Realtime
publishers

Implementation Strategies for Fulfilling and Maintaining IT Compliance

Kevin Beaver

sponsored by
QUEST SOFTWARE®

Copyright Statement

Chapter 3: Simplifying and Automating to Reduce Information Systems Complexity

Simple is better. Indeed it is when you're trying to sort through the IT compliance maze and gain control of your information security program. In fact, the complexity of your information systems environment is a key factor in determining how successful you're going to be with your compliance initiatives and the amount of information risk your business faces. Furthermore, simple network or not, if you don't have some semblance of control and visibility, compliance will be a continual uphill battle—that is, an energy drain and money pit.

> **Remember**
>
> Complexity is the enemy of information security and compliance. Simple is better.

Simplifying your network, applications, and overall IT environment wherever possible and using the proper tools to ensure things are kept in check are essential.

Side Effects of Overly-Complicated Network Environments

Given that most businesses are becoming increasingly dependent on their networks, computers, and applications to stay afloat and move ahead, eventually something's going to happen such as:

- An honest user unintentionally leaking sensitive information
- A hacker penetrating a Web application or wireless network from the outside
- A malicious employee deleting data or setting up a backdoor entry point for future access
- A hardware failure or database corruption that takes down critical systems

When something like this happens, how are you going to find out about it? Are you sure you'll even know about it at all?

Warning

One of the bad things about security incidents and data breaches is that without the proper tools and insight, you might not ever find out about them Don't let the data breach databases (www.datalossdb.org) and the media headlines fool you into thinking that things may not be all that bad. The reality is known security incidents that get reported are likely the very tip of a much larger iceberg that's yet to be uncovered.

If you don't have things in order with your operating systems (OSs), applications, databases, network infrastructure systems, and mobile devices, there's no real way to know for sure that everything's in check. Consider some of the issues that make up the information systems complexity in any given enterprise (see Figure 3.1).

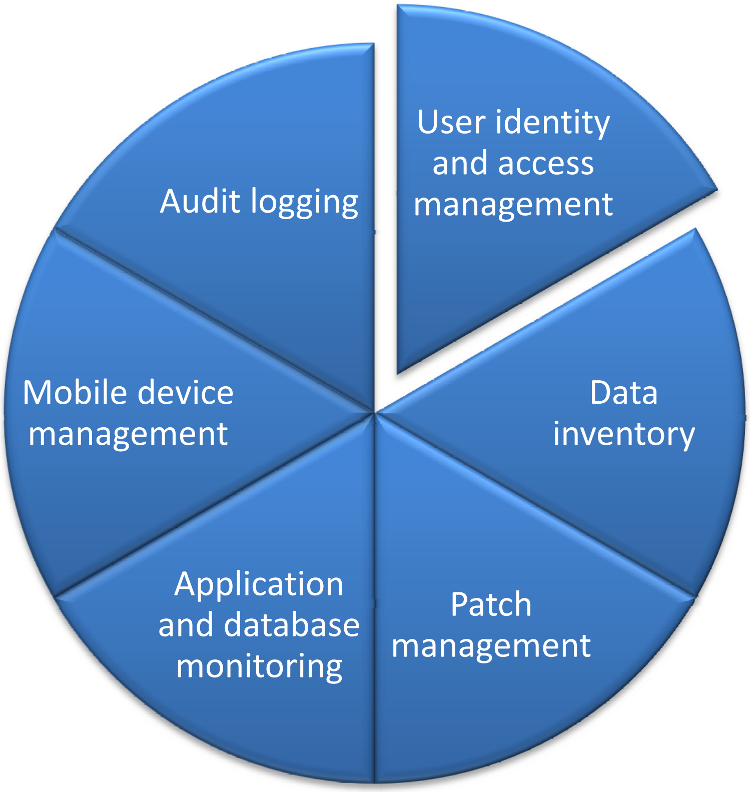

User identity and access management
Data inventory
Patch management
Application and database monitoring
Mobile device management
Audit logging

Figure 3.1: Elements contributing to information systems complexity in any given enterprise.

Audit Logging as an Example

Each of the areas in Figure 3.1 can be broken down into numerous subsections creating further complexity. For instance, consider audit logging. The logging and log monitoring function alone can place a tremendous burden on IT staff. The types of systems you're ultimately responsible for can be overwhelming when you think about it:

- Windows servers and workstations
- UNIX and Linux
- NAS, SAN, and other storage systems
- Active Directory (AD), LDAP, eDirectory, or other directory service
- Exchange and other messaging systems
- Web servers such as IIS and Apache as well as their associated applications
- Portal, document management, and collaboration systems such as SharePoint and Domino
- Database servers such as SQL Server, Oracle, and MySQL
- Virtualization environments from VMware, Microsoft, and Citrix
- Network infrastructure devices such as routers, switches, and firewalls
- Wireless networks
- Mobile devices

Logging and log monitoring can be especially burdensome when you don't even know what you need to log in order to minimize business risks and please the regulators.

Log Management Surveys Underscore the Issues at Hand

The *SANS Seventh Annual Log Management Survey Report*, which tracks the state of log management, uncovered interesting bits of information regarding the visibility people have into their networks. In particular, the top challenges for log management are normalizing and categorizing information, searching, and using logs for reporting and analysis. Interestingly, 16% of those surveyed don't collect logs for compliance purposes but of those who do PCI DSS was the leading regulation at 23%, SOX at 18%, HIPAA at 14%, and GLBA at 9%. The findings from this report show that most everyone is struggling in this area in one way or another.

Another SANS report called *Top 5 Essential Log Reports*, which outlines the log reports with the highest likelihood of identifying suspect activity while generating the lowest number of false positive reports, lists the following as the most important:

- Attempts to Gain Access through Existing Accounts
- Failed File or Resource Access Attempts
- Unauthorized Changes to Users, Groups, and Services
- Systems Most Vulnerable to Attack
- Suspicious or Unauthorized Network Traffic Patterns

Logging is only one component of your overall network environment, but it's no doubt a key factor in determining how much you really know about what's taking place.

Examples of Common IT Complexities

There's no real end in sight to the possible complexities of any given network. The set of tasks that IT staff members are responsible for on any given day is enormous. It's an unintended consequence of business progress—information overload at its finest. All of this leads to oversights in security and compliance that many businesses can't afford to take on.

Tip

Before you go down the path of looking for those needles in the haystack, you need to understand what "normal" looks like for both your logs and your network protocols. If you don't have a good baseline to compare, where do you start? It's much more difficult to detect anomalies, troubleshoot issues, and prove compliance if you don't know how things are supposed to look.

In many situations, increased information systems complexity leads to limited accountability. It's similar to government growth and complexity. The immeasurable number of laws and regulations (IT compliance included) in any given jurisdiction leads to oversights, blame and lack of personal responsibility, and ultimately little to no accountability. In fact, things often become so convoluted that new—and overlapping—laws are put on the books when existing laws would suffice if only the politicians knew about them and were willing to enforce them. The more hands in the pie, the easier it is to spread the blame. You'll often hear the following in IT circles:

- "I thought so and so was handling that."
- "But that's not really my job."
- "When are our outsourced developers going to start writing better code?"
- "I'm confident our IT staff has everything under control."
- "No need to worry, we passed our most recent audit."

More specific issues I see in my information security assessments include:

- Audit logging being enabled but no one actively managing it (arguably one of the toughest areas to get under control but one that can provide tremendous payoffs)
- Users being "required" to perform their own data backups and update their own patches and antivirus signatures (simply offloading responsibility to users doesn't solve the problem)
- Employees and contractors connecting personal mobile devices to business email and wireless networks at will

Warning

Personally-owned mobile devices such as smartphones, netbooks, and tablets are one of the greatest information security and compliance risks in any given organization today. You're probably not going to be able to stop the tide of consumerization, but you can set yourself—and your business—up for success by putting the proper mobile controls in place up front to keep things in check.

- Inconsistent steps in the user identity and access management process
- Different departments being responsible for their own systems maintenance and Web application security

Again, the more variables to the equation, such as people, policies, business processes, and technical controls, the greater the chance that something's going to be overlooked or mismanaged. Such complexities are no doubt brought on by human interactions, politics, and other intangible issues that hardly anyone is willing to take on.

Simplifying Processes Where Possible

As a person responsible for compliance and information security, one of the best things you can do is to step back and take a look at the overall problems your security management and compliance practices are attempting to solve. It will help to define what security and compliance truly mean. They're often different for many organizations depending on what you're trying to protect and what there is to lose. Ask yourself:

- How does the overall IT function tie in with the business's mission and goals?
- Are security and compliance really serving the business' needs?
- In what ways are security and compliance getting in the way of the business?
- How can we eliminate duplication of efforts and simplify what we're trying to accomplish?
- Are we really focusing on what matters?

You can't change what you tolerate in IT nor can you fix (or secure) what you don't acknowledge. Making improvements in this area requires what I briefly covered in Chapter 2—something called zero-based thinking. That is, knowing what you know now, what would you do differently to get your arms around security and compliance? In other words, if your security and compliance initiatives were perfect in every single way, what would be different? What would you do more of? Perhaps you could:

- Clean up your security policies and eliminate overlap and outdated information
- Invest in technologies that eliminate expensive manual effort and allow IT staff to focus on more analytical and strategic issues
- Determine how the effort and money you're putting towards complying with one regulation can actually help you fall in line with other regulatory requirements you're up against
- Keep management plugged-in to how information security and compliance are helping to move the business forward
- Provide examples of employees who contribute to security and compliance in positive ways

What would you do less of? Perhaps you could:

- Discontinue spending money on certain managed services or software maintenance programs that aren't contributing in positive ways
- Stop relying on high-level vulnerability scans that are often more for show than finding the real security issues that matter—things that would be uncovered by digging in much deeper and performing manual analysis
- Stop getting mired in specific regulations and, instead, focus at a higher level of information risk and then perform a simpler gap analysis to determine specific shortcomings for each regulation
- Stop relying on users to manage the security of their computers and data
- Stop assuming that employees, subcontractors, and other users are on board with security and compliance

If you're unsure where to start, Figure 3.2 shows common areas of IT management that many businesses could benefit from adjusting and simplifying in some way.

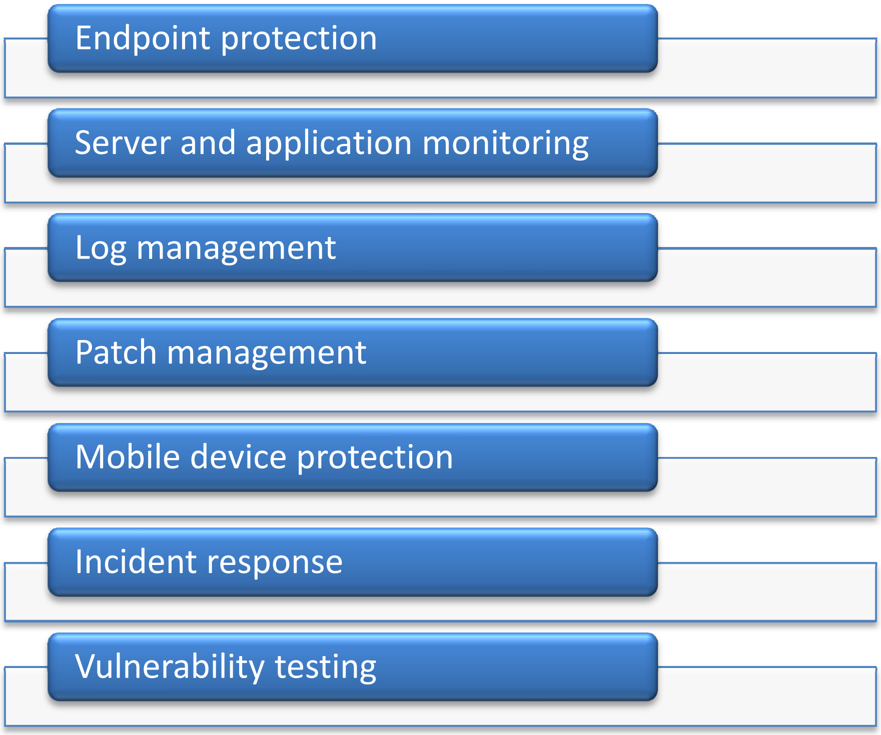


Figure 3.2: Elements that contribute to the complexity of information systems in any given enterprise.

Perhaps the most important thing is to ensure that your security controls—no matter how complex they are or how big the "Wow!" factor is—are not in place just for show. Checkbox items that merely exist to please business partners, customers, and auditors only serve to set everyone up for failure long term.

> **Tip**
>
> Take time out to step back and look at the big picture to see where improvements can be made. Start with a clean slate to the greatest extent possible. This can help you take a closer look not only at what you have under your control but also what you *do not* have under your control.

Network Considerations

As you're digging in to determine how you can simplify your network, one of the most important things you can do is to focus on the urgent issues on the important systems. That is, focusing on all the areas and issues based on the specific risks and specific compliance requirements you're up against.

Determining what's urgent and important is a basic time management and triage concept, but this exercise can help tremendously. The concept is simple:

- What information risks and compliance gaps are urgent for the business? Every situation is unique and only you and your business leaders can answer this question.
- Which systems are the most important, and therefore, need to be addressed first? This goes back to performing an in-depth information risk assessment, which Chapter 2 covers.

Table 3.1 highlights examples of urgent issues and important systems affecting businesses today.

Urgent Issues	Important Systems
No formal user provisioning, de-provisioning, and re-provisioning	AD and LDAP user directories
No standardized password policy	Server OSs, databases, and routers
SQL injection	Customer Web portal
Lack of whole disk encryption	Laptop computers
No malware protection and remote management capabilities	BlackBerry, iPhone/iPad, and Droid-based devices
Inconsistent patch management	Windows servers and SQL Server-based systems
Open (clear text) and WEP encryption enabled	802.11-based wireless networks behind the firewall
No formal change management process	Network infrastructure devices
No standardized security settings	VMware and Hyper-V-based virtual systems
Inconsistent software testing	In-house software development life cycle process
No performance monitoring and alerting	Public and private cloud-based applications
No formal security awareness and training program	Personnel accessing PII in critical customer applications

Table 3.1: Urgent issues and associated systems they're commonly found on.

The possibilities for urgent issues on important systems are infinite, but you get the point.

Once you spend the time, money, and effort addressing the critical areas you initially uncover, you must go back and review to determine what other areas need improvement. It's a continuous cycle you'll work through moving forward (see Figure 3.3).

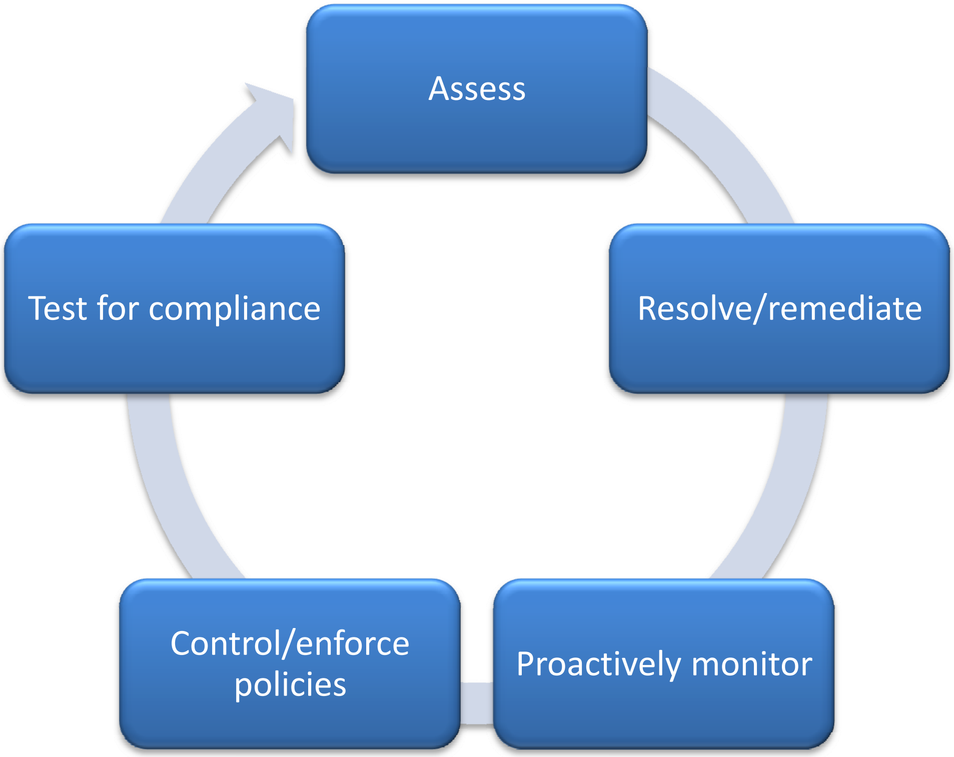


Figure 3.3: Cycle of assessment for network improvement.

Remember

Don't get caught up in the snapshot-in-time mindset. Taking a one-shot approach that looks at security and compliance and then puts it to rest is the formula for trouble. Sure, your security and compliance posture is what it is during any given assessment, but systems configurations, vulnerabilities, and business processes are sure to change at any given time; therefore, you have to revisit security and compliance on a periodic and consistent basis.

Create an Ongoing Process

Your ultimate goal is to have a *sustainable* and *repeatable* process that allows you to get more and more granular over time, uncovering the issue areas that matter. Chapter 2 offered three main pillars of information security compliance:

- Confidentiality—Helps ensure that data is revealed only to those authorized to see it
- Integrity—Helps ensure that data remains free from unauthorized creation, modification, or deletion
- Availability—Helps ensure data is available when access is desired

These pillars apply to practically every information security and privacy regulation across the board including:

- PCI DSS
- HIPAA
- HITECH Act
- GLBA
- Sarbanes-Oxley
- State breach notification laws

Some regulations focus on certain areas more than others. For example, PCI DSS and the state breach notification laws focus on data confidentiality and Sarbanes-Oxley focuses on data integrity. Your needs and requirments are going to be unique. That said, there's a common thread that runs through all compliance regulations: *protect electronic information*.

Well-Written Security Documentation Is Critical

One of the most commonly-overlooked areas for simplification is security documentation—that is, security policies, procedures, and formal plans such as incident response and disaster recovery plans. The interesting thing about security documentation is that it's rarely worth the paper it's printed on. Policies are often too broad or they're outdated and thus no longer apply to the business environment. Specific procedures that help carry out what policies state are often too generic or they don't exist at all. As for security plans, in all but the most advanced of midsize and larger enterprises, they're often non-existent.

> **Warning**
> It's not uncommon to find that employees are completely out of the loop on what's expected of them when it comes to information security and privacy. Many times, policies, procedures, and plans are in place yet very few people are aware of their existence and what they're trying to accomplish.

Many times, security documentation is put in place to please auditors rather than facilitate business and minimize information risks. This not only creates a false sense of security but also sets up the business for trouble down the road when a security-related situation actually occurs. The trouble can be in the form of:

- Failing to understand what actually constitutes a security violation or incident
- Not knowing how to adequately respond to the situation
- Getting caught up in the complexity of the documentation, which can make things worse including unnecessary data leakage, evidence spoliation, and more

Policies state "this is how we do things" here, and procedures and formal plans outline "this is what we have to do to carry things out."

Cookie-Cutter Templates Simply Won't Cut It

It's quite common for people who are not familiar with the inner workings of IT and information security to go online and download security policy and plan templates and call them their own without tweaking them for their unique business needs. This issue is especially prevalent in smaller businesses that know they have a need for such documentation but don't have the resources to do it well.

I never recommend people re-create the wheel when the grunt work has already been done by someone else. There are plenty of good starter templates available online. However, when it comes to security policies and plans, you absolutely have to adjust them to meet your needs. At least change the business name in the templates you use (don't laugh, it's happened)!

The reality is that you shouldn't create *any* security documentation unless and until you determine your information risks. By knowing what you're up against first, you'll have a clearer understanding of the technical controls, documentation, and associated business processes required to make things happen.

An effective security policy contains the following sections:

- **Introduction** that outlines the specific policy topic covered
- **Purpose** that states what the policy is attempting to accomplish
- **Scope** of departments, systems, people, and so on to which this specific policy applies
- **Roles and responsibilities** for those involved in managing or enforcing the policy and/or specific tasks for which each person is responsible
- **Policy statement** of the actual policy outlining what can or cannot be done (this is the meat of the policy document)
- **Specific procedures** to carry out or enforce the policy
- **How compliance will be measured** and tested to ensure that employees, systems, and so on maintain compliance
- **Sanctions** that outline the consequences of non-compliance with this policy
- **Review and evaluation** listing when and how this policy will be evaluated or audited for ongoing compliance and maintenance
- **References** of applicable regulations or standards sections
- **Related documents** of security standards (ISO/IEC 27002, etc.), other policies, and so on that tie into this policy
- **Revisions** listing who, when, and why information related to any changes made
- **Notes** for future reference as needed

Note the brevity of this layout. By concisely listing pertinent information, you can keep each policy simple and to the point. Doing so makes it easier to understand and update when needed. Also note that this approach has one policy per document, which can keep your policies better organized and easier to reference and manage going forward.

Common Policy Base

Every business' needs are unique; however, a specific base of policies is often needed regardless of the situation. This typically includes:

- Acceptable usage
- Change management
- Data backups
- Hiring and termination
- Information classification and retention
- Mobile device handling
- Patch management
- Physical security
- Remote access
- Travel
- User authorization
- Wireless networks

In the interest of simplicity and making your policies work for you, the following list highlights a few things to keep in mind on why security policies are violated:

- Users don't understand them
- Users don't buy into them
- Users know they won't be enforced
- The person's desire to violate a policy outweighs his or her perception of the risks involved

Ways that you can ward off policy violations and minimize your compliance gaps include:

- Establish and build trust by making sure employees completely understand what's going on
- Be sure to set clear expectations so that no one can say they were out of the loop
- Talk about the business reasons behind the policies
- Rather than being secretive, keep people in the know
- Ask for feedback and suggestions on policies—some of the best ideas come from people completely disconnected from IT and security

- Tie policies into employee reviews to give people an incentive to abide by them
- Lead by example to help influence your organization's culture
- Make sure your policies are actually enforced so that people understand the seriousness of the issue
- When someone does a good job following or enforcing a policy, make it known to others in your organization

Going beyond policies are your detailed security plans—in particular, your incident response and disaster recovery plans. This documentation lays out your flight plans for when something goes awry. They get everyone on the same page and contain specific steps that key players need to take during critical times when you may not have the capacity to think things through. The main difference between the two types of plans is that incident response plans address technical security incidents, malware outbreaks, data breaches, and the like while disaster recovery plans (often called business continuity plans) address what to do in the event of a natural disaster, physical destruction of a building, system outages, and so on.

Tip

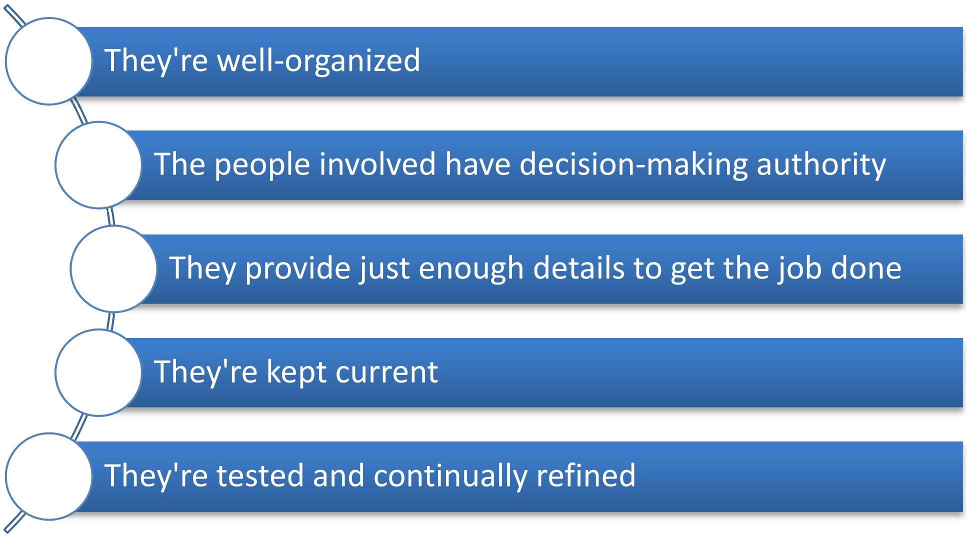
It can be argued that disaster recovery plans are different from business continuity plans and therefore address unique issues. It could also be argued that incident response procedures should be part of an overall business continuity plan. Semantics aside, just make sure you're doing *something* to address these critical—yet often overlooked—areas of information security and compliance.

For maximum value, approach incident response and disaster recovery with the following assumptions:

- Your building(s) and/or information systems will be damaged
- You cannot take anything with you once an emergency strikes
- You will not be able to gain access back into your building(s) or to your data

This simplified view of these critical functions can help ensure you're focusing in the right areas.

The details and nuances of security policies and plans could easily provide enough material for a dedicated book. However, there are a few key traits of effective security documentation (see Figure 3.4) that can help you get on track and rolling in the right direction.



They're well-organized

The people involved have decision-making authority

They provide just enough details to get the job done

They're kept current

They're tested and continually refined

Figure 3.4: Key traits of effective security policies and plans.

Remember

Security documentation isn't there just for the auditors. It's there to assist you in your security and compliance needs and to minimize your information risks over time. Everything is much simpler and less stressful when you have documentation and specific procedures in place when you need them.

A Committee Is Key

Interestingly, many organizations are without solid security policies as well as incident response and disaster recovery plans. This all-too-common oversight is something that hardly any business can afford to ignore—if anything, for the sake of being "compliant." Getting to the root of the problem, the absence of security documentation is often related to not having all the right people on board to make security and compliance decisions.

Forming a committee consisting of IT and compliance stakeholders is absolutely critical. It's also very important for such a committee to not involve too many people to avoid becoming overly bureaucratic and dysfunctional. Figure 3.5 shows the various roles within any given business that should be involved in the security and compliance decision-making processes.

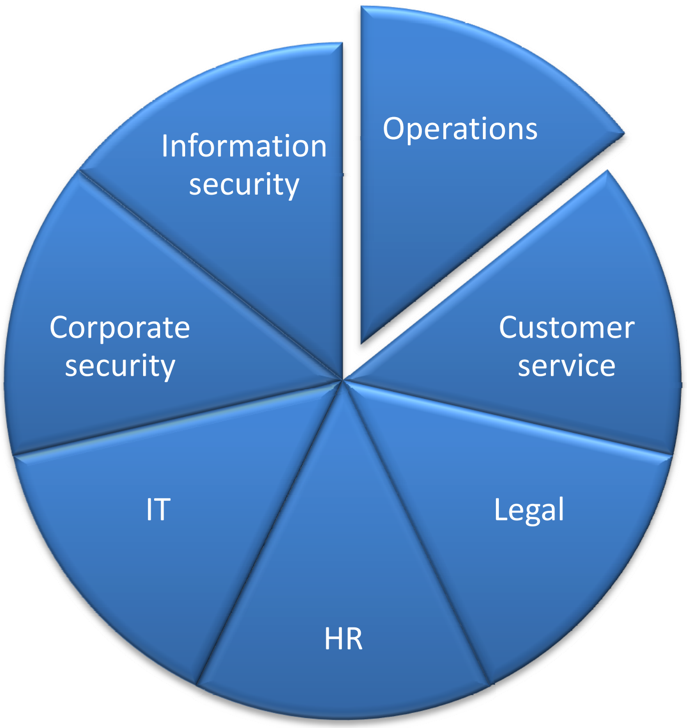


Figure 3.5: Business roles that need to be involved in a security committee.

Although commonly handled this way, security and compliance-related decisions aren't all about IT and the technical folks. Security and compliance have far-reaching implications into virtually every aspect of the business and, thus, key players in those functions need to be involved who are then backed by executives at the top. The reality is that businesses with functional committees addressing security and compliance oversight are much more adaptable and ready to handle challenges and problems that predictably crop up. The businesses that choose not to have such oversight are destined to run into trouble and be made to look bad in the process.

Tip

If you're currently trying to form a security committee or want to improve your existing group, one of the most important things you can work on is building your credibility and getting people on your side. The basis of doing so is building the relationships you have with these people, establishing trust, and doing things for them that helps them in their jobs without asking for anything in return. Key to this accomplishment is understanding what motivates people. People are motivated by two main factors: the desire to gain and the fear of loss. Whether you're doing so for other committee members, executive management, or your users, determine what people want—or are afraid they're going to lose—and focus your approach to security and compliance in those terms.

Using Technology to Automate

No matter how detailed and effective, your security policies and plans cannot stand alone. In many situations, the only effective way to ensure your policies are enforced and that your procedures and plans are carried out is to use technical controls wherever it's reasonably possible. People and processes cannot do it alone.

> **Remember**
>
> Policies state *this is how we do things here* and security procedures and plans outline *this is what we have to do to carry things out*.

Technical controls are essential for enforcing policies where it's unreasonable to have people and processes do it alone. In reality, compliance is dependent on a relatively small number of technologies:

- Account management
- Anti-malware, data loss prevention, and similar endpoint controls
- Audit logging
- Data backups
- Encryption (especially for data at rest)
- Network traffic monitoring and alerting
- Software patching
- Virtualization management
- Vulnerability scanning (penetration testing, source code analysis, and so on)

With a relatively small number of technical controls in place, you could not only have a secure network but also comply with the majority of compliance regulations.

> **Tip**
>
> Don't forget about the security controls built right into the systems you already have at your disposal. Your network infrastructure systems, OSs, mobile devices, applications, and databases likely already have—at a minimum—some rudimentary controls you can use to your advantage. If you determine you need more enterprise-level controls in certain areas, you can always expand out from there. Before doing anything, think long and hard about what you're trying to accomplish so that you don't have to address your technical controls multiple times moving forward.

As with any technology, your technical controls for security and compliance will have to be adjusted and customized over time. Given that security documentation is a work in progress, your policies and plans require continual adjustments as you adjust your technical controls. If you do one and not the other, gaps can form and you'll have even bigger issues on your hands.

Finally, showing the return on your technology investment is required if you're going to maintain buy-in. In other words, proving that all the time, money, and effort that goes into security and compliance is not in vain is essential for ongoing support. This proof can be acquired relatively easily as long as you're willing to do some legwork up front. Some proven methods are:

- Providing information on potential security breaches *prevented* because X, Y, or Z control was in place
- Showing how incidents that do arise were effectively handled because you had the proper plans in place
- Demonstrating how certain technologies (that is, identity and access management) and/or business processes (systems monitoring or vulnerability testing) are simplifying things and saving money over time

It's easy to throw money at a problem and be done with it. But if you don't go back and revisit the issues, see how things can be improved, and demonstrate how your controls or documentation are benefitting the business and providing some semblance of return on investment (ROI), then all of your efforts can be in vain.

Tip

ROI is defined as the value received from something divided by its cost over a given time period. It's often very tricky to quantify in terms of security and compliance. After all, we're IT professionals, not finance experts. It certainly doesn't hurt to try to work up some numbers to share with management—especially if you can get the help of a trusted source in your finance department! A good starting point is to use one of the many ROI calculators available online.

Compliance Case Study

Nissti & Company is a large medical group providing primary care, hospital, home health, and related services to a large metropolitan community. With its 10,000 plus employees and network of 12,000 business associate users—each of which has a unique user account within the Nissti & Company network—the business was looking for a way to minimize the effort involved in the process of provisioning (adding), de-provisioning (removing), and re-provisioning (moving or re-assigning) users. Along with assistance from the finance department, IT staff members were able to determine that user identity and access management was costing the company more than $100,000 a year. Furthermore, the process was creating security holes and compliance gaps that were putting Nissti & Company and its business associates in violation of the HIPAA and HITECH Act.

To see how things could be done differently and help bring resolution to the matter, Nissti & Company hired an outside consultant specializing in network management for an in-depth analysis and implementation project. Shortly thereafter, the consultant recommended an identity and access management application that tied in with Nissti's AD and LDAP implementations.

After a relatively short trial and rollout period, the true benefits of the new system became obvious. Approximately 85% of the manual effort involved with user management was done away with and users were able to be configured in a matter of seconds through a much simpler process. The new user identity and access management system also meant no more delayed user account creation and forgotten accounts creating security holes, and allowed both Nissti and its business associates to meet their compliance requirements. Perhaps most importantly, it freed up security, Help desk, and HR staff and allowed them to focus on more productive tasks to the point where the new system paid for itself within the first 9 months of implementation.

When the proper documentation and technical controls are put in place and everyone is working with a security mindset early on, things can be so much simpler. The odds are your business is going to grow as things move forward, and it's going to be a lot simpler and cheaper to put the right technical controls, documentation, and business processes in place now as opposed to waiting until some point in the future to try and integrate it or, worse, layer it on top of an unstable foundation.

Every single dollar and every ounce of effort you spend simplifying your environment will most certainly have dramatic payoffs down the road. It makes the most sense to focus on compliance now while your business and IT environments are (relatively) simple. If you do things well, the simplicity will continue and allow security and compliance initiatives to facilitate rather than hinder the business.

You cannot drain the ocean all at once. All of this is a work in progress that you'll improve over time. The most important thing is to begin and then concentrate on results.

Coming Up in the Next Chapter

Moving past the cost considerations, it's time to shift gears and talk more about network visibility and ongoing maintenance. In order to make things happen, you're going to have to dig in deeper—and that's exactly what Chapter 4 covers. The chapter will talk about pulling everything together into one cohesive system, asking the tough questions to keep everyone engaged, and seeing where things truly stand through ongoing security assessments moving forward.

Download Additional Books from Realtime Nexus!