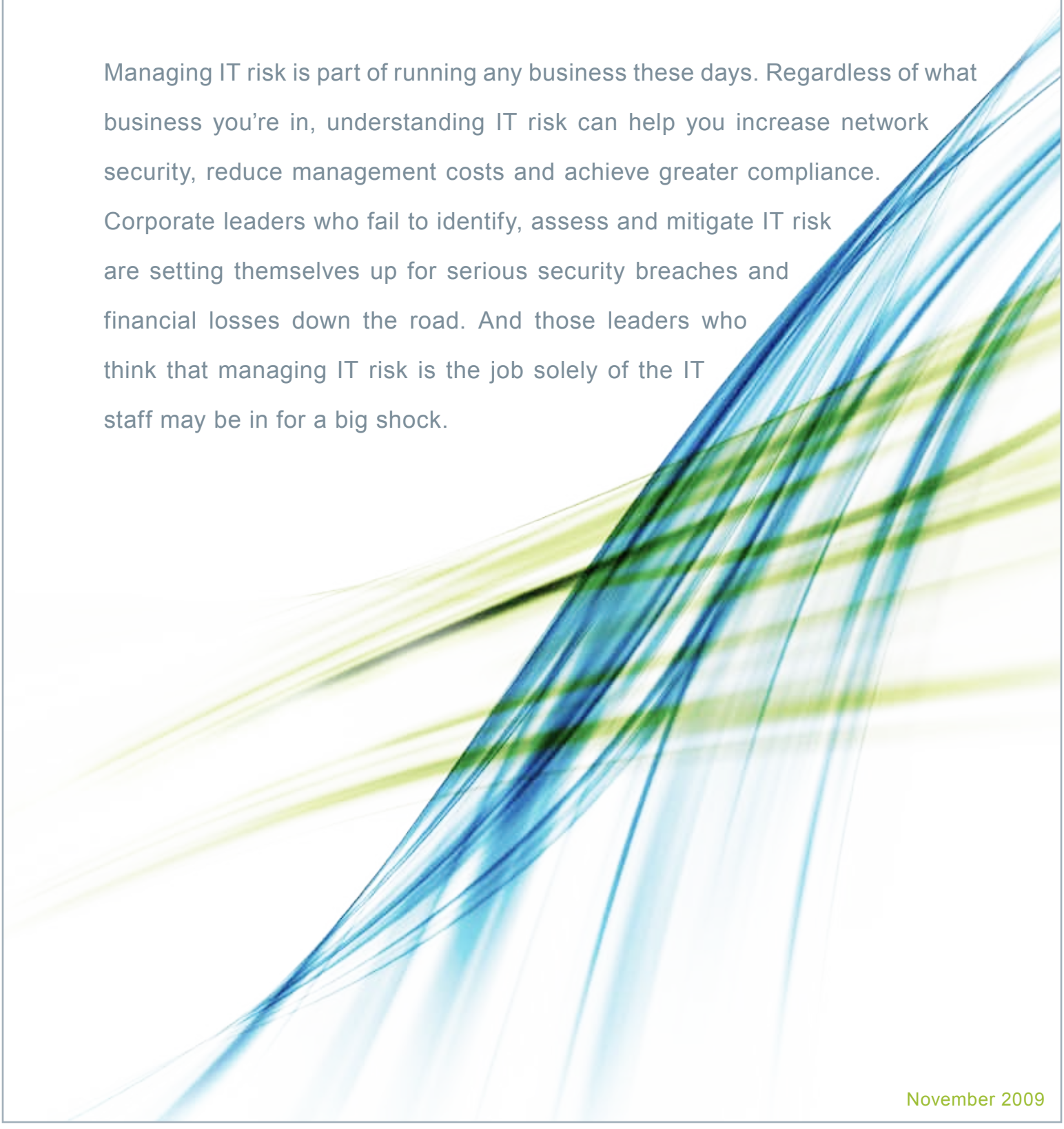
Demystifying IT Risk to Achieve Greater Security and Compliance

Managing IT risk is part of running any business these days. Regardless of what business you're in, understanding IT risk can help you increase network security, reduce management costs and achieve greater compliance. Corporate leaders who fail to identify, assess and mitigate IT risk are setting themselves up for serious security breaches and financial losses down the road. And those leaders who think that managing IT risk is the job solely of the IT staff may be in for a big shock.



November 2009

WP-EN-11-3-09

Overview

Managing IT risk is part of running any business these days. Regardless of what business you're in, understanding IT risk can help you increase network security, reduce management costs and achieve greater compliance. Corporate leaders who fail to identify, assess and mitigate IT risk are setting themselves up for serious security breaches and financial losses down the road. And those leaders who think that managing IT risk is the job solely of the IT staff may be in for a big shock.

Companies make considerable investments in people, processes and technology to ensure their businesses run smoothly. Understanding the relationships and levels of risk among these vital assets is paramount if you want to increase network security and achieve greater compliance. The challenge for most companies is to identify a repeatable process to identify, assess and remediate IT risk without interrupting their business activities.

Today, the IT risk environment is more threatened than ever thanks to the growth in sophisticated malware attacks and security vulnerabilities. Web 2.0 adoption (dynamic content sites such as Facebook and iGoogle) has added new layers of IT risk. Regulations across federal, state and local governments continue to increase, placing additional costs on organizations to meet these new and expanding requirements. Today, organizations need an intelligent approach to gaining the upper hand when it comes to assessing IT risk and managing compliance.

What Is IT Risk?

IT risk can be defined as any threat to your information technology, data and business processes. Organizations expose themselves to risk through:

- Improperly managing technology changes
- Failing to respond to deficiencies in a timely manner
- Failing to clean up dormant accounts

Mounting regulatory pressures have been at the heart of a shift of focus that's occurred over the last six or seven years. Management has a responsibility to identify areas of control weakness and respond to those weaknesses by improving processes, augmenting controls or, in some cases, reducing the cycle time between control testing to ensure that the organization is properly identifying and responding to IT risks.

In today's interconnected business climate, information security is critical to an enterprise's ability to operate. However, we know that because of labor and capital resource constraints, you can't mitigate all risk. There is always some degree of residual risk, either unidentified or known but unmitigated, that will carry forward despite your best efforts.

But the problem is that many organizations don't understand that managing their IT risk — from the shop floor to the boardroom — is critical to business success. IT's inherent risks show up in both complex and subtle ways, making IT risk management a very difficult concept to pin down and even harder to communicate and manage effectively.

> *In 2008, ISACA commissioned a survey of the top business and technology issues facing companies. Within the topic of "Managing IT Risk," the key area that respondents felt will be the most important over the next 12 to 18 months is the current lack of senior management commitment to and awareness of IT risk management, along with a lack of understanding of what IT risks are. This further illustrates that proper and frequent communication of IT risks to the management team is critical. Funding for IT risk management projects and the lack of IT risk management standards were also highlighted as areas of concern.*[1]
>
> *Within the topic of information security management, the key area that respondents believed will be the most important over the next 12 to 18 months is an inhibitor to security where the effectiveness of controls is not properly monitored. The lack of senior management involvement in setting direction for information security was also highlighted as a key area, which ties to information security being viewed as only an IT issue.*[2]

By aggregating and reporting on the impact of security risks within IT and how these risks impact the business, security professionals can become an integral part of business decision-making and help guide the organization to a more risk-aware culture.

Where Is My IT Risk?

According to a 2009 survey of 280 audit committee members conducted by KPMG in conjunction with the National Association of Corporate Directors, IT risk is a key area of concern. Survey respondents said that IT risk does not get sufficient attention by the board, and perhaps more alarming, 45 percent said they are only somewhat satisfied with their oversight of IT risk, making it the No. 1 issue for improvement. With 42 percent of respondents saying they are only somewhat satisfied with the quality of information they receive on IT risks, it's of little surprise that they feel its oversight is inadequate.[3]

Business leaders' profound lack of involvement in the risk assessment process, coupled with the lack of quality information being provided to the audit committee, shows a gap in the communication and articulation of risks between executive management and IT.

It's critical to the IT risk management process that executives not only be informed of risks, but that they assist in the quantification and definition of the business impact these risks impose. They need to sign off on the risk position adopted for the organization's assets. Only when the IT department and senior management are aligned in the identification, assessment and remediation of IT risk will a company be able to achieve higher levels of security and compliance.

To assist in bridging the gulf between IT and business executives on this important issue of IT risk management, Lumension has defined the following simplified process model to aid in the decision-making workflow regarding IT risk posture.

1. "Top Business/Technology Issues Survey Results" © 2008 ISACA .
2. "Top Business/Technology Issues Survey Results" © 2008 ISACA
3. "2009 Public Company Audit Committee Member Survey" © 2009 KPMG, LLP

Effectively Managing Your IT Risk

This process model can help elevate the IT risk conversation the appropriate business stakeholders.

1. Identify

» Identify optimal controls to meet your policy requirements

2. Assess

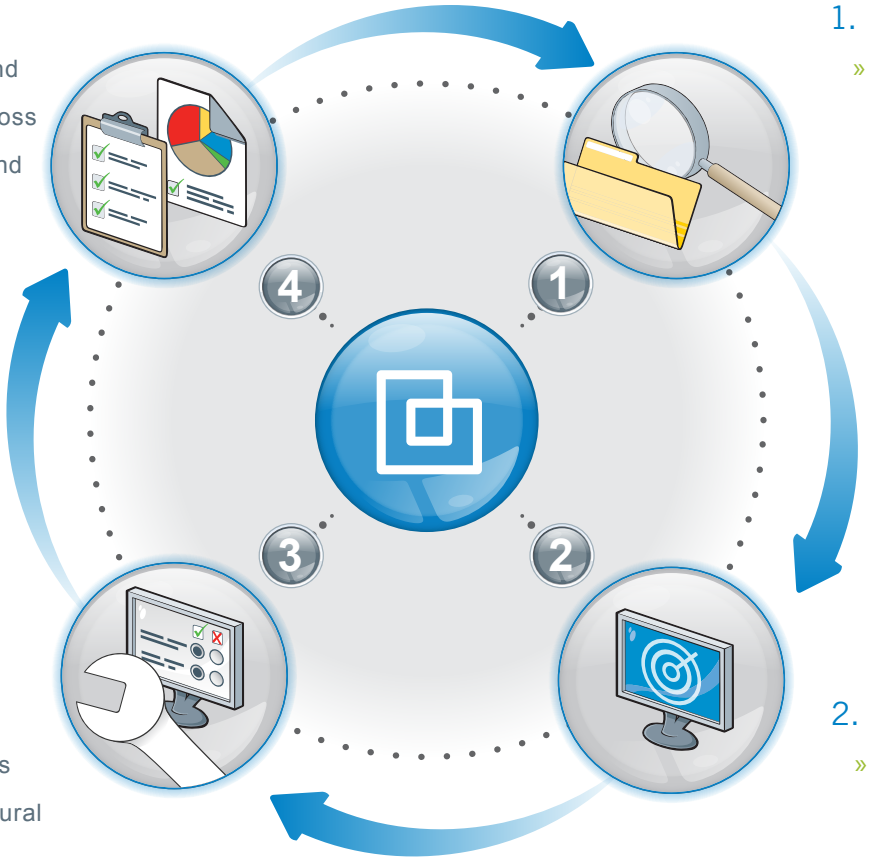
» Assess technical, procedural, and physical controls

3. Remediate

» Prioritize and address technical and procedural control deficiencies

4. Manage

» Create operational and strategic visibility across compliance, IT risk and control environments



Continued »

Step 1: Identify

The first step to understanding your IT risk is to identify the level of controls already in place for each IT asset in your organization. Based on the criticality of those assets and how they support key business processes, you can establish a profile of the risks these assets pose. To determine which IT assets are most important, you need to first understand what the business unit stakeholders worry about. There are a few core issues on everyone's minds, thanks in large part to the latest headlines.

First and foremost is privacy, or confidentiality of data. This is the risk that confidential or otherwise sensitive information (such as ePHI, cardholder information or even internal employee records) may be mishandled, divulged or otherwise made available to those who shouldn't have access to it. In many countries and regions, protection of sensitive information is required by law. Such protections are also being addressed on an industry-by-industry basis through organizations such as the PCI Standards Council for cardholder data and the HITRUST Alliance for medical information.

We're also focused on integrity risk, which is incurred when the underlying data — the lifeblood of nearly every organization — cannot be relied upon because it is incomplete, inaccurate or otherwise suspect. Tampering can be the culprit, but human error is just as likely. Perhaps it is through improper error checking on form submissions or simply an inappropriate configuration of a transaction server. Regardless of the cause, the impact to the business can be considerable, especially if the erroneous data is not discovered for some time.

Possibly one of the most well-known IT risks in an organization is availability. Many are familiar with the loss of service due to IT systems failure, but the more widespread outages of full-blown facilities failures are more infrequent. Still, weather (hurricanes[4], flooding, wildfires, etc.), civil unrest (like that witnessed in Seattle during the 1999 WTO riots downtown[5]) and critical utility disruptions (the fiber cut that disrupted communications in Silicon Valley[6]) all have the potential to impose a significant — and in many cases, long-lasting — impact on the daily operations of our businesses.

Conversely, relevance risk is rarely considered alongside IT risk, but it is perhaps one of the most common types of risk that we face. This risk has to do with not getting the right information to the right people, processes or systems at the right time. This often means that the right action is not taken or is taken too late. In the case of a trading floor or other financial operations, the effects can pile up very quickly and can have an impact that is felt globally[7].

Lastly, there is project risk, which is essentially a type of investment or expense risk — the risk that an investment made in IT will fail to provide the value we expect. This has become a favorite topic of conversation among audit and IT profession-

4. http://www.businessweek.com/bwdaily/dnflash/sep2005/nf2005097_3393_db035.htm
5. http://community.seattletimes.nwsource.com/archive/?date=20001130&slug=TTM02G0QO
6. http://news.cnet.com/8301-1035_3-10216151-94.html
7. http://www.usatoday.com/money/markets/us/2003-08-15-stocks-open_x.htm

als thanks to ISACA's development on their ValIT framework[8]. Frequently, though, the real reason IT projects fail to meet their objectives is a lack of accountability and commitment. With increasing emphasis on the role IT plays, it is vital that organizations make the most effective use of limited resources in the deployment of new technologies.

So, now what? The first step is to identify and classify your IT assets down to which servers hold sensitive and confidential information. Identifying your electronic assets requires scanning software that can inventory your network. Non IP-addressable assets (such as people and processes) require automated surveys of the key organizational areas. You can then tie IT assets to specific business processes. By understanding what your organization is trying to accomplish in the marketplace and how it fulfills that obligation to its customers and shareholders, you can find out what systems create and sustain that value. In other words, you must build a complete picture of how your assets correlate with your business functions.

Step 2: Assess

Once you have identified your assets and the outstanding IT risks to the business, you can then assign controls to them, and mitigate and manage IT risk to acceptable levels. Your organization needs to watch very closely that the implemented controls are indeed offsetting the IT risk. So far, as new risks have emerged, technologies have evolved to mitigate them, but monitoring those technologies has become an endless task.

The only way to effectively manage these growing data points is through the proper use of automation. Typically, automation efforts are focused on gathering controls data for audit support. This results in the ability to assess the environment more frequently, which has two main benefits:

1. Finding issues before they blossom into full-blown projects means that controls deficiencies can be remediated as part of existing operational efforts, as opposed to project-scale endeavors.

2. Knowing where trouble spots are before the auditors show up is a great way to show due care and that appropriate management controls are in place (despite a possible failing of a technical control).

While these two benefits showcase the power of automation, they are eclipsed by the sheer reduc-

8. http://isaca.org/Template.cfm?Section=Val_IT3&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=80&ContentID=51867

tion in labor in other areas. The packaging and production of information for auditors are emerging as new frontiers in automation.

For too long, generating and providing reports to auditors has been treated as a byproduct of the disruption they cause to our IT operations. However, by properly addressing the auditors' specific needs, by packaging and presenting relevant information, we can substantially reduce the costs associated with the process.

Automation can be used to produce meaningful and accurate reports tailored to the queries of inquisitive auditors. And by allowing auditors to serve themselves by interrogating a management systems expert (as opposed to endless meetings with IT subject matter experts), the number of billable hours spent in meetings, follow-up calls and in conducting raw data analysis can be dramatically reduced. An ancillary benefit of this approach is that it allows the audit team to add value in their assessment by reducing the amount of time spent collecting data and reporting on IT controls, and instead focusing on how the organization can best make use of its regulatory environment.

Steps 3: Remediate IT Assets

A commonly overlooked focal point to add value to the IT risk management process is in the step taken for remediation of any detected deficiencies. Organizations have limited resources to address the risks they face every day. There are three areas that can be addressed:

Capital / Labor / Time

By focusing and prioritizing IT work based upon the business impact and risk tolerances, organizations can make the best use of these scarce resources. By thinking more like a "traditional" business, security personnel can demonstrate how specific remediation activities (and even bigger project-level investments) will impact the organization's IT risk posture and where you can add the most value for each dollar spent. By assigning a business value to the remediation work, IT can show how the IT security spending has improved the organization's compliance and security posture.

After all, what is the cost of implementing new controls? By being able to assign a cost to, at the least, the implementation of new controls, organizations can begin to discuss which controls make the most sense for their given risk appetite.

> *In a recent survey by the IT Policy Compliance Group, the majority of firms surveyed are electing to choose control components from multiple frameworks[9]. The majority of the least mature firms surveyed are choosing to controls from four to five frameworks. Controls harmonization through a unified approach to enterprise controls selection, and rationalization can reduce the overhead associated with managing to multiple, often disparate, frameworks and can dramatically reduce the overall number of controls being rationalized and implemented.*

By further prioritizing controls implementation and remediation activities by level of risk , an organization can choose which activities yield the highest return on their security investment.

Once a value is assigned to an activity, though, it must be tracked. Through consistent (automated) testing and reporting on changes made by the remediation efforts, the positive results of those activities become clear. Trends emerge that can be used to show the audit committee and other key stakeholders that you are exercising due care on their behalf in responding to the shifting regulatory and threat landscape. In time, you can even show that you are continually working toward a better managed risk program.

Step 4: Manage

The goal of the management phase is to make sure there's a common goal of operational and strategic visibility in compliance, IT risk and control environments. The first requirement is to get to know your business' numbers.

All businesses run on numbers. The trick to making sound IT risk decisions is no different, and just as importantly, the first step is in finding good numbers that can be gathered (ideally in an automated fashion), and then effectively measuring and communicating those numbers.

For IT risk, it may seem logical to start with metrics generated by IT or information security; however, this tells just part of the picture. Look elsewhere in the business to see the impact of IT operations and effective security and compliance activities. This means understanding IT's business impact (as discussed in the Identify phase) and using the numbers generated by those business units to ensure that your success aligns with theirs. This way, your metrics for compliance and risk management are received in a language the stakeholders can understand — and that helps ease communication for everyone.

By frequently monitoring these numbers, you will have around-the-clock situational awareness of compliance and IT risk processes at your fingertips. Delays or long gaps in measurement can lead to doubt about the numbers' validity, potentially undermining a security department's credibility if those numbers are ever questioned. That's why it's important to leverage automation wherever pos-

9. "2008 Annual Report IT Governance, Risk, and Compliance", © 2008 IT Policy Compliance Group

sible to ensure that you are getting good quality data on a frequent basis without overburdening your staff or otherwise inefficiently using your limited resources.

This more frequent measuring of IT risk indicators allows the organization to spot trends, highlighting under- or over-performing portions of the enterprise. And this aids in the continued cycle of improvement through the Remediation phase. It also allows the organization to target areas that are underperforming well in advance of the audit and to show that management has a line of sight into those areas and that they are exhibiting due care.

Once the data starts streaming in, continue to engage those parts of the business that have been tapped for that data in your reporting efforts. This showcases the value of high-quality IT risk management, and provides a phenomenal platform from which to grow your influence and involvement in guiding IT risk decisions and improving your organization's overall risk posture. By assigning a value to the metrics you are tracking, you can build confidence in the decision support you provide to the business in terms of IT risk.

Be sure to use facts — not fear — to drive the IT risk program. It may be tempting to point out high-risk areas by elucidating the stakeholders on the incredible impact it can have on their business, but temper the rhetoric, and use real numbers to support your case. By managing with solid metrics and high-quality numbers, you are able to break out of the age-old problem of selling fear to manage risk, and build a stable base of credibility and business alignment that will pay dividends for years to come.

Conclusion

To effectively communicate IT risk and drive the mystery from this practice, IT staffs need to think and act like a businessperson, not a security person. By following this simple four-step framework, you will be able to drive value in the IT risk management process for your organization.

Remember, the keys to keep in mind when using this framework are:

- Relate IT risks to business goals
- Utilize good numbers and facts to support prioritization and remediation efforts
- Report on those numbers and highlight trends to demonstrate continued line of sight into critical areas
- Respond using fact-based decision support instead of gut instinct and fear
- Keep the business engaged to create support and executive involvement

IT organizations can take the lead in identifying, assessing, remediating and managing IT risk when they use the right tools. The result of such efforts allows companies to increase network security, reduce management costs and achieve greater compliance by effectively assessing and classifying IT risk.

About Lumension Security, Inc.

Lumension Security, Inc., a global leader in operational endpoint management and security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets. Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, and Compliance and Risk Management offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year. Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Virginia, Utah, Florida, Texas, Luxembourg, the United Kingdom, Germany, Ireland, Spain, France, Australia, and Singapore. Lumension: IT Secured. Success Optimized.™ More information can be found at www.lumension.com.

Additional Resources

- Five Ways to Reduce Your Audit Tax
- Video – Naked Truth about Compliance and Risk: Bottom Up vs. Top Down
- Webcast – Harmonizing Controls to Reduce Your Cost of Compliance
- Aberdeen Group Research – IT GRC: Managing Risk, Improving Visibility and Reducing Operating Costs

Product Information

- Lumension Risk Manager Demo-in-Depth
- Request a Personal Demonstration of Lumension Risk Manager

Lumension
IT Secured. Success Optimized.™

Global Headquarters
15580 N. Greenway-Hayden Loop, Suite 100
Scottsdale, AZ 85260 USA
phone: +1.888.725.7828
fax: +1.480.970.6323