



Security Compliance Best Practices

Abstract

There are numerous new laws related to corporate governance, financial reporting practices, protecting personal information, counter-terrorism, and the potential for litigation. These laws impact an organization's data backup and storage requirements, electronic documentation, and overall security strategy. Plain and simple, many organizations are not prepared to comply with these laws. This white paper discusses what organizations must do to get prepared.

The Challenges

New Regulations

Below are some of the major initiatives requiring businesses to upgrade IT infrastructures.

- ✚ **HIPAA**, which deals with the portability and security of a patient's medical data.
- ✚ **Sarbanes-Oxley**, which mandates that both a company's CEO and CFO sign off on pertinent financial reports.
- ✚ **U.S. Patriot Act**, which requires strict adherence by financial services organizations to anti-terrorism and anti-money laundering regulations.
- ✚ **Gramm-Leach-Bliley**, which regulates how financial institutions use private customer data.
- ✚ **Federal Rules of Civil Procedure**, as amended, which impose new requirements on record retention in the event of litigation.
- ✚ **PCI DSS**, which deals with the security of credit card holder data and mitigating credit card fraud risks.

A common saying states that the only constants are death and taxes. Today, regulatory compliance should probably be added to this list.

Regulatory compliance has existed as long as there have been governments. In our lifetime, regulatory compliance has included such things as driver's licenses, taxes, and passports for international travel. Some of the newer, better known regulations today include [Sarbanes-Oxley](#), [Gramm-Leach-Bliley](#), [HIPAA](#), and the [U.S. Patriot Act](#). The text box to the left provides descriptions of these regulations. The type of business determines which regulations a particular business must comply with. For instance, pharmaceutical trials require record keeping beyond their business revenues. Retailers supporting credit card transactions must be concerned with the [Payment Card Industry's Data Security Standards](#) (PCI DSS).

Despite the potential, upcoming rollback on the Sarbanes-Oxley rules, a new regulation took effect December 1, 2006. The Federal Rules of Civil Procedure will require most businesses to retain electronic records—emails, instant messages, and text documents—and be able to retrieve them in economically feasible ways. The rules also require IT managers within those companies to be able to show how electronic records are stored and what mechanisms are used to retrieve them, as well as when and how those records are deleted.

Unfortunately, most companies are not prepared to comply with these new rules. A recent study by the Enterprise Strategy Group (ESG) notes that 90 percent of organizations with more than 20,000 employees have experienced an electronic discovery within the past 12 months ([Connor](#)). However, another study by Cohasset Associates notes that almost half of all organizations have no email retention policy! Companies must start preparing such policies.



No One Is Immune

Most organizations will be impacted by the ever-increasing number of regulations. IT professionals now know that information security is no longer a “nice to have.” The price of noncompliance is to risk a financial liability as a result of civil or criminal prosecution.

In order to stay compliant, enterprises must adopt fundamental security, business continuance, and disaster recovery plans, along with document management practices and technologies. It all starts with an organization’s security policy, security processes, a business impact analysis, and a team effort. This is a strategic business program, one that should be taken seriously.

It’s More Than Just Technology

Develop a Plan First

Amazingly, many organizations still believe that security is about buying a firewall or an intrusion detection system. Implementing technical controls is only one aspect of an overall information security program. Technology changes rapidly today, and often what happens is that companies implement too many technical controls that do not align, or support the business process. Or worse, the technical controls create more challenges than they solve. To escape this vicious cycle, organizations must develop an information technology strategy and guiding principles based on corporate governance, standards, and the security policy. Unfortunately, according to a recently published [survey](#) on business continuance and disaster recovery planning by AT&T, nearly 25 percent of U.S. businesses do not have a business continuity plan. Of those that do, nearly 40 percent have not tested it within the past year.

The good news is that things are improving. According to the [2006 Global State of Information Security Report](#), business continuance has climbed to fourth on the “to do” list for 2007; data backup is number one.

Purchase the Technology Second

Once companies develop a business continuity plan, they should purchase the technology to enable the plan. Technology can help address security compliance goals. When moving towards compliance, companies should consider moving to an up-to-date data and telecommunications network infrastructure, which includes some of the considerations below.

- Companies should move to a LAN or WAN that can ensure secure internal business communication and collaboration and also support secure, confidential customer and supply chain communication.
- Companies must be able to support end-users. Therefore, companies might consider updating from point-to-point services or frame relay and ATM over SONET to newer MPLS-based network solutions. Companies might also consider remote access and VPNs, which will support end-users as well as new business requirements.
- Companies that offer remote access will need to purchase security software. Here, companies must consider multifaceted authentication, encryption services, and anti-spyware. Perhaps a hosted service is worth considering since providers can often throw multiple resources at any number of challenges more cost effectively than a single business entity can.



Organizations can no longer take a wait-and-see approach to compliance. Rather than looking at compliance as a nuisance, organizations should view it as an opportunity to improve business processes, implement appropriate controls, and build customer trust. Implementing business process changes to ensure compliance can also go a long way to improving shareholder value—an added bonus for public companies.

Compliance Best Practices

So what are some of the key steps organizations must take to achieve compliance today? What are some key questions organizations must ask themselves?

- Obtain commitment from the executive levels that this is important to the business.
- Create a solid security program, policy, and team. Assign responsibility for dealing with information security. Establish business continuance and disaster recovery procedures. Determine how security breaches should be dealt with and reported. Document all this.
- Assess your business environment carefully, and objectively.
- Ensure that you understand the regulatory requirements for your business. If you do not have a legal expert on staff, get some outside legal advice to ensure you know what regulations apply and what needs to be done to ensure compliance.
- Assess your risk. What are the risks and vulnerabilities? What are the priorities that should be addressed? How much quantifiable risk are you willing to tolerate?
- Perform a business impact analysis based on the regulatory compliance requirements.
- Apply technology prudently based on the above business impact analysis. (Remember that the goal is risk mitigation, not risk elimination.)
- Ensure that you have sufficient resources in place to manage the security framework. (If not, consider out-tasking some of the more tactical aspects to allow you to focus on the strategic.)
- Inform and train your employees about information security, and what they are expected to do as part of their jobs, and in the event of a security breach.

Key Questions to Ask

- ✚ What is the impact if key aspects of your business are not available, or fail?
- ✚ Do you regularly update and verify the status of your security policy and plans?
- ✚ Are you authenticating all parties that have access to your information and data?
- ✚ Are you able to monitor who has access to your network and how it is being used?
- ✚ Have you established a business continuance and disaster recovery program?
- ✚ Is your mission-critical data backed up off-site?
- ✚ Have you implemented a tiered storage structure?
- ✚ Are you required to archive your data? How quickly can it be retrieved?
- ✚ Do you know your real RPO and RTO?
- ✚ Can you prove or demonstrate compliance to your mandated regulations?
- ✚ Do you have a means to deal with security violations?
- ✚ Who heads your security committee?

A key consideration is to ensure that the security program put into place aligns with the overall objectives of the business. Information Technology organizations have become much more than pure technology groups. Understanding business processes and impacts to the bottom line will go much farther than adding another box to solve what appears to be a new challenge.

Security Standards That Matter

The sheer number of security standards can indeed be overwhelming. This section will help guide organizations through the complex process of compliance.



In October 2005, the final version of a new ISO security standard was published. It was the start of an updated series of standards (ISO 27000) to support information security. It is still a work in progress.

Several references are available online, including an [overview](#) of the 27000 series as well as a [document](#) that compares ISO 17799 (the historical standard) and ISO 27002 on the ISC² website. A brief description of the pieces of the ISO 27000 series appears below.

- ISO 27000 contains the vocabulary and definitions for all the information security management standards.
- ISO 27001 is the Information Security Management System requirements standard (specification) against which organizations are formally certified compliant.
- ISO 27002 will be the new name for the standard currently known as ISO 17799 and is the code of practice for information security management describing a comprehensive set of best-practice security controls.
- ISO 27003 will be an implementation guide.
- ISO 27004 will be an information security management measurement standard to help measure the effectiveness of information security management system implementations.
- ISO 27005 will be an information security risk management standard.
- ISO 27006 will be a guide to a certification/registration process.
- ISO 2700x is supposed to be a new disaster recovery standard.

In addition, organizations should consult other references like [ISO 13335](#) on IT Security Management. More information will be forthcoming from ISO. Organizations should check the ISO series standards often, as they are likely to be updated frequently.

Another good reference for security guidance is CobiT. CobiT is an internationally applicable and accepted IT governance and control framework for aligning IT with business objectives, delivering value and managing associated risks. Available through the IT Governance Institute (ITGI), CobiT was first published in April 1996; [CobiT 4.1](#) is the current version. CobiT provides a reference framework for IT management, users, as well as IT audit, control, and security practitioners. Its policy guidance can help an organization implement effective governance throughout IT, and to get the most value from IT investments.

How Hill Associates Can Help

Understandably, many organizations feel overwhelmed and confused by security compliance in this new world of constantly evolving technology and regulations. Businesses are often bombarded with numerous proposals for addressing this challenge.

Just remember, compliance is not a box. Nor is it an end result. It is a constantly evolving effort as part of an overall security program. Hill Associates can help you put all the pieces together using our C3E framework. We develop education around technology, applications, and products that is contextual, connected, continuous, and experiential (C3E).



Contextual ensures that the technology and products address key business concepts that concern your customers. Connected relates all of the things happening with the telecommunications industry and in the world at large, not just one particular technology or product. Continuous means that learning is ongoing, not just a one-time event. Finally, experiential means that your team members must participate in order to learn.

Our C3E concept is designed to be a consistent, holistic structure that enables the maximum performance from a sales and marketing organization within a telecommunication company. This unique concept has led our partners to achieve the goals they seek related to their business objectives in today's competitive market.

In addition, Hill Associates understands the players working with you to suggest solutions to your business challenges. Our value is that we can provide an unbiased, vendor-neutral complex business solution—one that also addresses rapidly changing technology. We can also help you maximize limited funds so that you can effectively use your chosen technology. You need an organization that can provide trusted, reliable advice. Let us help you navigate the road to success.

About Hill Associates

Hill Associates is a premier provider of Education and Marketing Services. For over 25 years, we have demystified the complex world of telephony, network, security, and data communications for the most recognized players in the industry. Today we offer a variety of programs: leader-led courses, hands-on workshops, self-directed e-learning, and virtual classroom e-learning—all focused on enabling success in this rapidly evolving industry. Our Marketing Services bring objective industry and subject matter expertise to sales events, customer meetings, white papers, and Webinars.

At Hill Associates, our collaborative approach addresses each client's unique needs and challenges. Whether it's strategic executive briefings, programs for field teams or corporate IT, or marketing initiatives designed to bring knowledge to prospects, Hill Associates delivers your solution.

Visit our website (www.hill.com) for more information. While there, check out our newsletter, blog, and podcasts.

About the Author

Mark Steinberg is the Director of Business Development for Hill Associates. Mark has spent more than 25 years in the business of technology, providing consultative services regarding the strategic implications of technological change.

Business leaders rely on Mark's insights as they determine their business and technology strategies. His knowledge of convergence, both voice and data and wireline and wireless, has allowed him to create a variety of programs that address these business strategies. His engagements have been with companies such as CANTV, Telstra, AT&T, Qwest, Global Crossing, BellSouth, Verizon, Cingular, Ernst & Young, and Sprint—in the U.S., South America, Europe, Asia, and Australia.

A Senior Member of the Technical Staff, Mark has been with Hill Associates since 1994. He is a Certified Information Systems Security Professional (CISSP #49990) and holds an MBA in International Finance from the University of Santa Clara, CA, a BA in Pre-med/Biology from Hartwick College in Oneonta, NY, and has done graduate work in Astronomical Physics at the University of Colorado, Colorado Springs, CO.