

A man in a dark suit and glasses is pointing upwards with his right hand, holding a blue pen. He is looking towards the top right of the frame. The background is a light green grid pattern.

Join the Discussion  
Connect

# Scaling Risk Management

By Benjamin Tomhave – ISSA member, Northern Virginia, USA Chapter

**Your organization - regardless of size - will be increasingly pressured to formally manage risk. The challenge comes in meeting the definition of “formal practices” without being crushed by them in the process. This article looks at a way to scale practices in a useful and meaningful manner while still accomplishing the necessary objectives.**

## Abstract

Risk management is the topic of the year. Forget about “APT” (not really). If your organization is not starting to feel the push on defining and following formal risk management practices, then you are either very lucky or about to experience a sea change.

There is an increasing amount of pressure on businesses to formalize risk management practices.<sup>1</sup> A major driver is the financial services sector, which is just now coming to grips with the 2008 credit crisis.<sup>2</sup> Unfortunately, what may be good and useful for the financial services sector is not necessarily feasible or useful for other industries. The scale of requirements and workload alone does not translate

to the SMB space. If your organization has 2,500 or fewer employees, then it seems unlikely that you can afford a handful of full-time resources just for risk management (RM). If your business has less than 100 people, then it seems laughable that you can afford to dedicate even one full-time resource to RM. And, yet, that’s what most of the extensive, formal practices being advocated would amount to.

Complicating matters is the foreseen shift to applying legal defensibility theories to your overall strategy. PCI DSS first started referencing the use of risk management several years ago with respect to patch management. We are now starting to see similar language, along with references to “risk assessment,” included in drafts circulating in Congress (e.g., the Blumenthal “PDPBA Act” Bill). The time is fast approaching where not having formal risk management practices in place will be counted as a negative, and may result in fines or other legal sanctions.

How, then, do you tackle this problem? Small firms account for 99.7 percent of all employer firms in the United States and

1 For more information, see the InfoLawGroup’s summary article, “Blumenthal Bill Bumps Up Big Fines for Data Thefts and Security Breaches,” which is available from <http://www.infolawgroup.com/2011/09/articles/privacy-law/blumenthal-bill-bumps-up-big-fines-for-data-thefts-and-security-breaches/>.

2 “A New Approach for Managing Operational Risk: Addressing the Issues Underlying the 2008 Global Financial Crisis” available from <http://www.soa.org/files/pdf/research-new-approach.pdf>.

employ more than half of all private sector employees.<sup>3</sup> These businesses do not have the resources necessary to practice RM at the same level as large multi-national corporations or the U.S. Government. There must be a way to scale practices in a useful and meaningful manner while still accomplishing the necessary objectives.

## The what's what

Before embarking into any discussion on risk or risk management, it is first imperative that a baseline be set for the conversation. Specifically, two key areas should be addressed: current literature and current terms and concepts.

## Literature review

There is no shortage of literature on the topic today. New works seem to be coming out on at least monthly basis. Here are some of the things you need to be aware of:

- **ISO/IEC 27005:2011 and 31000:2009**<sup>4</sup>: ISO 27005 was updated this past June, and focuses on integration with the rest of the 27000 series around the Information Security Management System. Its focus is on information security risk, whereas the 31000 series looks at the broader topic of enterprise risk management (ERM). In the style of ISO standards, both tend to be high-level in nature, and it bears noting that the “standardization” advocated in 31000 for harmonizing risk management processes is not the same as defining an acceptable risk management process. ISO 31000 also does not align with the current push around Operational Risk Management (ORM).
- **U.S. NIST**<sup>5</sup>: For anybody working in or with the U.S. Government, an awareness of the Risk Management Framework (RMF) is a must toward understanding FISMA compliance. How good a job RMF does of managing risk is often questioned, with a common first critique looking at how risk is assessed in the first place.
- **U.S. DOE**<sup>6</sup>: The Department of Energy recently released a new document for the electricity sector titled “Electricity Sector Cybersecurity Risk Management Process Guideline.” The document aligns with NIST RMF and FISMA, and may provide marginal value overall (its effectiveness remains to be seen). It should be noted that this recent draft document chooses to align with RMF rather than the current progressive thinking on ORM. There is a potential opportunity here for DOE to help the energy sector leapfrog a generation and go straight into modern ORM and ERM practices.

3 “How important are small businesses to the U.S. economy?” available from <http://www.sba.gov/sites/default/files/files/sbfaq.pdf>.

4 ISO/IEC 27005:2011 is available from [http://www.iso.org/iso/catalogue\\_detail?csnumber=56742](http://www.iso.org/iso/catalogue_detail?csnumber=56742) and 31000:2009 is available from [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=43170](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170).

5 For more on the NIST Risk Management Framework, please see <http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/index.html>.

6 The DOE’s draft “Electricity Sector Cybersecurity Risk Management Process Guideline” is available from [https://public.commentworks.com/CW\\_DOE\\_WF\\_InitiativeDocFiles/46/RMP\\_Guideline\\_Draft\\_for\\_Public\\_Comment\\_08312011-1.pdf](https://public.commentworks.com/CW_DOE_WF_InitiativeDocFiles/46/RMP_Guideline_Draft_for_Public_Comment_08312011-1.pdf).

- **Basel III**<sup>7</sup>: The Bank for International Settlements (BIS) operates the Basel Committee, which has released two previous frameworks relative to financial risk management. Their third release appears to increase the focus on modern ORM, in part to address issues identified by the 2008 financial crisis.
- **Modern ORM**<sup>8</sup>: Three actuarial societies have released a joint paper introducing what they term “Modern Operational Risk Management,” which looks at errors identified in traditional approaches that contributed materially to the 2008 financial crisis. This new paper puts a premium on quantitative methods, and will likely begin to set the new benchmark for risk analysis and risk management going forward.
- **COSO**<sup>9</sup>: A discussion of risk management is not complete without noting the seminal work from the Treadway Commission upon which much of the pre-2008 efforts around risk management were based.

Much more could be said about key works, such as mentioning CERT/SEI’s OCTAVE, Risk Management Insight’s FAIR, or ISACA’s RiskIT, but these start to get into risk assessment or risk analysis specifics that are best left to other debates as the focus here is risk management.

## Key terms and concepts

Being aware of key literature is useful from a research perspective, but getting down to brass tacks means setting a baseline on key terms and concepts. These definitions are meant to be usable, but it is fully expected that some readers will disagree with categorizations made. Universal agreement is not expected or likely today, which makes this step useful for providing internal consistency and reference. First, some key terms:

- **Risk**: The “Modern ORM” paper defines risk as “a measure of adverse deviation from the expectation, expressed at a level of uncertainty (probability).” This definition is a bit complex and can lead to some confusion. The FAIR methodology provides a slightly less complex definition, calling risk “the probable frequency and probable magnitude of future loss.” This latter definition actually aligns adequately with the “Modern ORM” definition and is useful for the purposes of this paper.
- **Threat**: A threat is anything that can act against an asset. It may be nature, technology, or people. Oftentimes it is helpful to think about “threat agents” and “threat communities” rather than trying to isolate to a single threat.
- **Vulnerability**: This term is often misunderstood and abused, in part due to common vernacular “vulnerabilities” associated with the vulnerability assessment/man-

7 For more information, please see <http://www.bis.org/bcbs/basel3.htm>.

8 See the paper “A New Approach for Managing Operational Risk: Addressing the Issues Underlying the 2008 Global Financial Crisis” available from <http://www.soa.org/files/pdf/research-new-approach.pdf>.

9 For more information, please see <http://www.coso.org/-ERM.htm>.

agement vertical. For the purposes of this article, the term represents the probability that a threat agent's actions will result in a loss. Instead of talking about "vulnerabilities," the term "weakness" will instead be used.

- **Frequency:** An estimated number of events in a given time period, which is typically represented as a statistical distribution. For example, how many times do you expect *Y* to happen per year?
- **Likelihood:** Fundamentally, this is a probability estimate for a single event. For example, what is the likelihood (or probability) that the Earth will experience a direct hit from an asteroid?
- **Probability vs. Possibility:** It is not unusual for people to confuse these two terms, or incorrectly interchange them. Possibility refers to a binary condition (0 or 1) of whether or not something can happen. In contrast, probability deals with a likelihood estimate on a spectrum ranging from 0 to 1. For example, if you load a single bullet each into a six-chamber revolver and the clip of a semi-automatic pistol, then the possibility that pulling the trigger will fire the bullet is 100% for both guns. In contrast, the probability of the revolver firing is 1/6 (~17%) whereas the probability of the semi-automatic firing is 100%.

There are also a few concepts to baseline that will provide additional value here.

- **Risk Tolerance<sup>10</sup>:** the "hard limit" on the amount of risk liability your organization is willing to carry.
- **Risk Capacity:** the "soft limit" on the amount of risk liability your organization is willing to carry.
- **Risk Appetite:** the amount of risk liability your organization will actively seek out.
- **ERM, ORM, etc.:** There are several different types of "risk management." Thinking about RM hierarchically, Enterprise Risk Management (ERM) is generally positioned as the umbrella category. Under that will fall sub-disciplines, such as Operational Risk (ORM), Credit Risk, and Market Risk. Information Risk (or "IT Risk" or "Information Security Risk") is now deemed a sub-discipline of ORM, which will lead to additional perspective changes in the near future.

## The pragmatic risk analyst

Given the surplus of information available on risk management, the variance in terms and methods, and the overall complexity of the topic, one might conclude that RM is simply not supportable in a formal capacity outside the rank-and-file of the large financial services organizations. Fortunately, nothing could be farther from the truth.

In its most fundamental structure, a formal risk management process looks like Figure 1. Identify an asset; assess it for val-

ue, threats, and weaknesses; perform an analysis on that data that includes consideration of the business's risk tolerance and risk capacity; and then chart a plan to address any gaps between current estimated risk levels and the desired future risk levels.

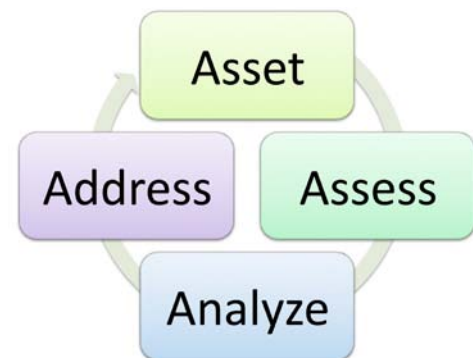


Figure 1 – A basic risk management process

Most people and organizations appear to get bogged-down in two key areas. First, there is often confusion around the first step in the process. Many people and methodologies incorrectly try to start with the desired conclusion and work backwards. For example, the OWASP Risk Rating Methodology<sup>11</sup> lists the first step as "Identifying a Risk." However, in order to identify a risk, you must first go through the process described above. How could "identify a risk" then be the first step?

The second area where people get confused is around the use of specific methodologies. Are qualitative assessments useful? Or must all risk assessments be quantitative in nature? What metrics should analyses leverage? Ultimately, the answer is the use of evidence-based methods and the development of a few key risk metrics. Confused yet? It is understandable if you are. Without devolving into a detailed discussion of various risk assessment methodologies, it is important to make a few assertions:

- The method must make sense.
- The method should produce consistent, repeatable results for all analysts.
- The method should at most make cautious use of arbitrary number schemes that seek to make qualitative assessments seem quantitative by giving word labels a numeric value (or weight).

Defining the process and methodology can provide an initial challenge. However, if you keep the above assertions in mind, then you can avoid some common pitfalls.

Understanding the foundational process of risk management is good and constructive, and should help you see that RM is not insurmountable, even for the smallest firms. There are a few other considerations to keep in mind as you develop your approach:

<sup>10</sup> For more on the author's thoughts on risk tolerance, risk capacity, and risk appetite, please see "Risk Tolerance, Capacity, and Appetite" available from <http://www.secureconsulting.net/2011/09/risk-tolerance-capacity-and-ap.html>.

<sup>11</sup> For more information, please see [https://www.owasp.org/index.php/OWASP\\_Risk\\_Rating\\_Methodology](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology).

# cloud security. can you see beyond the problem? you can

The #1 issue for companies migrating to the cloud is identity and access management. But for the agile business, *know*-ing users is always better than *no*-ing them.

In fact, agile businesses, using our Content-Aware Identity and Access Management solutions, have been able to reduce security risk while improving productivity, access and efficiency. More effective compliance, reduced IT risk, broader, more secure customer and partner relationships.

That's what happens when *no* becomes *know*. And security turns into agility.

To see how we can help make your business more agile and secure, visit [ca.com/cloudsecurity](http://ca.com/cloudsecurity)



agility  
made possible™

**ca**<sup>®</sup>  
technologies

- **Strategy:** First and foremost, you need a strategy. At a minimum, this will amount to understanding the business's risk tolerance and capacity. How aggressive should the risk management strategy be pursued? What is legally defensible for your organization or industry? If survivability is the goal, then how do you achieve that mission? These are some basic questions that will help you quickly set a strategy without devolving into academic minutiae.

**Rather than starting from everything and narrowing down to your needs, it will oftentimes be more valuable to start from the bare minimum and scale up as necessary and appropriate.**

- **Fluff and chuff:** There is a lot of noise out there. Ignore most of it. ISO/IEC 31000 might provide a useful tool for analyzing ERM approaches, but it is not the end-all-be-all. Rather than starting from everything and narrowing down to your needs, it will oftentimes be more valuable to start from the bare minimum and scale up as necessary and appropriate.
- **What's your vertical?** Not all industries are the same in terms of the requirements for formal risk management. Financial services compared to manufacturing or tourism is going to have different strategies and different needs for RM complexity. Adjust expectations according to what is most appropriate to your line of business.
- **What's "at risk" anyway?** If you cannot answer this basic question, then you need to stop everything else and start here. What is most important to the business? What are your assets? What is the value of those assets? Do you have data assets? If so, how does it enter, move around, and leave the enterprise? This is a good starting point that is often overlooked.
- **First-adopters vs. mainstream realities:** As a general rule, not everyone can be at the forefront of new methods. Formal risk analysis provides a ready example where the financial services sector is clearly pushing the envelope, but where the mainstream is well behind on the adoption curve (this is okay and expected). That said, if your organization is ready to start building a formal RM program, then there is no good reason not to start with the Modern ORM approach rather than using an older approach that may have less benefit (e.g., RMF). It is also important to note that the imperative for the mainstream to achieve parity with the first-adopters may come

sooner than expected, as indicated by recent guidance from the SEC.<sup>12</sup>

The signal-to-noise ratio around risk management is unfavorable these days, making it very difficult to extract what your business really needs. Fortunately, there is a simple approach that can help you achieve the Pareto principle effect (aka "80/20 rule").<sup>13</sup>

## Scaling risk management

Maybe you are just getting a start on formal risk management, maybe you are wondering how to even get started as there is so much to consider, or maybe your organization has some formal risk management practices, but the effectiveness just does not seem to be there today. Ultimately, scaling-down RM practices consolidates into three key steps:

1. Know thyself
2. Elucidate vision and strategy
3. Find your balance

### Step #1: Know thyself

There is one absolute place to start, and it is here: asset inventory. If you do not know what you have, then you cannot assess the risk surrounding it. Assets can be systems, products, facilities, data, methods, intellectual property, people, or any other number of things.

In addition to inventorying assets, it is also imperative that assets be valued. Not only will this information be useful when performing a risk analysis, but it can also be useful in prioritizing the spend on analysis and protective measures. If you have low-value assets, then spending a lot of time and money doing a detailed quantitative risk analysis on loss scenarios for those assets may not be cost-effective. On the other hand, if certain assets represent a disproportionately high value to the business, then that may help you prioritize efforts to invest in analyzing loss scenarios for that asset. This information will also help with setting a strategy.

### Step #2: Elucidate vision and strategy

Once you know what you have and have gauged the relative value of each asset, it is then time to set a vision and strategy. Vision, in this case, applies to metrics and measurements, whereas strategy applies to the overriding goals of the risk management program. Metrics is oftentimes where organizations bog down today as it is very difficult to find useful numbers for monitoring and trending. Let's come back to this topic in a minute.

Setting a risk management strategy can be reduced to a discussion on risk tolerance and risk capacity. Note that a formal risk analysis has not been performed yet, and that is okay.

<sup>12</sup> For an excellent analysis of the recent SEC guidance, please see the InfoLawGroup blog post "SEC Issues Guidance Concerning Cyber Security Incident Disclosure," available at <http://www.infolawgroup.com/2011/10/articles/breach-notice/sec-issues-guidance-concerning-cyber-security-incident-disclosure/>.

<sup>13</sup> For more information, please see [http://en.wikipedia.org/wiki/Pareto\\_principle](http://en.wikipedia.org/wiki/Pareto_principle).

Knowing and valuating assets is adequate to enable the business to make high-level decisions about how much is enough. How much loss is tolerable to the business? How much loss can the business absorb annually? Answering these questions can help set a baseline for risk tolerance and risk capacity. If the business can tolerate a lot of loss, then that will lead to a much different risk management program than one that cannot afford to lose much at all. In contrast, the strategy must also take into consideration just how much can be invested into formal risk management. Smaller firms may be tempted to stop with asset inventory and valuation, though it would be advisable to at least go the next step and start evaluating threats, weaknesses, and vulnerability.

As the strategy emerges, key metrics should also start to become evident. Tracking losses can be a good starting point. Additionally, grouping assets can help simplify trend analysis, just so long as it does not obscure important data points. Having a strategy is important, but only if you can measure progress against it. That is where vision comes into play.

### Step #3: Find your balance

All organizations are not equal. Multi-million-dollar multinational businesses have a far different resource profile than smaller firms working in one region. You would not ask your local mechanic to employ a staff of three full-time risk analysts to perform a comprehensive quantitative risk analysis on every little aspect of the business. At the same time, even the smallest business needs to be aware of the fundamental assets that it owns, and how to protect them toward ensuring continuance of the business. How much more risk management is needed beyond that simple analysis is up to the business to determine.

When finding the right balance, the business should consider its industry vertical, what other businesses in its vertical are doing, and what is expected of it by stakeholders and regulators (as applicable). Practices must be legally defensible, especially as applied to information risk. Government is beginning to catch-up, which means that the regulatory landscape will change.

### Conclusion

Your organization - regardless of size - will be increasingly pressured to formally manage risk. It will no longer be legally defensible to simply rely on gut calls, even if that is how business has historically been run. The challenge comes in meeting that definition of "formal practices" without being crushed by them in the process. Clearly, doing everything that the big guys do is not reasonable or scalable. There is, however, hope for scaling-down these practices. You can still build a formal process that is adequately robust and sensible. And, even better, you can leverage formal quantitative methodologies. Tools are starting to emerge that can also reduce the load in this area and help facilitate better practices. Time is of the essence. Change cannot happen overnight, and if you wait until new laws drop into place mandating that you adopt formal RM, then you will incur far greater costs than if you start slipstreaming these necessary changes now.

### About the Author

*Ben Tomhave, MS, CISSP, is Principal Consultant with LockPath, Inc., a GRC software provider. He holds a MS in Engineering Management from The George Washington University, is co-vice-chair of the ABA InfoSec Committee, and is a published author and experienced speaker. You may contact him at [ben.tomhave@lockpath.com](mailto:ben.tomhave@lockpath.com).*



## On Connect...



Chad  
Campbell

### Confused Where to Start

Hello everyone. I do not have much experience in security. I am getting my BS in Information Assurance & Security and have my Associates in Computer Networking Systems, but I do not know what certification to start. I am thinking along the lines of SSCP, CISA, and CISSP. I have the experience for the SSCP. I am looking at the CISSP, but I do not have near the experience.... Any advice would be great, I just need to know where to start.

Join the Discussion  
**Connect**



Kevin Spease

### Re: Confused Where to Start

My advice: For now, put certification out of your mind. Continue to pursue your degree while staying very active in your local chapter. You'll get better job opportunities by forging friendships and demonstrating your commitment to the community. If you have "extra" time (yeah, right) consider volunteering for non-profits who needs assistance doing security tasks. It will not only help the non-profit, it will also give you a "feel good" experience.



Donald Glass

### Re: Confused Where to Start

Before getting completely drawn by any certification have a feel of the field and the work it involves. Being an active member of the ISSA local chapter and ISACA (since you mentioned CISA) is a must do. The idea behind those certifications is to prove what you already know, not a way to jump start a new career, IMNSHO, of course. Regards, good luck and count on us to help you whenever you need it.