Budgeting
- Sensitivity analysis
- KRI's and KPI's that are explicitly tied to risk appetite

These big picture capabilities help an organization gain a clear and explicit understanding of its risk landscape, and which levers can be used to greatest advantage in managing it.

Speed

When you understand the value proposition that FAIR offers, it can be tempting to want to make sweeping changes quickly. That's not always a recipe for success though, because existing processes and mindsets often resist change.

You should keep in mind that although benefits of better risk measurement can be realized quickly, it can take months — and in some cases, years — for organizations to fully evolve their approach to risk. The keys to long-term success are to be smart about where, when, and how you introduce change, and persistence.

As adoption of FAIR continues to spread globally, many of the challenges associated with adoption will diminish because the herding tendencies of our profession will switch from acting as inertia to be overcome, to a being a driver for change.

From a problem solving perspective, the first two levels of depth support clearer thinking and communication about risk, and improve high-level prioritization of risk-related concerns. Because the last three levels leverage quantification, they:

- Provide much better prioritization fidelity than can be achieved qualitatively
- Enable cost-benefit analyses
- Communicate risk in terms that are inherently meaningful to executives — i.e., FAIR's value proposition is more obvious to stakeholders.

CHAPTER 4
Preparation

A colleague recently shared the phrase, "Culture eats strategy for breakfast."

You can, of course, replace "strategy" with "logic," "rationality," or almost any other noun that might conflict with the subjective tendencies and group dynamics that make up an organization's culture.

The wisdom here is that you have to account for an organization's political and cultural realities in your efforts to introduce something like FAIR.

Another very applicable saying is, "It takes a village to raise a child." The point is that successfully ingraining something like FAIR (at least with any depth or permanence) always requires the support of multiple key stakeholders, especially if it's to become a foundational element of your risk management program.

Because of the two points above, socializing FAIR and gaining key stakeholder support are crucial, particularly if your adoption scope is broad and/or deep. The steps below provide an outline that has proven successful in organizations of various sizes and complexity.

Identify the Key Stakeholders

The first step is always to identify the stakeholders who strongly influence an organization's culture, particularly within the risk management domain. Don't make the mistake, however, of believing that these will just be risk management professionals. Very often, these can be business executives or leaders within the IT organization. It can also be people outside of the organization, like external auditors and regulators. If you're lucky, your organization will have formed a risk council made up of these executives, which can make identification easier.

By the way — there are stakeholders, and then there are "stakeholders." By that we mean that you can categorize stakeholders into two rough buckets — those at the top of the house (CFO, CEO, COO, head of Internal Audit, CRO, CIO, etc.), and those below that level but who wield influence. You'll want to be aware of who the players are in both of these buckets.

Common Risk Council Membership

- *Internal Audit*
- *Compliance*
- *Operational Risk Management*
- *IT Leadership*
- *CISO*
- *Technology Risk Management*

Once you've identified the players, it can be helpful to find out where they stand in the pecking order. This may or may not align perfectly with formal reporting relationships, as sometimes you'll find someone a couple of levels down from the top who wields a lot of influence due to their personality, expertise, or personal relationships.

If possible, it can also be helpful to find out which ones have a particular interest in risk. Some of these will be obvious, but some less obvious executive roles might also have a strong interest because they have significant risk-related pain (e.g., constantly missing audit finding closure deadlines, etc.).

Socialize & Demystify

After identifying the stakeholders, you'll want to begin having conversations with them. If your title/position in the organization doesn't provide you with access to those executives, then you need to gain the active support of someone who does.

There are three primary objectives of these discussions:

1. Identify potential supporters/advocates and the risk-related pain points FAIR can help them with
2. Identify potential opposition to using a more formal approach to risk measurement like FAIR
3. Familiarize them with FAIR, and begin the process of socializing its benefits

Very often, the executives you speak with will not have heard of FAIR.

As a result, there are a set of common questions they're likely to ask:

What is FAIR?

FAIR stands for Factor Analysis of Information Risk. Simply stated, FAIR is a risk model that clarifies and simplifies risk analysis and measurement.

Is FAIR only applicable for quantitative analysis?

FAIR can be used to perform qualitative analyses more effectively, or for measuring risk quantitatively.

Is FAIR credible?

Yes, FAIR has been in use for years and has been closely evaluated in academia, by regulators, and by experts in other risk domains (e.g., actuaries and underwriters). It has also been adopted by the Open Group, an international consortium, as an open international standard for risk measurement, and is being taught in numerous universities as part of the cyber risk curriculum. Many business executives also welcome the fact that FAIR leverages methods they probably were exposed to in a graduate degree program (e.g., decision support methods, Monte Carlo functions, PERT distributions, etc.).

Who else is using FAIR?

FAIR is being used by organizations of all sizes and in virtually all industries, including the government.

Does it replace what we already do?

FAIR is complementary to most of the risk assessment frameworks and processes currently in use (e.g., NIST CSF, ISO, COBIT, COSO, etc.), by filling a gap that those don't cover. Specifically, those frameworks are designed to identify risks and control deficiencies, but they don't provide a means of measuring how much risk exists.

What's wrong with how we've been measuring risk?

Most executives assume that the qualitative risk statements they've been getting are accurate. They don't realize that the scope of what's been measured is rarely clearly defined, that the models used to arrive at the measurements were unexamined mental models, and that the definition of high/medium/low is rarely clearly defined. As a result, the risk measurements they've been relying on are, in fact, unreliable. That said, it can sometimes be counterproductive to come right out and say this. Very often, it's more effective to refer to FAIR adoption as "a refinement" or "supplement" to current measurement practices. Advocate evolution versus revolution.

Why bother (or, what's in it for me)?

The best answer to this question depends in part on what their needs and interests are. Our experience is that executives who aren't happy with how risk is currently being managed can be your best allies because they're looking for change. Find out what those pain points are and describe how FAIR helps relieve their pain. Sometimes the pain is very specific (e.g., unsatisfactory board reporting, requirements imposed by regulators, or being buried in "high" risk), while other times it's simply that cyber and technology risk is an inscrutable problem they can't wrap their heads around.

Opportunities & Challenges

In most organizations, if one executive is experiencing serious pain with the risk landscape, others are feeling it too. Consequently, as you have conversations with the stakeholders, listen for themes that may lead you to a particularly meaningful value proposition (meaningful in the stakeholder's eyes).

You'll also want to listen for themes that suggest there are common concerns related to FAIR adoption. If there are, then you can be more strategic in addressing those concerns. With that in mind, we'll share that although almost every business executive we've worked with has been readily enthusiastic about the potential benefits FAIR offers, executives from the risk management domain (e.g., internal audit, enterprise risk, operational risk, technology, security, etc.) have sometimes needed more help releasing old habits.

The reasons have included:

- FAIR challenges their world view and what they're familiar with (e.g., "It's all about compliance")
- They prefer cyber risk to be mystical in the eyes of business executives
- They view the world as being purely black and white (the opposite of critical thinking)
- They feel invested in traditional methods and/or are more comfortable following the "herd"
- They've bought in completely to fallacies and misperceptions about risk measurement and quantification

Some of these can be overcome by patiently educating the individuals. Others will melt away as the profession (the herd) continues to migrate toward risk quantification. Others, we're afraid, (e.g., the folks who view the world as black and white) may never come around. The better option is to position FAIR as complementary to, or at least not incompatible with, their world view. Focus on your allies, and let time and success win the others over.

CHAPTER 5

Selecting an Initial Objective & Strategy

If the initial adoption effort extends beyond your immediate sphere of control and influence — and especially if it involves risk quantification — then your objective and strategy need to be selected with a clear understanding of who your stakeholder champions are and what they care about.

Figuring this out may be relatively simple based on just an initial dialog with the stakeholders, or it may take multiple conversations. Take as much time as required to be confident in your initial objective and strategy because an initial failure can make subsequent efforts more difficult.

There are two primary considerations when selecting a starting point for adoption that has executive visibility: **meaningful results, achieved quickly.**

Meaningful results simply means demonstrating how FAIR relieves risk-related pain that one or more key stakeholders care about.

Most often, this means that FAIR analysis results are valuable in making one or more decisions. Getting a quick win is important because a clock starts ticking as soon as you get the go-ahead. This clock represents a sort of "expiration date" before interest and support begin to wane as other imperatives tug at stakeholder attention. Taking too long also might leave stakeholders wondering whether FAIR is too difficult (pro tip: it isn't!). As a result, whatever you choose for an initial objective should be something you can confidently achieve relatively quickly.

A useful rule of thumb is to demonstrate meaningful value in less than 90 days. And if you have any experience at all with project management you'll know how important it is to account for potential delays, so don't push your luck timing-wise.

The following are some examples of relatively short-term analytic efforts that organizations have found value in.

Cost-Benefit Analysis of a Major Risk Management Investment

We have yet to encounter an executive who wouldn't like to know how much risk reduction they're getting for their investments in risk management technologies, processes, policies, etc. As a result, this can often be an ideal starting point for FAIR. Something to keep in mind however, is that you can't do a cost-benefit analysis using qualitative measurements — at least not one that will stand up to scrutiny.

Comparing Risk Management Investments

This is a step beyond the basic cost-benefit analysis because it requires that cost-benefit analyses be performed against two potential solutions to a risk management objective. Note that if you're going to go this route, the solutions you're comparing probably should be quite different in nature (e.g., comparing encryption of data at rest versus two-factor authentication). You aren't likely to see a material difference if you compare two similar risk mitigation approaches (which could be useful, of course, if the costs for the two solutions are significantly different).

Pure Risk Reduction

Some organizations have started out by telling the stakeholders that within 90 days they'll use FAIR to identify a practical means of driving $1M (or whatever amount) of loss exposure out of the organization's risk landscape. This is a relatively open-ended promise that can certainly get attention, but that shouldn't be gone into blindly. If you're going to use this approach, you need to be sure to do your homework so that you are absolutely confident in hitting a home run. If you nail it though, support for further adoption would likely be assured.

Swamp Draining, Part 1: Cleaning Up the Risk Register

Most organizations use some form of application, database, or spreadsheet to record and track their risk-related concerns. However, these "risk registers" are often misused and can generate more noise than value. This is particularly unfortunate because it impedes the organization's ability to accurately identify and communicate top risks to executives and other stakeholders.

You can apply FAIR as a framework for sifting through the contents of the risk register to identify which entries are, and are not, risks. Once that's done, you can perform a basic triage on the risks to at least identify which risks fall into high/medium/low buckets. This can be incredibly clarifying for organizations that have succumbed to and feel overwhelmed by the noise that many risk registers suffer from.

If you wanted to take the next step (and if you have time), you can then do a quantitative analysis on the risks in the "high" bucket, which can help validate and communicate their significance for stakeholders.

Top Risks

Identifying and quantifying an organization's top risks should be an objective within any risk management program, and a foundational element in the board report. For those organizations that maintain a risk register, this can be seen as a natural extension of the risk register cleanup objective described above.

Note that quantifying an organization's top risks is likely to take longer than 90 days to complete unless it's treated as a top priority.

3rd Party Risk

Most organizations of any size have hundreds or even thousands of 3rd parties that are connected to them through the network, have access to sensitive information, and/or provide critical services. It's also common for organizations to be managing that herd of cats using questionnaires.

Whenever severe deficiencies in security and risk management conditions are identified at 3rd parties, an organization is forced to decide how much pressure to apply to the 3rd party, or perhaps whether to maintain the relationship at all. When faced with this problem it can be very helpful for the business executives to understand how much risk the deficiencies actually represent. FAIR can be used qualitatively (or quantitatively) to evaluate and communicate the risk associated with a laggard 3rd party so that business executives can more confidently address the concerns

CHAPTER 6

Achieving the Initial Objective

Once you've chosen an initial objective and socialized it appropriately, the rest is all about strong execution.

What this looks like will vary depending on the scope and level of depth you're starting out with. The one constant, irrespective of scope/depth, is that you always start with training and education.

FAIR Training & Education

There's a difference between being educated about FAIR, and being trained in it. Education means you understand the framework, terminology, and principles, while training means you're able to apply FAIR competently. We mention this because an adoption effort should entail both education and training.

For personnel who will be performing risk analysis and measurement, training should be considered essential. You can become educated about FAIR and get a head start as an analyst from reading the FAIR book*, but that isn't going to be sufficient for most people to reach competency as analysts.

Organizations that are strengthening their risk management programs using FAIR typically engage RiskLens to conduct onsite training. There is also a self-paced online training program through RiskLens that is a good alternative for individuals, smaller organizations, and organizations with geographically dispersed personnel.

Personnel in your organization who won't be performing FAIR analyses, but who will be contributing data, using the results to make decisions, or keeping an eye on how it's being used, should be educated in the basics as well. Examples of personnel who typically fit in the education category includes auditors, senior network, application, and system technologists, as well as members of the compliance and operational risk organizations.

This is usually as simple as a four-hour workshop where they learn about the FAIR model, terminology, and analysis principles, and where misperceptions are cleared up. Or, of course, they could read the book.

An even more condensed version of the education material should also be provided to key executives. This can take as little as an hour or as long as two hours, depending in large part on their availability.

Speaking of Resources...

Effective risk analysis requires personnel who are strong critical thinkers, have a grasp of basic probability principles, and are comfortable with numbers. Larger organizations may not have the bandwidth or the people on staff that have the necessary skills to get the FAIR-based risk management program off the ground in the desired timeframe. Consultant retainer services and staff augmentation from RiskLens can be a good bridge to enable quick results as internal resources come up to speed.

Some mid-sized and smaller organizations have no intention of doing FAIR analyses themselves, preferring to outsource that responsibility. This can be a good option, but they'll want to be sure that the personnel they engage to do FAIR analyses are well-qualified. Fortunately, these resources are becoming more available all the time, and some consulting practices are building out FAIR-based services just for this purpose.

Software

If your organization's objective is to leverage quantitative risk measurement, including strong triage, or quantitative tactical or strategic problem solving (e.g., cost-benefit analyses, portfolio analysis, etc.), then risk analysis software is in your future. The question then becomes, what type of software?

Free tools such as the FAIR-U training app or Excel-based home-grown solutions are a good way to learn FAIR **but do not scale to the needs of enterprise-level analyses and do not include enterprise-grade security features.** Similarly, traditional GRC tools **do not natively include robust risk analysis capabilities.**

An enterprise-ready solution needs to natively embed not just strong security and mathematical simulations such as Monte Carlo, but also a variety of advanced reporting features such as risk aggregation, trending, what-if analysis, and sensitivity analysis. In addition, features that drive greater efficiency are crucial, such as data libraries, guided data collection workflow, APIs to GRC tools, and the list goes on...

For enterprise capabilities, your organization is going to need to use RiskLens. It's the only available commercial solution purpose-built on FAIR, and it has the advantage of having been in the market and constantly evolving through collaboration with its customers — which includes many of the world's leading companies.

Project Management

For any adoption effort that has a broad scope and/or a depth greater than basic triage, you'll want to leverage typical project management processes to help ensure success. Having a dedicated project manager greatly enhances chances of success of your initiative.

Don't make the mistake we saw one organization make, where they seemed to believe that because this was "just a change in how we measure risk" they didn't treat the effort with any rigor. The project went more slowly and painfully than it needed to.

Data

Similar to software, this aspect of adoption is a bigger deal when you're going to quantify risk. Yes, you need to consider data at any depth of adoption, but it warrants special attention and discussion when you're quantifying risk. We discuss this elsewhere in this document as well, but for the sake of thoroughness we're also going to cover it here because it can be such a critical concern when an adoption program is just starting out. When it comes to data, do not let "perfection become the enemy of good." If you aren't familiar with that phrase, in this context it means that you absolutely have to resist the urge to have "enough" data — at least "enough" as described by those who don't understand the real world of risk analysis. Yes, having lots of data can be helpful and can improve the precision of your analyses. But high precision isn't the point; accuracy is.

We learned this from the actuaries, underwriters, and scientists we've worked with, and it's discussed in the book on FAIR, in numerous FAIR Institute blog posts, and in Douglas Hubbard's books, so we're not going to get into the details here. The bottom line is that we have witnessed analysis efforts get needlessly bogged down because someone insisted that they needed hard data, when in fact they could get very good analytic results by leveraging calibrated subject matter expert estimates using very little (and in some cases, no) hard data.

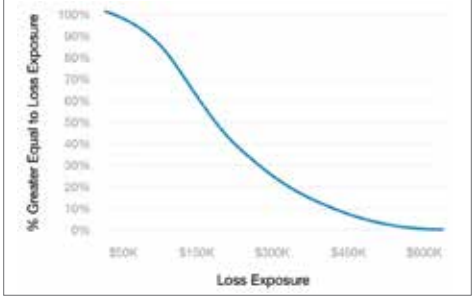
Just keep in mind that for most analyses, diminishing returns happen very quickly in terms of data volume versus analytic quality.

Reporting & Decision-Making

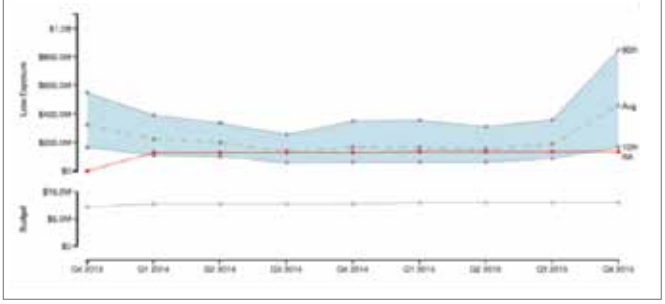
FAIR's ultimate purpose is to help organizations make better-informed risk-related business decisions. This is crucial to keep in mind because your initial adoption effort should clearly demonstrate that value proposition. Ideally, at the end of the initial effort, analysts, decision-makers, and stakeholders should be able to say without hesitation that FAIR's value has been proven in that regard.

In order to help achieve this, you should make it an explicit focus of the report to stakeholders. Call out the difference between the type and quality of information being delivered using FAIR from what has been available in the past.

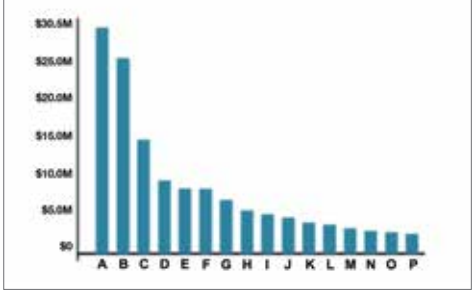
LOSS EXCEEDANCE CHART



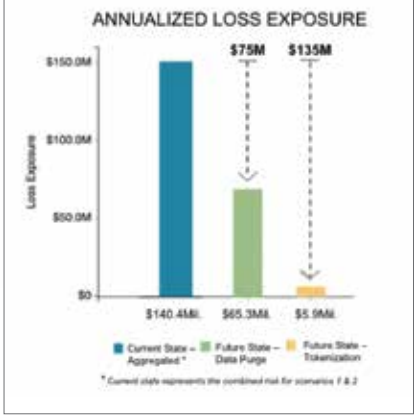
HOW IS RISK TRENDING VS. APPETITE



WHAT ARE OUR TOP RISKS?



LOSS EXPOSURE REDUCTION



Loss Exposure Reduction - By How Much Can We Reduce Risk By Implementing Certain Controls?

One last thing to be aware of when delivering the very first FAIR analysis results is confirmation bias. This form of confirmation bias occurs when someone looks at the analysis results and says, *"Yeah, that's what I would have come up with too, but without all of the analytic effort."*

What they fail to grasp are several things:

- The fact that actual analytic rigor was applied means the results are far more likely to stand up to scrutiny.
- If quantification was used, the results can be leveraged to answer cost-benefit questions, they can be aggregated with other analytic results, and the uncertainty in input and output values can be faithfully represented. The results can also be validated or adjusted through logical and rational probing. None of these are available from their wet finger in the air.
- Perhaps someone other than themselves would have been responsible for waving a wet finger in the air and perhaps that person would have come up with different results (again, because no rigor or normalized analytic framework had been used).

If someone makes this kind of claim, it's a clear sign that additional education is called for because they don't understand the nature of risk analysis and measurement.

CHAPTER 7

Potential Adoption Challenges

This chapter covers some of the more common and significant challenges organizations can run into when adopting FAIR.

Misperceptions About Risk Measurement

It is remarkable how many people still believe the old wives tale that cyber and technology risk can't be quantified. This myth originated when people attempted to quantify risk without first having the model for risk analysis that FAIR provides, and without leveraging modern measurement and analytic methods like calibrated estimation, PERT distributions, and Monte Carlo functions. Without those as a foundation — the skeptics are right — you can't quantify risk. Fortunately, the foundation exists now, so those concerns can and should be put to rest. You can anticipate, however, that you will run into this belief at least once in your adoption effort so it's important to be prepared to answer this concern, particularly if the person who has this misperception is a key stakeholder.

> **LEARN MORE:** Check out "An Executive's Guide to Cyber Risk Economics" eBook by Jack Jones, FAIR Institute Co-Founder and Chief Risk Scientist.

Churn

We've seen churn challenge adoption efforts more commonly than any other issue — the champion behind FAIR adoption gets lured away to another company. This, however, was before our customers figured out the importance of the "It takes a village..." principle. The simple fact is that churn happens, and the best way to make an adoption effort resilient to churn is to have more than one executive championing it. The more, the better.

Another churn-related problem can arise if an organization only has one FAIR-trained analyst. These people are increasingly in high demand, and we've seen adoption efforts stall when an organization's one-and-only analyst gets lured away to another company. Until there are more qualified analysts in the market, the solution here is to have more than one qualified analyst on staff, or to temporarily bring in a qualified consultant until you find a replacement.

Unreasonable Expectations

There are two principles that we've found to be very important when setting executive management's expectations regarding risk measurement:

1. You get what you pay for
2. Law of diminishing returns

You Get What You Pay For

Most organizations are used to a near zero cost for risk measurement. Someone simply proclaims a concern to be high/medium/low risk based on their gut, and that's that. It happens in an instant, there's no explicit scoping of what risk scenarios are/are not relevant, which threat communities are/aren't relevant, or which controls may/may not be in play. Essentially, there's no critical thinking, analysis, or cost involved. Because the risk landscape is complex and dynamic, the odds of a measurement like this being accurate is about what you'd expect given the lack of rigor. Unfortunately, this is what people are used to, which means it's an expectation you often have to adjust.

Bottom Line:
FAIR-based risk analyses require some level of rigor, dedication and effort.

Make sure that your budget contemplates the appropriate resources to make your FAIR initiatives successful.

Diminishing Returns

This principle is a counterbalance to the one above. Very often there's a belief that you must spend weeks or months gathering hard data in order to perform reliable quantitative risk measurement. Fortunately, that's not the case. Thanks to methods and tools like calibrated estimation, PERT distributions, and Monte Carlo functions, you can make excellent use of limited data and even subject matter expert estimates. Douglas Hubbard discusses this at great length in his book, *How to Measure Anything*, which is highly recommended reading.

The level of effort in risk measurement can be reduced even further, and analysis quality improved, with a well-designed software application like RiskLens provides.

Low Expectations & Entrenchment

It's unfortunate, but many executives have become acclimated to heat maps, thinking that's as good as it gets from a risk measurement perspective. Until they know that strong risk measurement is a pragmatic option, and understand the value it brings, they aren't going to ask for it. In some organizations this is a problem because the political and cultural climate is so entrenched that until change is called for by the top of the house, no change is going to occur.

This can be especially challenging to overcome if one or more of the people at the top of the house are the ones so firmly entrenched, because they often feel threatened by change. If this is the case where you work, you'll want to tread carefully and find influential allies.
In some cases, that might require choosing evolution versus revolution — feeding those heat maps for a while with more rigorously developed data and supplementing specific reports with quantitative highlights until stakeholders appreciate how a financial measure of risk can enable cost-effective decision making.

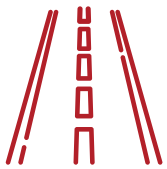
Incidents

Another potential adoption-killer is if an organization experiences a major breach. When that happens in an organization that doesn't really understand FAIR's value, then focus can become hyper compliance-focused. The result is a tendency to "fix everything at once," which is rarely effective and never cost-effective.

The best way to protect against this is to ensure that executive management truly understands FAIR's value proposition. This includes making sure they understand that measuring risk well, and being cost-effective in risk management is not the same thing as having no risk. Loss events can still occur — even large ones. Better risk measurement simply reduces the odds and improves efficiency.

CHAPTER 8

Long-Term Integration



With the success of your initial project, the goal becomes operationalizing FAIR as a cornerstone of your risk management program so that the organization can leverage FAIR more broadly, consistently, and efficiently.

This also helps to make its use resilient to changes in personnel and leadership.

Baking FAIR Into Operational Decision-Making Processes

Established business processes exist to ensure consistency, reliability, and efficiency (at least in theory). Regardless, because they are operationally embedded, those processes that involve decision-making can be an ideal opportunity to broadly leverage FAIR.

Some examples include:

- Policy exception requests
- Change management
- Patching prioritization
- Project management
- Technology/application design reviews
- Merger and acquisition process
- Annual budget allocation turf wars

For some of these especially, it's important to keep analyses as streamlined as possible. Do not let FAIR become a boat anchor to the process. Some of these should be more triage-like analyses that help the organization gauge whether something deserves deeper analysis and attention.

Swamp Draining, Part 2

This one could easily fall into the decision-making process section above, but because it's associated with the risk register cleanup discussed earlier we thought it deserved to be highlighted here.

Many organizations have to wrestle with vast numbers of "risks" that have accumulated over time in their risk registers.

Cleaning up this mess is a two-part process:

1. Dredge through the existing muck (which was part 1)
2. Improve the quality of what gets added going forward (this part)

As audit findings, security test results, regulatory exams, annual risk assessments, etc. take place, you can use FAIR to validate whether something gets added to the risk register, and with an appropriate level of attention, or is added to a separate tracking mechanism. This can help your organization remain focused on the things that matter most.

Increase Visibility at the Top

This one is easy to understand. Once senior executives become accustomed to quantitative risk reports (or qualitative reports that are supported through quantitative analyses), they'll never choose to go back. When combined with leveraging FAIR on strategic issues (discussed below), integration is about as permanent as you're going to get.

Pursue Strategic Use-Cases

This often is tied to the point above regarding top-level visibility, because when an organization is using FAIR to answer big picture questions, it's a very strong indicator that stakeholders understand its value proposition and that it's there to stay. It also almost always means that the organization has already integrated FAIR at lower levels of adoption, because it's often not practical to start at this level.

Examples of strategic use-cases include:

- Measuring and managing aggregate loss exposure at an enterprise and/or business unit level
- Leveraging sensitivity analysis to identify an organizations most cost-effective risk management opportunities
- Trend analysis
- The annual budget allocation process
- Reporting to the board of directors
- Defining and managing to a quantitatively expressed risk appetite

Develop In-House Expertise

Now that your organization takes risk measurement seriously and isn't relying on traditional zero-cost low reliability wet fingers in the air, it faces the question of when and where to use internal versus external resources for risk measurement.

For some organizations the answer is simple — they have the resources to hire dedicated risk analysis personnel. Smaller organizations, or those that choose to primarily use FAIR in a less sophisticated mode, have an alternative. They may choose to train one or a few people in FAIR, and have those people use FAIR at the simpler levels of adoption for day-to-day triage, and then outsource deeper analysis to qualified contractors on an as-needed basis.

Regardless, if your organization is going to adopt FAIR then it needs someone in-house who knows it well, if for no other reason than to ensure that contractors doing analyses for you are generating quality work.

Manage Risk Analysis Quality

Because FAIR analysis helps to inform real-world decisions, good quality is crucial. Ideally, no analysis should be considered complete without at least one extra set of eyes first looking it over critically. In many cases, more than one person will contribute to the analysis anyway, which helps to reduce the potential for significant error, but sometimes analysis resources and time are scarce.

In these cases, peer reviews — particularly if it's a complex analysis — are golden. It should be obvious, but whoever's doing the peer reviews also needs to have been trained and experienced in using FAIR.

If it isn't feasible to have every analysis double-checked, then a selective and/or periodic review process should be implemented where especially complex or important analyses are reviewed. As reviews take place and mistakes are identified (as they will inevitably will be from time to time) it's important to do a root cause analysis. Does the person who performed the review need additional training? Were they given bad information? Do they have the innate skills to do this kind of work well?

A quality management process we've seen work well in larger organizations is to have regular (e.g., weekly or monthly) lunch meetings where people bring particularly tough or interesting analysis they're working on for group brainstorming/feedback. It's a great opportunity to learn from peers and continually improve everyone's skills and identify areas where data collection can be improved.

It can also help to have a formally (or informally) identified internal FAIR expert who others can turn to for help with tougher analyses. In larger organizations, these people might also play a role in training newcomers to the team as growth or churn takes place.

Another great opportunity for continued improvement and quality control is for personnel to take part in local FAIR chapter meetings, which is part of the FAIR Institute community. In these meetings they'll be exposed to experts and other analysts, evolving methods, and interesting analyses. If there isn't a chapter in your location, consider starting one.

Learn more about the FAIR Institute and its active community by visiting **www.fairinstitute.org**

CHAPTER 9

Wrapping Up

FAIR can result in profound improvements in an organization's ability to make well-informed decisions, which equates to a far more effective risk management program.

That kind of significant change, however, also means that adoption is often not a trivial matter.

In order to achieve success, you need to:

- Understand who the key stakeholders are and what they care about
- Socialize and demystify quantitative risk analysis and FAIR in the eyes of key stakeholders (and anybody else who has influence)
- Design an adoption strategy that is meaningful to stakeholders and achievable within the context and constraints of your organization's culture, politics, and resources
- Commit to your adoption strategy
- Educate and train the people who will be involved in the use of FAIR or who will use its results in decision-making
- Avoid common mistakes that can slow down or hurt an adoption effort, and
- Identify and leverage opportunities to integrate FAIR for the long-haul

This is fairly simple, but not necessarily easy.

Your organization's culture may be primed for this type of evolution, or not. In either case, it is possible for FAIR to gain a foothold and provide increasing amounts of value over time if you're strategic in your approach.

The good news is that you're in good company. The pace of FAIR adoption is growing rapidly, which means that you're less likely to have to forge new ground and the herd adoption tendencies of our profession will begin to work in your favor. Furthermore, a growing number of board members, business executives, regulators, auditors, and chief risk officers are becoming aware of FAIR and its benefits, and these stakeholders are raising the bar for their organizations.

RiskLens continues to help a growing number of large enterprises, government organizations and risk consultancies develop their expertise in building quantitative risk management programs based on FAIR. Through its sponsorship of the FAIR Institute and as its Technical Advisor, RiskLens contributes to the advancement of our profession by sharing its expertise with the wider market and by incorporating new advancements in its software solutions and training programs.

Resources & References

Measuring and Managing Information Risk: A FAIR Approach.
(Jack Jones and Jack Freund). Available on Amazon (http://amzn.to/2pXshs0)
in both softcover and electronic form.

The FAIR Institute (www.fairinstitute.org)
Blog posts, white papers, working groups, community forum, training software, annual conference.

RiskLens, the leading provider of cyber risk quantification solutions built on the FAIR method.
For more information, visit www.risklens.com.

An Executive's Guide to Cyber Risk Economics
eBook by Jack Jones, Co-Founder and Chief Risk Scientist of RiskLens. Available for download here

---

The Open Group online (https://www2.opengroup.org/ogsys/catalog/C13K)
Training and reference materials, a professional certification in FAIR,