Realtime publishers

Implementation Strategies for Fulfilling and Maintaining IT Compliance

Kevin Beaver

sponsored by

QUEST SOFTWARE®

Copyright Statement

Chapter 4: Establishing a System of Network Visibility and Ongoing Maintenance

Snapshots in time showing reasonable compliance and security are relatively simple to achieve. It's the foresight and effort required to truly make your technologies and processes work together for long-term information risk management that sets the true IT and security leaders apart.

Being in a position where you're continually reacting to the things thrown at you in IT creates unnecessary work, headaches, and business risks. By establishing a solid system of processes and technologies, you'll have what it takes to manage your environment proactively. You'll not only be able to keep things in check but also be prepared to respond in meaningful ways to the incidents that do occur.

Pulling Everything and Everyone Together into One Cohesive Structure

Sure, Rome wasn't built in a day, but you'd better be on the right track to building a solid information systems environment if sensible compliance and risk management are your ultimate goals. As with anything grand—a city, a corporation, or an IT department—there are many, many components that must work together for the greater good. In IT, this includes:

- Administration
- Assessments
- Audits
- Business continuity and incident response
- Technical support

The need for visibility is at the core of such IT functions. But what exactly does "visibility" mean? Visibility is insight and clarity. In the context of information systems, it means clearly understanding what's taking place. In other words, visibility is the what, when, where, why, and how of your applications, computers, users, and so on. Visibility not only involves the *gathering* of data but also the art and science behind doing something with it to ensure that no stone is unturned and that anomalies are brought to the forefront.

Remember

Visibility of your network environment is knowledge derived through the acquisition and analysis of the *right* information.

The need for visibility spreads across all facets of IT. At a high level, it involves your technologies, your business processes, your documentation, and your people. But drilling down further, there are numerous IT functions where visibility is required, such as those shown in Figure 4.1.

Figure 4.1: The many areas of IT requiring good visibility to be effective.

The following list highlights examples of areas where visibility could be improved in the context of compliance:

- Has Health Insurance Portability and Accountability Act (HIPAA)-regulated electronic protected health information (ePHI) been identified within your storage environment?
- Who has access to critical financial reporting applications and databases as that data relates to the Sarbanes-Oxley (SOX) Act? What access levels do these users have? Are any abuses of privileges being observed?
- Which systems are being monitored to ensure Payment Card Industry Data Security Standard (PCI DSS) compliance? Are any anomalies being observed?
- What mobile systems are present in your environment? What's their current level of protection?

Effective IT management doesn't stop with visibility. Another key component is *maintenance.* That is, keeping your systems in tip-top shape so that you can keep the joint running as efficiently as possible. Maintenance can come in the form of general software updates, disk defragmenting, file and database cleanup, and so on. Without proper tools and discipline, your information systems environment can end up in a state of dysfunction creating unnecessary work and problems that could have been prevented.

> **Remember**
>
> System maintenance in the IT world is just as important as the maintenance required for the cars we drive and the homes we live in. If we're going to get the best out of anything of value, we've got to do what we can to keep things in good running order.

Becoming Compliant as a Result of Properly Managing Information Risks

At its core, information risk management is an environment of security controls working together to ensure your information systems are kept in check and people are held accountable, followed up by the appropriate actions such as avoiding, mitigating, transferring, or accepting risk. But what exactly does this mean? It's easiest to understand when you look at what the work "risk" means.

Risk in this context is the likelihood that a *threat* (an indication of intent) is going to exploit a *vulnerability* (weakness). Figure 4.2 presents common threats and vulnerabilities.

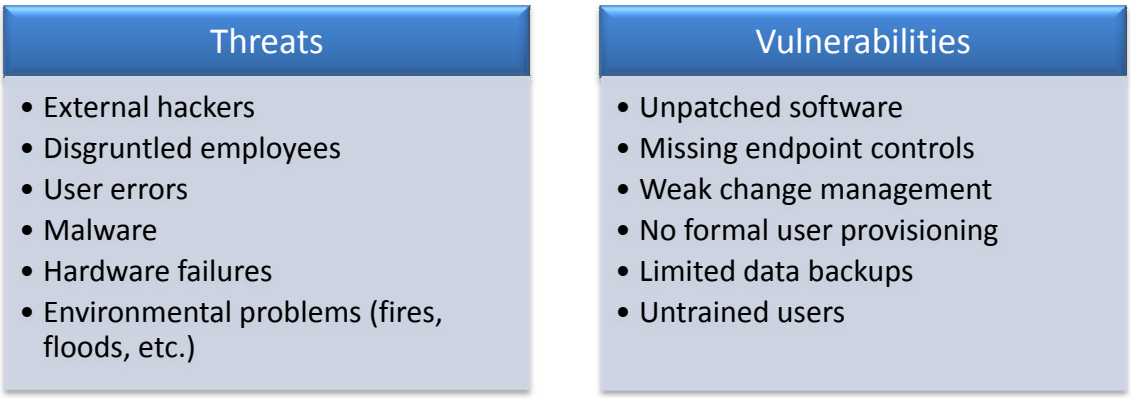

Figure 4.2: Common threats and vulnerabilities that lead to information risk.

An example of information risk is the likelihood that a threat such as a rogue insider is going to exploit a known weakness such as a gap in network account management which, in turn, leads to the subsequent remote access after the employee is terminated and repercussions associated with lost intellectual property or a data breach—not to mention potential violations of HIPAA, the Gramm-Leach-Bliley Act, PCI DSS, and so on.

Additional components involved in the information risk equation include:

- Ease of exploit that could lead to a breach
- Compensating controls that can prevent a breach
- Value of the asset or assets at risk
- Response and recovery from attack in order to minimize risk
- Legal and regulatory compliance consequences and subsequent business issues
- Diminished reputation and potential loss of business

The "management" part of information risk management involves the choices you make to minimize the threats and vulnerabilities. In other words, the steps you take to move your organization *closer* to enhanced security or push it *away* from enhanced security. You can choose to address information risks at various points in time:

- Before an incident occurs
- During an incident
- After an incident occurs
- Never

There's no doubt political and cultural factors impact how information risks are managed. Every business has its own unique issues in these areas. Looking beyond these hurdles, we know what needs to be done in order to manage information risks. It's simply a matter of getting the right people on board and knowing the best way of applying controls to make things happen.

Tip

Your overall goal of managing information risks is to come to the necessary conclusions that allow you to determine whether you need to avoid, mitigate, transfer or accept the risks you uncover.

If you focus on information risk, compliance should come naturally. By establishing an ongoing process and system where you're proactively managing your information risks rather than trying to adhere to one-off compliance mandates and checklists, you're going to be able to address risks on a consistent and ongoing basis. It's all going to come naturally as a result of the choices you make and the systems you have in place.

Remember

Compliance will emerge as a result of a well-run information risk management program.

Using Real-Time Data When You Need to Check Your Existing Compliance Status

The thing about "compliance" is that it represents a snapshot-in-time status of your information systems environment. Given the fluid nature of IT and the fact that information risks come and go, any given state of compliance is just that—a representation of where things stand *right now*.

Remember

You cannot rely on any one-time compliance status. If you do, it's easy to let your guard down and become complacent assuming that all's well when it's actually not.

It's reasonable to need to determine where things stand in the moment. You just don't want to rely on snapshots long term. Instead, look at compliance as an extension of information risk management in that it's a process—a journey.

Even with the snapshot-in-time factor, with the proper tools and processes, you can gain the insight necessary to monitor your compliance status on a real-time basis. This will allow you to monitor your environment and be able to respond immediately when gaps arise. You can hand your reports over to your auditors rather than have them tell you where things are broken. It's this type of proactive stance that will allow you to get ahead of the curve to the point where compliance becomes second nature.

Remember

You cannot secure what you don't acknowledge. You need to be in the know and on top of these things on a consistent basis.

As Peter Drucker once said, "If you can't measure it, you can't manage it." You need good data from all the critical points across your enterprise. The only way you're going to be able to acquire it with any degree of quality and certainty is by using good tools. Enterprise-level tools that gather real-time data from your environment (operating systems—OSs, applications, databases, and network infrastructure devices) are a must if you're going to make good decisions. For example, a user identity and access management system, enterprise data backup software, and a comprehensive patch management system can make or break your ability to properly manage risks and adhere to any of the given regulations you're up against.

A word of caution: Before you go out and invest your money in numerous tools, you have to make sure you know what you need to accomplish your goals. Requirements are often missing such as:

- What are you trying to accomplish long term? Example answers include: minimize business risks, lower operational costs, obtain a competitive advantage, etc.
- What are your specific risk management and compliance needs? Insight, reporting, uptime, etc.
- Which systems and information do you need to secure? OSs, databases, mobile devices, etc.
- What do you need to protect against? Criminal hackers, rogue employees, malware, etc.

All too often, people don't know what they want or understand what they need. Lack of this awareness can lead to miscommunication among staff members as well as between you and your vendors. The result can be a lot of time and money poorly invested.

Remember

All the key stakeholders in information security and compliance must be on the same page.

The Engaged Compliance Manager

I've worked with numerous compliance managers over the past few years and have found that the level of compliance knowledge and IT and information security involvement vary wildly. The businesses that have it together the most are usually the ones whose compliance managers are deeply engaged with the various aspects of IT and security.

The businesses that tend to have the greatest compliance gaps are those where the compliance manager exists in title but is otherwise disconnected from IT and security. In fact, in such instances, compliance gap analyses and security assessments requested by these businesses are often limited in scope. In other words, these compliance managers—and their colleagues inside the business—often request a finite set of checks on the technical or operational side, but rarely both.

Oftentimes, compliance managers trust—without question—the state of compliance that network and systems administrators report. However, when digging deeper, numerous flaws often exist, such as:

- Patches are often missing; the patch management process is often broken
- Web security flaws are a dime a dozen; Web security testing is often glossed over
- Weak passwords exist on the network; the main network OS password is one thing—it's all the other systems, applications, and devices on the network where the real weaknesses exist
- Audit logging and proactive monitoring are often dismissed; there is no acknowledgement that being connected into what's happening at any given time is one of the best ways to detect and prevent security breaches

Highly-engaged compliance managers know that they can—and should—utilize the tools in place to keep business information systems in check. They know they don't have to rely on what their network administrators are saying about compliance and security. Instead, they use the tools themselves. This has a direct tie-in with internal audit, and underscores the importance of everyone working together.

One of the greatest benefits of a well thought-out centrally-managed control environment is that it provides separation of duties and it ensures a system of checks and balances to help prevent the common scenario of the fox guarding the henhouse. Everything from employee monitoring to system patching to system activity logging—anything that gathers data, anything that speaks to the current compliance status of the network environment—can help compliance managers do their jobs better and make more informed decisions that are then passed up to executive management. The best way for compliance managers to ensure they're getting good data is to trust but verify.

Ensuring All Key Players Stay on Board and Are Held Accountable

Contrary to popular belief, information security and compliance are not just an IT problem. In fact, one of the real hurdles to getting management on board with security and compliance is the perception that it's all about bits and bytes—things that the techies can handle. As many businesses have learned the hard way, security and compliance are a critical business function—way more than what IT can and should take on.

Fortunately, we've come a long way in recent years with legal counsel and internal audit helping to drive the compliance component. That said, there's often still a disconnect when it comes to having all the right people on board to manage information risks. To have a useful security committee, the roles that Figure 4.3 highlights need to be on board.

Figure 4.3: People who need to be on your security/compliance committee.

In many situations, the people who need to be sailing the ship and calling shots are not involved, or worse, they're afraid to get involved. Alternatively, they simply create a set of unreasonable security and compliance policies and make those the law of the land. As Mike Krzyzewski once said, "The truth is that many people set rules to keep from making decisions." Or they believe they have enough IT knowledge and network insight that they fail to make truly informed decisions.

For this reason, the establishment of leadership is so important. There needs to be one person who chairs the committee—likely the CIO or CTO. Regardless of the role, the person needs to have a long-term vision of how information security and compliance can contribute to the business. He or she needs to be a decision maker who can add value and take action to inspire not only the other committee members but also all employees throughout the organization.

> **Tip**
> A security committee led by someone who's active and visible in the business and can lead by example will shape the outcome of the committee as a whole.

In addition to good committee leadership, the following considerations can help you ensure your committee stays connected and on track:

- Have standing meetings once a month, once per quarter, or whatever suits your business best. Don't meet for the sake of meeting. Rather, ensure your meetings are necessary and focused on the issues that impact the business the most.
- Be open-minded about outside influence and suggestions—especially from users who are impacted by your security policies and processes. It's often the people outside of IT and security who make some of the most valuable suggestions.
- Ensure a focal point of the committee is to understand how security and compliance impact the business along with developing solutions to help make sure neither gets in the way of people doing their jobs.
- Make sure the committee stays small. A lack of accountability can emerge in large committees creating a mindset of "that's someone else's responsibility."
- Get executive management involved. One of the best ways to ensure everyone stays on track is to make sure at least one executive is part of the committee from the get-go. I've seen situations where such committees report directly to the board of directors to ensure a system of checks and balances is in place.

The most important thing about a security committee is to get started. Find a colleague you know is on your side, determine the proper roles and people for your committee, and get rolling. As with all things security and compliance related, you don't have to ensure perfection. Just get started and fine tune as you move forward.

Conveying the Right Message to Executive Management

Even after you've established a security or compliance committee, you're going to have to keep the right people in management abreast of what's going on. If executive management is going to stay on board with your initiatives and provide the political backing and budget you need, they really need to know where things stand on a periodic and consistent basis.

> **Remember**
>
> Your security committee can serve as the bridge between what's taking place on the ground and executive management. Keeping your executives in the loop is absolutely essential for ongoing support.

There's a lot of talk about management being able to make informed decisions, but what does that really mean? Much of the decision making taking place at the top involves accepting certain risks. Be it a Web application risk, an IT operations risk, or a specific compliance gap that's creating business risk, you can't afford to have executives out of the loop and ignoring the issues at hand. Interestingly, what many people refer to as accepting a risk is actually management failing to learn all the pertinent facts necessary for making informed decisions.

Management relies heavily on security committee reporting as well as their IT and information security staff to keep them in the loop with what's actually taking place in the enterprise including:

- System availability
- Policy enforcement *and* policy gaps that need to be addressed
- Participation in user training and awareness programs
- Known security incidents
- Breaches of personally-identifiable information (PII)
- Current needs and forthcoming budgetary requirements

You have to be careful, though. You can talk about information risk all day long. What management needs, however, is an explanation of how these issues are impacting your specific environment and business as a whole.

> **Warning**
> It's one thing to hand over a bunch of raw data to executive management and quite another to be able to distill what that data means in your specific circumstances. Management doesn't want to know specifics about security and compliance but rather trends that will help them pull everything together so that they can make the best decisions possible.

In addition to sharing trends within your environment, you can pull together data on trends within your industry and show what similar businesses are doing. You can also share data on security incidents involving your competitors, business partners, customers, and vendors. Take, for instance, the email marketing vendor Epsilon that experienced a breach of names and email addresses along with the downstream ramifications it had on Epsilon's corporate customers. In these instances, *all parties* involved—not just the breach victim—have to understand the facts so that indirect risks can be addressed.

How Technical Staff Can Keep Management Engaged and Supportive

If there's anything that IT professionals can do to propel their careers, it's being able to communicate well with management. This means being able to see the bigger picture of the business and translate technical minutiae into something management can comprehend.

To do so has one simple requirement: Tone down the *geek speak*. By communicating on management's level and translating the bits, bytes, and protocols into something meaningful, you can gain a tremendous amount of credibility and build trust over time. To get the point across, Table 4.1 shows common terms used by technical IT staff along with what management really needs to hear.

Geek Speak	Plain English
• We're going to poke a hole in the firewall to let the extranet traffic through.	• Our network has been configured to allow our business partners to connect.
• We recently implemented whole disk encryption on our mobile devices.	• Data on our laptop computers is now more secure.
• I'm seeing some signs of Denial of Service (DoS) on the network.	• Our network is under attack.
• We need to beef up our endpoint protection with DLP and better anti-malware.	• Our workstations need better software to keep them more secure.
• Our directory service database is full of orphaned user accounts that should've been disabled.	• We're having communication problems with HR.

Table 4.1: Common IT jargon translated into words management can understand.

In so many situations, management is simply not hearing what you're saying. If you're going to contribute in a positive way to compliance and information risk management—not to mention move your career ahead—do whatever it takes to step out of this mold and become a better communicator.

Technical staff members can also get the ear of management by staying involved with more aspects of the business. This means attending business meetings and providing ideas on how IT and information security can help solve current business problems. Networking with the bigwigs at business events or even outside of work in sporting events or clubs may be in order. It may even require going back to school and earning a business degree. You'll know what approach is best based on the culture and politics within your business. Regardless, the important thing is to show genuine concern for management's needs by getting—and staying—connected for the greater good of the business.

Security Assessment Strategies

It's absolutely critical to have the right tools that provide the necessary insight into your environment backed up with solid documentation and processes to bring security and compliance full circle. That said, you still need to assess where things truly stand—how they look to the outside world—on a periodic and consistent basis through detailed information security testing.

Remember

There's no replacement for the value of information security testing that determines how things actually exist—and can be exploited—by malicious outsiders and rogue users.

When it comes to managing your IT compliance initiatives, it's often what you *don't know* that puts your business at risk. That's where information security assessments come into play.

It's important to understand the various types of information security testing. Many people use vulnerability assessments, penetration testing, audits, and information risk assessments interchangeably, but there are significant differences among these approaches (see Figure 4.4).

Vulnerability Assessment	Penetration Test	Security Audit	Information Risk Assessment
• Provides in-depth view of all facets of your technical weaknesses • Scope can be external or internal systems, often both • Relies heavily on a broad set of testing tools • Often doesn't include the exploitation of weaknesses found	• Less structured based on hacking techniques • Scope tends to be smaller, including all or a portion of external systems • May or may not include social engineering testing • Relies heavily on a more limited set of tools • Includes exploitation to prove controls are missing	• Highly structured based on control standards • Tests policies vs. actions • Includes business process reviews • Determines whether controls exist • Often references regulations/ security standards • Provides a comprehensive view of current compliance status	• Highly structured based on security frameworks and best practices • Looks at both technical and operational weaknesses • Determines overall business risk • Provides a comprehensive view of current information security status

Figure 4.4: The various types of information security testing.

There's no one best way to go about performing your security assessments. The important thing is to understand the differences between the various types and stick with a testing type that best suits your business needs and requirements. Arguably, the best approach is to combine two or more types of testing, such as penetration testing combined with security audits or vulnerability scanning combined with information risk assessments, on an ongoing basis.

> **Warning**
>
> A high-level run-through, checklist, or self-assessment is often not enough to determine what's truly exposed in your network environment.

Considerations for Doing It Yourself or Hiring a Third-Party

You know your information system best, but does that mean you're ready to take on information security testing? When determining whether to assess your own security risks, you have to ask yourself:

- Am I allowed to perform my own security assessments per customer, business partner, audit, or regulatory requirements?
- Can I really look at things from an outsider's perspective knowing what I know?
- Do I have the necessary vulnerability scanners and testing tools to find all the technical flaws that matter?
- Do I have a reasonable understanding of the common technical and operational issues that create business risk and know where to look for them?

Assessing your own security can be like a radiology patient reviewing his own MRI results or a home builder doing his own home inspections without any real training or expertise and a system of checks and balances. There's something valuable about having a third-party information security validation. It can uncover flaws and risks you might not have thought—or known—about otherwise.

> **Remember**
>
> Be careful testing your own environment. It's easy to create a conflict of interests—the *fox guarding the hen house*—which can skew your results.

If your business is lucky enough to have its own internal audit department, using internal audit professionals to perform these assessments can be a cost-effective measure as well. That is, assuming they have the relevant expertise and necessary tools to do the job well.

If you end up hiring an independent third party to perform your security testing, you need to choose wisely. There are a lot of people and businesses doing this type of work, and experience and quality of deliverables are all over the map. Some questions to ask prospective consultants and vendors to ensure you're getting what you need include:

- How long have you been doing this type of work?
- What tools do you use?
- What do you do beyond what the tools do to validate the vulnerabilities?
- What areas of our environment do you intend to look at?
- Will you need to interview any of our employees?
- Will you assess our IT and security processes?
- What deliverables can we expect? Can I see a sample report?
- Can you share references and testimonials?

You also need to find out what competitive advantages your prospective consultant or vendor brings to the table. Perhaps most importantly, after meeting or talking with the person or team, do you feel comfortable doing business with them?

Commonly-Overlooked Technical Issues to Test For

Whether you do it yourself or you hire an independent third party, be sure the technical security flaws that Figure 4.5 highlights are considered—they're some of the most common, yet most detrimental issues you can't afford to overlook

Figure 4.5: Commonly-overlooked technical issues.

In order to find the technical security flaws that matter, you're going to need the following tools at a minimum:

- OS vulnerability scanner
- Web application vulnerability scanner
- Database vulnerability scanner
- Wireless network cracking tools for WEP and WPA/WPA2 encryption
- Network analyzer
- Open share finder and PII search tool
- Operating system password cracker(s)

> **Warning**
>
> These tools are going to find/do everything. Manual validation of many technical security flaws is required, which takes a keen eye and a malicious mindset.

Keep in mind that you usually get what you pay for with your security testing tools. Commercial products typically find more of the flaws that matter and have superior reporting than their freebie alternatives. At least try to stick with commercial vulnerability scanners and use freeware and open source tools for more niche testing that the commercial vendors can't perform.

Seemingly Benign Operational Risks You Need to Be Aware Of

Technical security issues are only half the equation. There are also numerous operational security weaknesses that contribute to compliance gaps and information risks. From poor documentation to flawed IT processes, operational weaknesses actually create many of the technical issues mentioned.

> **Warning**
>
> You might as well not have any security policies or procedures if they're not going to be followed. Security documentation that's ignored can come back to haunt you in the event of a data breach or compliance violation.

Figure 4.6 lists common operational security problems that tend to get overlooked.

Figure 4.6: Commonly-overlooked operational issues.

Finding the unique technical and operational issues in your environment will not only help you minimize business risks but also allow you to determine where you need customized controls for specific regulations, business partner agreements, and so on.

Compliance Case Study

Dabbitz Financial is a financial services firm that provides portfolio management services for wealthy individuals. Given the regulatory environment in the financial industry, Dabbitz had a fairly strong information security program in place. In fact, the organization had never experienced a security incident and only had minor infractions in a number of IT audits over the past 10 years.

Management was on board with information risk management, especially given that the COO of the company was on the security committee. Outside the committee, IT staff members and the internal audit team kept management abreast of the current status of security and compliance.

Then one day it happened—a serious data breach put Dabbitz Financial in the headlines. Tens of thousands of records were exposed even though everything appeared to be in check.

A follow-up information risk assessment determined that numerous technical flaws and operational gaps were present that contributed to the breach including:

- SQL injection in the business' online portfolio management application
- Network and database accounts belonging to previous employees that were still enabled
- Missing database server patches dating back nearly 10 years

It was also determined that both IT staff and management assumed that because firewall policies and Windows Group Policies were in place that no formal security policies needed to be documented. Ditto with incident response. It was assumed that event logging on individual systems was enough without any correlation of events or formal processes to follow once a suspected incident occurred.

In so many situations, management blindly takes the word of IT and, in certain cases, internal audit that shows all as well when indeed plenty of problems exist. This is a case of in-depth and independent information security testing not being performed until a breach occurs—once it's too late.

Wrap-Up and Call to Action

Compliance is a big issue. It's practically impossible to avoid in business today. However important compliance may be in and of itself, you cannot stop there. You need to *manage information risks*. By focusing on information risk, compliance will come naturally. If you establish a system where you're proactively managing your information risks rather than trying to adhere to one-off compliance mandates and checklists, you're going to be able to address security issues as they arise on a consistent and ongoing basis.

Back in the 1990s when many of our existing technologies were being put in place, you had to manually manage everything. There was limited logging, awful reporting, and so on. But fast-forward to today and there are tons of solutions available. If compliance and information risks are going to be properly managed, you need to have the right visibility, understand the long-term consequences of the risks you uncover, and ensure controls are in place to minimize the impact in the event something goes awry. That's where good tools, good documentation, and good processes come into play. You need to be proactive. You need to get started now.

Download Additional Books from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this book to be informative, we encourage you to download more of our industry-leading technology books and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.