CHAPTER 5

Manage Risk in the Language of Business

For too long, information risk management has been lost in translation. Technical risk analyses were unintelligible to the business and even security practitioners lacked common terms, definitions, or analysis models. Without a working risk management framework, security and business leadership have found it hard to agree on priorities, policies, or budgets. Even security teams struggle prioritizing which controls to implement.

But this need no longer be the case. In this Chapter, we’ll learn how businesses can use the standard ISO 31000 Risk Management framework, and Open Factor Analysis of Information Risk (FAIR) models as the basis for a comprehensive set of well-aligned processes. Using quantitative criteria such as the monetary value of loss events and the probable frequency of occurrence makes it easier to roll information risks up into the enterprise risk map and report them in the language of business, i.e., dollars, pounds, euros, rupees, etc. We will also discuss ways to assess risk efficiently across a broad class of issues and assets throughout the organization.

Using these recommendations, businesses can

- Understand and employ risk management framework standards
- Establish the context for the risk program (and gain stakeholder buy-in)
- Implement a tiered risk assessment process (and weave it into IT and the business)
- Perform enterprise risk assessments to identify top risk scenarios
5.1 Address Common Challenges

Despite the availability of standards, the industry still struggles with risk management. And yet risk is the reason we have cybersecurity programs. Challenges include

- Lack of consistent information risk terminology and alignment with other enterprise risk domains
- Unrealistic expectations and ineffective risk analysis methods
- Myopic focus on control assessment while ignoring other risk treatment options
- Analysis paralysis and uncertainty about where to start

5.1.1 Lack of Consistent Information Risk Terminology and Alignment with Other Enterprise Risk Domains

Definitions for key risk terminology – particularly “risk,” “threat,” “vulnerability,” and “impacts” – are found in various security standards, guidelines, and other writings. However, these definitions vary widely. Without consistent terminology, business and security teams cannot be certain they are even communicating about risks – let alone develop effective risk treatment programs.

Worse, in some organizations, security staff seem to be running around with the proverbial “hair on fire” syndrome. They treat every single risk-related issue (e.g., vulnerability, threat or pen test report, compliance gap, etc.) as if it were a clear and present danger before even analyzing the business risk scenarios.

Information risk encompasses both true cybersecurity risks from cyberattackers acting on vulnerabilities and IT operational risks from operator error or IT component breakage. Due to its complexity, businesses need security and risk professionals to perform the analyses. However, as discussed in Chapter 1’s section “Taking Accountability for Risk,” business leaders need to understand information risk in
business terms. Information risk must also be quantified, like financial risk, to roll up from the security organization to the business level.

Fortunately as we’ll discuss in section “Understand and Employ Risk Management Framework Standards,” the industry has solutions that businesses can adopt for a consistent risk management vocabulary.

### 5.1.2 Unrealistic Expectations and Ineffective Analysis Methods

Many people who don’t understand cybersecurity believe businesses should try to avoid or prevent all information risks. Such thinking is valid for life-or-death safety objectives, but many other security objectives should be balanced against the costs or other business impacts of the required effort. It’s critical to have an objective framework for such analysis.

Businesses often employ ineffective qualitative methods for risk analysis, and it is still somewhat unusual to find a business using a quantified risk appetite agreed between stakeholders to identify what types and levels of risk are acceptable. Qualitative risk analyses assign ratings such as “low,” “medium,” and “high” or numerical risk scores. The analyses may rely entirely on subjective criteria, and even expert analysts may have cognitive biases. When business and security leaders can’t agree on a transparent and objective method for evaluating risk, communication is difficult.

When expectations are unrealistic and risk analysis processes poorly defined or lacking objectivity, it should be no surprise that the results can be difficult to defend. Business executives will often ask security leaders to present on risk and then challenge the output: “What’s in that yellow dot on the heat map anyway?”

As Jack Jones, Chairman of the FAIR Institute, likes to say, “For most companies, security spend is like the advertising budget. You know you’re wasting half of it; you just don’t know which half.”

### 5.1.3 Myopic Focus on Control Assessment While Ignoring Other Risk Treatment Options

Often cyber-risk teams focus on risk mitigation using controls for reducing risk to the exclusion of other risk treatment options such as avoiding, accepting, disaggregating, or transferring risks. Risk assessment becomes little more than control assessment in which the lack of a control, such as data-at-rest encryption, is automatically assumed
to be a risk. Although that isn’t always untrue, it can cause businesses to misjudge both the amount of resources required for cybersecurity and how to allocate those resources. Fortunately, the risk program can incorporate tiered risk assessment methods to triage out unimportant issues, and a holistic risk treatment program can consider all the options to help the business conserve and prioritize resources.

5.1.4 Analysis Paralysis and Uncertainty About Where to Start

In a FAIR Institute risk management maturity survey, only 17% of respondents report having strong risk analysis or assessment practices. Reviewing this survey, the criteria required to be “strong” are somewhat daunting to all but the best-funded and most effective security organizations. For example:

- Putting senior business executives’ performance incentives to manage information risk on a par with product, schedule, and financial incentives or other key performance indicators
- Hiring specialists in quantitative risk analysis and threat intelligence and applying a formal quantitative risk analysis model (which may require premium tools and data sources)
- Performing rigorous root cause analysis of all noncompliant conditions
- Conducting regular independent review of risk-based decision-making processes

For a security leader struggling to get business buy-in (another challenge with risk management just like all else security), those tough criteria may seem out of reach. Fortunately for the typical business, a risk program only needs to be “strong enough” in the right areas. The security team would not need to score 100% on the FAIR Institute maturity survey to become effective, and even getting to 60 or 70% could move the needle significantly toward improved cybersecurity program outcomes.

---

1 “The Road to Cyber Risk Maturity 2018 Risk Management Maturity Benchmark Survey,” FAIR Institute, January 2019
For example, section “Implement Tiered Risk Assessment” explains how some risk analysis processes can be implemented quickly from the bottom up by a small team and distributed to other groups in the organization.

5.2 Understand and Employ Risk Management Framework Standards

If the business has taken steps to establish control baselines, simplify and rationalize IT, and promote the right security culture and governance model, risk management can fit right in as the keystone to these efforts. Businesses just need an organizing framework for it. So, if we could get our organization to implement a risk management framework that was objective and crossed silos, what would it look like? Although multiple framework standards exist (including one from NIST), I recommend these two: ISO 31000:2018\(^2\) for the overall framework and Open FAIR for the quantitative risk analysis model.\(^3\)

5.2.1 ISO 31000 Risk Management

In the ISO model, security and business leadership first set the context for risk. Staff perform risk assessments and risk treatments and monitor risks for changes. Business leadership communicates risk appetite, preferences, and decisions to security leaders. Security leadership communicates new risks, status of known risks, and programs for remediation to all stakeholders. Risk practitioners from IT teams, the CISO, and the Chief Risk Officer (CRO) monitor IT operational risks, cybersecurity risks, and enterprise risks, respectively.

5.2.2 Open Factor Analysis of Information Risk (FAIR)

We recommend using the Open FAIR definition for any kind of risk. FAIR defines risks as “The probable frequency and the probable magnitude of future loss,” and, in fact, one can substitute the words “loss exposure” for risk at any time per this definition. Loss exposure, or risk, in FAIR concerns itself with assets that have value which can be lost,

\(^2\)ISO 31000 Risk Management, International Organization for Standardization (ISO), 2018
\(^3\)“Open Group Standard: Risk Analysis (O-RA) (C13G),” The Open Group, 2013. Accessed at https://publications.opengroup.org/c13g (free registration and login required)
stolen, or affected in negative ways. FAIR also describes an ontology of risk component definitions, starting with frequency and magnitude of loss. Once trained on these definitions, business and security people can talk about risk in the language of business.

Many in the industry are aligning on the Open FAIR risk model (shown in Figure 5-1). It provides a comprehensive set of risk terminology definitions and a quantitative method for estimating loss expectancy (i.e., a range of annualized loss).

![Open FAIR Model](image)

**Figure 5-1. Open FAIR Model**

**“RISK” AND OTHER RELEVANT DEFINITIONS**

**Risk (per FAIR):** The probable frequency and magnitude of future loss

**Information risk scenario:** A threat acting on a vulnerability against an IT or business information asset to produce a loss event

**Risk-related issue:** Any reported event, circumstance, or concern that could affect one of the FAIR model components (boxes)

FAIR offers a consistent way of describing information risk and performing quantitative risk assessments. FAIR also provides ways to quantify the level of risk assessors’ confidence and addresses the multivariate nature of information risk using Monte Carlo simulations. The assessors must have a clear understanding and shared assumptions about the scenario under analysis. Using FAIR-based tools efficiently across a broad range of scenarios requires risk assessors to have considerable real-world experience with the tools and a good storehouse of risk data that is specific to
the business. Performing large numbers of full quantitative analyses requires a level of maturity and some risk analysis tools from the business.

5.2.3 Tiered Risk Assessment Process

I recommend that security teams adopt the FAIR methodology for risk analysis and train security risk professionals and the core security team in FAIR concepts so that they can speak about risk consistently. However, FAIR does not yet include a lightweight method of triaging risk scenarios that can be rolled out to business and IT staff without requiring many hours of training. I’ll address this challenge in section “Use a Lightweight Method to Triage Risk Scenarios.”

Businesses can come up to speed on FAIR in the spirit of “crawl, walk, run.” Initially, train the core security and risk management teams on the model. Develop the capability to use it for in-depth risk assessments. Lightly train business risk owners and IT or security operations leaders to understand FAIR analyses using examples of risk scenarios pertinent to the business. Deepen FAIR adoption over time until it becomes possible, if desired, to replace qualitative shortcuts used for lightweight risk assessments or other needs.

Figure 5-2 illustrates a conceptual risk management framework combining the ISO 31000 and Open FAIR standards. The remaining sections of this chapter cover each major process in the framework.
5.3 Establish the Context for the Risk Program

Businesses should define the scope of information risk programs based on the types of assets, regional or organizational boundaries, risk scenarios, or compliance issues to be covered. The following key to cybersecurity-business alignment summarizes a work program to establish the risk context. It also outlines the contents of this section.

Prepare analysis of business risk scenarios and propose an information risk framework. Socialize the proposed risk framework to obtain broad stakeholder buy-in. Seek top-level sponsorship for the risk management program and formalize risk management accountabilities.

Figure 5-2. Conceptual Diagram for the Major ISO 31000 Risk Management Framework
5.3.1 Prepare Analysis of Business Risk Context

Ideally, security leaders have top-level sponsorship up front for investments of time and resources in the risk program. Since that’s not always the case, confident security leaders can prepare a business case for the program that includes an analysis of the business risk context and an outline of a proposed risk framework. Consider this required “homework” to gain top-level support and build the actual risk program later.

Consider using PESTLE analysis⁴ to understand and document the risk program’s business context for risk leaders:

- **Political:** Who are the business and security stakeholders and what is the governance framework?

- **Economic:** How does the business make money? What are the core processes (i.e., sales, marketing, research, value delivery, value development, finance) that could be at risk?

- **Social:** Who are the users, managers, and executives that will be impacted by the risk program, what training will be required, and how to get buy-in?

- **Technological:** In which existing management processes and tools (e.g., IT governance, risk, and compliance (GRC), asset management, IT service management (ITSM), vulnerability management, third-party management, etc.) will risk management capabilities be embedded? What new tools may be required?

- **Legal/regulatory:** What regulatory requirements influence risk management for the business? Do they specify how risk management must be done?

- **Environmental:** Who are the secondary stakeholders (i.e., customers, investors, regulators, society as a whole) that would be impacted by IT outages, data breaches, or other losses?

⁴“What is PESTLE Analysis? A Tool for Business Analysis,” accessed at https://pestleanalysis.com/what-is-pestle-analysis/
5.3.2 Outline a Proposed Risk Framework

As described earlier, I recommend using the ISO 31000 risk management framework and Open FAIR for risk analysis. In this chapter, I’ll provide additional information on risk assessment, risk monitoring, risk treatment, and risk communication processes for the framework.

Business and IT leaders generally require some education on information risk terminology and a briefing on how the program would work. Develop a briefing describing how ISO 31000 and Open FAIR concepts can be used in a risk management program for the business. Prepare a briefing on the need for a consistent language to identify, describe, and assess threats, vulnerabilities, impacts, and risks as well as an outline of the risk processes required.

5.3.3 Obtain Top-Level Sponsorship

Top-level sponsorship from a CEO, CFO, President, General, Provost, and other top business leaders is fundamental to a risk program. If required, build a business case from the analysis of risk context and, in presenting it, consider the guidance in the “Board Communication” section of this chapter.

However, security leaders need more than the sponsor’s signature. They need a formal assignment by the executive of business risk accountability to business leaders and some mechanism for holding business leaders accountable. Businesses can do this in different ways.

---

**STORIES OF BUSINESS LEADER ACCOUNTABILITY FROM THE FIELD**

“At the Bank, we had the view that technology doesn’t have risk, businesses do. Our role is to help make them aware of the risk and advise them on the alternatives. Our risk acceptance process was based on a simple memorandum. The form explained the risk and if we felt it was egregious ended with a single line that read: ‘Moving forward with this is against the recommendation of the CISO.’ The number of these that a business leader filed would have been counted, but we never had one signed off. In the Bank’s culture, it was better for the business leader to remediate the issue than to explain why it was necessary to overrule the CISO.”

**Steve Katz, CISO**
“Business and IT leaders would come before the Corporate Ethics and Compliance Oversight Committee at least once every 2 years to present a self-assessment of the entirety of risk to their business unit. I sat on that Committee along with officers for audit, HR, legal, financial, and other functions. Completing the assessment was a rigorous 6-month process to which each of us would assign a support person to help the business unit understand what was required. The assessment process drove accountability to the business and issues flowed up to the enterprise risk map.”

Malcolm Harkins, CISO

Businesses have different ways of holding business leaders accountable for risk, and multiple models can work provided that the idea of managing risk tightly has top-level support. The key is to get security and business leaders collaborating through an established risk management forum (see Chapter 3, section “Risk Management Forums”) and to create a risk acceptance process with enough granularity and coverage to take in all issues critical or important to the business.

Locate and work as closely as possible with executive stakeholders responsible for financial risk, operational risk, and other forms of business risk; they may be found chairing or preparing reports for Audit Committees, corporate social responsibility committees, or other compliance-related functions.

5.3.4 Socialize Risk Framework for Broad Stakeholder Buy-in

Stakeholder buy-in for the risk program is required to successfully operationalize it. Security leaders must convince stakeholders of the “why” of, or reason for, the information risk program by explaining the business risk context, outlining the framework, and telling stakeholders how they would be impacted. Often, it is helpful to work through one of the business’s top risk scenarios using FAIR analysis with the stakeholders and present the results to top executives as a way of showcasing the proposed methodology.

As noted earlier, a risk management framework could start with information risk (requiring only CISO and/or CIO sponsorship), or it could be integrated into an ERM program with CXO sponsorship. Present the briefing with a proposed risk taxonomy, framework, and processes to the appropriate business, IT, developers, and other stakeholder audiences. The presentation can be tweaked for different audiences and adjusted based on audience feedback.
5.3.5 Define Accountabilities, Risk Appetites, and Risk Processes

After completing the work discussed previously as well as gaining the necessary sponsorship and stakeholder buy-in, security leaders can continue to define and operationalize the risk program as follows:

- **Identify accountability**: Senior business, IT, or security leaders of the company should be identified as strategic risk owners via policy documents or formal memos from the top-level sponsor. Formally define and announce the accountability mechanisms such as signoff memos, self-assessments or performance evaluations, incentive structures, and other measures.

- **Determine risk appetites**: The thresholds for acceptable, unacceptable, and catastrophic impact from information risk often aren’t well defined. It can take some analysis and deliberation to tease risk appetites out of the “executive subconscious” into explicit definition. Security leaders can ask questions like: *How long could the electronic order taking system be down before the company takes a material loss?* Then extrapolate the risk appetites for downtime or financial loss based on the answers to such questions. Often, the risk appetite information emerges dynamically whenever staff present risk analyses to executives.

- **Weave risk management into cybersecurity governance**: Governance must encompass core cybersecurity accountabilities and cross-functional coordination functions for risks, operations, and other program functions (see section “Institute Cross-Functional Coordination Mechanisms” in Chapter 3).

- **Plan risk management processes**: Organization-wide processes for developing IT asset risk profiles, performing risk analysis and risk treatment, monitoring, and communication can be formally developed at this point and become part of the risk management context.
5.4 Implement Tiered Risk Assessment

Risk assessment – which in the ISO model includes risk identification, risk analysis, and risk evaluation – is the core of risk management. It exists in a feedback loop with risk treatment and risk monitoring. However, as we discussed in section “Analysis Paralysis and Uncertainty About Where to Start,” most businesses haven’t yet begun to assess information risks comprehensively in a consistent and objective manner.

The good news is that security organizations can work with IT and the business to triage issues from the bottom up and sort out risk scenarios for quick treatment or further, detailed analysis.

5.4.1 Use a Tiered Risk Assessment Process

Figure 5-3 depicts a tiered risk assessment model that I recommend for clients.

![Tiered Risk Assessment Model](image)

**Figure 5-3.** Tiered Risk Assessment Model in the Risk Management Framework
The tiered risk assessment process is designed to

- Eliminate > 90% of the issues that can be resolved through standard operating procedure (SOP) before they become a significant IT operational risk or a cyber-risk
- Engage business and IT staff in the issue triage and early risk identification processes
- Remediate or gain routine exceptions for > 90% of IT operational and cyber-risks at the business or IT team level
- Focus the resources of the information risk team professionals primarily on the top risks that represent the highest loss exposure to the business

Security Architects Partners, a consulting company I work with, has developed a form of tiered risk assessment called the Agile Risk Management (ARM) Framework\(^5\) and implemented it for several clients. Some examples in the sections that follow come from this framework, and readers can get more detail at the link.

The idea with tiered risk assessment is that staff should first identify which issues in an IT environment are in fact risks and which can and should be resolved through business-as-usual processes. Most issues aren’t risks until they exceed defined thresholds derived from business or information risk appetites. Therefore, issue triage should be done as the first step in a tiered assessment process.

### 5.4.2 Implement Asset Risk Profiling

Often the importance of an issue (such as a vulnerability) is relative to the asset(s) it affects. A tiered risk assessment process needs an easy asset risk profiling method that can be done on the fly whenever potential risk to the asset is identified. The method can also be added to asset inventory processes. An asset risk profile should contain asset risk metadata and an overall asset risk score that represents a quick summary of how the asset could contribute to risk. During triage, staff need only evaluate the asset risk score, but during risk assessment, trained risk advisors should consider more detailed risk metadata collected during the profiling process.

\(^5\)“Agile Risk Management Framework,” Dan Blum, Security Architects LLC, January 2020, accessed at [https://security-architect.com/RiskManagementResources](https://security-architect.com/RiskManagementResources)
IT, development, and LOB staff can easily be trained to use a tool to generate asset risk profiles. It’s possible to create asset risk profiles for a single asset, such as a server, or an application or system that aggregates many atomic assets.

The ARM methodology provides a taxonomy for asset risk metadata, a way to capture it on the fly, and the ability to calculate risk scores for first time use on an asset. On-the-fly asset risk profiling can be accomplished in minutes by the asset owner and can populate an existing asset inventory for future reference. Readers can learn more about ARM5 or devise a similar method.

5.4.3 Identify Issues That Could Bubble Up to Risk Scenarios

Risk-related issues can come from any circumstance or report that factors into one of the risk model components from Figure 5-1. Risk issues include vulnerabilities, software defects, third-party deficiencies, threat or penetration test reports, compliance gaps, audit findings, new business models, and more. But unless an issue can combine with other risk model components (e.g., a threat finds a vulnerability and causes a loss event), there’s no risk scenario. Many risk scenarios are highly unlikely to occur. Others can be easily treated.

To triage issues with the ARM framework, staff members can use the severity rating of the issue and the risk metadata of the asset to look up an issue remediation time window. The easiest way to explain this is to consider a simplified vulnerability prioritization example from a procedure we worked up for a client:

1. Describe the vulnerability issue, such as a new OpenSSL vulnerability affecting 60 web servers. Look up or quickly calculate the assets’ risk metadata and match it against the vulnerability severity using the critical, high, medium, or low (CHML) scale provided by most vulnerability management vendors.
2. Look up a remediation time window from a table that matches the affected asset’s risk score and the issue severity.

3. Estimate how long would be required following standard operating procedures to close vulnerability issues.

4. Escalate vulnerability issues that cannot be remediated within the remediation time window.

5. Record all issues, issue-to-risk triage outcomes, and issue remediation outcomes in an issue management system, such as Jira.

6. Monitor the issue until it is resolved, and repeat issue-to-risk triage anytime there is a material change to the issue’s severity, assets affected, or remediation schedule.

Organizations can use this procedure to triage any type of issue that relates to a specific asset (such as an application). Some issues, such as penetration test reports and audit findings, aren’t necessarily specific to a single asset but can affect entire systems, applications, or aggregated assets. No matter. Organizations can tweak remediation time windows, severity values, and other parameters within the procedure.

For issue identification and triage, staff need not be knowledgeable about how vulnerabilities or other issues could affect the assets. They only need to know how to use the triage methodology and to specify how long it takes to resolve the issue. Thus, asset risk profiles and severity scores provide all the context required. Generally, the more important the asset, the shorter the remediation time window.

**5.4.4 Use a Lightweight Method to Triage Risk Scenarios**

When an issue can’t be resolved in time or according to standard operating procedures, it should be escalated for a quick or lightweight risk assessment. Because digital businesses tend to generate many information risk scenarios, risk assessors (in an ideal world) should be able to quickly identify risk scenarios that

- Have already been analyzed and should be treated the same way as a previous scenario
- Exceed risk appetite for the affected information assets and must be escalated for in-depth analysis and reviewed by senior security or business leaders
• Do not exceed risk appetite and can be treated immediately according to the recommendations of the asset owner or risk advisor

This model of lightweight risk assessment could be accomplished by a centralized risk team whose members are trained in the FAIR model, have access to an organized database of previously assessed risk scenarios, and have identified risk appetites (i.e., tolerable amounts of loss exposure) for many types of information assets and business risk owners.

In my experience, even if they like the idea of FAIR, most organizations have only a few resources dedicated to risk assessments. This is true for all but the largest organizations that are most committed to risk management. Yet the typical digital business is either identifying or (often) ignoring many more risk scenarios than a few full-time or fractional resources can deal with.

The need for a lightweight method that nonexperts can use is even more important for businesses committed to a decentralized or agile management approach and a lean centralized security organization.

**LARGE TECHNOLOGY COMPANY’S AGILE RISK MANAGEMENT STORY**

Early on in working with agile risk management (ARM), a very large client threw us an interesting curve ball: This company is all agile. Not only software development projects, but all projects, use the agile methodology complete with standup meetings, nine-person “squads,” and so on. To fit the company culture, our client wanted risk advisors to be part of the agile squad or at least the surrounding “tribe.”

My first reaction was: Are you crazy? You can’t train that many risk advisors! Over time, however, the idea of engaging large numbers of IT and development staff in the early tiers of risk assessments grew on me. Isn’t this what the meme “security is everybody’s business” is all about? We developed an online form consisting of questions staff should know the answer to plus some artifacts for lightweight risk assessment customized to the client’s needs.

How could a business scale risk management to cover many issues across large populations of users and assets? ARM proposes a Lightweight Risk Assessment (LRA) process based on FAIR that can be used by lightly trained nonexpert staff to prioritize risks by estimating the probable frequency as well as the probable financial, operational, liability, or strategic loss magnitude of a risk scenario. Parameters for estimation are
provided in a lookup table for the staff to use as they go through the LRA by answering a short set of about five questions. Based on these answers, the ARM tool calculates a risk score. If the score is below a certain number, the assessor can select the risk treatment and sign off on the scenario. If the score is too high, the risk scenario must be escalated for in-depth analysis or a higher level of signoff. Either way, the results of the analysis go into an operational risk database for review by the business risk owners and the risk management team.

The Binary Risk Assessment provides another lightweight method. It includes an open source application that asks staff ten questions covering threats, vulnerabilities, protection strength, assets, and impacts. It outputs a low, medium, or high risk rating after staff answer the ten questions. As with ARM, nonexpert asset owners or risk advisors could be trained to answer the questions based on consistent parameters; they could decide on risk treatment for low and medium risks, but more senior leaders or risk management professionals would decide on high risks. The results of all risks that aren’t escalated for a higher level of signoff should be documented and periodically reviewed by risk management professionals.

Use tiered risk assessment processes to engage business, IT, development, and other staff in risk management. Provide automated tools that make it easy for asset owners or risk assessors to triage risks by asking staff role-appropriate questions they should already know the answer to.

### 5.4.5 Develop Risk Scenario Evaluation Processes

The final phase in risk assessment is the in-depth risk scenario evaluation (or just risk evaluation, per ISO). Detailed risk scenario evaluations should provide a more detailed analysis of how a risk would materialize and a method for ranking potential risk treatments or controls. Such evaluations can include full quantitative FAIR analyses of loss exposure before treatment (aka inherent risk) and after treatment (residual risk). As the core information risk team performs in-depth risk assessments and reviews the

---

6“Binary Risk Analysis,” Ben Shapiro, 2011, Whitepaper, accessed at [https://binary.protect.io/](https://binary.protect.io/)
results of lightweight assessments and issue triage, it can feed higher risks up into an enterprise risk assessment process.

A tiered risk assessment method could triage 90% of the issues before they became risks and handle 90% of the lower risks in a routine manner. The information risk team for a retail firm with 5000 employees might identify 100 higher risks in a year. Some of the most serious ones could materialize from multiple scenarios and merit more than one assessment. On the other hand, risks dealing with similar issues – such as vulnerabilities, software deficiencies, or audit findings on weak internal controls – might be grouped into a handful of assessments. Having a well-defined process to organize and analyze risk scenarios is important.

Focused risk assessments can be done for any of the following reasons:

- Scenario-based analysis of a specific risk(s)
- Business case development
- Security program planning and control prioritization
- Reporting to regulators, stakeholders, or investors

**Scenario-based analysis:** Focuses on a single risk scenario or groups multiple related scenarios into one. For example, financially motivated cybercriminals might be able to compromise a web-based ecommerce application at a retail company via any one of multiple vulnerabilities and implant ransomware of different types to cause multiple loss events. Once analysts have developed calibrated estimates for the threat, controls, and impact factors in the scenario, they can perform a quantitative analysis using the Open FAIR risk tool\(^7\) or a commercial system such as the RiskLens product. By following an objective quantitative discipline, the leadership can perform data-driven analysis informed by multiple stakeholder experts (e.g., legal on liability, marketing on reputational, sales on competitive, and IT on remediation cost impacts).

**Overall risk input for a business case:** The security or risk organization can perform one-off risk assessments for a business case, for example, to get approval for funding mitigation of application vulnerabilities. Risk analysts could calculate the estimated costs to fix the vulnerabilities or to apply other controls for the ransomware scenario and recalculate the Open FAIR analysis with the controls in place. The before and after results

\(^7\)“Introducing the Open Group Open Fair Risk Analysis Tool,” The Open Group, March 2018, accessed at [https://blog.opengroup.org/2018/03/29/introducing-the-open-group-open-fair-risk-analysis-tool/](https://blog.opengroup.org/2018/03/29/introducing-the-open-group-open-fair-risk-analysis-tool/)
yield a return on security investment. For example, one might determine that by using an offsite backup system, incident response upgrades, and multifactor authentication at a total cost of $750,000, the retail company could reduce the ransomware risk (as an annualized loss expectancy) by $5 million.

**Report risks to stakeholders, regulators, or investors:** In some countries, companies are required to report risks to investors and/or regulatory authorities. In the case of the USA, public companies listed on the stock exchanges must disclose material risks to investors. Recent guidelines by the Securities and Exchange Commission (SEC) establish an expectation that corporations quantify risks being reported.

### 5.4.6 Perform Enterprise Risk Assessments to Identify Top Risk Scenarios

Sometimes, security leaders are tasked to quantify the aggregate information risk to the business, and CROs may need to do the same for all enterprise risks. More often, security leaders must simply identify the top information risks (aka strategic risks). Data for the enterprise risk assessment can be collected in the following ways:

- **Bottom up:** Collect information from any documented risk assessments. Estimate costs of documented incidents or breaches to the business or similar organizations during recent years. Identify any gaps in the range of issues covered by the assessments; unless there’s a healthy mix of assessments from vulnerability- or software defect-related issues, red team and threat-focused issues, and audit findings, consider expanding the set.

- **Business impact assessment (BIA) information:** Obtain any available lists of critical assets identified by the business continuity and disaster recovery (BC/DR) team. Cross-reference known risk scenarios against the assets. Use and improve the BC/DR team’s interdependency analysis for critical assets to find the most critical areas of IT and security infrastructure for systemic risk analysis.
- **Enterprise risk map:** Consult the ERM risk map or any list of (noncyber) risks created for the Board or a Board Committee such as the Audit Committee. Attempt to identify information risks that could directly or indirectly factor into the top enterprise risk scenarios that business leaders are most concerned with.

- **Systemic risk analysis:** You may have read about systemic cybersecurity risk to the economy, or financial systems, but what about the risk to your own business? Looking for the top information risk scenarios to “Tier 1” assets from the BIA or the top enterprise risks is a great start, but what might you have missed? Answer: You need to do a BIA for any parts of the security infrastructure, or security program, that the BIA didn’t cover. What if your directory, authentication, or key management services go down? What if two or three senior security engineers or responders become unavailable?

- **Infrequent but high impact scenario analysis:** As I wrote in “Waking Up to Cybersecurity’s New COVID-19 Reality,” many security professionals treated the early 2020 pandemic outbreak as a theoretical concern and probably missed early opportunities to prepare for a surge in remote access, supply chain risk, and business continuity needs. In hindsight, security leaders should maintain access to data on what the impacts of an infrequent but devastating (outlier) risk scenario like a pandemic could be. Also through risk management processes, prompt risk teams to watch for early warnings of outliers materializing. Although it isn’t normally reasonable to overprepare for them, significant outliers should be addressed as a cyber-resilience issue (see Chapter 9’s section “Develop Contingency Plans and Cybersecurity Strategy for Resilience”).

After all major risk concerns have been collected, normalize them using the FAIR model. Group closely related risk scenarios together. Rank using a rapid or exhaustive quantitative estimation methodology. Determine a risk appetite or maximum tolerable

---

8“Waking up to Cybersecurity’s New COVID-19 Reality,” Dan Blum, March 2020, accessed at: https://security-architect.com/waking-up-to-the-new-covid-19-cybersecurity-reality/
loss. Present the risks on the list that exceed the risk appetite as the “top risks.” Maintain
the list of top risk scenarios as events warrant between major refreshes of the enterprise
risk assessment.

GLOBAL HIGH TECHNOLOGY MANUFACTURER CISO’S ERM STORY

“Prior to being the head of security at the company, I’d worked in various business units,
including the controller’s department. At our Corporate Ethics and Compliance Oversight
Committee, I found the enterprise risk map. I brainstormed with the executives whose teams
had analyzed these risks to learn how cybersecurity issues might contribute to them.

As of the early 2000s, the risk map had 9 items including sole source factory failure,
competitive core products, and antitrust actions. I was able to weave direct or indirect cyber-
risk causal scenarios into 2 of the top enterprise risks. During a similar exercise in 2015, I
found an enterprise risk map with 25 items and wove 18 cyber-risks into them. I believe this
shift has occurred for almost every company. Today, for example, ransomware could be a
major risk driver to sole source factory controllers and logistics systems.”

Malcolm Harkins, CISO

Work with the executive responsible for preparing the enterprise
risk map for the Board. Weave direct and indirect information
risks into the risk map. This exercise will increase the relevance of
cybersecurity and educate security leaders on senior executives’
perception of business drivers, business risks, and risk appetites.

5.5 Treat Risks Holistically

Risk treatment can take four forms: accept, avoid, transfer, or mitigate the risk. And yet,
many security leaders put practically their entire focus on mitigation through applying
controls such as those in the control baseline from Chapter 6.
“To win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill.”

Sun Tzu, *The Art of War*

5.5.1 Formalize Risk Acceptance and Risk Exception Processes

When a risk owner decides not to treat a risk, the risk should be formally accepted. Otherwise, the business is open to accusations of not having a competent risk management program or, worse, of covering up risks that it could reasonably be expected to recognize. Once accepted, risks should be periodically reviewed.

A risk exception process is subtly different from risk acceptance. Risk acceptance is explicitly acknowledging a potential loss exposure and allowing it to continue. A risk exception, on the other hand, is a temporary acknowledgment of noncompliance with policies, laws, or regulations that is also creating exposure to loss, but that the business intends to remedy.

The exception process should include signoffs, require compensating controls in some cases, and make exceptions temporary in nature. Also, as changes to the IT environment or the threat environment unfold, the information risk team should monitor accepted risks in the registry for material changes to their probability of materializing or impact worsening.

5.5.2 Educate the Business on Risks to Avoid

In some cases, business leaders choose to avoid risk. For example, a retail business might decide not to engage an out-of-country credit card processing service provider due to concerns about transferring customers’ personal data across borders in violation of national privacy regulations in some jurisdictions. The time spent educating business leaders, IT leaders, developers, and staff on risk pays dividends later. Security-related processes can also proactively provide IT and business leaders with other options. For example, Chapter 7’s section “Manage Cloud Risk Through the Third-Party Management
Program” describes a financial institution’s third-party risk management case study. If an LOB proposes to use a vendor with a high risk score, the security team can explain the issues with the vendor and propose alternatives to stakeholders during a 30-minute meeting.

5.5.3 Share Responsibility, Outsource, or Obtain Insurance to Transfer Risk

Transferring risk to a third party isn’t always possible, and often only some of the risks can be transferred. The adage “You can transfer responsibility but not liability” is usually true. Because risk transfer isn’t a perfect solution and requires much nontechnical input into the how-to, security professionals often tend to overlook or neglect it. However, businesses should take advantage of the following risk transfer opportunities:

- **Implement a framework for determining third-party shared responsibilities, service-level agreements (SLAs), and contracts:** Contracts with third parties can often induce them to reduce risk more efficiently than the business could through its own efforts. SLAs provide a way to measure third-party efforts and assess any third-party deficiencies. (For more information, see Chapter 6’s section “Apply a Shared Responsibility Model to the Control Baseline.”)

- **Consider whether cyber-insurance is right for the business:** Cyber-insurance is a type of general insurance that covers information risks. First-party cyber-insurance covers direct losses to the business from breaches, outages, or other incidents. Third-party coverage addresses secondary losses from claims and legal actions against the business as a result of information risks. Cyber-insurance can make a lot of sense as part of the cyber-resilience strategy, especially when a business knows it cannot afford to cover high impact losses but does not see a good return on security investment from trying to mitigate them because they occur too infrequently. Also, cyber-insurance may be required for credit agreements or other contracts. In such cases, cyber-insurance could keep a small company out of bankruptcy and preserve even a larger, financially strong organization from credit downgrades or steep stakeholder losses. Also, carrier-provided
breach response and other services can be helpful. See Chapter 9’s section “Develop Business Continuity and Disaster Recovery Plans” for more information.

Think outside the box of risk mitigation controls to develop a robust set of risk transfer practices. Consult the legal team on contracts and cyber-insurance, the finance team on cyber-insurance, and the vendor management team on contracts and shared responsibility frameworks.

5.5.4 Evaluate Business Changes and Controls for Risk Mitigation

Security leaders often focus almost all their attention on creating new controls or bringing an existing control to bear on a new risk because that is, well, what they can control. However, risks can also be mitigated by business changes to process, partners, facilities, or activities as well as controls. Perhaps being able to help business or IT leaders and staff find more secure options for getting their work done without having to implement additional controls is the “acme of skill” from the Sun Tzu quote at the beginning of this section. For example, an LOB could consider modifying privacy-related business practices (such as collecting or reselling personal information without consent) that might violate regulations.

All this being said, at least some of Sun Tzu’s “one hundred victories” must come from “battles” or the use of actual security controls. In Chapter 6’s section “Develop Architectural Models and Plans for Control Implementation,” we recommend developing an initial control baseline and security architecture road map for building the controls. For the ARM project, we developed a Control Library that helps clients track which of the NIST Cybersecurity Framework controls and/or customer-defined controls are required, how they are implemented, and in which IT environments. Similar artifacts are available in some IT governance, risk, and compliance (GRC) systems.

During focused risk assessments, analysts can determine “what if” risk treatment options, assessing and evaluating the effectiveness of potential controls and other mitigation or transfer options. Using metadata about the controls (such as strength or type), they can select the right ones to apply to each risk scenario.
After selecting one or more controls for treating a risk scenario, analysts can update the IT GRC system or Control Library with the control information. In this way, the security team keeps the control baseline continuously risk informed.

### 5.6 Monitor Issues and Risks Continuously

The risk management framework must monitor known, new, and changing risks. It must track them in issue management systems and operational risk registries. Not all risks can be treated up front, and risks change over time. Monitoring risks is often as important as analyzing them in the first place.

As shown in Figure 5-4, risks should be monitored on an event-driven basis as well as through scheduled or periodic review.

- **Issues**: Risk scenarios can develop from the types of issues shown in Figure 5-4. Some – such as threat intelligence that cyberattacks exploiting a known third-party deficiency are increasing against an LOB – may recur over and over. They may need to be reanalyzed.
from time to time and may prove to have higher or lower ratings than before. If so, security business leaders should reevaluate existing treatments or exceptions for these risks.

• **Risk treatment projects:** Review risk assessments whenever a risk treatment project or activity completes; for example, a new technical control mitigating access risk is ready to move into production, or a cyber-insurance policy expires and is offered again at similar terms. For the top risks in the business, reviews may also be required when treatment milestones are missed and/or at arbitrary time intervals. If residual risk remains and is higher than required thresholds, escalate the risk for new exception signoffs and/or new risk assessments.

• **Exception lists:** Review the risk assessment for a risk whenever an exception expires. If the risk is still higher than the risk appetite, escalate the risk for new exception signoffs and/or risk assessments.

### 5.7 Communicate Risk to Stakeholders Effectively

Risk should be the common language for communication between security and the business. The risk framework provides the feedback loop to collect information for risk analysis and treatment and to communicate risks to stakeholders. In alignment with the CRO and the ERM program, CISOs can communicate effectively at multiple levels with

- Business staff and associates
- Business risk owners
- Board of Directors and Executives

#### 5.7.1 Business Staff and Associates

Employees of the business, long-term contractors, and even third parties are – to a greater or lesser extent – part of the risk program. For one of our clients using ARM, multiple business and IT staff will take on risk advisor roles. Still more staff in that company and others like it will perform the issue-to-risk triage process. The risk program can make staff more conscious of the risk dimension to their day-to-day duties and well versed in the use of issue and risk management tools and processes.
To engage the business staff and associates, organizations of all sizes should

- Provide information on basic security issues all organizations face and generic risk scenarios through security awareness programs.

Larger organizations, especially ones under high security pressure should

- Create awareness, training, and communications channels for risk-related roles such as business risk owners, risk advisors, asset owners, and data stewards.

- Identify potential risk management champions among the staff being trained or prepped for risk management roles. Assign individuals on the information risk team to recruit or mentor champions, and work with them to provide informal meetings and other communications to the business and IT.

- Work with HR and/or LOB managers to ensure appropriate performance goals and incentives for those in the champion roles.

### 5.7.2 Explaining Risk to Business Risk Owners

Business risk owners include CXOs and - in larger organizations - also LOB, IT, or development leaders. They are accountable for effective risk management and vested with the authority to accept known risks and/or allocate resources to treat the risks. As we discussed in the section “Establish the Context for the Risk Program,” businesses should make such accountability explicit and tangible through a visible business process. Security and risk leaders can provide role-specific training and communication channels for the business risk owner role.

Security and risk leaders should

- Advocate for explicit accountability to business owners for working with the risk management program to define risk appetites, risk treatment, and formal risk acceptance.

- Seek and maintain informal relationships with business risk owners and any business information security officers (BISOs) outside of the enterprise security department in a large organization.
• Bring training and awareness efforts to life by helping business leaders recognize risk scenarios that can materialize from information risk

• Advocate for business leader participation in security steering committees or forums

5.7.3 Board Communication

The Board of Directors is accountable for oversight to ensure the business accomplishes its mission, such as delivering investment returns to owners, providing services, or meeting other key objectives. Most Boards for larger organizations maintain committees, such as an Audit Committee. Risk management often lies within the Audit Committee purview, but some financial services and other highly regulated companies maintain a separate Risk Committee or another compliance-related forum. Some Boards in the defense industry or critical infrastructure industries maintain a Cybersecurity Committee due to the strategic upside as well as downside importance of safely aligning operational technology (OT) with information technology (IT).

WHAT'S THE STORY ON BOARD-LEVEL ENGAGEMENT?

In general, many Boards still struggle to address information risk oversight. Engagement remains low in critical areas; for example, a recent Shared Assessments group survey found only 32% of respondents stating that their Boards have a “high engagement and level of understanding” on the important topic of “cybersecurity risks relating to vendors.”

According to knowledgeable sources I interviewed such as Professor James Tompkins (Kennesaw State University) who researches corporate governance and Board-level risk oversight, there currently is no standard format for the risk documents or presentations (i.e., risk registers or risk maps) that Boards receive. However, Boards always want to know what the top risks to the company are and to understand or

---

9“Vendor Risk Management Benchmark Study: Running Hard to Stay In Place,” Shared Assessments Program and Protiviti, April 2019, accessed at www.prnewswire.com/news-releases/2019-protiviti-and-shared-assessments-survey-finds-board-involvement-a-key-indicator-of-vendor-risk-management-maturity-most-organizations-will-drop-vendors-to-de-risk-300827875.html
quantify them in business terms such as lost revenue, delayed product delivery, breach recovery costs, opportunity costs, competitive impairment, and so on.

To ensure they can oversee information risk effectively, security leaders can advocate that as an industry best practice, Boards should

- Include at least one member who is knowledgeable about cybersecurity. Though technically literate, this individual(s) need not be highly technical; it is more important that they have a deep background of business experience with cybersecurity from previous roles.

- Maintain a committee structure well suited to the oversight of risk management.

- Have direct contact with the security leadership and ensure their alignment with the business and their support from the business and that they obtain the resources required to run a cybersecurity program.

In leading companies, the CISO presents to the Board Audit (or other) Committee meetings regularly. For many businesses, there is a cybersecurity, or risk, agenda item for the CISO to present to full Board meetings at least once a year. The CISO may also present on significant security incidents (such as the breach of the business or one of its competitors) on request.

Advocate for more Board engagement on information risk, but don't assume Board members have time to acquire much technical knowledge. Always communicate risks in terms of business impacts. Keep presentations concise and actionable.

Security leaders should

- Advocate for effective Board information risk oversight through personal contacts with existing Board members and top executives, providing copies of National Association of Corporate Directors (NACD) information risk–related guidance and offering to invite Board-level security experts from other organizations to visit or speak.
• Advocate for the CISO’s ability to regularly brief the Board and Board Committees on information risk programs. Regardless of where the CISO reports in the organizational hierarchy, this engagement will help the CISO understand the top-level business requirements better and be more effective in the role.

• Maintain informal relationships with individual Board members, especially those chairing key committees covering risk and/or technology-savvy Board members.

• Coordinate information risk reporting with the CRO or whichever function in the organization handles ERM.

When presenting to the Board (or making executive presentations in general), keep the content simple, short, and to the point with backup information available at need. Avoid getting into technical detail but do focus on the organization’s cybersecurity situation, on the top risks, the program for managing those risks, and any executive actions or support requested. For more tips, see Chapter 4’s section “Make Enhancing Communication a Top Security Team Priority.”

Content typically presented in board presentations is generally unsatisfactory according to Catherine Allen, CEO of Santa Fe Consulting and a Corporate Board member. “The worst of it is PowerPoint presentations, death by PowerPoint. Pictures are good but don’t contain enough detail. Bulleted lists are better but either tend toward verbosity or leave out details.” Allen provides a piece of advice to CISOs presenting to Boards: “The best option for me has been to see infographics.”

Even if the Board holds the CISO in high regard, it may demand independent third-party assessments of the security program itself. The security leadership should support such assessments. Additionally, CISOs should help the Board get benchmark data when requested on what other organizations in their industry are doing for cybersecurity. This information is available from trade press articles, Information Sharing and Analysis Centers (ISACs), and the CISO’s own network as well as independent research companies.
5.8 Call to Action

The core recommendation for security leaders from this chapter is to manage risk in the language of business as follows:

- Establish the context by adopting a consistent framework – I recommend the combination of ISO 31000, Open FAIR, and a tiered risk assessment process.
- Obtain top-level sponsorship and establish clear business risk owner accountability.
- Work with the IT and business teams responsible for asset management on creating a lightweight asset risk profiling mechanism.
- Create a tiered risk assessment process.
- Develop a focused risk assessment or risk evaluation method to select controls and other risk treatment approaches, including risk acceptance and risk transfer processes.
- Work with the executive responsible for preparing the enterprise risk map for the Board and weave direct or indirect information risks into the list.
- Monitor issues, risks, top risks, risk treatments, risk acceptances, and risk exceptions.
- Create risk communications programs tailored to staff, managers and stakeholders, and the Board.

**Action – Make a quick assessment of the state of the organization’s information risk management program.**

Ask yourself the following short set of questions and score the answers in the Success Plan Worksheet’s Section 3, Table 3. Base your score on whether you would answer most of the questions with a strong “no” (1), a strong “yes” (5), or something in between.

---

10“Rational Cybersecurity Success Plan Worksheet,” Dan Blum, Security Architects LLC, May 2020, accessed at [https://security-architect.com/SuccessPlanWorksheet](https://security-architect.com/SuccessPlanWorksheet)
1. Are business owners held accountable for information risk?

2. Are business, IT, and security teams using consistent terminology for discussing risk and consistent criteria for assessing risk?

3. Are stakeholders coming to security for guidance or advice before taking important decisions that could create risk?

4. Are risk assessments used to prioritize security projects, manage third parties, or make other decisions?

5. Is a quantitative risk analysis methodology in use?

6. Are issues, risks, exceptions/acceptances, and top risks monitored in an issue management system; IT governance, risk, and compliance (IT GRC) tool; and/or risk register?

7. Are top information risks being regularly communicated to executives and the Board, and is the dialogue constructive?

**Action – Define 1–3 improvement objectives for risk management**

Note improvement objectives in Section 4, Table 6, of the worksheet. The following are some guidelines and examples.

If the business doesn’t yet have a formal information risk management program, look for improvement objectives in the section “Establish the Context for the Risk Program.” For example:

- Perform a PESTLE analysis\(^4\) to understand and document the risk program’s business context and discuss it with at least one business or IT executive sponsor.

- Task security and risk team members unfamiliar with FAIR to read section “Open Factor Analysis of Information Risk (FAIR)” and the Open Group Standard: Risk Analysis (O-RA)\(^7\) and other FAIR resources.\(^11\)

---

\(^4\)“FAIR Resources,” Dan Blum, Security Architects LLC, January 2020, accessed at https://security-architect.com/RiskManagementResources
To improve a risk management program that’s up and running, consider the following sample improvement objective:

- Review the organization’s asset inventory program and identify an IT champion willing to work with the risk management function on devising a method to capture asset risk scores and risk metadata as described in section “Implement Asset Risk Profiling.”

To improve the identification of top information risk at the executive level, consider the following sample improvement objective:

- Meet with executive stakeholder(s) responsible for reporting risk to an Audit Committee (or other risk management forums). Identify or discuss
  - Who are, or could be, accountable risk owners for categories of information risks?
  - Potential overlaps between information risks and top enterprise risk scenarios

Don’t limit yourself to these examples. Look for improvement objectives that fit the gaps and priorities you’ve identified for your business.