PenTest magazine
Aud & Stand

Risky Business:

IT security risk Management Demystified

As a career security practitioner and Chief Security Officer to several companies over the years, I was responsible for reduction or elimination threat exposures to its core business assets. Depending on the nature of that business and its size, this might be a daunting task at first blush, however, I have discovered that with an organized, systematic approach, you can approach risk management effectively.

As a career security practitioner and Chief Security Officer to several companies over the years, my significant responsibility to the organization I am responsible for is simply to reduce or eliminate threat exposures to its core business assets. Depending on the nature of that business and its size, this might be a daunting task at first blush, however, I have discovered that with an organized, systematic approach, you can approach risk management effectively. Risk simply put is the negative impact to business assets by the exercise of vulnerabilities to those assets, considering both the probability of that event as the *Single Loss Expectancy* (SLE) and the resulting impact of the occurrence, otherwise known as the *Annualized Loss Expectancy* (ALE) both terms of which I will define more in depth shortly.

This article is focused on helping you understanding the core elements of a successful IT security risk management program for a commercial enterprise, the processes of calculating the cost of a risk exposure and what the appropriate costs of mitigating those risks should be.

We must first understand what the essence of IT security risk management is which can be defined as the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. The resulting impact of an event can be described in terms of loss or degradation of any, or a combination of any, of the following three security characteristics: integrity, availability, and confidentiality. The following list provides a brief description of each security goal and the impact of its not being met: Figure 1.

IT security risk management plays an essential role in protecting an organization's intellectual property and information assets and subsequently, the business mission, from information technology related security risks. Each organization is unique and the thresholds for how much risk it is willing to accept, otherwise known as their risk appetite, will have a measurable impact on the IT security risk management program implemented. Regardless, every effective IT security risk management plan should contain three essential facets; something I refer to as The Security Trifecta in one of my books, *Governance Documentation and Information Technology Security Policies Demystified* which is a combination of governance, technology and vigilance. If you are preparing to lead a company's security function or improve what you have implemented already, I'm going to lay out a sustainable IT security risk management plan for you that should be part of your first one-hundred days on the job or at the very least, implemented during your tenure as soon as possible.

Traditionally, IT projects are approved using the *return on investment model* (ROI) and it's an essential financial measurement for any business venture and one that must be positive, or at least neutral, in order to demonstrate the viability of the proposition being examined. There are certain essential business functions however that does not provide a return on your investment; one being information security, both physical and digital unless IT security *is* your business.

They are not investments providing a return, like an ATM or e-commerce site. Security expenses if utilized correctly, earn their keep in risk avoidance or mitigation which does translate into tangible financial savings. They are about avoiding losses associated with business risks, not about financial return. The traditionally difficult part about getting funding for security expenditures is collecting accurate quantifiable measurements to base our propositions on, fortunately, there is such a model for accomplishing this and it is to leverage the mathematic power of the *Annualized Loss Expectancy* (ALE) which is the expected monetary loss that can be expected for an asset due to a risk over a one year period of time. An important feature of the ALE is that it can be used directly in a cost-benefit analysis.

To provide hopefully a brief explanation of how it is calculated, there are two factors that comprise the ALE which I mentioned briefly above. They are the *Single Loss Expectancy* (SLE), which is the percentage of the business asset you are attempting to protect with an IT security system or process that would be lost in a single exposure, and the Annualized *Rate of Occurrence* (ARO), which is the frequency the loss event I just defined occurs in a year. Those two factors multiplied together give you're the ALE (ALE = SLE * ARO). Because risk in general is grounded in uncertainty, taking a scientific approach and attempting to consistently apply a logical measurement for the likelihood the event might occur and a reasonable impact is prudent; you must find balance.

For example, suppose than a business asset is valued at $500,000 and the single cost of exposure is $150,000. Your SLE is now defined as $150,000 right? How many times in a year do we expect this exposure event to occur in a year? If we expect an exposure to occur once every year, then ARO is 100% whereas if we think there is a 50/50 shot, our ARO is now 50% right? For discussion purposes, let's suggest we think there is a 50/50 chance an exposure might occur so our ARO is .5. With our SLE equaling $150,000, multiplied by our ARO of .5, the ALE is $75,000.

In my example, if you were to spend more than $75,000 for risk mitigation by purchasing some security product or insurance, you are spending too much. You are most certainly spending too much if the product or service you deploy does not eliminate the risk or reduce it to an adequate percentage. If spending $75,000 does not set your ARO to zero, but say, cuts the risk down by 75% instead, you should reduce that $75,000 mitigation expense by 25% to bring everything back into a cost-effective risk avoidance measure.

Now, let's break down the required activities that will get us to our strategic roadmap for elim-

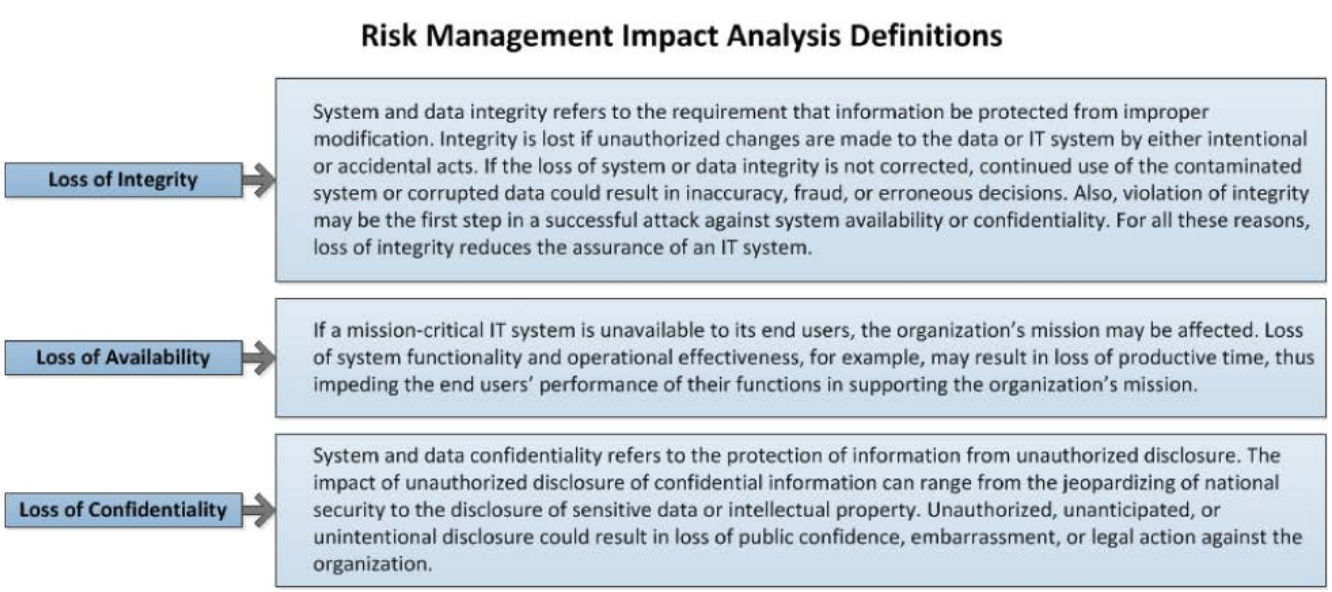

Figure 1. *Risk Management Impact Analysis Definitions*

inating business risk from technology threats. Something to remember is that IT security risk management is the close cousin to enterprise risk management and the methodology is very similar. My focus in this article is entirely on IT security risk management although technologists who understand that this methodology works for business risk evaluation is helpful as you build your business acumen; a valuable commodity if you aspire to sit at the same table with other corporate executives. You are certainly free to utilize any framework or methodology you are comfortable with but I would strongly suggest leveraging an international standard such as the ISO 27000 series, but particularly ISO 27005 for IT security risk management.

Remember, to determine the likelihood of a future negative event, threats to an IT business system must be assessed in conjunction with the threat exploiting potential vulnerabilities balanced against the controls implemented for the particular IT system. Risk impact refers to the magnitude of business damage that might be caused by the successful execution of a threat. The level of business impact is influenced by the potential business impacts we placed a value on when we calculated our ALE in the example above. This in turn produces a relative value for the business assets and business resources affected which varies depending on the mission criticality, the companies risk appetite, and sensitivity of the data threatened. These nine processes represent the basic activities you will work through during a risk assessment of your organization.

- System Characterization
- Threat Identification
- Vulnerability Identification
- Control Analysis
- Likelihood Determination
- Impact Analysis
- Risk Determination
- Control Recommendations
- Results Documentation

You might be wondering after you read through this list if any single task might be conducted in parallel? Absolutely! As a matter of fact, there are four tasks that you might want to execute in parallel to accelerate your IT security risk analysis. The following illustration represents a basic critical path diagram you might adopt for your own IT security risk assessment taken from the nine tasks listed above (Figure 2).

Now, let's dig a little deeper into each of those nine IT security risk management tasks.

System Characterization

In assessing risks for an IT system, the first IT security risk management task is to define the scope of the effort. In this step, the boundaries of the IT systems and processes are identified, along with the resources and the information that constitute the system or process. Characterizing an IT system establishes the scope of the risk assessment effort and provides information essential to defining the risk prior to defining IT security risk gaps.

I might add a further note concerning the system characterization exercise and that is it helps you define other essential IT security processes or metrics. An example would be the establishing the *recovery time objective* (RTO) used for *disaster recovery* (DR) and *business continuity plan* (BCP) policies (Figure 3).

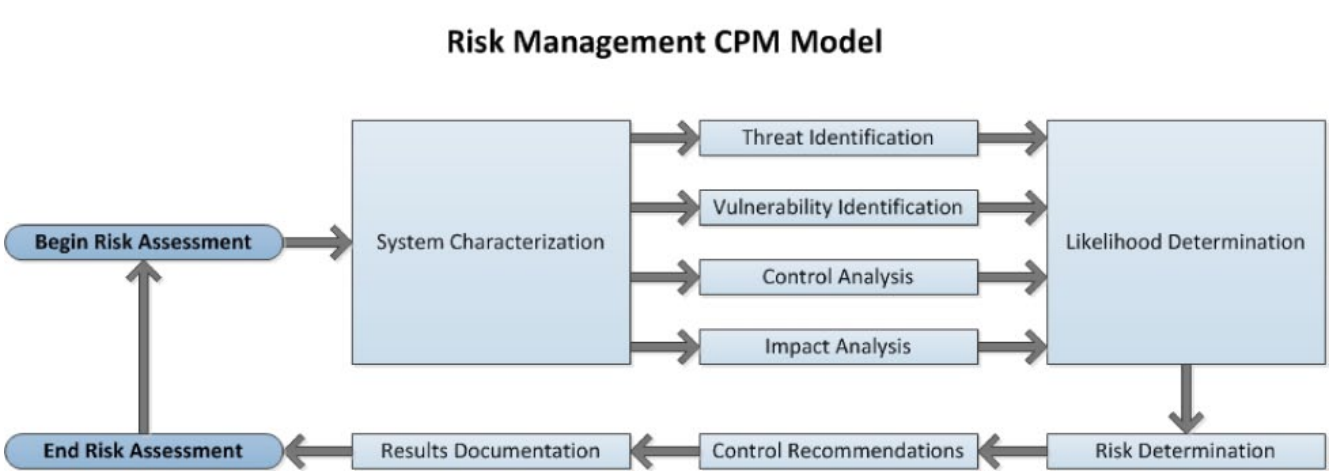

Figure 2. *Risk Management CPM Model*

Your task is to define the boundaries of the IT security risk management exercise for your enterprise. You may discover later on in the process that something has been inadvertently overlooked and those may be rolled in at any time.

Threat Identification

The goal of this IT security risk management task is to identify the potential threat-sources and compile a threat statement listing potential threat-sources that are applicable to the IT system being evaluated. Some common threats you should consider are:

- *Human* threats are by far the most unpredictable due to the fact that they may be intentional or accidental. For example, a terrorist flies a commercial aircraft into your office building. While you might not have thought about that, the fact that aircraft fly near your facility, or train passes by should have been part of your risk mitigating decisions. Another very important threat comes from your trusted employees. What if you had a database administrator who decided to leak confidential information to other employees or competitors?
- *Environmental* threats such as power outages or industrial accidents that cause IT outages. Keep in mind there are always external forces out of your control that you need to mitigate risk against. For example, what if your business was located in a flood zone and the levy failed due to an engineering flaw.
- *Natural* threats such as earthquakes, flooding, tornadoes or some other natural threat that is likely in your business region. There is a reasonable amount of data available now that you can compile a reasonable ARO metric.

You should leverag as many sources of credible information that are available to you in your particular country or region such as federal agencies, state and local government agencies, local news broadcast and publishing bureaus and other reputable public sector organizations.

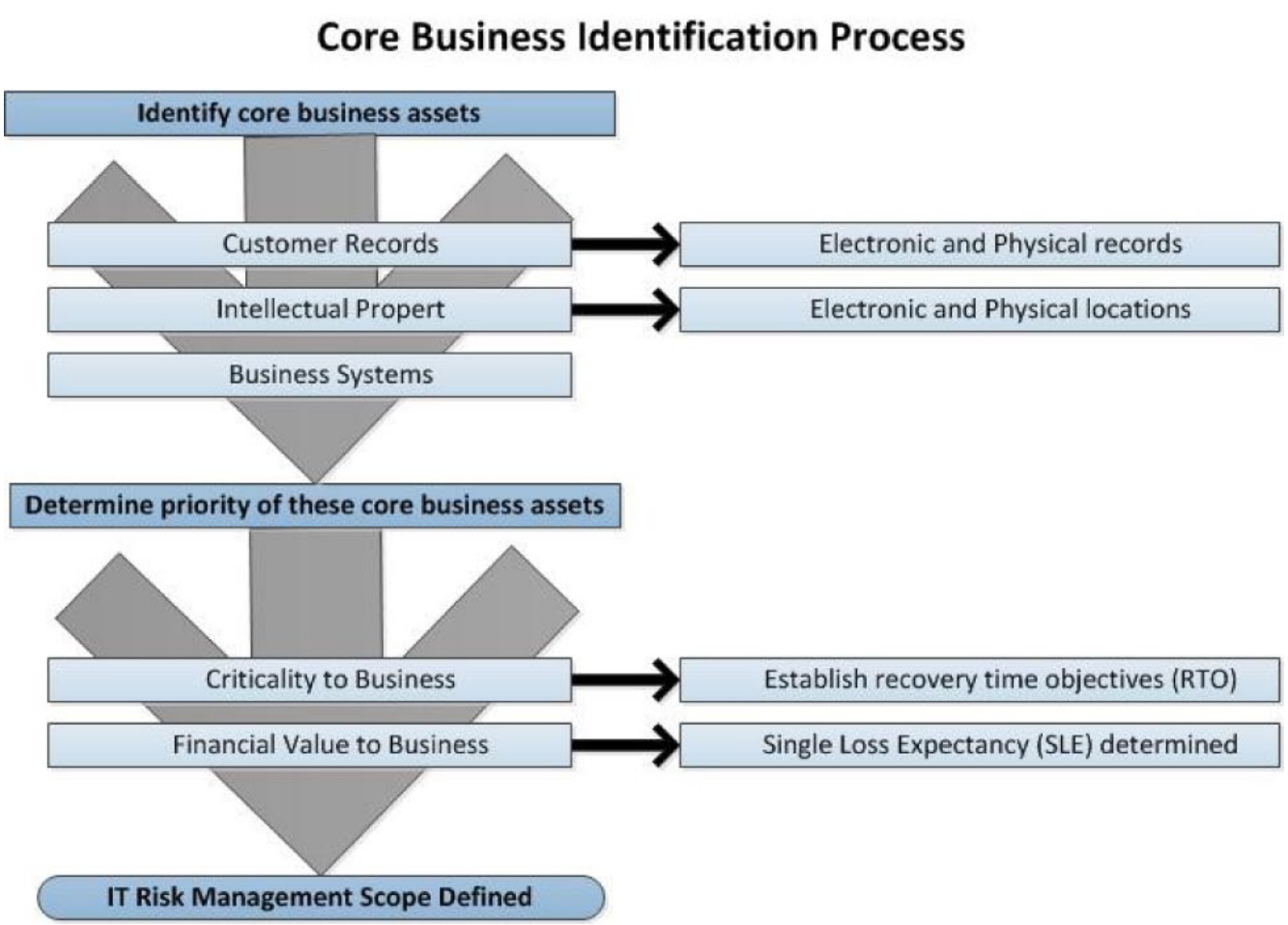

Figure 3. *Core Business Identification Process*

Vulnerability Identification

The goal of this IT security risk management task is to develop a list of system flaws or weaknesses that could be exploited by the potential threat-sources you identified in IT security risk management tasks two (2) above.

These may be found in system security procedures, through software development and system development life cycles or other internal control. Some common vectors for vulnerabilities are:

- Patch management procedures are not deployed, rigorous enough or tested.
- Employee termination checklists are not implemented properly causing control gaps in secondary access vectors such as Internet facing application administrative access.
- Firewall egress rules permit unrestricted access from trusted networks inside going out facilitating data leakage through alternative protocols.
- Policies that govern change controls, architectural reviews, project management methodologies, or software development and system lifecycles do not exist or are neglected.

Try to think like a criminal; how would you circumvent technology controls utilized? Or, what would happen if through forces of nature, connectivity to your cloud provider were interrupted; how would you process transactions or authenticate customers? You identified the sources of threats already in IT security risk management task two, now apply those findings to the systems you are examining in order of priority.

There will be significant variance in your testing and auditing opportunities due in part to whether or not the system is already in production or at the planning stage of the *software or system development life cycle* (SDLC) for example. In the initialization phase, policies and project management are of paramount importance whereas vulnerability and penetration testing are vital to production systems.

Control Analysis

The goal of this IT security risk management task is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the probability of a threat exploiting a system's vulnerability.

To get a pretty good idea of the probability an exploit event will likely occur, you should consider what the threat-source motivation and capability may be, the nature of the vulnerability and if controls currently exist and their effectiveness. For example, perhaps the threat-source motivation and capabilities, otherwise known as the means, the motive, and the opportunity in law enforcement circles, is an employee or third party with access to the centralized database systems. Without proper audit and access controls in place, the threat potential increases. Another example might be a vulnerability introduced by a software bug and the patch is available. The nature of the vulnerability is a software vulnerability that when exploited, causes the IT security risk event.

Rank your findings with a simple one, two, three numeric value or even better, a value of high, medium, or low to describe in layman's terms your control analysis (Figure 4).

Include the following facets of your operational environment in your examination:

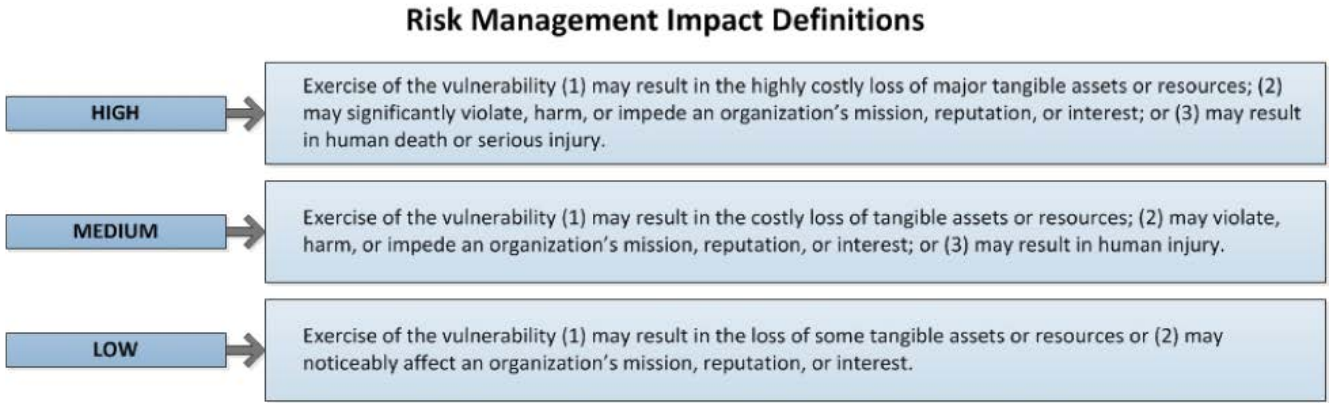

Figure 4. *Risk Management Impact Definitions*

- Identify the technology used to support core business assets such as:
  - Database and data sources: these may reside with service providers, within the enterprise or even with employees potentially.
  - Applications: both proprietary and commercial applications used for both the enterprise owned and employee owned equipment must be evaluated.
  - Operating systems: commercial and open sourced for both the enterprise owned and employee owned equipment must be evaluated.
  - Infrastructure: service providers play an important role in increasing or decreasing your enterprise risk.
  - Third party infrastructure: again, service providers play an important role in increasing or decreasing your enterprise risk.

During your identification phase, be on the lookout for what the assets command and control capabilities are. Try to determine if any control gaps exist and if there are, are any gap mitigating processes or technologies being used to remedy the risk situation?

Are there any:

- Compliance gaps?
- Technology gaps?
- Process gaps?
- Policy gaps?
- Human resource gaps?

Likelihood Determination

The goal of this IT security risk management task is to take the defined core assets and the threats you have determined to exist and attempt to evaluate the potential that risk will be exploited. Here, in this illustration, are simple questions to ask that will help you define what the IT security risk exploitability likelihood might be (Figure 5).

Impact Analysis

The goal of this IT security risk management is to take all of your measurements and calculations such as ALE into account. The key to your success will begin with solid statistics, factual data and consistent calculations. One challenge with IT security risk management is that the threats change rapidly. With the sheer number of high-profile breaches reported on recently, our exposure estimates will become more accurate.

Still, it is nearly impossible to forecast with certainty the probability of threat exposures. When you are dealing rare and exotic risk events, it probably will come down to your best guess. Your opinion may be completely different than the CFO's opinion and we all know who controls the budget (Figure 6).

This risk scale presents actions that senior management must take for each risk level. I would certainly enlist the help of your security vendors to provide these numbers. They have a vested interest in your success and their data may be compelling enough to sway the CFO.

Keep in mind though that the game is rigged in favor of the vendor's products and getting several independent examples might provide a reasonable

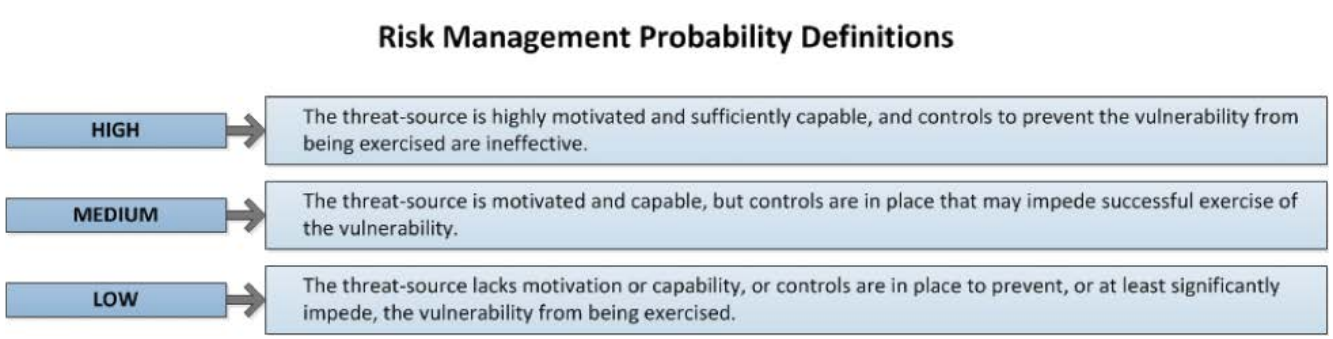

Figure 5. *Risk Management Probability Definitions*

Figure 6. *Annualized Loss Expectancy (ALE) Formula*

snapshot that is useful to your ROI, or more accurately, your ALE case (Figure 7).

Many of your calculations will be easy to quantify due to obvious impacts to revenue losses while others as I've mention, such as reputational damage, is a bit more esoteric and your best educated guess will need to suffice.

The organizations maturity will play a big role in this step because long term business data that places tangible values on business assets such as customer accounts will produce more accurate medians than the same information provided by a new company for example.

Risk Determination

The goal of this IT security risk management task is to assess the level of risk to the IT system.

The determination of risk for a particular threat or vulnerability pair can be expressed as a function of the likelihood of a given threat-source's attempting to exercise a given vulnerability, the magnitude of the impact should a threat-source successfully exercise the vulnerability and the adequacy of planned or existing security controls for reducing or eliminating risk.

As we have traversed the previous steps, we have collected certain metrics that we can now use to develop a holistic IT security risk management picture of our organization.

It is only once we understand what we are protecting can we then go about the business of protecting it.

At this point, we know what business assets supported by IT are important to the business, their values, and what out spending thresholds are going to be set at when we decide about IT security risk mitigating solutions.

Control Recommendation

The goal of this IT security risk management task is simply to provide recommendations to your organization for the mitigation of risks you have identified. Your plan should contain quantified values for the cost of mitigation as well as risks ranked in order of priority based upon the recovery time objectives and level of risk criticality to your organization.

Your recommendations will help to build a strategic roadmap reflecting at least a three year plan; possibly more and an analysis if all inflight projects for possible reevaluation if they have not been appropriately evaluated.

It is worth mentioning that not every recommendation will or can be implemented to reduce risks. The keystone to making decisions should be your ALE calculation. Some risk mitigation strategies are not viable and the risk should be either just accepted formally by management or other compensating controls may be more appropriate.

Results Documentation

The goal of this IT security risk management task is to document the findings of your risk assessment that includes threat-sources and vulnerabilities identified, IT security risks assessed, and the recommended risk mitigating controls compiled in an official report.

Some of these reports will be:

- An executive summary: This is a really high level dashboard containing a summary of prioritized risks and mitigation potentials.
- Proposals using ALE calculations: Proving business value either in profits gained or in losses reduced makes the business machine

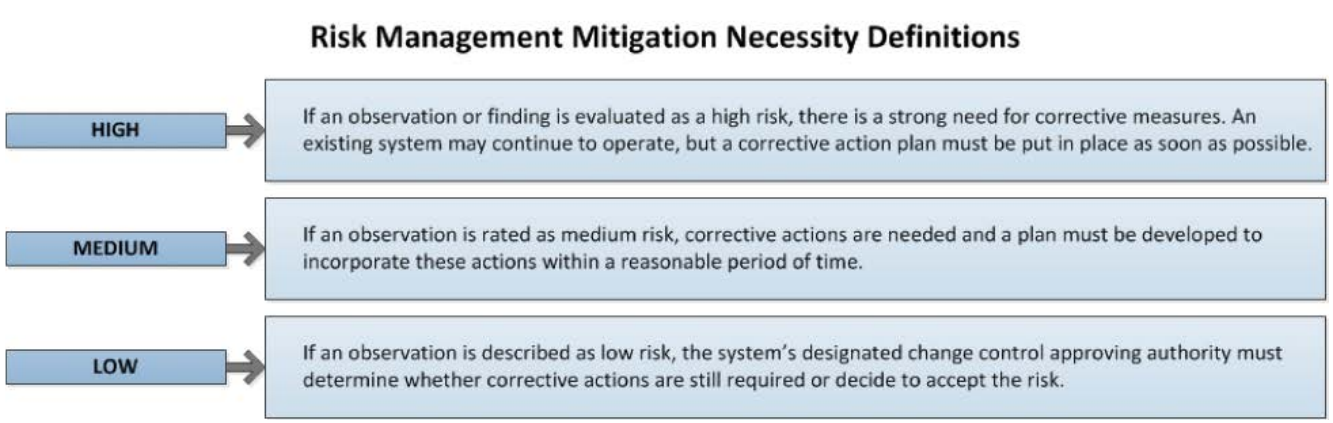

Figure 7. *Risk Management Mitigation Necessity Definitions*

run and in the security department's case, knowledge is power and it is the only way to articulate the return on investment the CFO should expect. Don't get shot down by being ill prepared. Your career, credibility and company are all on the line.

- Risk acceptance memo: Some risks will be accepted, even against your better recommendations. In that event, do yourself a favor and document the situation.
- Strategic project management plan: This report will be just high level suggestion that support your strategic roadmap for risk mitigation. If will resemble a critical path model due to the adherence to risk priorities you established already.

Conclusion

Your IT security risk management program should be recertified annually to maintain its relevancy to your enterprise and to maintain a responsible level of command and control. The IT security risk mitigating controls you put in place should be engaged continuously. This applies to the organization as a whole that was identified in the current IT security risk management exercise.

Successful risk management hinges on senior management's commitment to risk management; the full support and participation of the IT team you identified; the competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific site and system, identify IT security risks, and provide cost-effective safeguards that meet the needs of the organization; the awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization; and the commitment to the ongoing evaluation and assessment of the IT-related business risks.

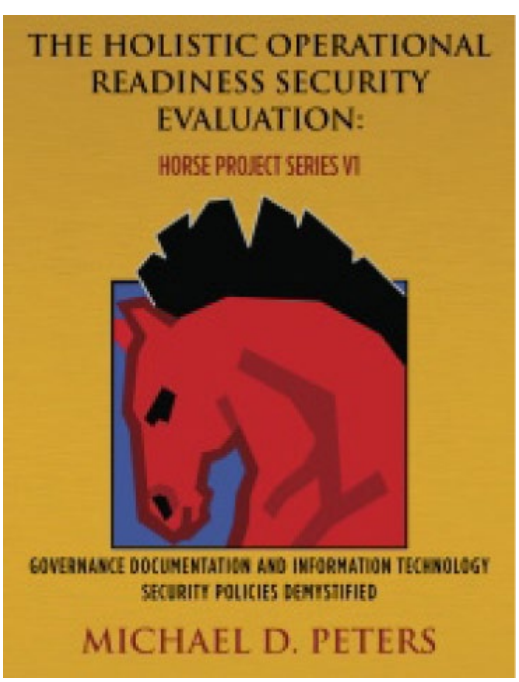

Figure 8. *Governance Documentation and Information Technology Security Policies Demystified*

Closing Comment

I've mentioned many policies in this article. You may already have these ratified but in the event that you do not, a comprehensive suite of governance documents are available in my book *Governance Documentation and Information Technology Security Policies Demystified* which will put your organization on the fast track (Figure 8).

MICHAEL D. PETERS

Michael D. Peters has been an independent information security consultant, executive, researcher, author, and catalyst with many years of information technology and business leadership experience. He has been referred to as the "Michelangelo of Security". Michael's current and previous executive positions include Chief Security Officer, Chief Information Security Officer and advising Chief Information Officer.

From a credential perspective, Michael holds an Executive Juris Doctor in Cyberspace Law; a certified MBA in IT Management, undergraduate degree in IT Security, CISSP, CRISC, CISM, CCE, CMBA, SCSA and he is an ISSA Hall of Fame recipient.

In the realm of thought leadership, Michael is the author of "Securing the C Level", "Governance Documentation and Information Technology Security Policies Demystified", "The Security Trifecta" and thousands of blogging, tweeting, social media networking and professional network syndication and industry feature publications. He has contributed significantly towards curriculum development as adjunct professor for graduate degree information security, advanced technology, cyberspace law, and privacy programs and toward industry standard professional certifications.