Rocks and Shoals

Navigating Risk Management

SMOOTH SAILING SOLUTIONS

Acknowledgments

This white paper and the associated program is based on *A Minimum Viable Risk Management Program* by Rachael Lininger of Leviathan Security Group, available at www.leviathansecurity.com/white-papers/a-minimum-viable-risk-management-program. The publication of this document would not be possible without their support. This program and document are derived in part from the “Binary Risk Analysis methodology” and is licensed under the Creative Commons ShareAlike 3.0 license.

MVRP01-1.0

19 February 2019

smoothsailingsolutions.com

1 The Risk Management Problem

All human activity involves risk. Business owners and executives understand this better than most – it's a fundamental part of the job. Explore new markets, or focus on existing customers? Invest in new production capacity, or retool existing plants? What marketing strategy will deliver the best returns in upcoming sales quarters?

Perhaps because risk is so common in their experience, many executives don't spend a lot of time systematically assessing risk. After all, if you have to make a dozen risk decisions before noon, you're probably not that interested in making the process more cumbersome. And risk management is not known for being a fast and easy process.

In fact, risk management isn't often considered a "business" tool at all. People think of it as a compliance item, something required as part of a regulatory framework, a means of ensuring you're in compliance by checking all the right boxes. Outside of that, it's mostly in the realm of the insurance adjusters and accountants – necessary, perhaps, but a specialist tool for specific circumstances and functions.

But it doesn't have to be that way. Rather than making things more cumbersome, risk management can simplify executive decision making by reducing the number of decisions that require executive involvement, as well as clarifying the issues surrounding the decisions that do. With a robust program in place, long-term planning and strategy development become easier and more structured.

Yet we don't see that happening very often. Risk management programs remain in the back room, relegated to secondary items for compliance purposes, perpetually underfunded and underutilized. When a risk management program is driven by compliance, as an annoyance to be completed at minimum cost, the result is often a paradoxically high-cost waste of time and resources. The line item in the annual budget may appear small, but the benefit to the organization is negligible or even a net negative.

In order to avoid this fate, we need a model we can use to build an effective program, one that can both pass a compliance audit and deliver a visible return to the organization. It should be easy to create, scalable, and usable in a wide range of environments and organizations.

So what does that look like?

1.1 This Isn't About the Board Game

For a start, let's make sure we're all talking the same language. *Risk* gets defined in many ways these days. It's a popular buzzword, and that means it gets used as often as possible even when it's not appropriate. Even among authoritative sources, the term is sometimes used interchangeably with "threat", "vulnerability", "loss", "uncertainty", and many others.

For our purposes, both in this document and in the associated program, we're basing our definitions on those used by the FAIR Institute[1] in their *Standard Quantitative Model for Information Security and Operational Risk*, as well as a few terms from the Carnegie Mellon University Software Engineering Institute.

Risk: The probable frequency and the magnitude of a future loss. You'll often see this simplified as "probability times impact equals risk".

[1] www.fairinstitute.org

Asset: Any definable item of value. Most people associate assets with physical objects, but it can also refer to information, concepts, even relatively abstract ideas. If it can be assigned a monetary or operational value by an organization, it's an asset.

Frequency: How often a loss may occur within a given timeframe.This generally gets reported in terms of percentages or occurrences per year, but it's important not to take those numbers literally. You're rarely certain about risk frequency.

Qualitative risk: An estimate expressed in words, e.g. "High, Medium, Low". Generally used for rougher estimates or fast decision-making.

Quantitative risk: An estimate expressed in numbers, e.g. "financial cost per year". Despite common cognitive biases, these are not inherently more precise than qualitative estimates.

Risk Matrix: A method of measuring risk by plotting the probability or frequency of a risk event against the impact of that event. Points are then assigned a qualitative risk score based on their distance from the origin point of the graph.

Risk Response: The chosen action taken by an organization in response to a recognized risk.

Risk Appetite: The level of financial, physical, or other loss an organization is willing to accept without mitigation or external resources.

Threat: Something that may act to cause a loss.

Threat event: The activity a threat may perform to cause a loss.

Vulnerability: A characteristic or situation that may permit a threat to cause a loss.

Loss event: The specific loss incurred by a particular threat event.

Secondary loss event: Losses that may occur in addition to those directly caused by a loss event, e.g. fines or reputational harm.

Maturity: A definitional measure of operational efficiency and process optimization, generally defined by the five levels of the *Capability Maturity Model* from Carnegie Mellon University[2].

On occasion you will see risk defined as “uncertainty”, with both positive and negative effects. Optimism as a personal philosophy is a fine choice, but from both a regulatory and practical perspective combining “opportunity” events into risk management brings little benefit for significant increases in complexity. In particular both in our definition above and in most operational contexts “risk” is always defined in terms of cost and negative impacts, and as such the potential positive impacts of an event will not be formally considered.

[2] cmmiinstitute.com

2 The Basic Plan

The Minimum Viable Risk Management program is implemented by following these steps:

1. Define program scope,
2. Inventory assets,
3. Assign asset ownership,
4. Sort the inventory by granularity,
5. Perform a Binary Risk Assessment,
6. Asset owners determine risk responses,
7. Executive review and approval,
8. Document and review program results.

2.1 Define Program Scope

This first step is relatively simple, but it is extremely important to the overall success of the program. There are two main threats that must be addressed in these early stages.

First, an effective risk management will inevitably create some discomfort in the initial stages. Driven by fear of change, unfamiliarity with the program's goals and purpose, or perhaps concern about having earlier work re-examined, there will be those within the organization who resist the program's efforts. They may respond by attempting to redefine the definition of risk, by questioning the utility of the program, or by refusing to accept the outcomes of risk management decisions.

Second, a new risk management program must not be overly broad; its scope should address a narrow set of requirements, such as those mandated by a compliance effort. A broader scope necessarily involves increased complexity, particularly in working with more diverse business functions and personalities which may not be as familiar with or open to the realities of a risk management program.

The best solutions to this problem are also the simplest: define a relatively narrow scope in the early stages, and declare executive sponsorship or direct ownership of the program. Visible investment, particularly in time and attention, helps ensure the program is not dismissed or resisted. This in turn makes it far easier for a program to grow and achieve its goals of improving organizational operations and decision making.

In defining your program scope, consider the following key factors:

- Scope of upcoming audits,
- Known assets subject to regulation, such as personally identifiable information and the systems accessing that information,
- Assets belonging to customers, and
- Trade secrets.

2.2 Inventory Assets

Once the scope of the program is determined, it's time to inventory the assets within that scope. You cannot assess risk, or for that matter take any other steps to protect the organization, without knowing what you're assessing.

This might seem straightforward, but it's often one of the most difficult parts of the process. The trouble is that we're not just concerned with salable assets, or depreciable assets, or the sorts of physical plant equipment that automatically has a record somewhere. There are many other assets to consider. As a general guide, your organization will have assets in all of the following categories:

- Information assets: contracts, email, human resources records including sensitive personal information, accounts payable and receivable, perhaps intellectual property, business plans, etc.
- Software: Computer operating systems, business software, industry-specific applications and tools used to do business, etc.
- Physical assets: Computers, storage devices, tools and production hardware, desks and other furniture, office space, and physical plant.
- Services: Anything your organization contracts from the outside that's essential to business operations, such as heating, cooling, power, lighting, Internet connectivity, communications services, etc.
- Intangibles: Often overlooked, this category includes things like brand integrity and recognition, the reputation of the organization, business processes and goals, cultural elements, etc.

For every asset, you should be able to identify at least four things: the location of the asset (even in the case of intangibles – e.g. brand recognition is in the public eye and media), the value your organization assigns to the asset, the purpose of it, and how critical it is.

Determining the answers to these inventory questions is frequently a complex process. Interviews with staff, both at the management and individual contributor level, will give you a lot of general information but can't be considered entirely reliable. At the same time, there's no effective means of building a full inventory through automatic data collection. You'll need a combination of techniques, a strong and effective leadership team behind the process, and probably some level of acceptance that the first pass will be incomplete.

But inaccurate or no, that first pass inventory is still a big step forward.

2.3 Assign Asset Ownership

You'll often see this combined with the previous step, but that tends to introduce complications. Get the inventory first, then assign ownership. This reduces some of the inclination to either forget inconvenient assets or engage in empire-building.

In assigning ownership, you want to think about two primary questions: who benefits the most from the existence of the asset, and who has to account for it in the budget? Often the answers point in the same direction, but that won't always be the case. Resolving this will require judgment and care, but it's essential the process end with every asset having an owner. Avoid the temptation to assign ownership to committees or groups; use the head of that organization instead. And in all cases, the owner should have an appropriate level of responsibility and authority for the role. It's a common mistake to assign ownership to someone who can't take appropriate action without outside authorization.

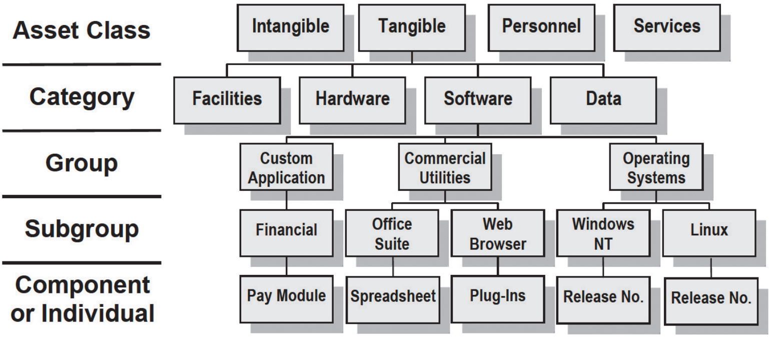
You will find it helpful to establish a guideline early on in the process, and the simplest method is one based on the asset's assigned value. If you determine that an asset cannot be owned by anyone who doesn't have the budget or financial signing authority for the item's value, you narrow the pool of potential owners and help ensure the chosen owner will have the authority to accomplish the necessary tasks. By the same reasoning, your asset owners are more likely to be managers, directors, and other organizational leaders than individual contributor team members.

The more you can define these types of guidelines for assigning asset owners, the easier the process will be. Just remember that you're setting guidelines and so on to assist your team in this process, not to constrain them.

2.4 Sort the Inventory by Granularity

Once the assets have been inventoried and assigned owners, you'll want to put some structure to the inventory to make the rest of the process easier to manage. We do that using "granularity", where assets are categorized in a hierarchical structure. The higher the granularity of the asset, the farther down the hierarchy it can be placed, and the more specific information should be available for assessing the asset. Comparing the details of your inventory this way can also help you spot assets that need more attention.

Appendix B-2 of the *Harmonized Threat and Risk Assessment Methodology* published by the Royal Canadian Mounted Police[3] includes an excellent example:



[3] publications.gc.ca/collections/collection_2017/cstc-csec/D96-7-2007-eng.pdf

You can see that an asset, e.g. the pay module of the accounting system, has a direct line from the highest rankings to the lowest appropriate categorization. The tangible assets of our example organization includes “Software”, with one group of that category being “Custom applications”. Some custom applications are “Financial” applications, and among those are the “Pay Module”. And just like that, you have a clear, easily navigated map for all your organization’s assets.

Once you’ve sorted your assets in this way, it’s easier to organize your thinking and plan your risk assessment process. This method is straightforward and comprehensive, and it results in a simple and easily manageable organization to your program’s forward progress.

You might be thinking “but shouldn’t we tackle the biggest risks first?” The problem is that while it might seem obvious where those risks lie, beyond the top few it quickly becomes a bit of a mess to sort out. Then as you go through the assessment process, items would change their place in the ranking and potentially result in your team having to scramble and reorder schedules and plans to accommodate those changes. On top of that, people prefer things to remain settled; once an item became associated with a level of risk based on its position in the list, it may take more than logic and reason to change it. The granularity of an asset is generally far more stable and a lot less likely to change without some sort of advance warning.

2.5 Perform a Binary Risk Assessment

With the assets defined and categorized, make a plan to assess the risk to individual assets. Start with a well-defined, self-contained asset, preferably one you already have a good understanding of potential threats, and then perform a Binary Risk Assessment on that asset.

Binary Risk Assessment (Binary) is a lightweight risk assessment methodology developed by Ben Sapiro[4]. The methodology is Creative Commons licensed, free for commercial use, fast, transparent, and compatible with other risk assessment methodologies. It's designed to be approachable and usable with almost no training or preparation.

One point to keep in mind is that the assessment has a bias towards information security in general and malicious attacks in particular. This bias is apparent in the phrasing and content of the documentation, but that doesn't mean we can't use the methodology and framework of the assessment for our purposes.

An assessment involves creating a hypothetical threat event relevant to the asset being evaluated, answering a consistent set of questions in relation to that scenario, and then mapping the answers to a risk matrix.

Rather than reproducing all the detail on performing Binary, we refer to the original Work Card, presentation, and white paper for the method. Our examples here will rephrase the original language of Binary to use the terminology defined at the beginning of this paper, but the method itself is unchanged.

[4] binary.protect.io

For each assessment, answer the following ten questions:

1. Can the threat event happen without skilled malicious intent? (i.e. Could it be random, accidental, or simple to execute, or does it require conscious intent by an actor?)
2. Can the threat event be completed without unusual resources?
3. Is the asset protected against the vulnerability in any way?
4. Are there known weaknesses in the existing protection?
5. Is the vulnerability in the asset always present?
6. Can the threat event occur without meeting preconditions?
7. Will there be consequences from internal sources?
8. Will there be consequences from external sources?
9. Does the asset have or create significant business value?
10. Will the repair or replacement costs of the asset be significant?

It's not always easy to come up with an answer to these questions even in thoroughly straightforward situations, but they do enable clear and productive discussions of the actual issues. The outcome of the threat assessment is a High, Medium, or Low risk ranking.

Each assessment should only take 5 to 10 minutes to complete, and starting with a well-understood asset gives your team time to train itself in the assessment methodology. Your goal is to make the process routine, almost habitual, to the point that the majority of the assessments can be completed in as little time as possible. That gives you time and attention to focus on the more complex or poorly understood assets and threat-event scenarios facing your program without sacrificing thoroughness.

As you go through this process, it can be difficult to decide the threat scenarios to assess for a given asset. The methodology is particularly designed with a narrow scenario scope in mind; that's part of what makes it possible to address scenarios in only ten questions. That means you're very likely to need to perform multiple assessments for a single asset. Don't be overly concerned about having "too many" assessments to perform. It's one more reason for starting off with a narrow scope, and a key reason why we chose Binary for the assessment method.

Finally, remember that we defined risk as the *probable* frequency and magnitude of future loss. Reject the urge to consider movie-plot scenarios and crazy hypotheticals – they are not in scope for this program.

2.6 Asset Owners Determine Risk Responses

One of the hardest things about effective risk management is making and standing behind risk management decisions. There are many potential issues, but the simplest ones are that people are afraid of being wrong and being held accountable. Pull off a herculean effort to solve a problem, and you're a hero – even if the problem could possibly have been seen and avoided with a little preparation. But engage in a process of prediction and evaluation where the end result is a minor unforeseen difficulty, and it appears as though you've failed. It can literally be more career-enhancing to neglect risk management entirely, and just be seen solving problems when they happen, rather than trying to avoid issues in the first place. After all, no one notices the maintenance technician who solves every issue before it happens; there aren't any problems, so what's to notice?

This is another point in the program where executive support and ownership can make all the difference. On one level, of course, executive sponsors can simply demand asset owners make and be accountable for risk decisions. Far more importantly, they can act to encourage and reward effective risk management and decision making, valuing the benefits of successful planning and preparation over the visibility of occasional misses.

It's also critical to ensure that the asset owner is the one to make decisions and evaluate risk responses. Far too often, organizations give this responsibility to the risk managers themselves. This fails both on the scale of the decision-making capacity required of a relatively small group of people, and the impossibility of that group being able to accurately assess the appropriate risk response for every asset. No matter how well-informed or capable they might be, they will not be able to respond with the knowledge and assurance of those who actually work with the asset in question.

Each assessed risk requires a response plan. Rather than getting bogged down in the details of all the ways an issue can be addressed, begin with a simple response category for issues. For each identified risk, the asset owner must choose one of four options:

1. Avoid: eliminate the risk by removing a vulnerability, usually through removal of the asset. This is particularly useful in cases where a tangible but non-physical asset such as personal information has been collected out of routine rather than actual business need.

2. **Mitigate:** a response based in making the threat less likely or of lower impact. This might be accomplished by implementing additional access controls or authentication for the use of an asset, adding redundancies or backup procedures to make systems more resilient, or initiating a project to create and maintain response plans should a specific threat event happen.
3. **Transfer:** lessen the impact of the threat by transferring it outside the organization. The most common example of this is to obtain insurance against the risk, but it can also be done through outsourcing a high-risk function (e.g., payment processing).
4. **Accept:** the organization decides that the loss associated with this risk is an acceptable one. Be careful with this. "Management accepts the risk" is an easy thing to say, to the point that it's a bit of a joke among risk management professionals. Make sure that when your organization says this, it's able and willing to back it up.

The response for each risk must be documented and accepted. You should create a standard document template for Risk Decisions, documenting the decision and the information used in reaching that decision.

All four actions require a plan and execution. Even the acceptance of a risk means determining the probable impact and getting management to agree to pay the cost should it become necessary. There are many ways to make this work, but for a new or immature program the best is to use a financial model associated with signing authority, where the asset owner (or in some cases, a more senior executive) signing off on a risk response must have sufficient signing authority to cover the cost of the response.

This model also makes it easier to determine an organization's "risk appetite". For any organization, there's a financial cost level that is deemed insignificant, where the administrative overhead of close accounting at that level is greater than the benefit. In effect, the downsides of minimal oversight on low levels of spending are more important than the advantages of tracking every dollar spent. If a risk response were to cost less than that level, obviously the organization should not spend a lot of time on debating it.

On the other end of the scale, there are financial impacts so great the organization couldn't accept them, where the failure of the business is preferable to incurring such a cost. If a risk response represented a financial impact above that level, it's equally obvious that the organization should not spend a lot of time rejecting the response action as inappropriate.

Most risk responses will be somewhere in the middle, with greater and lesser degrees of attention warranted in evaluating the responses. Many formal risk management programs depend on determining the organization's appetite for varying levels of risk in advance, but that's difficult in a new or immature program. If at all possible, use the next step – the approval process – to determine your organization's risk appetite, and use it to refine the approach you take to making risk response decisions and approval levels.

2.7 Executive Review and Approval

Executive management must review the risk responses. This process includes adequate review periods, discussion, and the opportunity for the risk management team and asset owners to provide support for their decisions. At the end of this stage in the process, executive management either formally signs off on the asset owner's decision or returns it with recommendations for adjustment. Be cautious with adjustment recommendations; remember that the asset owner is more familiar with the asset and its risks than the executives in most cases. Adjustments should only be recommended when they're based on information not available to the asset owner, or on strategic considerations above their level of authority. Adjustments are never made to address personal preferences or disagreements with asset owners.

This is the third and final point where executive involvement is critical to success. In signing off on the risk responses, executives do not take the responsibility for those decisions away from the asset owners but instead formally endorse those decisions. In earlier steps we talked about the problem of encouraging responsible decision making in risk management. This step is the culmination of the executive role in preventing that problem. The goal is to remove as much of the anxiety around making the risk response decision as possible, while at the same time encouraging the asset owners to make good decisions and follow through on their responses.

One possible exception to this is with High risk determinations. The asset owners are still the best people to develop risk responses and lead remediation efforts, but the potential impact of these risk events probably makes it inappropriate to leave the risk response authority and accountability on their shoulders. Instead, the review process should involve a more in-depth executive review and discussion, and the final decision should probably be made at the executive level. The actual delineation of this point will depend on the organizational structure, size, culture, and risk appetite, but it should be made and documented in the organization's risk management process.

One additional point to keep in mind during this process is that an asset with more identified risks or even high risk levels is not necessarily a riskier asset. The number of risks and their level is a function of the imagination and thoroughness of the assessors, not objective reality. Risk aggregation, an activity defined as the collection, processing, and refinement of numerical risk data, is only possible in very mature risk management programs. In these early stages, work the individual risks rather than drawing broader conclusions.

3 Documentation and Process Management

An effective risk management program is based on a consistent, measurable framework and process. That means documentation, rigorous process management, and an effective culture of review and improvement. Documentation and review are also key requirements for regulatory compliance in risk management, for much the same reason.

Any risk management program audit will require artifacts of compliance. The Minimum Viable Risk Management Program does not require expensive Governance, Risk, Compliance (GRC) tools, although they may be helpful, but there is a minimum set of documentation that is required. Happily, the required set for compliance and the essential structure for effective programs are very similar. The document set includes:

1. A formal Risk Management policy,
2. A Risk Management process,
3. Risk assessment templates and completed assessments for the record,
4. Risk treatment decision templates and completed decision documents,
5. Risk register,
6. Meeting minutes.

You'll need to adjust this to fit within your organizational culture and documentation structure, but keep in mind this is the *minimum* set. We'll address the purpose, contents, and utility of these elements below.

3.1 Risk Management Policy

The *Risk Management Policy* documents the intent and purpose of the risk management program. The documentation should include the purpose of the risk management program, its scope, the schedule for risk assessments, and a statement that the organization will treat risks to reduce loss exposure to an acceptable level. In addition to these requirements, document the principle that asset owners must define and approve risk treatments with the support of executive leadership.

The policy must also define how often risks and treatment decisions will be reviewed, as well as the timing and cadence of regular reviews of the policy, process, and associated documents.

3.2 Risk Management Process

The *Risk Management Process* document supports the policy by providing details, procedural steps, and approval processes for risk management. It will identify the steps we've outlined above, as well as any necessary components, such as management approvals or required consultations with various departments or resources. It's helpful to create and include a RACI matrix (Responsible, Accountable, Consulted, Informed) for the various roles involved in the risk management process. Example roles you should include are:

- Risk Management Process Owner: accountable for the process, executive sponsor.
- Risk Management Process Manager: responsible for managing the process itself.
- Asset Owner: resource accountable for an asset and associated risks.

- **Process Manager:** resource responsible for risk assessment on an asset.
- **General Counsel:** legal resource to assist in identifying regulatory or legal concerns.

3.3 Risk Assessment Templates

A *Risk Assessment Template* (RAT) is a standardized way to document a risk assessment. It may be a document, a work flow ticket, or anything else that works for your organization. The completed risk assessment documents must be retained in the system of record for compliance reasons.

3.4 Risk Treatment Decision Templates

The *Risk Treatment Decision Template* is a way to document risk decisions. This may be part of the risk assessment template or separate. This form should include a description of the asset, the risk assessment, the risk rating, an executive summary of the chosen course of action and its business justification, whatever discussion points or execution outline is valuable to the organization, and a signature (or equivalent) by the accountable asset owner and/or leader. Again, completed risk treatment decision documents are retained in the system of record.

3.5 Risk Register

The *Risk Register* is a list of all risks and treatment decisions. Many audit frameworks will ask for this document by name, so it is important to maintain one. Depending on the audit framework being used, identifying a problem (such as a control deficiency, unaddressed risk, or other matter) in the risk register may mean that an audit finding is not issued, because the organization is aware of the problem and is addressing it.

3.6 Meeting Minutes

One often overlooked compliance artifact is evidence that your program is active, maintained, and proceeding. The simplest method of demonstrating this is to document and retain *meeting minutes* for the proceedings of the risk management program. The minutes should track the purpose of each meeting, the date and time, attendees, items reviewed, and any decisions made.

3.7 Process Review

Risk management is a process, but the maintenance of that process is a program in itself. There is no final state, no end to the project of risk management, where an organization's risk is completely understood and documented – unless the organization itself is dead. If nothing else, changes in an organization's assets mean the process must be repeated to ensure that asset assessments are accurate. New assets must also be assessed and documented. Documentation for retired assets must be updated to record the retirement of the associated risks. There may be program scope changes as more assets come under the purview of the risk management program. The program must be able to adjust as the organization changes; for auditability, the program must include formal review and documentation of those adjustments.

The frequency of these reviews depends on the needs of the organization. The review requirements should be documented in the *Risk Management Policy*, with accompanying elements in the *Risk Management Process*. Regulatory frameworks may require annual or more frequent reviews, which should be included in your process planning. Regardless of your chosen schedule, each review must evaluate the content and potential updates to all of the above documents (including the format of the *Meeting Minutes*).

4 Scaling, Growth, and Next Steps

A new risk management program should have a limited scope to make it manageable and increase the potential for program success. At some point, however, leadership will likely want to expand the scope as the success of the program makes the utility of risk management more obvious. When this happens, the program must scale up to meet the needs of the organization.

Factor Analysis of Information Risk (FAIR)[5] is a robust risk management and risk assessment methodology, developed by Jack Jones and adopted by the Open Group as its standard for risk management[6]. FAIR is free to read and has a sliding license scale for commercial use. The training is relatively inexpensive. FAIR can provide qualitative or quantitative analyses and does not require any vendor tools, although a platform enabling risk aggregation does exist. A single assessment takes an experienced analyst approximately two hours – considerable more than a Binary assessment, but still far less than many other methodologies.

Most importantly, FAIR uses the same narrowly-scoped scenarios that Binary does, enabling FAIR as a drop-in replacement for assets where more information is needed – and only those assets. The program can still be conducted using Binary, with FAIR assessments only used where you see a need for a more in-depth analysis. Performing Binary first requires a minimal amount of time and helps ensure that the scenarios are correctly scoped.

[5] www.risklens.com/what-is-fair

[6] www.opengroup.org/subjectareas/security/risk

When conducting a qualitative FAIR assessment, analysis doesn't require any additional tools – the assessment requires only pen and paper. The quantitative assessments use Monte Carlo techniques readily available in Excel, the R or Python programming languages, or the RiskLens platform[7].

FAIR supports the highest levels of risk management complexity and maturity. FAIR risk management programs can be fully quantitative, and they effectively aggregate that quantitative risk to show loss exposure for the whole organization. However, it's not required: the basic program outlined above (using Binary with FAIR occasionally added for clarification) is sufficient for compliance, effective at providing business value, and sustainable over the long term.

Because there is so much information available on FAIR, training may not be necessary. However, because it is very different from common risk management approaches a practitioner may have learned elsewhere, the training can be useful to clarify understanding and correct misconceptions.

[7] Everything needed to perform the assessment is documented in the Open FAIR Body of Knowledge or the companion textbook: www.opengroup.org/subjectareas/security/risk.

5 A Final Caveat

The risk management program outlined above is not perfect. Its greatest weakness is the use of Binary, which is not a robust risk assessment methodology. Careful readers might notice that it doesn't actually meet the definition of risk used throughout the paper: "probable frequency and magnitude of future loss." Binary is focused on technology, and it's sometimes difficult to come to clear decisions about non-malicious threats. Binary also does not account well for secondary losses, which aren't always obvious but can be disproportionately large. Breach notifications, fines, and reputation loss can far outstrip the immediate costs of a compromise, but they are not considered in the Binary framework. Finally, Binary is ambiguous regarding low frequency / high impact risks, which are common throughout the business world.

The use of High-Medium-Low risk rankings, while common to most risk assessment methodologies, are also problematic. Risk matrices, equally common, have their own issues. And as noted, risk aggregation and detailed analysis is impossible until your organization and program have achieved a relatively high level of maturity.

For all its weaknesses, Binary has an extraordinarily high return on investment compared to other assessment methodologies. The uncertainty reduction per minute of Binary exceeds everything else – probably by orders of magnitude. It does not require formal training: that alone democratizes the entire process. By giving untrained staff a structured way to talk about risk, it allows staff to train themselves to discuss risks effectively. The "culture of risk management" discussed in so many management journals actually becomes possible. In addition, smaller and less mature organizations are not able to tolerate much ramp-up time for a risk management program. Other methodologies may or may not provide more information in their assessments and more rigor in their practices, but they do so while requiring a major investment in training, staff time, and processing.

This program and the Binary assessment method are not designed to be your organization's end goal of risk management, but rather a starting point. The above program is achievable even for very small or immature organizations, most of which are unable to implement more rigorous risk management practices. Binary and this program will allow an organization to teach itself how to think about risk, approach it in a rigorous and defensible way, and begin to climb that maturity curve with a minimum of wasted effort and resource.

Think of this program as a scaffold: when the construction of your mature and robust risk management program is complete, there probably won't be a single piece of it left standing. Yet without the scaffolding, the project would have been much more difficult to accomplish.

6 Conclusion

Developing an information risk management program is a challenging task. Most current guidance is based on the practices of large, mature organizations that can support expensive processes and tools for the sake of audit requirements. However, there is a real need to bring solid risk management to smaller and less mature organizations that cannot afford the time or tooling required by the current guidance.

The measure of a risk management program is not whether the program passes an audit. That may be necessary, but it is the lowest possible bar – and far too many risk management programs do no more than that. The measure of a risk management program is the business value it brings. Are the processes aligned with business needs? Are potential sources of loss identified? Are problems brought to the right level for decisions, and are those decisions executed? Do the results support business objectives?

The goal of this white paper is to present a true risk management program that can be effectively implemented by a small or immature organization and that will provide value right away. While the initial assessment methodology, Binary Risk Assessment, has weaknesses, it has proven a remarkable tool for generating productive conversations about risk and allowing an organization to raise its own maturity through practice.

◈◈◈

SMOOTH SAILING SOLUTIONS

The days when a “good enough” packaged solution could meet your needs are gone. Truly effective security and privacy programs must be integral to your business, a core component of company culture.

We work with your business across the board, combining the useful aspects of your new or existing solutions with policy and procedural changes that work within your company culture and infrastructure, rather than trying to bolt on to it or replace it.

It’s your company. Your strategy. Your vision. Our crew brings the knowledge, expertise, and experience to help you transform and get you where you want to go.

smoothsailingsolutions.com