

**Realtime**  
publishers

"Leading the Conversation"

# The Essentials Series

# IT Compliance

*by Rebecca Herold*

---

# The Business Leader Data Retention and E-Discovery Primer

by *Rebecca Herold, CISSP, CISM, CISA, FLMI*

July 2006


Many organizations are taking advantage of using a wider range of communication systems and technologies than ever before. For example, just to name a few:

Voice over IP (VoIP) is used not only for voice communications but also often integrated with the corporate email system.

Instant messaging (IM) is commonly used to allow real-time interactive business communications.

Blackberry messaging devices are used by a large number of business personnel to send and receive email no matter where they are at, at any time of the day.

These are certainly timesaving and efficient business tools. However, business leaders need to consider the archiving, retention, and discovery requirements that are involved with these technologies to ensure they are not unknowingly putting the business at information security, privacy, and/or legal risk with the ways in which the technologies are implemented.


 What does “discovery” mean? The Encyclopedia Britannica defines legal “discovery” as “In law, pretrial procedures providing for the exchange of information between the parties involved. Discovery may be made through interrogatories, written questions sent from one side to the other in an attempt to secure important facts. It also can be made through depositions, whereby a witness is sworn and, in the presence of attorneys for both sides, is subjected to questions. (The written record of the proceedings also is called a deposition.) Other forms of discovery include an order of production and inspection, which compels the opposing party to produce relevant documents or other evidence, and requests for medical examination in cases in which a party's mental or physical condition is at issue.”

The following discussion is provided to raise awareness of these issues and should not be considered legal advice. Discuss all applicable laws, requirements, and interpretations with your legal counsel to determine how they apply to your particular organization’s unique situation.

---

## Data Retention

Penalties for noncompliance with retention of data in all forms, for a large number of laws and regulations, range all the way from warning letters to multi-million dollar fines, prison time, and business closure.

 In 2003, the U.S. Securities and Exchange Commission (SEC) Final Rule: Retention of Records Relevant to Audits and Reviews went into effect. If you fall under the SEC, you should familiarize yourself with this regulation. Voicemail records generally would not fall within the retention requirements scope of this particular rule “provided they do not contain information or data, relating to a significant matter, that is inconsistent with the auditor’s final conclusions, opinions or analyses on that matter or the audit or review.” However, voicemail would need to be retained “if that item documented a consultation or resolution of differences of professional judgment.” Content and specific types of information are a major consideration for organizations when making retention decisions.

A few of the U.S. laws that have very specific security and retention requirements include:

21 CFR Part 11: Electronic Records, Electronic Signatures

21CFR58.195: FDA Good Laboratory Practice

Age Discrimination in Employment Act

Americans with Disabilities Act

Commodity Futures Trading Commission (CFTC) Rule 1.31

Communications Assistance for Law Enforcement Act (CALEA)

Department of Energy (DOE)10 CFR 600.153 Retention and Access Requirements for Records

Employee Retirement Income Security Act of 1974

FDA Good Manufacturing Standards

Federal Wiretap Act

Gramm-Leach-Bliley Act (GLBA)

Health Insurance Portability and Accountability Act (HIPAA)

Internal Revenue Code Title 26

Mammography Quality Standards Act of 1992 (MQSA)

NASD 3110 and 3111

Occupational Safety and Health Act

Sarbanes-Oxley Act (SOX)

Securities Exchange Act Rules 17a-3 and 17a-4

Social Security Administration (SSA) Records Retention

---

USA PATRIOT Improvement and Reauthorization Act (the reauthorized USA PATRIOT Act)


Toxic Substances Control Act

U.S. Forestry Service

US Code Title 44 (Paperwork Reduction Act)

USA PATRIOT Act

White House's National Strategy to Secure Cyberspace

 On June 30, 2006, amendments to CALEA were proposed that, if enacted into law, would greatly impact businesses, particularly ISPs. In particular the amendments would:

- Require routing and addressing hardware manufacturers to offer upgrades or other modifications needed to support Internet wiretapping.
- Authorize the expansion of wiretapping requirements to “public interest” commercial Internet services including instant messaging and VoIP.
- Require ISPs to be able to search customers’ communications to identify VoIP calls, instant messages, and other specific types of communications that could go through the Internet.
- Eliminate the current legal requirement for the Justice Department to publish a yearly public notice of the actual number of communications interceptions.

In addition to the plethora of U.S. laws, there are many more security and retention laws worldwide. For example:


European Union (EU) Data Protection Directive

EU Directive on Telecommunications Privacy

Australia's Privacy Act of 1988

Canada's Personal Information Protection and Electronic Data Act (PIPEDA)

Japan's Personal Information Protection Law

 See the March 2006 paper “Data Retention Compliance” for some of the specific requirements of many of these laws (<http://www.realtime-itcompliance.com/LearningCenter/ReadingRoom/tabid/103/Default.aspx>).

---

## Retention Challenges

There are two very basic challenges to meeting all the data retention requirements. Typically, the retention requirements govern the specific types of data that must be retained but not the corresponding forms in which the data is stored. And often the data retention requirements for the same types of data are in conflict throughout multiple applicable laws. Accompanying and complicating these challenges is that many of the laws are vague and open to interpretation, and most governments do not disseminate specific requirements for compliance except for the most high-profile regulations.

### ***Forms of Data Storage Are Constantly Increasing***

Many years ago, when many of the data retention requirements were established, they did not pose as big of a challenge as they now do; data existed primarily on paper and electronically in a centralized database such as on a mainframe. With the blossoming number of ways in which data can now be stored, the challenge that was a short hurdle for most businesses has now increased to become an endless marathon with no finish line in sight.

Just a few of the places where data can be stored beyond on paper and within a centralized structured electronic environment include:

- Email messages


- Voicemail

- IM

- Portable data storage devices, such as USB thumb drives


- Storage-capable printers and fax machines

An additional complicating factor is that technology allows for data created in one form to be automatically transformed to other forms. For example, the capability exists for voicemail to be integrated and saved as email using VoIP technologies. Businesses must determine and document the data retention requirements involved when the data is in both forms. For example, if your organization has a policy to delete email after 2 weeks, any voice messages that were converted to email will also be deleted after 2 weeks. Will this create problems for your company? Do you need to modify email retention based upon your use of VoIP? Would it be best for your organization to automatically purge VoIP files instead of archiving based upon the file type of the attachment, such as it being a WAV or MP3? Or, would just retaining the messages but not the attachment suffice?

 The key to success is first identifying and classifying the data item types, determining the retention requirements for these data types, then determining the storage locations for the data types.

---

To be successful, organizations must consider and decide how to deal with the different retention requirements in each applicable law. For example, should your organization retain all VoIP data to satisfy the regulation with the longest applicable retention time? Or, should you determine which types of VoIP calls are covered under applicable regulations and only retain those calls, purging the rest? One consequence of deciding to archive all calls for a long period of time is that the discovery process will become more difficult, lengthy, and costly because of the huge volume of archived calls.

 Be sure to include data retention within your business continuity and disaster recovery plans.

### ***Conflicting Law Requirements***

Businesses are often faced with trying to decide which law to follow when there are conflicting data retention requirements. For example, with regard to ISP information:


The U.S. has no law currently on the books with specific data retention length requirements for ISP records. There is currently a proposed Child Pornography and Obscenity Prevention Amendments that would require ISPs to retain records for 1 year.

On March 26, 2006, France published new rules that require ISPs, cybercafé operators, and telecommunications firms to retain connection data for 1 year.

On February 19, 2006, the EU Justice and Home Affairs Ministers approved a plan that will require European telephone service providers and ISPs to retain data on all phone calls and emails for 6 months to 2 years.

Ireland, Slovakia, Poland, and Slovenia all have laws requiring data retention for periods longer than 2 years.


Conflicting data retention legal requirements impact all industries and virtually all organizations. Businesses must carefully consider and hold discussions among legal, privacy, and information security leaders about the applicable laws, corresponding data retention requirements, and the best way to resolve conflicts with the requirements.

 Always document your decisions and your basis for them. They will provide evidence that you considered the issues if your organization is ever under investigation for a matter related to data retention.


---

## Electronic Discovery Issues


Electronic discovery (e-discovery) generally involves the activities necessary for organizations to gather and process information contained in electronically stored documents for litigation. As mentioned previously, these documents can include email messages, voicemail, IM files, VoIP files, video files, and individual files stored in multiple formats on many platforms that are geographically scattered across the globe.

 Ensure that information written by old versions of software can be read with current versions to meet data retention requirements and allow for electronic discovery activities.

The data required for a court case might have to be obtained for individuals, departments, teams, project groups, or a combination of these. Finding the requested information is usually a laborious and time-consuming process. Even if the files are found, much of it cannot be quickly or easily searched because of the format in which it is stored.

 According to the October 2005 Fulbright & Jaworski 2005 Litigation Trends Survey, “E-discovery is the number one new litigation-related burden for general counsel at companies with annual revenue exceeding \$100 million.”


Organizations have faced additional hardships and criticisms because of their retention practices, or lack of, and how it impacted litigation. For example, on June 22, 2006, 49 state attorneys general submitted a letter to the U.S. Congress asking them to require a national standard for ISPs to enable enforcement of investigations, in particular those associated with online sexual predators. This request came after an investigation over a 4-month period of the online video of a sexual attack on a 2-year-old girl in Wyoming was traced and determined to have originated through an ISP in Colorado. However, the ISP’s data retention procedures are to delete their logs after 31 days. According to the letter from the attorneys general, without the information, the case was dropped because the perpetrator was not found. Data retention and e-discovery will continue to have more impact on businesses as technology expands and captures information about activities that can be linked to physical as well as cyber crimes.

 Keep in mind that physical information, such as on printed papers, has legal retention requirements as well.

---


## ***New Electronic Discovery Rules***

E-discovery situations have potentially huge legal and financial impact on businesses and must be managed carefully and diligently according to e-discovery rules and orders.


 On October 19, 1999, a federal judge required Philip Morris USA to preserve “all documents and other records containing information which could be potentially relevant to the subject matter of this litigation.” Despite the order, Philip Morris continued to delete electronic mail, according to their procedures, which was over 60-days old, on a monthly system-wide basis for at least 2 years after the judge’s requirement. In February 2002, the defendants became aware of the situation, and that some emails relevant to the lawsuit were, in all likelihood, lost or destroyed. It was not until June 19, 2002, 4 months after learning about this situation, that Philip Morris notified the Court and the Government. Additionally, despite becoming aware of the problem in February 2002, Philip Morris continued the monthly deletions of email in February and March of 2002. Subsequently, on July 21, 2004, a federal judge ordered Philip Morris USA, Inc. to pay \$2.75 million in sanctions for destroying these emails.


On April 21, 2006 the U.S. Supreme Court approved new and amended federal court rules that will take effect December 2006. Among other issues, these include electronic discovery rules covering how electronic information is handled or acquired. Some of the more significant amendments that will impact businesses include the following:

The safe harbor amendment to Fed. R. Civ. P. 37, Rule 37(f) will allow parties to not be subjected to court sanctions if electronically stored information was deleted or lost as a result of the “routine, good faith operation” of their computer systems. Many businesses are concerned that this wording will lead to corporate defendants modifying their computer systems to “routinely” destroy information needed in litigation.


 Clearly document data retention requirements for your organization, for all types of data, to help diffuse such allegations. Make sure these requirements are clearly communicated to all areas responsible for retention.

The amendment to Rule 26(b)(2) requires the responding party to identify the sources of potential information that it has not searched or produced because the costs and burdens of accessing the information would be excessive. If the requesting party still demands the information, the responding party must demonstrate that the information is not reasonably accessible. Even if the responding party demonstrates this, the new rule allows a court to order the organization to produce the data with “appropriate terms and conditions,” which could include requiring the requesting party to pay for the responding party’s costs of producing the data.

 Businesses must consider not only the cost of data retention but also those involved with retrieving and producing data during discovery. Searching all storage locations and collecting electronic files, duplicating hard drives, restoring backup tapes, and sometimes implementing legacy software to read the files can cost hundreds of thousands of dollars.


 According to e-discovery software vendor Attenex, “Lovells, the sixth largest international law firm in the world, was tasked with evaluating potential conspiracy and fraud claims arising out of a complex multi-party transaction. During the investigation stage, the firm set out to review 35GBs (two million pages) of restored email data under tight staffing and cost controls. Using traditional electronic discovery methods, the case was estimated to take one year and cost \$4-5 million.”

An amendment to Fed. R. Civ. P. 26(b)(5) allows parties to retrieve information that was provided to other parties unintentionally during discovery. After being notified by the producing party that it had received privileged information, the receiving party would be required to return it. If the receiving party believed it was entitled to the information, it would have the burden of making its case to the court. Data is often unintentionally provided to litigation parties within metadata.


 Metadata is commonly described as data about data, and is defined as “information describing the history, tracking, or management of an electronic document” within the Federal Rule of Civil Procedure that goes into effect December 2006. Appendix F to The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age defines metadata as “information about a particular data set which describes how, when and by whom it was collected, created, accessed, or modified and how it is formatted (including data demographics such as size, location, storage requirements and media information.)” Metadata created by any software application has the potential for inadvertent and unintentional disclosure of confidential or privileged information in both a litigation and non-litigation setting.

Other amendments to Rule 26 and Rule 16(b) require parties to address disclosure and discovery of electronically stored information issues early in the litigation.

A revision to Civil Rule 33 states that the responding party “may be required to provide some combination of technical support, information on application software, or other assistance” to enable the requesting party to understand the business records produced.


 Organizations should work with the information security and IT areas to create e-discovery procedures and identify the staff that will be involved to provide such assistance.

An amendment to Rule 34(a) would add a specific category of “electronically stored information” that would be included as information expressly subject to production in discovery along with “documents,” which would remain as a separate category.

 Electronically stored information could be anything within electronic storage devices, including such things as logs, audit trails, voicemail, instant messages, streaming video, information from other types of computers—such as digital video recorders, fax, and copy machines memory—and so on.


Another amendment to Rule 34(d) would permit a requesting party to specify the form in which electronic data must be produced. If a party does not specify the form of production, a responding party must produce the information in the form in which it is “ordinarily maintained,” or a form “which is reasonably useful by the requesting party.”

---

 According to the 2006 Workplace E-Mail, Instant Messaging & Blog Survey from American Management Association (AMA) and The ePolicy Institute, 24 percent of organizations have had employee email subpoenaed, and 15 percent of companies have gone to court to battle lawsuits triggered by employee email.

## Keep Data Proliferation to a Minimum

Minimizing the locations in which critical business data is copied and located will reduce the risks of data retention noncompliance, and the exorbitant costs involved with e-discovery. All the more reason for implementing sound policies regarding data classification, defining the appropriate locations to store certain types of data, and ensuring tight controls that limit storage of massive databases on unlimited numbers of end-user storage devices.

 Unless absolutely necessary to support critical business requirements, do not allow entire databases of customer and employee information and associated data to be stored on mobile computing and storage devices under the control of personnel while outside of the enterprise facilities.

Discuss data retention and discovery issues with your legal counsel prior to establishing policies, procedures, and standards for these issues. Planning ahead for addressing data retention and e-discovery issues will save your organization significant time and money, in addition to reducing the risk of associated fines and penalties.

---

# The Business Need for Information Security and Privacy Education

by *Rebecca Herold, CISSP, CISM, CISA, FLMI*

July 2006

Your personnel hold the security and privacy of your company information in their hands; both figuratively and literally. Businesses depend upon their personnel to handle their valuable data responsibly and securely. Without effective personnel education, businesses face significant negative business impact and even possible business failure from the consequences.

There are many compelling reasons for businesses to implement an effective information security and privacy education program—three of particular significance include:

Growing numbers of laws and regulations require information security and privacy education.

Personnel must be educated to understand how to effectively follow the procedures that support the privacy promises.

Education will help to reduce the insider threat of personnel committing computer crime and disruption.

Organizations must know how to create an effective education program, deliver the program, and target groups who need specialized training and awareness to protect their business by improving personnel knowledge.

## Meet Legal and Regulatory Requirements

There are a growing number of laws and regulations that require, either directly or indirectly, businesses to implement formal information security and privacy education programs.

Lawmakers recognize the importance of educating personnel about how to properly protect data as evidenced by the laws that include requirements to educate personnel on how to securely handle personal information.

A few of the laws that include some type of information security and privacy education requirements include:

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)

European Union Data Protection Directive

Japan's Personal Information Protection Law

U.S. 21 CFR Part 11 (Electronic Records/Electronic Signatures)

U.S. Fair Credit Reporting Act (FCRA)

U.S. Federal Information Security Management Act (FISMA)


U.S. Gramm-Leach-Bliley Act (GLBA)

U.S. Health Insurance Portability and Accountability Act (HIPAA)

U.S. Sarbanes-Oxley Act (SOX)

---


The Organization for Economic Cooperation and Development (OECD) Privacy Principles, which serve as a framework for the majority of data protection laws throughout the world, stress the importance of education for ensuring the privacy of personal information. Judgments and consent orders specifically require organizations to establish formal information security and privacy training and awareness programs.

 An SQL attack was conducted on Petco in June 2003. The attacker was able to read clear-text credit card numbers stored in Petco's database. The FTC consent order required, among other things, that Petco must not misrepresent the extent to which it maintains the privacy and security of personal information. It ordered Petco to establish, implement, and maintain "a comprehensive information security program that is reasonably designed to protect" the security of consumer personal information that included a formal information security and privacy training program. Petco also must obtain an assessment that the program and training is reasonable from a qualified independent third party biennially for 20 years. Petco must also provide copies of the assessments, including training materials, to the FTC within 10 days of each assessment.

Having a formally documented information security and privacy education program that is clearly supported from executive management helps to demonstrate your organization's due diligence for reasonably protecting personally identifiable information (PII). It is also much less expensive for your organization to invest in an effective information security and privacy program than it is to pay for 20 years of expensive ongoing consent order compliance activities following the aftermath of an incident that could have been prevented with proper awareness.

## **Prevent Mistakes and Actions Based Upon Lack of Knowledge**

Mistakes happen during the course of business. Actions are often performed by workers with good intent, but result in devastating consequences, just because they did not know any better.

 On March 30, 2006, the Connecticut Post reported that the Social Security numbers of 1250 teachers and school administrators in the Connecticut Technical High School System were mistakenly sent via email to "the system's 17 principals...to inform them about a coming workshop. The file with the Social Security numbers was attached to the email by mistake...At least one principal...then forwarded the email to 77 staff members without opening the attachment containing the Social Security numbers."

You cannot expect your personnel to protect company information if you do not communicate effectively with them about how to protect the information. The greater awareness personnel have about information security and privacy, the more securely they will handle PII and other sensitive information, reducing the likelihood of mistakes and actions that put PII and your business at risk.

---


Your organization cannot protect PII and other mission-critical data without ensuring all your personnel:

- Understand their roles and responsibilities for protecting the information as part of their job

- Understand your organization's information security and privacy policies, standards, procedures, practices, and expectations


- Possess the knowledge enabling them to protect the information and related technology resources for which they are responsible


People are the weakest link in your information security and privacy program. The key to actually attaining a reasonable and appropriate level of security and privacy is educating your personnel. An efficient enterprise-wide information security and privacy education program is critical to ensure your personnel understand their information security and privacy responsibilities, then to appropriately use and protect the information resources entrusted to them.

 Without effective information security and privacy education programs, incidents will occur that could have a devastating impact to your business.


## Prevent Deliberate Fraud and Disruption

Trusted insiders can do bad things with the information that they are authorized to use. Your authorized users are, and will always be, a threat to the information to which they have access.

 On May 25, 2006, Computerworld reported that a former Red Cross worker allegedly used the information to which she had authorized access, including names, Social Security numbers, and birthdates, to open credit card numbers using their names and then go on shopping sprees. As of the report date, at least four people had been confirmed as being victims in this identity/credit card fraud incident.


 The U.S. Department of Justice site reported on March 1, 2006 that a systems auditor who had access to place software on the computer he was auditing "used that access on numerous occasions to view his supervisor's email and Internet activity as well as other communications, and to share those communications with others in his office. Kwak carried out his crime and invaded his supervisor's privacy for personal entertainment; there is no indication he profited financially from his actions." The auditor pleaded guilty and "faces a maximum penalty of five years in prison and a fine of \$250,000 for the crimes to which he pled guilty."

Providing ongoing awareness and training for information security and privacy will help all your personnel not only know what they should be doing but also know how to identify when others they work with are doing something wrong. Establish, and consistently enforce, sanctions for policy non-compliance. Doing so will help to dissuade at least some potential crooks.

 For more statistics and information about insider threats, see the joint CERT/CC Carnegie Mellon University and U.S. Secret Service insider threat studies at [http://www.cert.org/insider\\_threat](http://www.cert.org/insider_threat).

---

Use actual examples within your awareness messages and training content to get your messages across even more effectively.

 You can find more actual examples of insider threat incidents in my blog, <http://realtime-itcompliance.typepad.com/>.

## Target Training and Awareness Messages

Education must be ongoing, delivered in multiple ways, and tailored to different groups within your organization. Training and awareness content for target groups must be specialized for the specific issues that they need to understand as it relates to their job responsibilities.

Some training and awareness should be given to all your employees. You also need to have different training and awareness content and information for specific target groups to directly address their job responsibilities. You need to identify your target groups based upon your own unique organization, environment, industry, and regulatory requirements. The following list highlights potential target groups to include:

- Executive management
- Legal personnel
- Mid-level managers
- IT personnel
- Marketers and sales representatives
- Physical security personnel
- Research and development personnel
- Internal audit personnel
- Public relations personnel
- Human Resources personnel
- Information security and privacy personnel
- Third parties (vendors, outsourced companies, and so on)
- Physicians and medical providers
- Trainers
- Customer service and call center personnel

---

For example, the type of information you could cover within customer service and call center awareness and training materials includes:

- How to respond to customer privacy and security concerns and complaints
- Customer security and privacy compliant procedures and forms
- Identity validation methods
- How to identify social engineering
- How to identify fraud attempts
- Who to contact when an incident is reported
- How customers can opt-in and opt-out
- Customer opt-in and opt-out procedures
- How to give access to customers' corresponding PII
- How to update incorrect customer information

## **Invest Adequate Resources in Privacy Education**

There are many business benefits of an effective information security and privacy education program. Unfortunately, many businesses do not invest nearly enough time, effort, personnel, or resources to their information security and privacy education efforts—and even more alarming, most do not allocate an information security and privacy education budget at all.



According to the 2006 Deloitte Global Security Study, less than half of organizations allocate a budget specifically for information security and privacy awareness and training activities.

Take time to create an effective education program, and realistically determine the budget you will need to fulfill the program. The investment will be small compared with the impact of incidents, penalties, and judgments that can occur without an effective education program.

---

## Your Business Needs Information Security and Privacy Education

There are many convincing benefits for establishing an effective privacy education program that is built around your business processes and goals and addresses your unique business challenges:

- Reducing numbers of privacy and security incidents

- Preventing privacy and security incidents from occurring

- Motivating personnel to do the right thing during the course of performing their business responsibilities

- Making personnel aware of the risks involved with handling PII and, in turn, having them work in a more secure manner

- Retaining customers who can see the business is protecting their personal information

- Demonstrating due diligence within business activities where personal information is handled, stored, and accessed

- Ensuring business partners and outsourced businesses appropriately protect the data that your organization has entrusted to them

- Meeting legal and regulatory compliance requirements for appropriate awareness and training

- Meeting the organization's privacy policy and other contractual obligations and promises

- Strengthening personnel trust and confidence in your organization management and leadership

The bottom line is that organizations must have an effective information security and privacy education program. Not only do laws require it, but it demonstrates due diligence and helps reduce the number of costly incidents and fraud.


---


# The Business Leader's Primer for Incorporating Privacy and Security into the SDLC Process

by *Rebecca Herold, CISSP, CISM, CISA, FLMI*

*July 2006*

It is important for business leaders throughout the enterprise to understand the system development life cycle (SDLC) and how decisions made can impact, negatively or positively, the entire business. First and foremost, systems and applications must be built to support the business in the most efficient and effective manner possible. Business leaders must be involved with the process to ensure systems and applications are being developed to meet this goal; the information technology (IT) areas cannot create applications and systems on their own and reach this goal. Second, applications and systems must be created to reduce risk to the level acceptable by the business as well as to meet compliance with applicable laws, regulations, and contractual requirements.

 Business leaders are key components of the SDLC and must understand the basic phases as well as the information security and privacy issues that must be addressed within each phase.

 The information for the rest of this paper is built around the SDLC topic discussion within a portion of the 2-day workshop "Effectively Partnering Information Security and Privacy For Business Success" by Christopher Grillo and Rebecca Herold

## What Is the SDLC?

Smart organizations follow an SDLC to ensure applications and systems are created and updated in the most efficient and consistent manner possible to support the business need. Over the years, there have been a variety of SDLC methodologies created and used. They are typically very similar, as demonstrated in Table 1.

<b>NIST 800-30</b>	<b>U.S. Department of Health and Human Services</b>	<b>ISO/IEC 12207</b>
Initiation	System Concept Development Planning Requirements Design	Investment Analysis Acquisition Requirements Analysis Design & Engineering
Development or Acquisition	Development	Development
Implementation	Integration, Test & Implementation	Testing & Implementation
Operation or Maintenance	Operations and Maintenance	Operations and Maintenance
Disposal	Disposition	Retirement

**Table 1: Comparison and mapping of SDLC phases.**

---

Very generally, SDLC processes include the phases as labeled by NIST 800-30:

**Initiation**—The need for a new system, application, or process and its scope are documented. Security categorization standards are identified to help select the appropriate security controls. A preliminary risk assessment reveals the type of threat environment for the planned system.

**Development**—A large number of activities occur during this phase, most of which need to consider information security and privacy impacts. Such activities include a formal risk assessment, analysis of the necessary security requirements, determination of how much of the development cost should be allotted to information security and privacy, plan for security to ensure all security and privacy controls are fully documented, security controls development, security and privacy test and evaluation plans, and other related planning components. The system or process is designed and requirements are gathered and documented.

**Implementation**—This phase includes assurance-testing activities to validate and verify the information security and privacy specifications are within the deliverables and to ensure integration of security controls, security certification, and accreditation. The system is implemented in production.

**Operation or Maintenance**—This phase includes activities to ensure appropriate security and privacy configuration management and control as well as continuous monitoring to ensure the controls continue to be appropriate and effective.

**Disposal**—This phase is when the system is retired and no longer used. It is critical but often overlooked with regard to information security and privacy considerations. It includes activities for information preservation to meet data retention requirements, media sanitization as necessary, and appropriate hardware and software disposal.



Incorporating information security and privacy considerations and activities from the very start of the SDLC will not only result in more secure and compliant applications and systems but also help the business by being less expensive and more effective than trying to band-aid information security and privacy onto the final application or system.

Organizations must ensure that information security and privacy are constructed throughout the SDLC:

To ensure systems and applications support corporate policies and procedures

To protect data throughout the entire information life cycle

To meet data protection laws and regulations requiring information protection, such as access controls, access logging, availability, and so on

---

## People in the SDLC


There are many key players who must participate in SDLC projects involving personally identifiable information (PII) and other sensitive information to ensure information security and privacy are appropriately addressed. The key players to involve within an SDLC include:

- Business unit leaders
- Project sponsors
- Marketing and sales
- Project managers
- Business analysts
- Business managers and users
- Technical IT administrators
- Information security
- Consultants and vendors
- Privacy
- Legal and compliance
- Auditors
- Human Resources

Organizations need to include other areas as appropriate to their own unique situations and environments. For example, healthcare providers will likely need to include physicians and nursing staff; manufacturing will likely need to include their standards and quality control staff; and so on.

## Where Do Information Security and Privacy Fit In?

Information security and privacy must be addressed throughout the entire SDLC process. Historically, organizations tried to patch on security in the last week or two before systems or application deployment to production, or even following production deployment. This did not work, and it still will not work!

 Addressing information security and privacy for the first time during the production phase puts your business at significant risk of security incidents, privacy breaches, and noncompliance with laws and contractual requirements.

Organizations must follow a well-defined SDLC process to address information security and privacy every step of the way through the use of policies, procedures, standards, privacy impact assessments (PIAs), and information security risk assessments.

---

PIAs will determine:

- Where PII will be obtained, stored, transmitted, and retired

- Applicable data protection laws and regulations

- Who should have access to PII

- The PII data flow map

- Risks throughout the data flow

Information security risk assessments will identify:

- Technical, administrative, and physical risks within the planned system

- Cost-effective controls to reduce the identified risks to an acceptable level

## Initiation Phase

The objectives and goals of the initiation phase are to:

- Describe the envisioned project

- Identify the project sponsor and budget

- Identify project resources

- Establish the preliminary project plan estimates

- Obtain management review and approval

- Engage the business requirements team

- Determine business requirements

During this phase, your information security and privacy goals are to:

- Integrate privacy and security into the project initiation phase to communicate any initial security and privacy requirements and risks upfront

- Determine privacy and security requirements

- Plan and perform preliminary privacy and security training

- Collect applicable infrastructure policies and standards that apply to the project

- Perform a preliminary information risk assessment and security categorization

- Conduct a PIA to identify PII, regulations, laws, contractual requirements, threats, and so on

It is important to identify applicable laws and regulations during this very first phase to ensure all issues and compliance requirements are then successfully addressed throughout the development of the application or system. The regulations that have information security and privacy requirements must be identified. Responsibility for ensuring requirements are met should be formally assigned to someone on the development team.



Examples of regulations that have information security and privacy requirements include, but are not limited to:

- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley Act
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
- European Union Data Protection Directive
- State-level laws

It is also critical to ensure you have identified all the contractual requirements with business partners, vendors, and others related to systems and applications development. For example, many service and product agreements include clauses that have stipulations for notification for applications or systems changes, updates, or implementations.

During this phase, the policies, procedures, and standards associated with the project should be identified. This identification includes not only your internal information security policies but also all the information security and privacy policies your organization has on Web sites. You also need to check whether are obligated to follow any of your business partners' information security and/or privacy policies.

### ***PIAs and Security Risk Assessments***

PIAs should be performed during the initiation stage to determine:

Whether PII will be used within the system or application

Where PII will be obtained, stored, transmitted, accessed, and retired

Applicable data protection laws and regulations

Who will have access to PII

The planned PII data flow

Where are the risks throughout the flow

Information security risk assessments should be performed during the initiation stage to identify:

If risks involved could be mitigated to an acceptable level to pursue the project

Technical, administrative, and physical risks within the proposed system

---

## Development Phase

The objectives and the goals of the development phase are to:

Finalize business requirements

Develop business use cases and finalize process flows



Use cases describe the functional view of what the system or application should do. They describe the sequence of actions the application or system performs with regard to interaction with the end users. In many SDLC use case procedures, the end users are referenced as “actors.”

Obtain business owner approval of the plans

Engage the development team in coding, documentation, testing, and other activities

Determine technical specification and design requirements

Develop code using secure coding techniques and standardized security and privacy coding procedures

Create and review the proposed development and testing strategy

Create and review the quality assurance (QA) testing plan

Develop and document the application or systems operating and training manuals and accompanying plans

Develop and document the deployment plan

During this phase, your information security and privacy goals are to:

Review the requirements specifications to verify privacy and security requirements are documented, understood, and responsibilities assigned

Approve the information security and privacy standards and design requirements

Create the documentation for the project—such as the security plan, privacy laws requirements, technical configuration standards, business continuity and disaster recovery plan, and so on

Use secure coding techniques, including adequate controls to the source code library, version control procedures, and so on

Ensure security coding and the development of test cases with appropriate security and privacy tests

Conduct and document privacy and security tests

Ensure security and privacy functionality and protection

Perform system security and privacy tests and vulnerability and penetration tests

Address regulatory compliance and customer access issues


Plan for system security and/or privacy certification and accreditation as appropriate

---

## **PIAs and Security Risk Assessments**

PIAs should be performed during the development phase to:

- Ensure use cases address all OECD principles, applicable laws and regulations, contractual requirements, and international data flow issues
- Identify privacy changes from the initiation phase
- Identify and document privacy risks, controls, planning, and responsibilities
- Ensure there are no gaps with contractual, legal, or regulatory requirements
- Ensure PII database checks are made as appropriate within the system or application
- Determine whether programming tools such as P3P should be used

 The definition of P3P is provided by the World Wide Web Consortium Web site (<http://www.w3.org/>): *The Platform for Privacy Preferences Project (P3P) enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit.*

Information security risk assessments should be performed during the development stage to ensure:

- Use cases address technical, physical, and administrative security
- Appropriate access controls are created
- Security policies, procedures, and standards are followed
- Security procedures are created as necessary for the application or system
- Security specifications are followed
- Appropriate technologies are used, such as encryption, digital signatures, and so on
- A documented system security code review occurs

## **Version Control**


Most systems and applications consist of literally millions of lines of code and potentially thousands of programs, modules, screens, and forms. Version control is vital to the successful and productive use. Examples of version control considerations include:

- Is a version control system in place?
- What is the backup strategy?
- Does the source code contain sensitive or confidential business rules?
- Is the version control process secure?


---

## **Privacy and Security Testing Plan**

A thoughtful, well-documented testing plan must be used during systems and applications development not only to ensure all information security and privacy issues have been thoroughly tested and resolved but also to provide demonstrated due diligence that security and privacy were appropriately addressed during development.

 Organizations that do not carefully document and execute security and privacy plans for new and updated systems and applications might find themselves in legal jeopardy if a security breach subsequently occurs using the system or application.

Government oversight agencies have specifically indicated within their judgments and consent decrees that lack of or insufficient design and implementation of reasonable safeguards to control risks—and then lack of or insufficient regular testing of those controls—was of significance in determining the fines, penalties, or otherwise resulting actions the organization had to take.

 For example, the FTC consent decree against CardSystems Solutions, Inc. required many activities including the design, documentation, and implementation of reasonable safeguards to control the risks identified through risk assessment as well as regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

Many types of tests need to be performed during the development phase. Two types of significance are functional tests and code tests.

### **Functional Tests**

Functional testing can be used to confirm the correct behavior of the system's or application's security controls. Examples of functional security and privacy tests include:

- Ensuring only specific user groups can access certain databases or data fields

- Ensuring data is successfully encrypted within specified situations

### **Code Tests**

Code testing reviews the control structure, the data flow structure, decision control, and modularity of the program code to ensure the application is constructed appropriately, comprehensively, and completely. Code testing can be manual through visual inspection or automated. Examples of security and privacy code tests include:

- Reviewing access control code and modules


- Testing and validating the successful execution of encryption code

- Ensuring backdoors are not built into the code that allow access that would create risks or be in noncompliance with applicable laws and contractual requirements

---

## ***Use of PII During Testing***

Real PII should not be used for test or development purposes if at all possible. Not only is it a good idea and leading system development practice, it is against the law in some countries.

 A 2006 Compuware survey of U.K. IT directors found that 44 percent of companies use live data for testing even though the 1998 U.K. Data Protection Act states organizations should not use actual sensitive personal data for such purposes.

There are effective tools available to create dummy data for testing. If, for some reason, PII must be used for test data, you need to know what your privacy policy is regarding the use of PII and if such testing would be in noncompliance with your policy. You must also determine how the PII will be protected during all phases of the testing process.

## **Implementation Phase**

The objectives and the goals of the implementation phase are to:

- Successfully deploy the system or application

- Provide end user training

- Transition to operational support

During this phase, your information security and privacy goals are to:

- Re-certify and re-accredit the system or application

- Perform a vulnerability assessment

- Implement the information security and privacy assessment and monitoring plan

- Implement compliance monitoring

## ***Post-Implementation Review***

Soon following the move to production, perform a post-implementation review to document lessons learned from the team while they are still fresh in everyone's minds and to ensure the documentation actually is accomplished. Oftentimes, team members are already starting on other projects and this valuable documentation is never created.

Another objective of performing a post-implementation review is to obtain end-user feedback regarding how the new or updated system or application is working in the production environment and then tweak the system as necessary to get rid of any identified bugs or issues. The information security and privacy goals for performing a post-implementation review are to analyze the information security and privacy lessons learned throughout the project and improve the security and privacy SDLC processes accordingly.

---

## **PIAs and Security Risk Assessments**

PIAs should be performed during the implementation phase to:

- Ensure there is still compliance with all privacy laws and contractual commitments

- Ensure support personnel successfully follow privacy-related activities, such as appropriately responding to customer requests for access to their PII

- Ensure links with other production systems and applications have not created inappropriate access capabilities to PII

Information security risk assessments should be performed during the implementation phase to:

- Verify that the security monitoring plan is adequate and effective

- Ensure that integration with other production systems has not introduced new risks or vulnerabilities

- Verify that backup and recovery plans will work

## **Maintenance Phase**

The primary objectives and goals of the maintenance phase are to ensure the transition from development personnel to operations personnel is successfully completed, and that ongoing support of the system or application is achieved. During this phase, your information security and privacy goals are to:

- Follow proper configuration management procedures to ensure all security settings are where they should be

- Ensure adequate consideration of the potential security and privacy impacts due to specific changes to an information system or applications within the surrounding environment

- Follow secure change-control procedures

- Ensure security and privacy considerations are addressed for each change to the application or system

- Continuously follow the information security and privacy monitoring and assessment plan, being particularly vigilant during personnel changes for this responsibility

---

## Disposal Phase

The primary objectives and goals of the disposition phase are to ensure the successful sunset, or retirement, of the application or system with as little impact to the business as possible. During this phase, your information security and privacy goals are to:

- Preserve information as necessary for applicable data retention legal and business requirements

- Ensure that data is irreversibly deleted, erased, and written over on all storage media when retention periods end

- Ensure secure and appropriate hardware and software disposal

## Closing Thoughts

The objective of incorporating information security and privacy is not to totally overhaul an existing SDLC project management process but to add well-defined security and privacy checkpoints and security and privacy deliverables. The ultimate goal is to make the applications and systems as secure as reasonable based upon risk and to ensure compliance with applicable data protection laws.

Some lessons learned about incorporating information security and privacy into the SDLC (Source: “Effectively Partnering Information Security and Privacy for Business Success” two-day workshop by Christopher Grillo and Rebecca Herold):

- If you wait until an application or system is already in production to make it secure and address privacy, you’re too late to ensure effective security and privacy. Such a band-aid approach is dangerous to your business.

- Effective security and privacy practices need to be incorporated into all the applications and systems layers involved, such as the network, host, application, storage, end-points, and so on.

- Ensure clearly written and easily accessible information security and privacy policies, standards, and guidelines are used as frameworks for the security and privacy being constructed within the application or system.

- Implement, or follow the existing, policy deviation-exception process.

- Create checklists that include step-by-step instructions within every SDLC phase for information security and privacy.

- Personnel education is crucial to the success of incorporating security and privacy into the application or system; make sure it occurs, not just once but on an ongoing basis during the life of the application or system.

- Information security and privacy are ongoing and always changing processes; make someone responsible for addressing these issues during the lifetime of the application or system.

---

# Security and Privacy Contract Clause Considerations

by *Rebecca Herold & Christopher Grillo*

June 2006

*NOTE: Christopher and I created the table found within this article for our two-day workshop now entitled “Effectively Partnering Privacy and Information Security for Business Success.” The table has been very helpful for organizations addressing outsourcing and partnering security and privacy issues, so I am making it available here in the hope it will also be helpful to you. For more information about the workshop, in addition to Christopher’s biography, please see <http://www.gocsi.com/training/erc/pisp.jhtml>). - Rebecca Herold*

## Trust Cannot Be Blind

When you entrust business partners and vendors with your company’s confidential data, you are entrusting them with all control of security measures for your organization’s data. That trust cannot be blind. Many recent privacy and security incidents have resulted from inadequate privacy and/or security practices within outsourced organizations handling another company’s customer or employee data.

When you outsource critical data processing and management activities, you must take action to demonstrate due diligence, stay in charge of your own business data security, and minimize your business risks. You must know:

- Whether the business partner’s information security and privacy program is adequate for handling your organization’s data

- How the business partner is complying with your regulatory responsibilities

- How you can demonstrate to regulators that you are in compliance when someone else possesses your data

You must hold your business partners to strict security standards. In many instances, the standards applied to business partners will be more stringent than your organization’s internal security requirements.

---

## Perform Due Diligence

Organizations should plan to perform several activities to determine the adequacy of information security and privacy practices within business partners, vendors, and other outsourced companies. We have performed a significant number of these activities over the past few years, some of which include:

- Requesting the partner to complete a self-assessment information security and privacy questionnaire

- Having an independent party perform an audit of the partner's information security and privacy program and data handling enterprise

- Requiring the partner to obtain a security certification, such as BS7799 or SAS 70 Type II, for the scope of their enterprise involved with handling the entrusted data

- Going onsite to perform an audit of the information security and privacy program and view actual business practices

- Including specific information security and privacy requirements within the contracts with the partners

## Contractual Considerations

While performing these activities, we have compiled a listing of issues and important considerations to include within the contracts. The specific items your organization should include will depend upon your organization and the relationship with each of your partners.

As with any contractual activities, it is important to discuss with your legal counsel and choose the requirements and wording that is most appropriate for your organization. Use the following table as a checklist to go over with your legal counsel when discussing new contracts and when reviewing existing contracts to determine whether updates are necessary.

Service Levels		
Contract Area	Description	Notes
<b>Services to be provided</b>	General commitments of the organization and the third party of the functions to be performed, the deliverable to be produced and the user community to be served.	Ensure services are in compliance with applicable laws and regulations. If required by laws, ensure consent has been obtained from all individuals to outsource personally identifiable information handling to another entity.
<b>Service levels to be provided</b> (Service Level Agreements – SLAs)	The services provided will be in accordance with agreed-upon service levels (usually identified in a service schedule) and whenever possible, using a quantitative tool for performance measurement.	Ensure service levels are adaptable and meet your business requirements. Examples include security service levels for: patches, vulnerability identification, data availability, and incident monitoring and response timeframes. In the event of an outage, how many hours until service will be restored? Define the maximum allowable downtime in a worst-case scenario. Establish standard SLA criteria that must be agreed upon.
<b>Availability of services</b>	Specify requirements necessary to ensure service in the event of service failure.	Include measures to reduce risk of service loss, such as backup and recovery measures, contingency and disaster recovery plans. Contractually require documented backup and disaster recovery plans. Contractually require regular backup and disaster recovery plan tests.
<b>Termination of relationship</b>	Contractually require the business partner to return and/or irreversibly destroy all your company's data, as appropriate, immediately upon termination of your contract with the business partner.	Ensure the business partner does not continue to have access to your company's systems and data when your relationship with them is terminated. Termination of a business relationship presents great risk to your company; this is when the former business partner often stops protecting your data or mishandles it, putting your business at risk.

## System/Data Protection Responsibilities

Contract Area	Description	Notes
<b>Definition of responsibility</b>	Define responsibilities in all key privacy and information security areas (security administration, technical support, privacy, training and awareness, enterprise program, and so on.)	Contractually require a position or person to be named as responsible for information security and privacy issues and to be the primary point of contact for related communications.
<b>Compliance with relevant laws and regulations</b>	State the requirement of complying with applicable international, national and state level laws.	Spell out desired compliance obligations (e.g., HIPAA, GLBA, and so on). This is standard language to ensure that the vendor adheres to and contractually agrees to support regulatory requirements.
<b>Third party to comply with the organization's security policies and standards</b>	State that the third party must comply with your organization's privacy and information security policies and standards.	Reference appropriate components of privacy and information security policies which may include physical security of premises, clearance of personnel, data security storage, media handling, and so on. Contractually require the third party to have documented information security and privacy policies.
<b>Requiring confidentiality</b>	Contractually require a nondisclosure agreement/confidentiality clause with the business partner and insist that the business partner has confidentiality agreements with relevant staff (anyone who has access to your data) and subcontractors (outsourced relationships, and so on.)	This should be in your standard contract language, typically under "Confidentiality."
<b>Control use of systems and data</b>	Require the third party not to access, use, amend, or replace any application systems, data, software, hardware, or communications systems without prior authorization from a named person or position from within your organization.	Be sure to contractually require that the third party obtains your permission to use production data and purchased data lists for test purposes.
<b>Scope of access permitted</b>	The third party should have the minimum level of access to assets and data to meet the business requirements.	Limit the amount and types of information the business partner personnel can see and/or access based upon the business needs. For example, if the business partner contracted activity is to verify a customer is a good credit risk, don't send all parts of the application to the business partner; just send the information required to approve the application.

<b>Provide security awareness, training and written guidelines</b>	Contractually require business partner personnel to receive information security training for appropriate security practices prior to handling or accessing your company's information.	Don't limit the training to electronic data; if they handle storage media, paper documents, speak to customers about their data, or access data in any other way, make sure it is covered in the training. Contractually require regularly scheduled training and awareness to occur following the initial training.
<b>Anti-virus policy and procedures</b>	Include a clause to provide protection from viruses and other malicious code.	Due to the high risk from virus and other malicious code infection, include a specific clause requiring the third party to have up-to-date malicious code prevention systems implemented.
<b>Loss of customer data provisions</b>	Ensure that the business partner is contractually required to appropriately protect customer data or face penalties, such as fines, contract termination, prosecution, and so on.	If your business partner loses data your company is still ultimately responsible for the loss of customer data.
<b>Use of data - separation of data</b>	Contractually require your company's data to be protected and separated from competitor data.	Depending on the risk, ask for physical and logical separation of data from other organizations' data — particularly if the partner contracts with your competitors. Document the controls that a business partner must acknowledge and maintain to provide for the protection and separation of data.
<b>System development / change security risk assessments</b>	Contractually require the third party to provide documentation that an adequate risk assessment process was performed during system development and changes to the system.	Security risk assessments should be done as part of the design and implementation of new information resources and during the changes. Contractually require the business partner to provide a copy of, at the least, an executive summary of the most recent risk assessment upon your company's request.
<b>Monitoring requirements and incident response, disclosure, reporting</b>	Contractually require that the business partner monitor for security incidents defined in the business partner relationship and that they provide for the capability to respond to and resolve information security incidents effectively.	Related to this is incident disclosure; require the business partner to immediately report all security incidents to your company, expediting those that involve regulated information such as social security numbers, credit card numbers, and so on.

<b>Personnel exit policies and procedures</b>	Contractually require the business partner to have procedures in place to retrieve all your company's data and information assets from any of their employees immediately upon their termination from the business partner.	It is a high risk when a third party's employees who have been handling your company's data leave their company. This is especially true if the employee was allowed to work from home, used their own personal equipment, kept your data on mobile storage devices, and so on.
<b>Computing equipment disposal</b>	Contractually require the business partner to irreversibly remove all your company's data from all the hardware they retire, sell, donate to others, dispose of, or otherwise no longer use.	Many incidents have occurred when data is not removed from computing equipment that companies have sold, thrown away, or donated to other groups.

### Business Partner Privacy and Security Liaison

Contract Area	Description	Notes
<b>Third party security function</b>	Contractually require the third party to assign a person to coordinate security responsibilities.	Contractually require the third party to provide upon request the formally documented job description for the position with information security and privacy responsibilities.
<b>Lines of communication</b>	Establish clear lines of communication about information security and privacy with the third party.	Contractually require the third party to identify a point of contact with whom your company can communicate at any time about information security and privacy issues.
<b>Regular review meetings</b>	Contractually require meetings to review service levels and security incidents.	Meet at least once a quarter for business partners who handle customer and/or employee personally identifiable information.

<b>Business Partner Personnel</b>		
<b>Contract Area</b>	<b>Description</b>	<b>Notes</b>
<b>Suitability of the third party's staff</b>	Contractually require third parties to notify your company of any personnel who used to work for your company.	Make sure none of your disgruntled ex-employees are now employees of the business partner to which you are outsourcing your data handling. Such situations have had a devastating impact on companies.
<b>Recruitment policy and security clearances of the third party's staff</b>	Contractually require criminal and, where appropriate, financial checks to be performed on the business partner personnel prior to their hire.	No matter how many security safeguards are in place, it's difficult to stop an opportunist who will steal data for money, revenge, or some other reason. Ensure that the people handling your data have not been convicted of criminal activity that would make them a high risk for handling your data. This verification might be tricky in some countries because records of criminal activity may not be centralized, such information may be labeled differently, and in some countries doing such checks are against privacy laws.
<b>Disciplinary procedures</b>	Contractually require the third party to have clearly documented disciplinary procedures implemented that are consistent with your company's procedures.	Make sure the business partner personnel are well trained about information security and privacy procedures and legal consequences. Ensure documented sanctions policies exist.
<b>Subcontractor relationships</b>	Prohibit subcontractor relationships that would provide access to your organization's data or systems unless approved by your company.	Determine how to handle subcontractors. Prohibit subcontractor relationships in contracts and/or establish processes for approval of subcontracting relationships.

## Right to Audit and Monitor

Contract Area	Description	Notes
<b>Business partner self-assessment requirement</b> (prior to signing the contract)	Contractually require business partners to complete an information security self-assessment questionnaire (provided by your company) about their information security and privacy program.	When creating this questionnaire, structure the questionnaire around the ISO 17799 and OECD topics in addition to any specific regulatory requirements that are beyond these standards. Obtain these self-assessments prior to contractually committing to any business relationships, and then periodically following the formal establishment of the relationship.
<b>Right to audit</b>	Contractually require that regular information security reviews be done to ensure that the control architecture and supporting standards, baselines, procedures, and guidelines are being adhered to.  Recommend, or better yet require, that the business partner use an independent third party to assess information security and privacy controls.	Contractually require that copies of audits are made available for your review. Types of audits may include: SAS 70 (Type I & II), BS7799 certification audits, vulnerability assessments, penetration tests, and so on.  Ensure adequate access to all sites, records, documents, software, and so on. The third party should agree to independent or ad hoc audit inspections during the third party's normal working day with reasonable notice, such as seven to 15 days in advance.
<b>Audit review actions</b>	Contractually require the third-party to respond in writing with action plans arising from audit reviews.	When risks and vulnerabilities are discovered during audits it is important for the third party to provide a written plan for addressing the issues, and a timeline for issue resolution/correction.

Liability		
Contract Area	Description	Notes
<b>Warranty</b>	Provide the standard contracting language as provided or recommended by your acquisitions department.	Ensure the warranty includes wording for applicable data protection regulatory requirements.
<b>Damages</b>	Provide the standard contracting language as provided or recommended by your acquisitions department.	Include requirements for the third party to reimburse your company for information security and privacy incident damages involving your company's data that occur within their organization, such as if one of their employees loses a laptop with your data, if they lose a backup tape with your data, and so on.
<b>Consequential loss</b>	Provide the standard contracting language as provided or recommended by your acquisitions department.	Include requirements for the third party to reimburse your company for information security incident damages involving your company's data that occur within their organization, such as if a hacker obtains your company's database within their system, and so on.
<b>Insurance</b>	Provide the standard contracting language as provided or recommended by your acquisitions department.	Consider requiring the third party to have cybercrime insurance. Factors to consider are the types of data the third party handles, the geographic locations, the types of activities the third party does with the data, and so on.
<b>Loss</b>	Provide the standard contracting language as provided or recommended by your acquisitions department.	Ensure the amount of loss includes the value of the data and service time, not just the value of the hardware involved.

## Other Contracting Considerations

When including information security and privacy requirements within the contracts you have with your business partners include enough detail to cover all issues but don't be so specific that you allow them a way to avoid doing a security activity just because you did not specifically state it within the contract. Include citations of the specific laws for which your company must comply so that the business partner understands that they must also comply with such regulations.

Review the business partner's information security policies. Require within the contract with the business partner that information security policies must be made available immediately upon your company's request. Ensure the policies cover all the topics related to the activities that the business partner performs for your company. Ensure the wording within the partner's information security policy is strong enough to actually motivate the personnel for compliance. Look for executive endorsement of the policies and for clearly stated sanctions for policy violations.

---

## **Bottom Line: Responsibility Follows the Data**

The bottom line is that entrusting your data to another company, or outsourcing data handling, processing, and management, is a risky proposition for your organization. It is your responsibility to ensure strong security follows the data to your business partner and that safeguards remain during the duration of the business relationship.

You must perform due diligence to ensure your business partners are protecting the data according to your information security and privacy requirements. Remember, you are ultimately responsible for what happens to the data you've given to your business partners.

It is worth emphasizing that you need to be sure to discuss these issues with your organization's legal counsel and acquisitions areas. Modify business partner contracts and acquisition requirements according to what is best for your organization. Don't allow your organization's name to make the headlines because your business partners did not secure your data appropriately and subsequently experienced a security incident.

---

# What Healthcare Organizations Need to Know About HIPAA, Minors and Privacy

by *Rebecca Herold, CISSP, CISM, CISA, FLMI*


*June 2006*

The Health Insurance Portability and Accountability Act (HIPAA) has some specific requirements related to handling the protected health information (PHI) for minors and for the types of access that can be allowed to this information, even to parents and guardians. Many state-level laws also have requirements for restricting parental and guardian access to minors' PHI under certain conditions. With the commonplace practice of allowing individuals access to their account information via Internet applications, particularly among health insurance companies and pharmacies, it is important that covered entities consider the issues and impacts of providing access to the PHI of minors through such automated means as well as in person. However, there really is no guidance offered to covered entities (CEs) explaining ways to implement these restrictions.

The U.S. Department of Health and Human Services (HHS) has provided requirements restricting access to the PHI of minors. However, there really is no guidance offered to CEs explaining ways to implement these restrictions. Because of the subjective nature of regulatory text and actually putting such guidance into practice, it is important for organizations to know what is expected for compliance, document their decisions, and implement appropriate systems, applications, and procedures to support those decisions.

## HIPAA, Minors, and PHI

Parents generally have the right to make healthcare decisions for their children, and so are, by default, considered the personal representatives for decisions about PHI access, use, and disclosure for unemancipated minors. 45 CFR § 164.502(g) of the Privacy Rule addresses the issues of parents obtaining access to their minor children's PHI. The key consideration is whether the parent is considered the "personal representative" of the child under HIPAA.

 Clearly worded state laws preempt federal law on the issues of parents' versus minors' access to and control of information. However, when state or other applicable law is unclear concerning parental access to a minor's PHI, a covered entity has discretion to provide or deny a parent access to the minor's PHI if doing so is consistent with state or other applicable law, and provided the decision is made by a licensed healthcare professional in the exercise of professional judgment.

Because a parent or legal guardian typically has authority to make healthcare decisions about his or her minor child, the Privacy Rule generally considers the adult a "personal representative" with the right to obtain access to the minor's health information.

---

## When Parents Are Not “Personal Representatives”

There are important exceptions to note for when a parent is not considered a minor’s personal representative. Generally these include the following:

If a state, or other applicable, law does not require consent of a parent or other person before a minor can obtain a particular healthcare service, and the minor consents to the healthcare service, then the Privacy Rule does not consider the parent as the minor’s personal representative. The minor can involve a parent in healthcare decisions if he or she so wishes to without giving up the right to control the related health information. The minor can also choose to have the parent be his or her personal representative.

For example, if a state law provides a minor the right to consent to mental health treatment without the consent of his or her parent, and the minor obtains such treatment without the consent of the parent, the parent is not considered the minor’s personal representative under the Privacy Rule for that specific treatment.

If a court determines, or other law authorizes, someone other than a parent to make treatment decisions for a minor, the parent is not considered the personal representative of the minor under the Privacy Rule for the specific situation. For example, a court might grant authority to an adult other than the parent to make specific types of healthcare decisions for a minor.

A parent can also agree that a confidential relationship can exist between the minor child and the physician, in which case the Privacy Rule would no longer consider the parent as the personal representative.

For example, if a physician asks the parent of a 16-year-old if the physician can talk with the child confidentially about a medical condition and the parent agrees, the parent would not control, or even be able to access, the PHI that was discussed during that confidential conference.

When a physician reasonably believes in his or her professional judgment that the child has been or may be subjected to abuse or neglect, or that treating the parent as the child’s personal representative could endanger the child, the physician may choose not to treat the parent as the personal representative of the child.

In addition to the general situations described, the Privacy Rule also stipulates that state laws will not be preempted if they specifically address disclosure of health information about a minor to a parent (see § 160.202).

---

## Implications for Healthcare Organizations

So how do these requirements impact healthcare organizations? There are some significant and distinct issues all types of CEs must address. The following sections delineate the major issues involved, what CEs must consider, and possible actions to take.

### ***Determining Who Can Access a Minor's PHI***

Always document when a parent or legal guardian:

Has agreed to allow communications with a physician to be confidential

Has been determined by a physician to not be allowed access to a minor's PHI

Has legally been declined access to PHI by a minor



Typically, the determination of whether a parent or legal guardian can access a minor's PHI occurs at or before the time the minor receives medical treatment.

Healthcare providers should specifically send such documentation to applicable healthcare insurers, pharmacies, clearinghouses, and any other business associate that might provide access to the PHI in any form to the insured.

Healthcare payers, pharmacies, clearinghouses, and business associates with responsibilities for PHI should specifically request that healthcare providers offer notification for when parents or legal guardians are not considered as personal representatives and should not have access to a minor's PHI. Do not assume that the healthcare provider will automatically send you such notifications.



The general principle used by the HIPAA Privacy Rule is: If a person has a right to make a healthcare decision, he/she has the right to access and control information associated with that particular decision.

### ***Establishing Procedures to Limit Access to Minors' PHI***

CEs must establish procedures to ensure access restrictions are checked prior to giving access to a minor's PHI. This can prove to be problematic within online systems because, typically, the primary contact for an insured's family policy is a parent or legal guardian. CEs providing online access to PHI, such as within claims or prescription systems, must consider how to address two primary situations:

A newly insured with existing restrictions

An existing insured with a new restriction

---

The challenges and issues to tackle for restricting parents and legal guardians from a minor's PHI include:

- Communicating the restrictions to the personnel who manage the access rights to PHI
- Establishing a way within the applications, systems, and databases to flag the minors who have parental and guardian restrictions for accessing their PHI
- Preventing access to a minor's claim information containing PHI—such as medicines prescribed, physical symptoms, and so on—from parents and legal guardians
- Preventing access to a minor's prescription information from being given to parents and legal guardians

### ***Establishing Technology to Limit Access to Minors' PHI***

Once the issues and procedures have been identified for limiting minors' PHI access, technology must then be modified to support the procedures. Such updates can present some significant challenges, such as the following:

- Modifying existing applications and systems to restrict access to specific fields within the policy of an insured family
- Modifying existing database structures to be able to provide access to specific fields within an insured's policy record
- Establishing a separate user ID and password for the minor to access PHI to prevent the parent or guardian from obtaining access
- Communicating the separate user ID and password to the minor without revealing it to the parents and guardians when they live at the same address

There are several combinations of possible solutions to consider:

- Using federated identity management solutions to limit access within applications to the fields within the records of each insured
- Restricting access to the specific minor's fields within the insured's records and then creating a separate ID and password to allow access to those fields
- Creating copies of minors' PHI and storing it in separate records away from the parents, then deleting those corresponding fields within the insured's records; a separate application, or application option, would then need to be created to provide special access to the minors' PHI
- Communicate the minor's ID and password either directly over the telephone or send it by registered mail requiring the minor to sign for this information


Some CEs have chosen to notify the healthcare provider and minor that the current applications cannot restrict access to the minor's PHI to prevent the subscriber owner (the parent or legal guardian) from getting access to the information. This does not solve the problem of preventing access but might potentially limit the liabilities and negative impact of not limiting access to minors' PHI. This option should be very carefully discussed with the CE's legal counsel, as well as any other option being considered.

---

### ***Making Personnel Aware of Restrictions to Minors' PHI***

The best procedures, plans, and technology in the world will be ineffective if not communicated to the personnel that must follow and use them. Personnel must be told what to do in situations in which parental and guardian access to minors' PHI is restricted. IT must be told the goals for these restrictions so that they can effectively build the access controls into applications, systems, and databases.

As with any information related to information security and privacy, training and awareness must be ongoing. Simply publishing the information once is not effective. Organizations need to provide periodic reminders through intranet Web sites, memos, email messages, posters, presentations, and other communications channels. Procedures and standards for supporting this special type of access requirement must be clearly documented and included with the rest of the organization's procedures and standards. Communication and documentation are also vital if you ever find yourself in a legal dispute and must demonstrate you have effective policies and procedures in place.

 If you do not clearly and continuously communicate your policies, procedures, and standards and explain how they impact the organization, they will be ineffective, both within your organization and within a court of law.

---

## State-Level Breach Notice Laws as of June 7, 2006

*by Rebecca Herold, CISSP, CISM, CISA, FLMI*

As of June 7, 2006, I have found 32 state-level breach notice bills that have been signed into law, with the exception of the bill in Hawaii, which has been enrolled to the governor. Use the following table as a handy reference to these laws and their corresponding effective dates.

State Breach Notice Laws	Effective Dates
1. Arizona SB 1338	Effective 12/31/06
2. Arkansas SB 1167	Effective 8/12/05
3. California SB 1386	Effective 7/1/03
4. Colorado HB 1119	Effective 9/1/06
5. Connecticut SB 650	Effective 1/1/06
6. Delaware HB 116	Effective 6/28/05
7. Florida HB 481	Effective 7/1/05
8. Georgia SB 230	Effective 5/5/05
9. Hawaii SB 2290 [enrolled to governor]	Effective 1/1/07
10. Idaho SB 1374	Effective 7/1/06
11. Illinois HB 1633	Effective 1/1/06
12. Indiana HB 1101	Effective 7/1/06
13. Kansas SB 196	Effective 1/1/07
14. Louisiana SB 205	Effective 1/1/06
15. Maine LD 1671	Effective 1/31/06
16. Minnesota HF 2121	Effective 1/1/06
17. Montana HB 732	Effective 3/1/06
18. Nebraska LB 876	Effective 4/6/06
19. Nevada SB 347	Effective 1/1/06 [10/1/08 for mandatory encryption]
20. New Hampshire HB 1660	Effective 1/1/07
21. New Jersey A4001	Effective 1/1/06
22. New York S 3492 and S 5827	Effective 12/7/05
23. North Carolina SB 1048	Effective 12/1/05
24. North Dakota SB 2251	Effective 6/1/05
25. Ohio HB 104	Effective 2/17/06
26. Pennsylvania SB 712	Effective 6/20/06
27. Rhode Island HB 6191	Effective 3/1/06
28. Tennessee HB 2170	Effective 7/1/05
29. Texas SB 122	Effective 9/1/05
30. Utah SB 69	Effective date 1/1/07
31. Washington SB 6043	Effective 7/24/05
32. Wisconsin SB 164	Effective 3/31/06

---

# What IT Needs to Know About Compliance

by *Rebecca Herold, CISSP, CISM, CISA, FLMI*

*June 2006*

Businesses must always be vigilant about data security, particularly in the global information-based economy. Businesses are dependent upon information technology (IT). The risks that are an inherent part of IT make it necessary for IT leaders and IT personnel to know the data protection laws and regulations more than ever before. It is with this knowledge that they can incorporate information security and privacy within all the IT processes, throughout the entire systems development life cycle (SDLC).

## Regulations with IT Requirements in the United States

There are many regulations worldwide that have numerous data protection requirements. Some of these regulations directly apply to IT practices, but many indirectly impact IT, and it is important that IT leaders are aware of them. Within the U.S., the regulations that have received the most press and most explicitly define IT requirements include the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA). However, other laws that don't explicitly state information security requirements, such as the Federal Trade Commission Act (FTC Act), still profoundly impact information security activities.

### **GLBA**

The Safeguards Rule component of GLBA greatly impacts IT leaders. At a high level, this rule requires IT leaders to:

- Establish a security plan to protect the confidentiality and integrity of personal data.
- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal data that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.
- Establish ongoing information security training and awareness.
- Implement security for and within information systems, including network and software design and information processing, storage, transmission, and disposal.
- Implement methods to detect, prevent, and respond to IT attacks, intrusions, or other system failures.

---

Design and implement information safeguards to control identified risks and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

Ensure the security of business partners and service providers by taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue, and requiring them within your contracts to implement and maintain safeguards.

Regularly evaluate and adjust the information security program based upon the results of the testing and monitoring, material changes to operations or business arrangements, and any other circumstances that might have a material impact on the information security program.

**Technology Issues IT Must Address for GLBA**

- Authentication and identification
- Access controls
- Awareness and training
- Malicious code protection
- Risk analysis
- Business continuity and disaster recovery
- Data disposal
- Data retention
- Secure data transmissions
- Secure data storage
- Customer management databases
- Procedures supporting your published policies
- Third-party data sharing

---

## **HIPAA**

The Security Rule component of HIPAA also greatly impacts IT leaders. At a high level, this section requires IT leaders to:

Perform a risk analysis for the electronic protected health information (PHI) within the organization and establish appropriate controls based upon the risks.

Ensure the confidentiality, integrity, and availability of all electronic PHI that the organization creates, receives, maintains, or transmits.

Protect against any reasonably anticipated threats or hazards to the security or integrity of PHI.

Protect against any reasonably anticipated uses or disclosures of PHI.

Comply with the Security Rule standards with respect to all electronic PHI.

Review and modify security measures as needed to ensure reasonable and appropriate protection of electronic PHI.

Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule.

Provide ongoing information security training and awareness to all personnel handling PHI.

Ensure business partners have appropriate information security practices for the information your organization has entrusted to them.

### **Technology Issues IT Must Address for HIPAA**

Authentication and identification

Access controls

Awareness and training

Malicious code protection

Risk analysis

Business continuity and disaster recovery

Data disposal

Data retention

Secure data transmission

Secure data storage

Customer management databases

Procedures supporting your published policies

Third-party data sharing

---

## **FTC Act**


A regulation quickly growing in importance to IT leaders because of increasing compliance efforts, actions, and fines is Section 5 of the FTC Act. This basic consumer protection statute provides that “unfair or deceptive acts or practices in or affecting commerce are declared unlawful.” Although this regulation does not explicitly indicate information security requirements, the lack of security to support promises made to consumers, such as those commonly found in Web site privacy policies, can have significant impact on organizations. IT must implement security not only to support any posted policies and customer and business partner contracts that indicate information security measures exist to protect personal information, but they must also increasingly have such security measures in place as a basic expectation of a standard of due care.

### **Technology Issues IT Must Address for the FTC Act**

- Procedures supporting your published policies
- Access controls
- Third-party data sharing
- Firewalls and malicious code prevention
- Applications and systems development
- Secure data transmissions
- Secure data storage
- Secure data disposal

## **International Regulations with IT Requirements**

Throughout the world, there are numerous data protection laws that impact the decisions IT leaders make. Technology must be aligned with the requirements of the diverse geographic markets within which you operate.

 You must look at international information security and privacy differences in terms of what is expected and normal for the country within which you are storing, processing, or transmitting data—not in terms of what is expected and normal in your country of residence.

Just a few of the laws that have had significant impact on companies include Canada’s Personal Information Privacy and Electronic Data Act (PIPEDA), the European Union’s Data Protection Directive, and Japan’s Information Protection Law.

---

## **Canada's PIPEDA**

Canada's PIPEDA applies to every organization with regard to its use of personal information about Canadian citizens that it collects, uses, or discloses in the course of commercial activities, and about its employee's personal information. IT leaders need to:

Establish safeguards for personal information to ensure only those with a business need can gain access to it.

Establish retention practices to ensure personal information is retained for as long as is necessary to allow individuals access to it for pursuing actions to PIPEDA violations.

### **Technology Issues IT Must Address for PIPEDA**

Individual access requirements

Procedures supporting your published policies

Access controls

Third-party data sharing

Cross border data flow

Applications and systems development

Secure data transmissions

Secure data storage

Canadian provinces have generally been following the BS7799 standards for information security and the OECD privacy principles for many years. By adopting these practices and integrating them into your own IT standards, you will be several steps ahead in facilitating information data flows with Canada.

## **EU Data Protection Directive**

Any person or organization that collects or handles personal information from a citizen of any of the 25 EU nations and transfers the information across the country borders must comply with this regulation. To comply with these requirements, IT leaders must generally:


Establish policies and procedures to keep personal data accurate and up to date, document when a data subject informs you that data is inaccurate, and take reasonable steps to ensure that data is accurate beyond simply asking the subject when the data is collected.

Establish procedures to discontinue use of personal data and dispose of it when it is no longer necessary for the business purpose for which it was collected.


Establish appropriate security technology to prevent personal data from being hacked, lost, damaged, or stolen.

Establish procedures to prohibit the transfer of personal data outside the European Economic Area unless the country to which it is being transferred provides an adequate level of protection.

---

 Keep in mind that there is a traditional European 1-month-long holiday that can start anywhere between mid-July and mid-September. Schedule your IT upgrades and implementations to allow for the possibility that you might not be able to work with your IT counterparts in the EU countries during this time. If you don't, it could significantly impact your project and security, and potentially result in downtime your organization cannot afford.

Similar to Canada, the EU countries have been following the BS7799 standards for information security and the OECD privacy principles for many years. This should provide even more impetus to adopt these practices and integrate into your own IT standards—helping you to be positioned to successfully address legal requirements within these countries.

 You must be aware that each of the EU countries is mandated to have country-specific data protection laws that must, at a minimum, correspond with the EU Data Protection Directive. Some of the country-level laws go beyond the directive requirements.

There are very strict data protection laws within the EU for not only consumer data but also employee data. So, for example, if you are considering the implementation of a U.S.-based centralized SAP solution for all your worldwide offices, it is important to know that in some countries, such as France, the transmission of employee data across country borders is prohibited unless you work out an agreement with each of the applicable country's privacy commissioner.

#### **Technology Issues IT Must Address for the EU Data Protection Directive**

- International data flow restrictions
- Individual access requirements
- Procedures supporting your published policies
- Access controls
- Third-party data sharing
- Applications and systems development
- Secure data transmissions
- Secure data storage
- Secure data disposal

---

## **Japan's Personal Information Protection Law**

Japan's Personal Information Protection Law broadly provides for the protection of personal information used by the Japanese government, third parties, and the public sector, referenced as "Personal Information Handling Operators," that handle data about more than 5000 persons. As part of the compliance requirements, IT leaders must generally:

Establish procedures to keep third parties from accessing personal data except as required by law.

Establish procedures to retrieve personal data for specific individuals upon their request.

Establish procedures to correct personal data errors and inaccuracies as quickly as possible.

Establish procedures to discontinue use of personal data as soon as requested.

Establish safeguards for personal data.

### **Technology Issues IT Must Address for Japan's Personal Information Protection Law**

Authentication and identification

Access controls

Auditing and logging

Malicious code prevention

Secure data transmissions

Secure data storage

Third-party data sharing

Besides the aforementioned laws, there are literally hundreds of other international and U.S. federal and state-level laws with which organizations must comply. These laws cover not only customer and consumer personal information but also employee information.

---

### **More Incidents and More Actions in the U.S.**

IT leaders must know that as technology advances, information security lags behind those advances. Diligence is necessary to ensure the security of personal data no matter where it is located. If IT leaders do not participate in data protection efforts, the business is at high risk of being negatively impacted by resulting incidents, non-compliance fines, civil suits, customer loss, diminished stock value, and brand damage.

IT leaders need to be aware of the increasing numbers of information security incidents and regulatory oversight actions. For example:

As of April 2006, the FTC has filed five data security cases based on deception, which the commission and the courts have defined as a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances. In each of these cases, the commission alleged that the companies made explicit or implicit promises that they would take appropriate steps to protect sensitive information obtained from consumers. Their security measures, however, were grossly inadequate and their promises therefore deceptive. The FTC has also brought 12 other data security cases, 6 spyware and adware cases, more than a dozen financial pretexting cases, and more than 80 spam cases.

As of May 2006, the Department of Health and Human Services has received almost 20,000 noncompliance complaints and launched thousands of HIPAA noncompliance investigations, and two criminal cases have been brought for non-compliance with HIPAA.

The numbers of reported incidents of PIPEDA noncompliance in Canada have steadily been increasing over the past few years. In 2002, Canada launched approximately 1700 PIPEDA investigations. Canadian Federal Privacy Commissioner Jennifer Stoddart warned in a speech made public March 9, 2006 that she will make greater use of her statutory powers to crack down on privacy violations in Canada because organizations are not taking their privacy responsibilities seriously enough, and are not responding appropriately to the Privacy Commissioner's directives following violations.

The numbers of actions taken in EU nations has steadily been increasing over the past several years. As examples, in 2002, the Spanish Data Protective Authority fined approximately US\$900,000 against an organization for inappropriately sharing customer data with a subsidiary, and approximately US\$1.17 million for disclosing protected personal information to the public.

During the years 2001 to 2002, 483 privacy complaint cases were completed in Hong Kong by the Privacy Commissioner Office.

## **What IT Leaders Need to Know**

Noncompliance with laws and regulations can not only impact organizations significantly as an effect of regulatory fines but also through the greater impact from the potential civil actions and the long-lasting requirements of the regulatory agencies that result in organizations needing to implement more procedures and obtain more resources to demonstrate, for as long as 20 years following a judgment, that they have reasonable security measures in place. Many laws and regulations have requirements for protecting information that IT leaders must be involved with implementing, and in many cases, establishing and managing as an ongoing process to meet the requirements.

Critical to the success of the IT leaders is the visible and demonstrated support and backing of executive management. Executives set the examples their personnel emulate. If business executives are not strong supporters of information security initiatives, IT leaders will have a very difficult time meeting the technology requirements of data protection regulations and laws.

---

## ***IT Leader Regulatory Compliance Action Plans***

IT leaders must establish a unified regulatory compliance action plan tailored to their business to ensure that the business is addressing all technology compliance requirements. This action plan needs to include the following elements, which are explicitly stated components of an effective security program not only within regulations such as HIPAA and GLBA but also by regulatory oversight agencies such as the FTC (Source:

<http://www.ftc.gov/os/2006/03/P034101CommissionTestimonyConcerningSmallBusinessSecurity.pdf>):

Implement effective education programs to stay aware of regulatory requirements; make personnel aware of and provide training about the threats to information systems and the steps all business areas must take to address them.

Develop and communicate information security policies and procedures regarding the appropriate use and security of information and computer systems.

Incorporate security into the systems and applications development life cycle to ensure security is implemented and managed effectively.

Identify and inventory all personal data, including data flows, storage locations, and persons with access to the data.

Implement safeguards, such as encryption and access control technologies, to protect personal data in all locations and while in transit through untrusted networks.

Include security requirements within contracts of business partners entrusted with personal information or that have access to the organization's personal information.

Use malicious code prevention software, intrusion detection and prevention systems, and firewalls.

Establish personal data backup, retention, and disposal policies and procedures that comply with applicable laws, regulations, and contractual requirements.

Establish information privacy and security incident response and breach notification policies and procedures.

---

## Incorporate Information Privacy and Security into the SDLC

Based upon the discussion so far, you should recognize the recurring IT requirements necessary for compliance with the multiple laws and regulations. Look at all the lists as one composite set of requirements; it will unify compliance efforts and address many regulations within one set that should be made part of your regulatory compliance strategy.

### **IT Must Address the Following Requirements that Are Extrapolated from a Wide Range of Regulations and Laws**


- Access controls
- Applications and systems development
- Auditing and logging
- Authentication and identification
- Awareness and training
- Business continuity and disaster recovery
- Cross border data flow
- Customer management databases
- Data disposal
- Data retention
- Firewalls and malicious code prevention
- Individual access requirements
- International data flow restrictions
- Malicious code prevention
- Procedures supporting your published policies
- Risk analysis
- Secure data disposal
- Secure data storage
- Secure data transmissions
- Third-party data sharing

---

The most effective way to incorporate these issues consistently into the IT environment is to:

- Make them formally documented requirements within your SDLC process

- Assign specific positions or personnel with the information security and privacy activities involved to ensure they are addressed sufficiently

 IT must address information privacy and security throughout the entire SDLC.

Perform information privacy and security risk assessments at key points throughout the SDLC to ensure the related issues have been addressed, and to catch any showstoppers related to privacy or security.

### ***Performing PIAs***

The systems development and maintenance teams must ensure privacy impact assessments (PIAs) are performed to help ensure compliance with applicable laws and regulations:

- Throughout the SDLC

- To determine where PII will be obtained, stored, transmitted, and retired

- To determine applicable data protection laws and regulations

- To determine who will have access to PII

- To map the planned PII data flow

- To identify risks throughout the flow

### ***Performing Information Security Risk Assessments***

The systems development and maintenance teams must ensure information security risk assessments are performed to help ensure compliance with applicable laws and regulations:

- Throughout the SDLC

- To identify technical, administrative, and physical risks within the planned system

- To identify cost-effective controls to address the identified risks

---

# Managing Mobile Computing Risks

*by Rebecca Herold, CISSP, CISM, CISA, FLMI*

As demonstrated over and over again throughout the past several months, mobile computing devices and storage media present a huge risk to business and personal information. Because of the very portability of these devices, organizations are entrusting the security of the information stored upon them into the hands of the people using them. It is vital that an effective mobile computing device and storage media security management program is in place. This program should answer the questions:

How many people within your organization use mobile computing devices, such as laptops, Blackberries, and other types of Personal Digital Assistants (PDAs)?

What have you told them about how to properly secure these devices?

Do you simply rely upon having published a policy about this topic?

Have you gone a step further and actually trained them about how to secure these highly vulnerable mobile goldmines of information and access paths into your network?

Do you provide ongoing awareness to your mobile computer users about how to properly secure them?

## The Risks Are Increasing

Incidents involving mobile computing devices and storage media in the past few months seem to make headlines daily. The following list highlights just a few of the many recent stories of lost or stolen mobile computing devices and storage media:

On April 16, 2006, it was reported that a computer disk—as well as the computer holding the disk—containing confidential information about Vancouver’s Fraser Health Authority (FHA) employees and their participation in counseling services was stolen in March from the Vancouver office of the Employee and Family Assistance Program (EFAP) run by the Vancouver Coastal Health Authority.

On March 28, 2006, Mercury News reported that since January 2005, Palo Alto, California police received 65 reports of stolen laptops. The trend appeared to be stealing the laptops from rental cars outside upscale restaurants.

On March 21, 2006, Hewlett-Packard employees were told that Fidelity lost a laptop containing unencrypted information about 196,000 current and former HP employees; the laptop was stolen on March 15.

On March 16, 2006, a San Francisco finance manager was stabbed and his laptop stolen in a Mission District café.

---

On March 15, 2006, it was reported that an Ernst & Young employee had a laptop containing unencrypted personal information for thousands of IBM's current and past employees stolen from his/her car in January.

On March 13, 2006, two laptop computers were stolen from the campaign headquarters of Oakland, California mayoral candidate Ignacio De La Fuente.

On March 1, 2006, the Toledo Blade reported a man was arrested in San Jose, California in connection with the theft of digital records for a medical group. One of the stolen DVDs contained clinic visit records for almost 200,000 patients.

On February 28, 2006, a laptop was stolen from the car of the Vermont State Colleges' chief information officer (CIO). It contained 6 years' worth of personal information about as many as 20,000 to 50,000 faculty, staff, and current and former students of Lyndon State College, Johnson State College, Castleton State College, Vermont Technical College, and the Community College of Vermont. The information included unencrypted names, addresses, birth dates, and Social Security numbers.

On February 25, 2006, it was reported that an Ernst & Young laptop was stolen from the car of one of its employees. The laptop contained unencrypted personal information for an undisclosed number of its customers, including Social Security numbers. In an ironic twist, one of the customers was Sun Microsystems CEO Scott McNealy, who was quoted a few years ago as saying "You have no privacy. Get over it."

On February 23, 2006, the Sacramento Bee reported a laptop containing health information for 1746 clients of CARES, a Sacramento HIV/AIDS clinic, was stolen during a home burglary.

On February 9, 2006, four Ernst & Young laptops were stolen from the unattended conference room where they were left over lunch.

On February 1, 2006, Eweek reported that discarded printouts containing personal information were thrown into a dumpster, and subsequently were used to wrap fish at an outdoor market.

On January 26, 2006, it was reported that an Ameriprise Financial laptop containing clear-text information, including names and Social Security numbers, for 225,000 clients was stolen from an employee's car at an undisclosed location out of state.

On December 31, 2005, an employee of the Providence Health Systems in Seattle reported computer backup tapes and disks containing information about 365,000 patients were stolen from his car at his home. The data was not encrypted. The tapes and disks were taken home by the employee for off-site storage.

On December 15, 2005, a Deloitte & Touche employee left an unencrypted CD containing the personal information about 9000 McAfee employees in an airline seat pocket.

---

## **Mobile Computing Devices and Storage Media are Threats to Business**

According to Laptopsecurity.org, in 2005, more than 1.5 million vehicles in the United States were broken into and had items stolen from them; 100,000 of these items were laptops, which means that more than 270 laptops are stolen from cars every day in the U.S.

The threats to information security created by mobile computing devices and storage media are real:

According to Enterprise Strategy Group, 68 percent of computer administrators indicated laptops represent the biggest risk for the loss of confidential information.

According to the FBI, 97 percent of stolen computers are never recovered.

According to Safeware Insurance, more than 600,000 mobile computing device thefts occurred in 2004, totaling an estimated \$720 million in losses and an estimated \$5.4 billion in theft of proprietary information.

According to a 2005 Pointsec study, one-third of organizations report that removable storage media is used within their company without authorization.

Just because the data may be “difficult to interpret,” as company representatives often are quoted when asked about the loss of their laptops or storage devices, if the software used with the data is widely available, the data will likely be very easy to access. You must also consider that even though fraud or identity theft does not occur right away with the lost or stolen data, it does not mean that all is well. Smart thieves are good at doing their dirty deeds in ways that are difficult to notice, and they often wait what they consider is a safe amount of time before using someone else’s personal information for their personal gain.

## **Mobile Computing Device Self-Assessment**

Consider giving your mobile computer users the following short self-assessment, one of many I have created and used, as one of your many ongoing awareness activities. Put this online to not only allow each individual an easy and convenient way to take it but also enable you to compile the results and determine where you need to beef up your mobile computing security efforts. Provide feedback to each of the answers based upon your own organization, policies, and procedures. I have provided some examples of the feedback you could use, but be sure to modify it to meet your own organization’s needs. Also consider including some descriptions of actual incidents within your feedback to make it more interesting. Allow for each individual to take this assessment anonymously to encourage him or her to provide the most honest answers.

---

## Sample Online Self-Assessment

For each of the following questions, choose all the answers that apply to you. Please answer honestly; your responses will be anonymous, and they will help us to more successfully and efficiently implement ways to protect the personal and sensitive information stored on mobile computing devices, such as a laptop, Blackberry, PDA, and so on, as well as on mobile storage media, such as DVDs, CDs, USB thumb drives, backup disks and tapes, and so on.

1. Which of the following ways do you use to protect confidential information on your mobile computing devices and mobile storage media?
  - a. Encrypt the data using a strong encryption solution provided by the organization
  - b. Encrypt the data using a scrambling method developed by you or someone else in-house
  - c. Use a login password
  - d. Use a BIOS/boot password
  - e. I don't do any of these things; I didn't know I needed to
  - f. I don't do any of these things; they are too difficult to do and slow me down
  - g. I don't know whether any of these things are done or not

General feedback (remember, you need to expand upon these to fit your own organization) for each of the chosen answers:

- a) This is great! You are following our corporate policies. There are other actions you need to do, such as using passwords in addition to using encryption, as per policy.
- b) You are on the right track by trying to make the data unreadable, but using proprietary scrambling methods can be easily defeated. Use the corporate encryption solution to most effectively secure your data and to be in compliance with corporate policies.
- c) This is one very good component of overall data security for mobile devices and follows our corporate policy. Be sure you also use it in conjunction with encryption.
- d) This is very good. Using a BIOS, or boot, password is one of the layers of security you need to protect the information on your mobile computing device. See the corporate policy for other ways in which you need to be protecting the data on your mobile devices.
- e) Many significant incidents have occurred with mobile computing devices and storage media. It is critical that you take appropriate measures to protect the data on your devices. You should use boot and login passwords in addition to encrypting the data. See the corporate policy for details.

- 
- f) Yes, some security measures do seem to make it a little more difficult to use your computer or storage media. However, we have worked hard to implement technologies that are as easy and transparent to use as possible. Please contact the Information Security department if you are having trouble implementing encryption or setting your passwords. You can also see the “Mobile Device Encryption and Password FAQ” we have on our information security knowledge portal. Using passwords and encryption on your mobile devices is not only important for protecting our business and the data we are entrusted to protect but also required by our corporate information security policy, which you can also find on our information security knowledge portal.
  - g) The Information Security team can help you determine whether you are using encryption or passwords on your mobile devices. You can also see the “Mobile Device Encryption and Password FAQ” and the corporate “Mobile Computing Device and Storage Media Policy” on our information security knowledge portal.
2. In which of the following ways do you physically protect your mobile computing devices and mobile storage media?
- a. Keep the mobile computing device and storage media out of view of others
  - b. Carry the mobile computing device and storage media with you at all times
  - c. Lock your car when leaving the laptop in it
  - d. Use something other than a recognizable laptop case, such as a padded backpack, travel bag, or tote bag.
  - e. Use a cable to secure your mobile devices when leaving them in an unattended location
  - f. Ask someone to watch it for you in public areas, such as the airport, while you go to the snack bar or restroom
  - g. None of the above

General feedback (remember, you need to expand upon these to fit your own organization) for each of the chosen answers:

- a) Keeping your laptop out of view is a good start. How you keep it out of view is a crucial factor in keeping it secure. For example, leaving it in your car seat and just covering it with a today’s advertisement insert is NOT good security practice. See the “Mobile Device Physical Security FAQ” and the corporate “Mobile Computing Device and Storage Media Policy” on our information security knowledge portal for more details about this.
- b) This is a very good practice. Keeping your mobile devices with you is one of the best ways you can physically secure them. This is particularly important in airports, restaurants, conferences, and other public locations where many people are milling about.

- 
- c) Although it is good you lock your car, it is also very important where you keep your mobile device within your car. Do not leave it where it is visible from outside the car...and covering it with newspapers is not an acceptable way to hide it! Put it in a container that does not make it apparent it is a mobile computing device, and lock it in your trunk or glove compartment if you absolutely have to leave it in your car. Many laptop theft incidents have occurred in people's cars parked right by their own homes. The best practice is to take the mobile computing device and mobile storage media with you.
  - d) It is a great practice to use something other than a recognizable laptop case, such as a padded backpack, travel bag, or tote bag. Doing so helps to keep you from becoming a target of thieves looking for computing devices.
  - e) Using a cable is a good way to secure your mobile devices when you have to leave them in an unattended location, such as within a hotel room or in a meeting room. It is best, however, if you take the mobile computing device with you.
  - f) Ooh...this one is risky. If you ask just any stranger sitting close to you to watch it, as many people do, you run a very large risk of having your device and the person gone when you return. If you ask your trusted friend, family member, or business colleague, this is an acceptable practice; the key to this is that you can actually trust them to keep their eye on your stuff and not get distracted.
  - g) Yikes! If you are outside the corporate facilities, you are putting your mobile computing devices and storage media at great risk. See the "Mobile Device Physical Security FAQ" and the corporate "Mobile Computing Device and Storage Media Policy" on our information security knowledge portal for more details about this, or call our Information Security team to discuss.

## Ongoing Awareness

There are many more types of questions that you can use on an ongoing basis to keep information security issues in the minds of your personnel. I wanted to provide you with just a couple, though, to get you going.

Such short, two- to three-question self-assessments provide a non-intimidating way in which you can effectively raise awareness of information security issues within your organization and help lessen the probability of incidents occurring from personnel mistakes or lack of knowledge. Additionally, doing such activities will address the many regulatory and legal requirements for providing such ongoing awareness. You can either make these self-assessments mandatory or you can motivate personnel to take them by offering prizes, such as a restaurant or bookstore gift certificate, for participating. This can be done in such a way that anonymity is preserved.

---

## **Protect Your Mobile Computing Devices and Storage Media**

There are many actions organizations need to take to protect the mobile computing devices, storage media, and the data stored upon them. The following is a long laundry list of some precautions for you to take, as appropriate and applicable to your organization:

### ***Awareness and Training***

Train your personnel and provide ongoing awareness messages regarding how to appropriately secure mobile computing devices and storage media. Make sure they know how to protect their mobile computing device passwords.

Do not allow mobile computing devices to be shared; this is a train wreck waiting to happen. Shared devices eliminate responsibility for the device, and everyone using it assumes someone else is protecting it.

Communicate personnel's responsibility for the security of mobile computing devices and storage media. Implement a clearly written and well-communicated policy outlining personnel responsibility and have each person indicate in some form (written or electronic) their understanding of this policy and their agreement to follow it.

Require personnel to store only the minimal amount of data necessary on the mobile computing devices and storage media. Many well-publicized incidents have occurred with laptops containing information about hundreds of thousands of people.

### ***Physical Protection***

Require personnel to keep their mobile computing devices and storage media with them at all times while they are away from your facilities. Tell them not to leave the devices in cars, unattended meeting rooms, and so on. There are portable safes you may want to consider using, based upon the risk involved with your travelers who are carrying your sensitive information.

Provide physical security mechanisms, such as locks and cables, to personnel who take mobile computing devices away from your facilities.

Consider installing motion sensors or alarms on your mobile computing devices. The last thing a thief wants in a populated area is to have a 110 or more decibel alarm bringing everyone's attention to him or her. Of course, you need to train your personnel how to use them so they don't accidentally blast their own eardrums.

---

## ***Policies and Device Management***

Maintain an inventory of all your mobile computing devices and storage media and the people who are authorized to use them.

Use tracking labels and tags on all mobile computing devices and storage media.

Implement policies for the appropriate and acceptable use of mobile computing devices and storage media.

Document the software allowed to be used on mobile computing devices.

Establish backup procedures and tools for mobile computing devices.

Implement procedures to effectively and completely remove all corporate data from mobile computing devices when the person using it leaves the organization—if you have allowed personally owned devices to be used.

Do not allow mobile computing devices and storage media to be used for personal use.

Do not allow employee-owned mobile computing devices and storage media to be used for business purposes or storing business data.

## ***Encryption***

Require all confidential and personal information stored on mobile computing devices to be strongly encrypted.

Require all the data on mobile storage devices, such as USB sticks, to be encrypted.

Provide the encryption software to your personnel, and provide them with training about the importance of using it.

Use encryption for data transfers from mobile computing devices. Never send/receive sensitive data over a wireless link unless another more secure end-to-end encryption technology is also being used. Mobile devices that retain company sensitive information must implement a form of a company's standard encryption to safeguard such information.

## ***Data Issues***

Do not allow entire databases containing personal information to be stored on mobile computing devices. If personal data is necessary, use only the records the end user truly needs for business purposes.

Do not allow real personal data to be used for demonstration purposes, particularly on mobile computing devices.

Do not allow real personal data to be used for test and development purposes. Not only does this present great risk to the data, it is also against data protection laws in some countries.

---

## **Miscellaneous Technology Protections**

Require a software firewall to be implemented in all mobile computing devices.

Require malicious code protection software on all mobile computing devices, including a procedure to ensure that the software is maintained and up to date.

Implement a user identification and password authentication mechanism on all mobile computing devices to control user access to the systems.

Require a boot/BIOS password for all mobile computing devices.

Password-protect the systems administrator's account and root accounts on all mobile computing devices.

Also require a login password for all mobile computing devices. The more roadblocks you can establish for preventing unauthorized use of a mobile computing device, the better.

Implement procedures to ensure operating system (OS) updates will be installed in a timely matter on all mobile computing devices.

Implement procedures to disable all unused or unnecessary services on mobile computing devices.

Install and activate an inactivity timer or automatic logoff mechanism on all mobile computing devices.

Require wireless connectivity features (for example, 802.11, 802.16, Bluetooth) on all mobile computing devices to be set at the strongest level possible.

Establish procedures to update all spyware software on mobile computing devices with the same frequency as the organization's non-portable computers.

Disable file sharing on all mobile computing devices.

Enable auditing and logging on all mobile computing devices.

Disable displaying the last user logon name/ID.

Implement technology to allow you to destroy the data remotely if the mobile computing device or storage media is stolen or lost.

---

# ISMS Certification in the United States

*by Rebecca Herold, CISSP, CISM, CISA, FLMI*

Significantly fewer United States-based organizations are pursuing formal ISMS certification than in many other countries. In this article, I share my discussions with 10 chief information security officers (CISOs) from U.S.-based organizations about whether they are going to pursue ISMS certification and why. I also share the feedback given to me from a U.S.-based ISMS certification preparer group.

## Perspectives of U.S. CISOs

I spoke with CISOs from a wide range of industries of varying sizes, most with international presence. As Table 1 reveals, with the exception of one, they were not pursuing formal ISMS certification.

Industry	Number of Employees	International?	Have or Pursuing ISMS Certification?
Communications	80,000	Yes	No
Entertainment	150,000	Yes	No
Financial	115,000	Yes	No
Financial/Healthcare Insurer	20,000	Yes	No
Financial/Healthcare Insurer	28,000	Yes	No
Healthcare Insurer	3000	No	No
Manufacturing	8000	Yes	No
Manufacturing	200,000	Yes	No
Retail/Manufacturing	8000	Yes	No
Retail/Manufacturing	150,000	Yes	Yes

**Table 1: ISMS certification plans.**

---

## **Why Most U.S. Businesses Are Not Pursuing ISMS Certification**

With one exception, all the CISOs I spoke with asked to remain anonymous. The following are some of their revealing reasons for not pursuing ISMS certification:

The CISO for a multinational communications organization indicated she has built her information security program around ISO/IEC 17799, and has found the concepts extremely valuable, but does not see the business value to invest the time and resources in pursuing formal ISMS certification.

The CISO for a multinational entertainment organization indicated she has many other higher-priority information security initiatives to address before considering whether to pursue ISMS certification.

Ben Rothke, CISSP, the Director of Security Technology Implementation for AXA Technology Services, a division of AXA, the world's largest financial services company, offered his personal opinions about ISMS certification. "I have found many U.S. organizations are quite keen to ISO27001. When performing security audits or reviews, many of these organizations are requesting that the consultants that perform them map the results around the 27001 framework. One of the main benefits is that this standard ISO framework enables the organization to have a common way to look at the output, rather than each consultancy organizing the results to their particular methodology. Most organizations do not necessarily require the consultants or firms to be qualified auditors or implementers, rather to simply map the output to the standard. This is primarily due to the dearth of qualified auditors and implementers, combined with the fact that many organizations don't even know that qualified auditors or implementers exist."

Over the past year, the CISO for a multinational financial/healthcare insurer has been seriously considering whether to pursue ISMS certification. However, she has made the decision to focus her resources and efforts to regulatory requirements instead; she can demonstrate business value for regulatory compliance, but she cannot for ISMS certification.

The CISO from a multinational financial/healthcare insurer organization indicated her organization was not planning to pursue ISMS certification because her organization is "in the crosshairs of many of the current big hitters for information security-related U.S. legislative mandates" in addition to not having the funds to undertake formal ISMS certification. However, she indicated that she uses ISO/IEC 17799 within her information security program, but is just not going to get formal certification.

The CISO from a non-international healthcare organization indicated that he was not pursuing formal ISMS certification because other projects have higher priority, the maturation of his relatively new information security program did not lend itself to ISMS certification yet, and there was no perceived value within his organization to obtain ISMS certification.

---

The CISO for a multinational manufacturing organization indicated that although he was aware of ISO/IEC 17799, he was not aware it was possible to obtain certification based upon the BS7799 standards, was not aware of the change to ISO/IEC 27001, and had never heard of ISMS certification before I spoke with him about these topics. However, after learning about the ability to certify, he did not see the business value in obtaining ISMS certification. His organization's current policies and standards are based on ISO/IEC 17799, and he is currently incorporating COBIT, ITIL, HIPAA, SOX, and various privacy and FDA laws and regulations requirements into the program.

The CISO for a multinational manufacturing organization indicated his organization does not pursue any formal certification unless it is required by law or as a condition to do business (for example, ISO 9000). The primary issue for his organization is funding and management perception of business value, which they do not see with ISMS certification.

The CISO for a multinational retail manufacturing organization indicated that she created the security program based upon ISO/IEC 17799, but that other priorities must be addressed before she even thinks about ISMS certification, if at all.

### ***Why One Organization Did Obtain ISMS Certification***

One of the multinational retail/manufacturing organizations indicated they have obtained formal certification in more than 20 of their locations outside of the U.S. The scope for these certifications was for their commercial infrastructure management systems and their SAP services.

The primary drivers for obtaining ISMS certification at these locations was for an overall better security program for their customer-facing business and customer requirements. Security is very important to this organization, and obtaining ISMS certification is one of several ways that they are able to demonstrate to their customers that they take security seriously.

Additionally, as a U.S.-based organization, they have found certification has helped them with customer credibility not only outside of but also within the U.S. "Without the existence of a viable accreditation program and the accompanying demand from U.S. customers, though," this organization believes that, "other regulatory and legal pressures push ISMS certification to be a lower priority in the U.S."

---

## Current U.S. Organizations with ISMS Certification

How do the industries of the CISOs I spoke with align with the industries of the U.S. organizations that have obtained ISMS certification? I found only 27 unique U.S.-based organizations that are currently registered as having obtained formal ISMS certification. See Table 2 for the industries within which these organizations belong. This statistic does not include the one organization I spoke with that obtained certifications within their non-U.S. locations.

Industry	Number of ISMS Certifications in U.S.
Financial and Computer Processing Outsourcer	5
Manufacturing	5
Technology and Information Security Consulting	3
Financial Services	3
Software Development	3
Banking	3
Construction and Engineering	1
Pharmaceuticals	1
Digital Certificate Registration	1
Education	1
Legal Services	1

**Table 2: Current U.S. ISMS certifications.**

Based upon these factors and conversations I've had with several other information security practitioners at various conferences and professional meetings, it appears that the U.S.-based organizations that are most likely to seek formal ISMS certification are those in the outsourcing, manufacturing, consulting, financial services, software development, and banking industries. Based upon my own experience, I see a trend in outsourcers pursuing ISMS certification to make it more efficient for them to validate their security programs to their business partners.

### ***An ISMS Certification Preparer's Perspective***

Hotskills, Inc., based out of St. Paul, Minnesota, has participated in ISMS certifications for organizations based within the U.S. as well as outside the U.S. Tom Carlson with Hotskills indicates that the motivations for organizations to obtain ISMS certification differ. However, he has found the primary reason to be market differentiation, and the secondary is for regulatory compliance. Carlson also indicated that he believes the industries that are most likely to pursue ISMS certification are those that are heavily regulated, such as banking and finance, because of the third-party external validation and the inherent regulatory umbrella. According to Carlson, "It is a defensibility and efficiency issue."

A huge roadblock for an organization to obtain ISMS certification is to properly establish the scope of the certification. Carlson indicates, "Registration scope is one of the most misunderstood parts of the certification process. Most organizations do not scope wisely and bite off more than they can chew, resulting in project failure, or more than makes sense, which results in a waste of resources."

---

Many of the U.S. organizations I've spoken with that are aware of ISMS certification mistakenly believe that the certification must cover their entire organization. Raising the awareness and understanding of the need to properly establish the scope for the ISMS certification, which will typically be a subset of the organization, and often a very small subset at that, would likely lead to more U.S. organizations pursuing ISMS certification.

It is also important for U.S. organizations to realize there is not a typical timeframe within which ISMS certification can be accomplished; it depends upon a great number of factors and the scope of the certification. Some organizations could obtain ISMS certification within a few weeks, and for others, it could take well over a year.

Carlson described a hypothetical ISMS certification process and the factors involved. "A bank data center certification may be done as a result of both regulatory compliance and market differentiation motivators. The time, resources, and level of effort are totally dependent on the organization's information security program maturity. For example, some of the issues involved from my perspective as a certification preparer are:

Do I have to spend a lot of time in tutorial mode or is everybody a CISSP?

Will the organization dedicate a full-time person to shadow me and absorb knowledge transfer or will I spend a significant amount of time waiting for the client to respond?

"Experience has shown that a typical project will run from 6 to 12 months depending upon the answers to the questions above. I have run the gamut from a 2-week project to a 14-month project."

Many more U.S. organizations might pursue ISMS certification if they were more aware of the scope issues, the resources and effort involved, and the benefits for obtaining ISMS certification.

## **Five Things to Know**

Carlson provided the following five things he believes are most important for an organization to know when considering ISMS certification:

You can build a defensible information security program, based upon the concepts of ISO27001 and ISMS, without going the extra mile of obtaining certification.

Although ISO27001 certification requires an ISMS, an ISMS does not require ISO27001. An ISMS can be built around, or include, other standards such as COBIT.

Choose a scope that makes sense. Don't set yourself up for failure.

Realize that creating and certifying an ISMS is a process, not a product; your organization will be required to participate in the creation and maintenance.

Cross certification is the coming trend. There is wonderful synergy between ISO27001 (ISMS) and ISO9001 (TQM) as well as ISO20000 (ITIL).

---

## Benefits for Pursuing ISMS Certification

It is important to consider that the documentation created as a result of pursuing a formal ISMS certification will demonstrate due diligence to any regulators or outside auditors that are reviewing the adequacy of your organization's information security program. The CISOs I spoke with often indicated their regulatory requirements showed business value and the ISMS certification did not. Organizations need to realize that ISMS certification actually can be quite valuable in supporting regulatory compliance requirements.

I have performed many business partner information security reviews, and those who had already obtained ISMS certification not only saved themselves much time and effort when answering my questions but also saved me much time by having sufficient readily-available third-party validated documentation about their information security practices. ISMS certification can ease and facilitate business partner due diligence information security program reviews.

When an information security incident occurs, having ISMS certification will help demonstrate you took every possible precaution and had appropriate safeguards implemented to try to prevent the incident from occurring; it demonstrates your standard practice of due care as validated by an independent third party. The business value of ISMS certification will be clearer as organizations understand more completely what is involved with ISMS certification.

---

# Addressing the Risks of Outsourcing

*by Rebecca Herold, CISSP, CISM, CISA, FLMI*

Many organizations are outsourcing very specialized data processing and management activities in an effort to save money or because they simply don't have the resources, experience, or capabilities to do perform the tasks themselves.

-  According to a 2005 IDC report, the global market for outsourced IT services hit \$84.6 billion in 2004. IDC expects:
- The IT outsourcing market to grow 6 percent annually through the end of the decade, reaching \$112.5 billion in 2009.
  - The current \$33.8 billion U.S. market to grow at 4.2 percent.

Organizations also outsource to access specific expertise that they may not possess and cannot afford to hire full-time—trusting that the outsourced work will incorporate that expertise. For example, if you outsource application programming, you probably expect that the individuals doing this work know about application security and will incorporate it into the product they create for you. You probably also expect them to know how to protect information in a shared customer environment; making sure that the code they create for your organization is not accidentally sent to another customer.

Outsourcing is becoming commonplace, particularly with many top financial, health care, tax reporting, and credit reporting companies. Chances are there are people within your organization considering outsourcing some of your data processing activities.

## You Are Entrusting Another Entity to Protect Your Data

When you entrust business partners with your company's confidential data, you are placing all control of security measures for your organization's data completely into their hands. That trust cannot be blind. Many recent security incidents have resulted from inadequate security practices within outsourced organizations handling another company's customer or employee data.

When you outsource critical data processing and management activities, you must take action to stay in charge of your own business data security and minimize your business risks. You must know:

How the business partner is complying with your regulatory responsibilities.

How you can demonstrate to regulators that you are in compliance when someone else possesses your data.

You must hold your business partners to strict security standards. In many instances, the standards applied to business partners will be more stringent than your organization's internal security requirements.

---

## Ensure Your Business Partners Have Strong Security Programs

How you make sure your business partners are taking appropriate actions to protect the data with which you've entrusted them depends upon the situation and existing legal restrictions. The following list highlights general actions you should take:

Require a potential business partner to provide a copy of a recent security audit of their operations that was performed by an independent reputable party. Even if the audit is broad, it will demonstrate they have gone through an audit by a reputable company.

Require business partners to complete a security self-assessment questionnaire, provided by your company, about their information security and privacy program. When creating this questionnaire, structure the questionnaire around the ISO 17799 and OECD topics in addition to any specific regulatory requirements that are beyond these standards.

Include security and privacy requirements within the contracts you have with the business partners. Put in enough detail to cover all issues, but don't be so specific that you allow them a way to avoid doing a security activity just because you did not specifically state it within the contract. Include within the contract citations of the specific laws for which your company must comply so that the business partner understands they must also comply with such regulations.

Require business partner personnel to receive information security training for appropriate security practices prior to handling or accessing your company's information. Don't limit the training to electronic data; if they handle storage media, paper documents, speak to customers about their data, or access data in any other way, make sure it is covered in the training. Require regularly scheduled training and awareness to occur following the initial training.

Review the business partner's information security policies. Include this requirement in your contract with the business partner. Ensure the policies cover all the topics related to the activities the business partner performs for your company. Ensure the wording is strong enough to actually motivate the personnel for compliance. Look for executive endorsement of the policies and for clearly stated sanctions for policy violations.

Require an abbreviated form of the self-assessment, a type of information security and privacy attestation again provided by your company, that the business partner must complete each month or two, have their executives sign, and submit to your company as a requirement of continuing to do business. The signatures and contract language will help to demonstrate due diligence on the part of your company and will hold the business partner to a legal standard of due care.

---

For business partners handling particularly sensitive and/or regulated information, require a clean-room environment to keep information from walking out the business partner's door.



In a clean room environment, all the machines and output devices except for terminals are disabled. Copies of data cannot be made, hard drives cannot be used, mobile computing devices and desktop computers cannot download data from any of the computers, and data is otherwise not available for downloading, printing, copying, or accessing beyond the contracted purposes. The servers reside in your country of residence. There is no way for the information to leave the outsourced company.

Typically in such arrangements the outsourced company's employees are physically searched when entering and leaving. These are very strict precautions, so they will not work for every company, but they definitely should be used if your level of risk warrants such actions.

Limit the amount and types of information the business partner personnel can see and/or access based upon the business needs. For example, if the business partner contracted activity is to verify a customer is a good credit risk, don't send all parts of the application to the business partner; just send the information required to approve the application.

Require criminal and, where appropriate, financial checks to be performed on the business partner personnel prior to their hire. No matter how many security safeguards are in place, it's difficult to stop an opportunist who will steal data for money, revenge, or some other reason. Ensure that the people handling your data have not been convicted of criminal activity that would make them a high risk for handling your data. This verification might be tricky in some countries because records of criminal activity may not be centralized, such information may be labeled differently, and in some countries doing such checks are against privacy laws. As mentioned earlier, and worth emphasizing, make sure the business partner personnel are well trained about security procedures and legal consequences.

Make sure none of your disgruntled ex-employees are now employees of the business partner to which you are outsourcing your data handling. Such situations have had a devastating impact on companies.

Send personnel from your company to visit the business partner sites regularly, or at least occasionally, to view the facilities, meet employees, and monitor employee turnover and subcontracting activities.

---

## Common Business Partner Risks

The following list highlights several areas of recurring vulnerability that have appeared in past business partner security reviews:

The information provided within the business partner's security self-assessment responses might not match the security requirements within the business partner's security policies. For example, the respondent for the self-assessment may indicate the passwords used are a minimum of six characters, but the policy may indicate passwords must all be a minimum of eight alphanumeric characters. Such conflicting information should raise a red flag for you; it may indicate the business partner does not enforce compliance or communicate the security policy requirements to its personnel.

The business partner may be subcontracting the processing of your data to yet another company that does not have good security practices and/or may be located in a different country from yours or the business partner. Be sure to cover this within your contract with the business partner.

The business partner may not have any security policies or controls in place for mobile computing devices (laptops, PDAs, Blackberries, smart phones, and so on) or for their employees who work from home. However, they may have personnel who use these types of computers to process your data. Be sure appropriate security is in place for such situations.

Business continuity and disaster recovery plans are often either missing or were written several years ago and were never tested. Make sure the business partner has up-to-date plans in place and tests them regularly.

The business partner may not have any requirements to encrypt confidential data when transmitting through untrusted networks, such as the Internet. Be sure to require encryption as appropriate to how the business partner transmits your organization's data.

Encryption is often not used to protect information in storage, in transit, or on mobile computing media and devices, such as laptops, PDAs, backup tapes, USB drives, and so on. Be sure encryption is used by the vendor to mitigate the risk involved in such situations, including when the company is storing information from other companies on the same servers as they are saving your data.

The business partner may have been involved with a security or privacy breach. There are multiple services you can use to check on this, in addition to dozens to hundreds of good Web sites to search for news about the business partner and any published security breaches for which it was involved. If you find the business partner had a breach or incident, be sure to ask the company about it and find out what actions were taken to prevent such an event from occurring again.

---

The business partner may not have procedures in place to securely and irreversibly dispose of data when it is no longer needed or according to data retention requirements. Many business partners simply reformat hard drives or overwrite the drive once as part of their disposal practices. Business partners often also sell their retired computers to recoup their investment, but they do not remove the data from the hardware before doing so. Make sure your organization approves of the disposal procedures your business partner has in place.

The business partner may not have any security controls for sending backup media containing your organization's data to offsite storage and/or they may not have adequate security at the offsite storage site. Make sure your organization carefully reviews the business partner's practices for sending data storage media offsite.

## **Responsibility Follows the Data**

The bottom line is that outsourcing data handling, processing, and management is a risky proposition for your company. It is your responsibility to ensure strong security follows the data to your business partner. You must perform due diligence to ensure your business partners are protecting your data according to your security requirements. You are ultimately responsible for what happens to the data you've given to your business partners.


Be sure to discuss these issues with your organization's legal counsel and acquisitions areas. Modify business partner contracts and acquisition requirements according to what is best for your organization. Don't allow your organization's name to make the headlines because your business partners did not secure your data appropriately and subsequently experienced a security incident.

---

## Data Retention Compliance

by *Rebecca Herold, CISSP, CISM, CISA, FLMI*

Many laws and regulations exist throughout the world that require specific retention time periods and associated safeguards for a wide range of data types. Organizations need to be aware of these data retention requirements and plan to meet the compliance challenges.


 According to Network Appliance “Regulated Data—Headache or Opportunity?” (October/November 2003), more than 10,000 United States federal, state, and local laws and regulations address records retention requirements.

### Violations Have Significant Business Impact

Organizations that do not address data retention requirements face significant fines and penalties that can cripple business or even put an organization out of business. On December 3, 2002, the Securities and Exchange Commission (SEC), the New York Stock Exchange (NYSE), and NASD announced joint actions against Deutsche Bank Securities, Inc.; Goldman, Sachs & Co.; Morgan Stanley & Co., Incorporated; Salomon Smith Barney, Inc.; and U.S. Bancorp Piper Jaffray, Inc. for violations of recordkeeping requirements concerning email communications. The firms received fines totaling \$8.25 million (\$1.65 million each), along with a requirement to review their procedures to ensure compliance with recordkeeping statutes and rules. The regulatory agencies determined each of the five organizations:

- Violated Section 17(a) of the Securities Exchange Act of 1934, Rule 17a-4 under the Exchange Act, NYSE Rule 440 and NASD Rule 3110 by failing to preserve for a period of three years, and/or preserve in an accessible place for two years, electronic communications relating to the business of the firm, including interoffice memoranda and communications.
- Violated NYSE Rule 342 and NASD Rule 3010 by failing to establish, maintain, and enforce a supervisory system to assure compliance with NASD and NYSE rules and the federal securities laws relating to retention of electronic communications.

Organizations need to have a records retention and management plan, policy, and procedure in place to govern the security of the information they store, how long specific types of information must be retained, and how to securely and irreversibly dispose of the data when the retention periods have been met. In addition, they must know the data retention and management requirements within the laws and regulations applicable to their organizations.

 A useful resource to help with establishing data and records retention policies and practices is *BS ISO 15489-1:2001 Information and Documentation*, which provides guidance on managing records of originating organizations, public or private, for internal and external clients.

Organizations need to discuss data retention laws and regulation with their legal counsel to obtain an interpretation of the applicable requirements based upon their own unique enterprise circumstances.

---

## International Laws and Regulations

The following list highlights a sample of international laws and regulations (outside the United States) that specify data retention requirements.

1997 EU Directive on Privacy in Telecommunications:

- Article 6 requires traffic and billing data to be erased or made anonymous at the end of the period during which the bill may lawfully be challenged or payment may be pursued.

EU Data Protection Directive

- Personal data must be accurate and up to date.
- Organizations must not maintain data in a form that identifies specific individuals any longer than necessary for the purposes for which the information was collected or processed.

UK Anti-Terrorism, Crime and Security Act (ATCS) 2001

- Part 11 covers retention of communications data.
- Section 103 makes provision for a code of practice on data retention regulated under UK's RIPA part 1 chapter 2.

Canada Personal Information Protection and Electronic Documents Act (PIPEDA)

- Part 1 maps to the data-retention principle under the EU Data Protection Directive.
- Principle 4.5 requires personal information not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information must be retained only as long as necessary for the fulfillment of those purposes.

## United States Laws and Regulations

A sample of some U.S. laws and regulations with data retention requirements includes the following.

Sarbanes-Oxley Act of 2002:

- Fines and imprisonment of up to 20 years are proscribed for any person who corruptly alters, destroys, or conceals any records or documents to impair the use of them in any investigation.
- Failure to maintain audit/review work papers for at least 5 years can result in fines or imprisonment for up to 5 years.
- All audit and review information must be retained in a readily accessible and indelible format for 7 years.

---

Health Insurance Portability and Accountability Act (HIPAA):

- Covered entities (CEs) must not only ensure the security and appropriate access to health information while in transit through networks but also while the information is in storage.
- Such information must be maintained for 6 years from the date of its creation or 6 years from the date for which it was last in effect, whichever is later.
- Penalties include not only civil, but also potentially large fines and/or prison time.

Gramm–Leach–Bliley Act (GLBA):

- Financial organizations with customers and consumers who are United States citizens must implement security programs governing the security and retention of non-public personal information (NPPI).

21 CFR Part 11 (Electronic Records; Electronic Signatures):

- Requires all FDA-regulated program areas to follow technical and procedural standards for the processing, storage, security, and retention of electronic records and electronic signatures.
- Noncompliance can result in a range of FDA actions, including publicly available statements to closing the organization.

USA PATRIOT Act:

- Requires trades and businesses to record and report cash transactions of more than \$10,000 (or two or more related transactions involving more than \$10,000) and certain transactions involving monetary instruments to Treasury’s Financial Crimes Enforcement Network (FinCEN).
- Requires that a program be established to prevent money laundering through the use of policies, procedures, and internal access and security controls. Included in the requirements are specifications for recordkeeping, reporting, verifying customer identification, and responding to law-enforcement requests.
- Money services businesses that have computerized data processing systems must integrate into their systems compliance procedures, such as recordkeeping and monitoring transactions, subject to reporting requirements.

FDA Good Manufacturing Standards:

- Requires retaining all appropriate critical documents, such as development history reports, scale-up reports, technical transfer reports, process validation reports, training records, production records, control records, and distribution records.
- The retention periods for these documents must be specified within the procedures.
- All production, control, and distribution records must be retained for at least 1 year after the expiry date of the corresponding batch.
- For APIs with retest dates, records must be retained for at least 3 years after the batch is completely distributed.

---

21 CFR 58.195: Food and Drug Administration (FDA) Good Laboratory Practice:

- In general, documentation records, raw data, and specimens pertaining to a non-clinical laboratory study and required to be made by this part must be retained in the archive(s) for whichever of the following periods is shortest:
  - At least 2 years following the date on which an application for a research or marketing permit, in support of which the results of the non-clinical laboratory study were submitted, is approved by the FDA. This does not apply to studies supporting investigational new drug (IND) applications or applications for investigational device exemptions (IDEs), records of which are governed by the provisions of paragraph (b)(2) of this section.
  - At least 5 years following the date on which the results of the non-clinical laboratory study are submitted to the FDA in support of an application for a research or marketing permit.
- In other situations (such as where the non-clinical laboratory study does not result in the submission of the study in support of an application for a research or marketing permit), a period of at least 2 years following the date on which the study is completed, terminated, or discontinued.

Securities Exchange Act Rules 17a-3 and 17a-4:

- Certain records must be preserved for either 3 or 6 years, depending on the particular record.

Commodity Futures Trading Commission (CFTC): 17 CFR Part 1 Regulation 31.1:

- Requires all books and records required to be kept by a Futures Commission Merchant (FCM) for a period of 5 years from the date thereof, and that the required books and records be stored on micrographic or electronic storage media unless the documents are trading cards or other documents on which trade information is originally recorded in writing.
- Organizations in the futures and commodities industry that do not have automated recordkeeping must:
  - Show that recordkeeping meets pertinent regulatory requirements before converting it to electronic records.
  - Create a duplicate of both required records and an index of those records, and maintain the duplicate at a separate location.
  - Have an auditable system for transferring records to electronic media.
  - Ensure the commission has the information needed to access electronic records.
  - Provide an independent source for downloading records that are kept solely on electronic media.

---

Federal Energy Regulatory Commission (FERC): Part 125:

- Specifies regulations regarding protection from fire, floods, and other hazards and in the selection of storage space.
- Safeguard the records from unnecessary exposure to deterioration from various specified conditions.
- Software and hardware that is required for the retrieval of stored data must be maintained for the retention periods specified in Section 125.3—Retention Periods; examples include:
  - Annual reports—5 years
  - Meeting minutes related to stockholders—5 years (with conditions)
  - Titles, franchises, licenses—6 years (with conditions)
  - Procurement agreements—6 years
  - General accounting ledgers—10years
  - Plant ledgers—25 years
- This ruling applies to all forms of records, including unstructured forms, such as email.

Department of Energy (DOE) 10 CFR 600.153: Retention and Access Requirements for Records:

- Financial records, supporting documents, statistical records, and all other records pertinent to an award must generally be retained for a period of 3 years from the date of submission of the final expenditure report or, for awards that are renewed quarterly or annually, from the date of the submission of the quarterly or annual financial report, as authorized by the DOE.

Internal Revenue Code Title 26:

- Carries a penalty of up to \$500,000 and 3 years in prison for destroying records.
- Records must be retained based on the type of organization; in general, keeping records for at least 7 years to address this code is considered a good business practice.

---

Internal Revenue Service (IRS): Rev Proc 97-22:

- Part 03 Section 1.6001-1 (e) states “...the books or records required by Section 6001 must be kept available at all times for inspection by authorized Internal Revenue Service officers or employees, and must be retained so long as the contents thereof may become material in the administration of any internal revenue law.”
- The electronic storage system used must meet the following requirements:
  - Ensure the integrity, accuracy, and reliability of information stored
  - Prevent any type of alteration to the records as well as deletion or deterioration of stored electronic records

Americans with Disabilities Act (ADA):

- Information about persons whose employment was involuntarily terminated must be kept for at least 1 year from the date of the termination.

Age Discrimination in Employment Act:

- Any information containing advertisements or public notices for open job positions must be kept for 1 year from the date of personnel action.

Employee Retirement Income Security Act of 1974:

- Any email, notes, or other correspondence related to employee benefit plans must be kept indefinitely.

Occupational Safety and Health Act (OSHA):

- All documents that include information about monitoring employee exposure to hazardous substances must be retained for 30 years.

Toxic Substances Control Act:

- Documentation of any employee’s allegation of ill health effects or occupational injury must be retained for 30 years.

Mammography Quality Standards Act of 1992 (MQSA):

- Medical records related to actual original mammograms (films) and mammography reports must be maintained for:
  - A period of not less than 5 years, or
  - Not less than 10 years if no additional mammograms of the patient are performed at the facility, or
  - Longer if mandated by state or local law, or
  - Until a request is made by or on behalf of the patient, that her records be permanently or temporarily transferred to a medical institution, her physician or healthcare provider, or to the patient herself.

---

U.S. Code Title 44 (Paperwork Reduction Act):

- Some documents may never be destroyed; for example:
  - Certain presidential and presidential-related materials
  - Items as identified by the National Archivist
  - Agreements between states
- In general, federal computer systems must maintain travel-related records for 6 years, or until audit, whichever is sooner, then destroyed.
- For the Department of Labor, printed investigation forms generated by the WHISARD system must be retained in the investigative files of Wage and Hour District Offices. Database information must be captured on tape at the end of each fiscal year and retained for 25 years. The U.S. Forestry Service retains records indefinitely.

Social Security Administration (SSA) Records Retention:

- All SSA financial records and supporting documents must be retained for a period of 3 years as follows:
  - Financial records and supporting documents must be retained until resolution of federal audit findings and cost effectiveness measurement system (CEMS) compliance review findings.
  - Non-expendable property records must be retained until 3 years after the final disposition of the item.
  - Statistical records and records that pertain to the processing of disability claims must be retained for the length of time specified in accordance with the Department of Archival Records Administration schedule.

NASD Rule 3110:

- Securities firms must retain all correspondence of their representatives that are part of its securities or investment banking business. This rule spells out the requirements for maintaining recordkeeping, record formats, storage mediums, and records retention periods that comply with and support SEC Rule 17a-4.
- Affected firms must accomplish all of the following to be in compliance:
  - Thoroughly document and enforce records retention policies
  - Store data on indelible, non-rewriteable, and non-erasable media
  - Make a search/reference index available for of all stored data
  - Make data readily retrievable and viewable
  - Store data off-site

---

NASD 3010 (3) Retention of Correspondence:

- Each member must retain correspondence of registered representatives relating to its investment banking or securities business in accordance with Rule 3110.
- The names of the persons who prepared outgoing correspondence and who reviewed the correspondence must be ascertainable from the retained records and the retained records must be readily available to the Association, upon request.

New York Stock Exchange (NYSE) Rule 440:

- Broker and dealer firms must properly manage, search, and retain emails relating to the business while controlling the costs resulting from managing emails.

National Archives and Records Administration (NARA): Part 1234 and GA Schedule 24

- There are many retention and storage requirements found within the following sections:
  - Section 1234.22—Creation and Use of Text Documents
  - Section 1234.30—Selection and Maintenance of Electronic Records Storage Media
  - Section 1234.32—Retention and Disposition of Electronic Records
  - Section 6—User Identification, Profiles, Authorizations, and Password Files
  - Section 11—IT Infrastructure Design and Implementation Files

Department of Defense: DoD 5015.2:

- Section C2.2.9—Systems Management Requirement has several retention requirements within the regulation requiring:
  - Backup of Stored Records (C2.2.9.1)
  - Storage of Backup Copies (C2.2.9.2)
  - Rebuild Capability (C2.2.9.4)
  - Storage Availability and Monitoring (C2.2.9.5)
  - External Email Management and Retention (C2.2.10.2)

---

# How Encryption Supports Compliance

*by Rebecca Herold, CISSP, CISM, CISA, FLMI*

Encryption is an underutilized security tool. Facing the infinite number of today's risks, threats, and vulnerabilities, encryption can effectively keep unauthorized individuals and systems from accessing sensitive information and thwart many types of attacks. In today's business environment—with sensitive information being stored in multiple locations, many of them mobile—encrypting information is an effective privacy safeguard organizations can add to their arsenal of protection tools.

According to the December 2005 Congressional Research Service (CRS) report from the United States Library of Congress, in 2005, a stolen computer (desktop, laptop, or hard drive) was the cause of a security breach 20 percent of the time. If the information on these devices had been strongly encrypted, the theft would not have been thwarted, but information compromise could have been prevented if someone who did not have the decryption key stole the device.

Consider the growing numbers of electronic storage media and computing devices that are being retired from business use:

According to Gartner, United States homes and businesses combined discard 133,000 PCs each day.

The United States Environmental Protection Agency (EPA) reports that U.S. residents throw away 2 million tons of tech trash each year.

How many of these devices still have sensitive information stored on them when they are discarded? How many organizations remove the data from retired computing devices before trying to recoup some investment by auctioning or donating to charities? Does your organization completely remove sensitive information from retired computing devices?

Careless disposal of confidential information is posing greater problems for individuals and businesses and can result in identify theft, fraud, and legal noncompliance. Increasing numbers of laws and regulations require businesses to follow a standard of due care to protect personal information from unauthorized exposure. Such incidents involving stolen, lost, or purposefully sold storage media containing clear-text data is easily preventable through the use of encryption.

## Safeguard for the Unknown

No organization can completely defend against all threats. The number of potential risks and threats is infinite—new ones emerge every day, and many (if not most) are unknown or unanticipated. The incidents resulting from unknowns are typically the events that wreak the most havoc on organizations.

Organizations must implement appropriate safeguards to protect against threats and demonstrate due diligence. One of the best ways to protect information—particularly personally identifiable information that is covered by multiple laws and regulations—from unknowns is to make the information incomprehensible and unusable to unauthorized individuals by encrypting it. Organizations must expect that one of those infinitely unknown threats will result in an incident sooner or later. Strongly encrypting sensitive data will significantly lessen, and possibly eliminate, the negative business impact when a security incident happens.

---

## The Need for Encryption

The porous network perimeter; the growing number of mobile, small, and huge-capacity storage device types; and the numerous ways that data can be sent within milliseconds to multiple locations throughout the world has generated an increasing need to protect information by using encryption. Organizations replace computing hardware more frequently than ever because of how quickly technology is evolving; they subsequently resell the retired equipment in an effort to get some return on their investment. Contributing to these compelling technology factors is the exponentially increasing number of regulatory requirements that necessitate that organizations implement safeguards to protect data more effectively than has been demonstrated in the past.

It seems incidents involving personal information are reported almost every day. Just a few of the many reported incidents that have occurred recently include:

Reported March 4, 2006 in the Vancouver Sun—In mid-2005, the government of British Columbia sold 41 high-capacity data tapes containing clear-text personal information, including sensitive health information and medical notes about at least 65,000 individuals, for \$300 at auction.

Reported March 2, 2006 on CBS4 Denver—A Metropolitan State College of Denver laptop containing the clear-text names and Social Security numbers of 93,000 current and former students was stolen in late February from the home of an employee authorized to take the computer home.

Reported February 24, 2006 by the IDG News Service—On December 15, 2005, a Deloitte and Touche auditor left a backup CD on a plane. The CD contained clear-text names, Social Security numbers, and information about stock holdings held by more than 9000 of McAfee's current and former employees.

Reported December 25, 2005 in Iowa's Des Moines Register—Three-thousand Iowa State University (ISU) employees may have had their personal data viewed by hackers who gained access to two computers earlier in December. One computer held about 2500 encrypted credit card numbers of athletic department donors. The second computer contained clear-text Social Security numbers for more than 3000 ISU employees. The intruder could not read the credit card numbers because they were encrypted; however, the Social Security numbers are at risk of being inappropriately used.



Although encryption will not protect data from all kinds of incidents, such as when authorized insiders abuse or misuse their privileges, it does provide effective protection by ensuring only authorized users with valid decryption credentials can see the data.

Encryption keeps inappropriate viewing and use from occurring when data is lost, stolen, sold, or otherwise compromised. Just consider the June 2005 Citigroup incident in which a backup tape containing information about 3.9 million individuals was lost by UPS while in transit. If the information had been encrypted, the incident would have had much less, possibly negligible, negative business impact to Citigroup and would have presented significantly less risk to the individuals whose information was on the tape.

---

## Encryption Is Not Yet Widely Used

Unfortunately, many organizations still think current encryption solutions are too complex to realistically implement enterprise-wide or have too much negative impact on application and network response times. In August 2005, Forrester Research reported that only 16 percent of North American companies implement data-at-rest (storage) encryption for their databases, and only 48 percent implement data-in-motion (network) encryption to support critical applications. It will be interesting to see how encryption practices change throughout 2006.

Encryption solutions have advanced greatly in recent years. They are now easier to use, easier to implement, are more transparent to the end users, and are comparatively more economical than past encryption solutions.

## Legal Implications for Encryption

Organizations, typically at the direction of their legal counsel, will often only implement safeguards such as encryption if explicitly required by the law. For example, in the December 2005 ISU privacy breach, the fact that credit card numbers were encrypted on one system and the Social Security numbers were not encrypted on another system strongly implies that the organization was doing only what was required by the “letter of the law” or the “letter of the contract” rather than implementing a wider interpretation of what is right according to the spirit of the law or performing due care activities to protect sensitive information. Although this theory has not been verified, it is likely that the strict and specific requirements from credit card companies to encrypt credit card numbers while in storage—and the lack of similar explicit regulatory requirements to encrypt Social Security numbers while in storage—resulted in this inconsistent application of encryption.

Many organizations make it a matter of business practice to do only the minimum required with regard to safeguard implementations, including encryption, unless explicitly, contractually, or legally required to do otherwise. However, organizations should consider the impact of encrypting data in the event an incident does occur. Many current United States state breach notification laws, such as California’s SB1386, do not require organizations to report incidents involving personal information if the data was encrypted. The United States Federal Trade Commission (FTC) has indicated in many of their decisions that a lack of encryption to safeguard data violated regulations or contributed to an unfair and deceptive business practice. For example, in September 2005, the FTC determined Superior Mortgage Company violated the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule because, among other actions, it “did not encrypt or otherwise protect sensitive customer information before sending it by email.”




An excerpt from the FTC’s published Fair Information Practice Principles recognizes the value of encryption as a strong safeguard:

*Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem.*

---

Encryption is one of the most effective security tools available to protect the confidentiality of and access to sensitive data. New encryption solutions have made encryption easier to use and manage as well as more economical than ever before.

 Encryption is specifically stated in several laws—including the Health Insurance Portability and Accountability Act (HIPAA), GLBA, and California SB 1386—as a safeguard organizations must consider.

## Encryption Demonstrates Due Diligence

Even Iron Mountain, a company that lost backup tapes containing clear-text information about millions of people for at least four of their customers during the first 4 months of 2005, recommended in an April 22, 2005 report on internetnews.com that organizations should encrypt information on backup tapes. Data should also be encrypted on mobile computing devices as well as on other devices and systems as determined by risk. Encryption is an effective security practice that demonstrates due diligence as well as goodwill for the individuals' personal information.

Organizations need to take a second look at using encryption to protect sensitive data at rest and in motion; particularly if the organization handles confidential information and/or is covered by one or more data protection laws. Remember, when information is unreadable by the unauthorized, breaches from the unauthorized can be avoided.

---

# Do Compliance Requirements Help or Hurt Information Security?

*by Rebecca Herold, CISSP, CISM, CISA, FLMI*

Once upon a time, before there were any regulatory requirements for protecting information (well, at least very few), information security professionals often lamented, “Oh, if only laws would require information security then we wouldn’t beat our heads against the wall trying to secure our networks and systems!” Fast forward to today—now you commonly hear some of these same practitioners moaning, “Oh, there are just too many laws and too many different data protection requirements to feasibly comply with!”

I discussed this issue with seven seasoned information security and privacy professionals to get their opinions about whether regulatory compliance requirements help or hurt information security initiatives. They were wholly in agreement that compliance can help or hurt information security and associated initiatives depending upon the culture of the organization. Key points from each of them are included in the following discussions of how compliance helps and hurts information security.

Our discussion panel includes:

Dr. Peter Stephenson, Associate Director, Norwich University Master of Science in Information Assurance Program

Mike Corby, Sr. Director, Gartner Consulting

Peter Wenham, Director, Trusted Management Ltd. Information Assurance (IA) Consultants

Dr. Gary Hinson, CEO, IsecT Ltd. and [www.NoticeBored.com](http://www.NoticeBored.com)

Pam Poucher, Manager, Business Intelligence & Privacy, Cox Enterprises

Kevin Beaver, Owner, Principle Logic, LLC

Barry Jones, Principal Consultant, Tribridge, Inc.


---

## Compliance Requirements Help Information Security Efforts By...


### ***Legally requiring long-held information security standards and practices***

Some regulations requiring information safeguards reference the need to use what are considered industry-leading best practices. For instance, within Section III Analysis of, and Responses to, Public Comments on the Proposed Rule of the Health Insurance Portability and Accountability Act (HIPAA) regulatory text, it is recommended that those implementing the controls should:

*“...see NIST Special Publication 800–14, Generally Accepted Principles and Practices for Securing Information Technology Systems and NIST Special Publication 800–33, Underlying Technical Models for Information Technology Security.”*


 Jones: “Most of these standards are the same principles and practices that security professionals have been advancing since the birth of the profession. And most of these principles and practices have been either roundly dismissed or generally lip-serviced by organizations until now.”

Not only have the use of existing information assurance standards been referenced, but the various standards themselves—now held up as examples of how to appropriately safeguard information—have also been updated and improved upon. For example, ISO 17799:2000 was updated and made more applicable to today’s more challenging technology and business environments with the release of ISO 17799:2005 in June of 2005.


 Hinson: “One reason legal and regulatory compliance pressures mostly help is because they have undeniably forced improvements in governance standards.”

### ***Increasing management awareness of security and how management handles business risks***

When laws and regulations make business leaders personally accountable for implementing information safeguards, business leaders become concerned.


 Jones: “Mandates are providing management awareness, support, and budgets the likes of which we InfoSec professionals haven’t seen in our entire careers.”

The CIO Magazine—PriceWaterhouseCoopers “Global State of Information Security 2005” report indicates information security budgets will increase by 47 percent in all industries, and by 57 percent specifically in the highly regulated financial industry in 2006.


 Hinson: “Another reason legal and regulatory compliance pressures mostly help is because they are well publicized and force managers to read-up on governance-related topics.”

Sixty-seven percent of the Deloitte 2005 “Global Security Survey” respondents indicate regulatory requirements are “effective” to “very effective” for improving the information security program and reducing information risks.


---

 Corby: “If the compliance needs result in raising the awareness of security as an opportunity to manage several risks that are the thrust of the compliance issue, then security has the opportunity to move on to the next step; as a player with the opportunity to establish good governance and provide strategies for mitigating the risk of non-compliance.”


Sixty-one percent of the respondents to the Ernst & Young “Global Information Security Survey 2005” indicate regulatory compliance requirements have had the most significant impact to the information security practices within organizations.

 Stephenson: “Generally compliance requirements have forced executive management to pay attention to information security.”


### ***Forcing information security issues to be addressed that otherwise would not***

 Beaver: “Most business managers and executives haven't and, for the most part still don't, understand information risks. So, if the HIPAAs, GLBAs, and California Senate Bill 1386s of the world are what it takes to force people to keep private and confidential information private and confidential, then we're still better off in the long run.”

Most information security practitioners agree that if it were not for regulatory requirements, executives would not support or address information security risks and issues because information security costs have always been viewed as a discretionary cost to business and a drain to the bottom-line budget.


 Hinson: “Legal and regulatory compliance pressures also help because they force senior management to take their governance obligations seriously (they carry the weight of law).”

Executives now see, as Enron and Tyco executives are led to jail in handcuffs, that regulatory requirements should be taken seriously. Such images have great impact on the motivation of executives to comply with laws to avoid being the next top story on the nightly news.

 Wenham: “People do 'security' for one of two reasons: they have been 'had' (that is, been broken into, had stuff stolen, had a hacker in who messed up the Web site, had a disgruntled employee interfere with things, and so on) or they have to (that is, the law, compulsory legislation, or some other external factor means they have no choice).”


---

## ***Increasing public awareness of information security and privacy issues—the public then demands that businesses address the problems***


 Beaver: “I do believe these laws and regulations have brought more visibility to the privacy and security problems we have.”

According to Privacy Rights Clearinghouse, more than 53 million individuals within the United States have had their personal information put at risk as a result of a data breach in at least 106 publicized personal information breach incidents in 2005. These breaches were reported largely, and perhaps only, because of state-level regulations requiring notification. The public is reading and hearing about these incidents daily. Public awareness of information security and privacy issues has certainly been raised.


## ***Providing a solid new, or improved, foundation for information security within organizations that previously had no, or insufficient, information security programs***

 Poucher: “Compliance requirements can help an organization by providing a framework, a starting point so to speak, to work within to assist in identifying your risks and vulnerabilities.”

Many regulations very clearly define the types of information security and privacy safeguards that must be implemented by covered organizations. For example, both the Gramm-Leach-Bliley Act (GLBA) and HIPAA clearly outline the technical, administrative, and operational safeguards those organizations must formally implement. The implementation of these requirements then form the basis for the information security program at many organizations where, up until the regulations went into effect, information security may have just been a function given to a network administrator to help stem the tide of incoming malicious code—or even a non-existent formal business responsibility.

 Hinson: “Legal and regulatory compliance pressures help because they apply a common standard quite rigorously through the efforts of a small army of professional compliance officers, auditors, accountants, lawyers, and, of course, information security managers.”


Because of the preponderance of operational, policy, and training requirements, the regulations force information security and privacy professionals to work more closely with the rest of the business; they have to or they will not be in compliance with these personnel and business process directives.

 Corby: “Compliance offers the opportunity to measure, improve, and re-measure. Compliance is not an event, it is a process by which certain expectations are met, and then new expectations can be set and achieved.”

Data protection regulations overwhelmingly require organizations to measure risk, provide education, and monitor for threat on an ongoing basis. These actions must be documented to demonstrate compliance. For organizations that never performed these activities before, regulatory requirements are helping them realize their true information security postures and adjust accordingly to better protect their information assets.


---

### ***Clearly reducing subjectivity of interpretation of specific safeguard requirements when the regulations are written well***

 Hinson: “Well-written legal and regulatory compliance pressures help because they are written in formal language designed to reduce ambiguity.”


Although portions of regulations can be a bit wishy-washy and subject to a wide range of sometimes creative interpretation, they can also clearly specify compliance requirements. For example, the HIPAA directive to “Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored” and the accompanying regulatory implementation discussion makes it clear that covered entities must create a formal disposal process with appropriate tools and technologies to completely destroy and dispose of information that is no longer needed.

### ***Moving information security higher up in importance and in the organization chart***

 Hinson: “Legal and regulatory compliance pressures help information security professionals because they have increased salaries in related professions!”

More executives are paying attention to information security compliance requirements and putting information security functions at a higher role within the organization. As the PWC “Global State of Information Security 2005” finds, companies with the security function at the executive level have budgets and information security policies that are more aligned and ingrained with business, and a higher percentage of personnel comply with information security requirements and policies than in organizations in which the information security function is not at the executive level. Information security professionals may very well be moving up in the organizational chart; the SANS Institute’s 2005 Information Security Salary and Career Advancement study found that salaries for corporate security positions rose an average of 5.5 percent from 2003 to 2005.

### ***Requiring organizations to implement controls that are able to track activities for personal and sensitive information***

 Wenham: “Regulatory and legal compliance is now starting to put the emphasis on identifying who did what and when to 'information;' this, in turn, will lead to improvements in access control to 'information,' which, in turn, will mean improved audit logs and thus lead to vastly improved 'who did what and when' data, which feeds neatly into regulatory compliance and reporting.”

Regulations such as GLBA, HIPAA, SOX, and the European Union Data Protection Directive clearly require covered organizations to log and be able to track activities to sensitive and personal information. For example, HIPAA requires covered entities to, “Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.”


---

## Compliance Requirements Hurt Information Security Efforts By...


All is not wine and roses with regard to regulatory compliance helping information security. We need to remove our rose-colored glasses and look at the ways in which compliance requirements can also hurt information security efforts.

### ***Confusing companies with multiple conflicting requirements***


Many of the laws at the state, federal, and international levels contain requirements that sometimes conflict with other regulations. This conflict causes confusion, interpretation conflict, and challenges for the business leaders responsible for compliance, often resulting in implementation of safeguards only in areas in which organizations think regulators will check.

 Jones: “However much we may applaud the recent groundswell of state legislation following the example of California’s SB 1386, we are seeing an emerging patchwork-quilt of laws that differ enough between each other to become a new headache for us all.”


Trying to figure out preemption situations and mapping all the related requirements to the related applicable regulations within an organization can lead to extremes of actions; either the company will implement all the most stringent requirements across the board, regardless of any exemptions that may exist or the organization will throw in the towel and decide that doing nothing is the best course of action—they can always plead ignorance in the event of a noncompliance investigation.

 Stephenson: “Some companies do not know whether they have to comply with regulations. Some will assume the worst case and will do what they think they should to meet compliance, others will do nothing and hope they don’t get caught.”

### ***Establishing many requirements that are not feasible within most organizations***


 Jones: “Because legislative action all too often is forced by reaction to dire circumstances and the outcry of constituents, it all too often is not only reactive but over-reactive. Being over-reactive is the root of all kinds of ills, including requirements that strain at gnats but swallow elephants, focus on the branches but not the roots of the problems, breed new bureaucracies to enforce, and become so onerous that in the end, companies will seek to put forth the minimum to get by rather than embrace the spirit of the law.”

Some organizations simply do not have the means or resources to implement some regulatory requirements. For example, many small to mid-sized healthcare provider environments simply do not have the staff, experience, or budget to implement all the HIPAA Privacy Rule and Security Rule requirements.

 Beaver: “I have a problem with career politicians and their advisors writing legislation on subjects they know nothing about.”

---


## ***Being inadequate or leaving gaping loopholes, ultimately not improving security at all***

 Jones: "The legislative process typically involves compromises that have much more to do with expediency than with sound principles of information security."


Unfortunately, many regulations are written in ways that do not really require actions to fulfill the purpose of the law, or they leave significant loopholes and exemptions so that data protection really isn't improved as a result of the passage of the law. Many of the United States' state-level breach notifications laws contain huge exemptions for large percentages of organizations that handle millions of records containing personal information. For example, the Georgia S.B. 230 breach notification law only applies to "information brokers." And, without any penalties for noncompliance, it has no teeth to motivate the comparatively few covered organizations to comply.

### ***Taking resources from more critical initiatives***


Many organizations have found that the costs of implementing regulatory requirements for one law take away resources from other, possibly more critical, information security initiatives.

 Poucher: "There are additional costs and infrastructure to manage such as a compliance program that places a burden on an organization and can be an impediment to other projects."

I spoke with several chief information security officers (CISOs) throughout 2005 who were exasperated that significant portions of their already approved information security budget were diverted to the Sarbanes-Oxley Act (SOX) compliance efforts, leaving them with no money to implement their planned intrusion detection systems, hire more staff to handle the overwhelming amount of information security work required by other regulations, or to implement encryption on their mobile computing devices.

 Hinson: "The cost of compliance tends to diminish resources available for discretionary projects, and can be a significant cost for businesses already under pressure from tight margins."


### ***Resulting in compliance efforts that are more costly than self-regulation***

 Hinson: "Legal and regulatory compliance are more costly than self-regulation."


According to a study released September 19, 2005 by the Office of Advocacy of the United States Small Business Administration, organizations with fewer than 20 employees spend \$7647 per employee each year to comply with federal regulations, and organizations with more than 500 employees spend \$5282 per employee annually. The report also indicated that the annual cost of federal regulations compliance in the United States totaled \$1.1 trillion in 2004.

---


## ***Scapegoating compliance to implement security solutions***

 Hinson: “Legal and regulatory compliance requirements are sometimes abused to justify unnecessary or ill-conceived controls.”

I have heard many business leaders complaining, and vendors gloating, that now information security practitioners are using regulations to justify buying cool technologies that they previously could not get because, before compliance requirements, they could never convince the budget approvers of the business benefit of the requested purchase or show how it would improve security.

 Corby: “If the senior executive discovers that the security people are descending upon the CxO or board member with a host of warnings, cautions, crises, and other concerns, the security program can be dealt a severe blow. The one solid chance to become part of the strategic fabric will have been wasted, most likely forever, and certainly within the career tenure of the security director. A frequent occupational hazard is to promote security to the maximum extent it can be delivered. It can be difficult for someone immersed in the issues of security to remind themselves that security only needs to be good enough to mitigate risk to a certain point, but to do it well. Being 100 percent secure is unattainable, but being 100 percent certain of success at the 80 percent level is within reason. Compliance, as I read it, does not call for perfection across the board.”


## ***Creating management duress and ultimately creating the view of information security as a business cost not a business enabler***

 Hinson: “Legal and regulatory compliance requirements are complied-with 'under sufferance,' meaning begrudgingly, therefore increasing the general resentment, ill-feeling, and negativism towards information security as a cost rather than a source of business benefit.”

There have been dozens, perhaps hundreds or even thousands, of articles bemoaning information security as a huge cost to business. Many fewer articles discuss or demonstrate how information security can be a business enabler when done correctly.


## ***Generating high-priced compliance “solutions”***

The rise in numbers of compliance requirements generates new compliance snake-oil solutions and outrageous billing rates that damage the valid information security efforts.

 Hinson: “The small army of professional advisors is seen to be milking their clients of \$\$\$, thereby discrediting consultancy and other professional services.”


---

Fear of jailtime and personal monetary penalties drove huge corporate spending for SOX compliance efforts in 2005. Many vendors placed a “SOX Compliance” label on their products and services and bumped up the price to take advantage of this fear. I have heard many marketers within various information security vendor companies not only encouraging, but also threatening with potential job loss, their consultants and representatives to push the products and services by creating fear, uncertainty, and doubt (the FUD factor) within customers.


 Wenham: “One problem that the industry has is that, within the UK, people/companies are claiming to be InfoSec consultants/suppliers when all they have done is harden OSs, sell/install boxes, set up users and profiles, done some vulnerability assessments (and often sold such assessments as pen tests!!!).”

### ***Interpreting requirements in the most convenient way***


Many poorly written regulations result in organizations interpreting them to their own liking, twisting the intended requirements to what is most convenient for them and not addressing the spirit of the law.

 Hinson: “Despite the formal language, there are differences of opinion about their applicability and details, and some organizations are probably intent on 'gaming' (that is, deliberately interpreting or bending the rules).”

I have spoken with several lawyers from many different industries about how they view the implementation of information safeguards to meet regulatory requirements, and many indicate that if the regulations do not explicitly state they have to do something, such as encrypt personal information within email messages, they will not support the purchase or implementation of such solutions or processes.

 Stephenson: “There is a danger that some organizations do not do what they need to do, just what they can get away with for the cheapest cost and for the minimum requirements.”

### ***Not addressing important risks outside the compliance requirements***


 Hinson: “They may increase the risk of failing to address important areas just outside their scope.”

Organizations are focusing so intently on the specific regulatory requirements that important security risks often are not addressed. For example, information security practitioners have told me that they cannot get resources approved to secure the growing numbers of wireless technologies proliferating throughout their organizations because the entire information security budget has been earmarked to support compliance requirements, and no regulations specifically mention anything about wireless computing devices. Even though they fall under the umbrella of network security, business leaders often do not understand this.

---

## **Slapping on solutions not supporting business**


Many organizations are applying information security solutions in an effort only to meet compliance and without regard to the business.

 Wenham: “The understanding of a business, the information that it contains, and the associated business risks are often missing or paid lip service to. This is one of the reasons, I believe, that spending on 'security' has gone up but that the incident rate has not fallen. Quite the reverse, the incident rate has increased far more than spending (because the money has probably been spent on the wrong things or the priority of spending is wrong).”


When information security tools and processes are applied without any regard to the enterprise infrastructure or business mission and goals, it is likely they will be ineffective. Effective information security is applied based upon risk. Many information security initiatives are based upon fear of fines, negative publicity, and jail time. This reality was demonstrated numerous times by the information security spending for SOX compliance; SOX does not require information security to be implemented based upon analyzing the business risks, so SOX-labeled solutions were widely purchased and deployed without first analyzing risks. These organizations will find how effective those solutions really are.

## **So, The Answer Is “Yes!”**

So the answer to the question “Do compliance requirements help or hurt information security?” is “YES!” The side of the fence where the information security grass is greener, before compliance requirements or with compliance requirements, all depends upon your organization and your information security actions.

 Stephenson: “Take HIPAA as an example. Some companies truly did the right thing; had an outside independent in-depth review of their network and operations, remediated the noncompliance areas, then had another independent review to ensure they were then indeed in compliance. Other companies just did nothing because of the resources it would take, and now they hope they will not get caught.”

Organizations must look at the vast array of regulations that apply to them, create a comprehensive compliance plan, and implement it according to the risks within their own, unique business environment, and not based upon a slick high-dollar marketing campaign that catches their attention.

 Corby: “Success is measured in small steps, with new successes just over the horizon. Defining those small steps; achieving success, and setting out for the next milestone is critical in developing a compliance program that becomes a permanent part of the organization, not just a 3- or 6-month project that goes away.”

It is ultimately up to each organization how they implement information security activities and requirements throughout the enterprise. Their success or failure will be the key indicator for whether their response to regulatory compliance ultimately hurts or helps their information security efforts.


<b>Compliance Requirements Help Information Security By...</b>	<b>Compliance Requirements Hurt Information Security By...</b>
Legally requiring long-held information security standards and practices.	Causing confusion, conflict, and challenges for complying with multiple inconsistent laws, and leading to security implementation only where organizations think regulators will check.
Increasing management awareness of security and how business risks are managed.	Establishing many requirements that are not feasible within many organizations.
Forcing management to address information security issues that they would not otherwise.	Being inadequate or leaving gaping loopholes, ultimately not improving security at all.
Increasing public awareness of information security and privacy issues; the public then demands that businesses address the problems.	Requiring compliance costs that take away resources from other, possibly more critical, information security initiatives.
Providing a solid new or improved foundation for information security within organizations that previously had no or insufficient information security programs.	Resulting in compliance efforts that are more costly than self-regulation.
Clearly reducing subjectivity of interpretation of specific safeguard requirements when the regulations are written well.	Using compliance to justify unnecessary or poor information security solutions.
Moving information security higher up in importance and higher up in the organizational chart.	Creating management duress and ultimately creating the view of information security as a business cost not a business enabler.
Requiring organizations to implement controls that are able to track activities for personal and sensitive information.	Generating many compliance snake-oil solutions and outrageous billing rates that damage the information security reputation.
	Enabling subjective interpretation of poorly written regulations that allows organizations to bend the requirements to what is most convenient for them and not addressing the spirit of the law.
	Not addressing important risks outside the regulations compliance requirements.
	Applying information security solutions only to minimally meet regulatory requirements and without regard to the business.

---

# United States Federal Personal Data Privacy Bills

*by Rebecca Herold, CISSP, CISM, CISA, FLMI*

With most of the states in the United States having passed privacy breach notification legislation, and several federal breach notification bills of various flavors looming on the horizon, the issue of how to not only better protect personal information but also respond to breaches of personal information certainly should be on organizations' radar. There was a spate of bill writing activity during the summer of 2005, just before the August U.S. congress recess, and personal information security was at the top of the agenda. Three federal bills were proposed at that time addressing the protection of personal information.

 Vermont Senator Patrick Leahy, a sponsor of the Personal Data Privacy and Security Act of 2005, on June 29, 2005 said in a press release "We are seeing a rise in organized rings that target personal data to sell in online virtual bazaars. Insecure databases are now the low-hanging fruit for hackers looking to steal identities and commit fraud." For more information about this press release, see <http://leahy.senate.gov/press/200506/062905a.html>.

The most likely to pass of the proposed federal bills is the Personal Data Privacy and Security Act (PDPSA) of 2005 ([http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109\\_cong\\_bills&docid=f:s1332pcs.txt.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:s1332pcs.txt.pdf))—a bill “to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.” This bill has the broadest scope of the three bills and would create new safeguard requirements and restrictions for how personal information can be used. It would also impose criminal penalties for organizations and entities that violate it.

## The History of United States Federal Privacy Bills

Trying to create a federal law to protect personal information is not a new endeavor. One of the earliest of the many proposed “privacy” bills, alternatively called “data protection” and “data security” bills, within the U.S. congress was H.R. 126, the “Individual Privacy Protection Act of 1989” introduced January 3, 1989 by Rep. Cardiss Collins (IL) “To amend the Privacy Act of 1974 in order to improve the protection of individual information and to reestablish a permanent Privacy Protection Commission as an independent entity in the Federal Government, and for other purposes.” This bill died in committee; however, privacy concerns did not die along with it. Members of congress started listening more to their constituents, and many more bills were introduced to protect personal information and privacy with each subsequent session of Congress. For example, the Fair Credit Reporting Act (FCRA) requires credit report information to be used only for certain purposes. The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to safeguard personal information and prohibits them from sharing their customers' information with third parties without giving the customers the option to say no. And the Health Insurance Portability and Accountability Act (HIPAA) requires healthcare entities to establish specific privacy and administrative, technical, and operational information safeguards for defined protected health information (PHI).

The progression of the privacy protection bills continues. There were at least 362 federal bills proposed in 2005 that covered the protection and privacy of personal information in one way or another. The following sidebar lists just ten of those proposed bills that generated waves in the press.

#### Sample of Proposed United States Privacy-Related Bills in 2005

**H.R. 82, Social Security On-line Privacy Protection Act**—Introduced 1/4/2005 by Rep. Rodney Frelinghuysen (NJ); prohibits an interactive computer service from disclosing to a third party an individual's Social Security number or related personally identifiable information without the individual's prior informed written consent. The bill also requires such service to permit an individual to revoke any consent at any time.

**S. 29, Social Security Number Misuse Prevention Act**—Introduced 1/24/2005 by Sen. Dianne Feinstein (CA); amends the Federal criminal code to prohibit the display, sale, or purchase of Social Security numbers without the affirmatively expressed consent of the individual, except in specified circumstances.

**S. 116, Privacy Act of 2005**—Introduced 1/24/2005 by Sen. Dianne Feinstein (CA); to require the consent of an individual prior to the sale and marketing of such individual's personally identifiable information, and for other purposes

**S. 751, Notification of Risk to Personal Data Act**—Introduced 4/11/2005 by Sen. Dianne Feinstein (CA); requires a business or government entity to notify an individual in writing or email when it is believed that personal information has been compromised, with the exception of situations relating to criminal investigation or national security purposes.

**S. 768, Comprehensive Identity Theft Prevention Act**—Introduced 4/12/3005 by Sen. Charles Schumer (NY); creates a new Federal Trade Commission (FTC) office of identity theft to help victims restore their identities.

**S. 1216, Financial Privacy Breach Notification Act of 2005**—Introduced 6/9/2005 by Sen. Jon Corzine (NJ); amends GLBA to require a financial institution to promptly notify the following entities whenever a breach of personal information has occurred at such institution: each customer affected by such breach; certain consumer reporting agencies; and appropriate law enforcement agencies. Furthermore, it requires any person that maintains personal information for or on behalf of a financial institution to promptly notify the institution of any case in which such customer information has been breached.

**S. 1326, Notification of Risk to Personal Data Act**—Introduced 6/28/2005 by Sen. Jeff Sessions (AL); requires any entity that owns or licenses sensitive personal information to implement and maintain "reasonable" security and notification procedures and practices appropriate to the nature of the information; preempts any state laws which relate "in any way to electronic information security standards or notification."

**S. 1332, Personal Data Privacy and Security Act of 2005**—Introduced 6/29/2005 by Sen. Arlen Specter (PA) and Sen. Patrick Leahy (VT); deals with different issues relating to identity theft and security breaches, specifically providing security measures that require "business entities" that have information on more than 10,000 United States persons to adopt measures, commensurate with the sensitivity of the data and the size and complexity of the entities activities.

**S. 1336, Consumer Identity Protection and Security Act**—Introduced 6/29/2005 by Sen. Mark Pryor (AR); establishes procedures for the protection of consumers from misuse of, and unauthorized access to, sensitive personal information contained in private information files maintained by commercial entities engaged in, or affecting, interstate commerce.

**S. 1408, Identity Theft Protection Act**—Introduced 7/14/2005 by Sen. Gordon Smith (OR) and Sen. Bill Nelson (FL); strengthens data protection and safeguards, requires data breach notification, and further prevents identity theft.

---

## Challenges for Passage of Such Bills

There are some common threads running through these privacy protection bills:


Require prompt notification when a security breach occurs or is discovered

Grant more regulatory power to the U.S. federal government

Establish minimum standards for information security

Although there are a staggering number of bills that have been submitted to Congress, few have continued on to become full-fledged laws, illustrating the many challenges for passage of these bills. Lobbyists from large organizations that must comply with the laws have huge influence and strong voices in blocking these bills; they have historically lobbied to not make businesses responsible for security breaches. Privacy advocates also have huge influence and equally strong voices in blocking these bills; they have historically lobbied to make weak bills stronger and to prevent the passage of what they view would be watered-down laws with so many loopholes that any such law would be basically meaningless.


However, with the escalation in the number of reported personal information security breaches, as well as the sometimes hugely varying requirements of state-level breach notification laws that make it extremely challenging for businesses to find common compliance ground, lobbyists, privacy advocates, and already heavily regulated industries alike are now supporting the passage of uniform federal privacy laws.

 From the Prepared Testimony and Statement for the Record of Marc Rotenberg, President, EPIC; Hearing on “Identity Theft and Data Broker Services” Before the Committee on Commerce, Science and Transportation, United States Senate; May 10, 2005: “Congress can continue to deal with these challenges in piecemeal fashion, but it seems that the time has come to establish a formal government commission charged with the development of long-term solutions to the threats associated with the loss of privacy. Such a commission should be established with the clear goal of making specific proposals. It should include a wide range of experts and advocates. And it should not merely be tasked with trying to develop privacy safeguards to counter many of the government new surveillance proposals. Instead, it should focus squarely on the problem of safeguarding privacy. Congress needs to establish a comprehensive framework to ensure the right of privacy in the twenty-first century.”

---

## PDPSA Passage Likely

Pundits largely believe the PDPSA will meet with successful passage by congress. What makes this bill appealing to lawmakers is that it is one of the few, perhaps only, of the bills that establish criminal activities for entities that do not provide proper safeguards for personal information and that do not respond appropriately to personal information breach incidents.

 If the PDPSA is passed into law, there can be criminal penalties including as many as 5 years in prison for those who intentionally conceal information related to a security breach and as many as 10 years for breaking into systems maintained by data broker companies in the business of selling personal information.

The PDPSA would also restrict the sale and publication of Social Security numbers. This restriction appeals to the many members of Congress who have submitted bills specific to the protection of Social Security numbers. It also would limit the authority of states to write their own state-specific legislation of personal data protection—something that Congress believes will help in creating a more consistent level of privacy protection throughout the states.

The other proposed bills largely include only civil penalties and would place most of the enforcement and regulatory powers with the Federal Trade Commission (FTC). Most of them also explicitly preempt state and local laws involving the same issues, and detail a wide range of monetary penalties on entities that don't provide notification according to what many consider as ambiguous terms, such as "without unreasonable delay." The guidelines for breach notification also are different from bill to bill.

## Benefits and Detriments of Such Bills

The PDPSA would likely result in the FTC creating a new standard for minimally acceptable and reasonable security practices in addition to creating regulations requiring covered entities to

Develop, implement, and maintain an effective information security program that contains administrative, technical, and physical safeguards for sensitive personal information, taking into account the use of technological safeguards, including encryption, truncation, and other safeguards available or being developed for such purposes

Implement procedures for verifying the credentials of any third party seeking to obtain the sensitive personal information of another person

Implement disposal procedures for not only disposal of sensitive personal information but also secure transfer of sensitive personal information to third parties for disposal

As it is now written, it would not require federal preemption of any similar state law except if the state law were inconsistent with the PDPSA.

As information security and privacy professionals who have been struggling to keep up with regulations know, there are a variety of benefits as well as detriments to these assorted and sundry bills. Table 1 explores these benefits and detriments.

Benefits	Detriments
Increased awareness of information security and privacy issues by business leaders who, under the bills, become ultimately responsible for having adequate safeguards in place.	Overly broad notification requirements may result in so many breach notifications being sent that consumers—for typically “normal” security incidents such as virus outbreaks—start disregarding them. This oversight may lead to customer complaints, and result in weakened business leader support.
Subsequently increased budgets and resources for addressing information security and privacy issues in order to be in compliance.	Resources may be pulled from other vital information security and privacy projects because they are not explicitly cited in regulatory text, so they lose their funding. This situation could leave important risks unaddressed. Organizations have already been dealing with this situation with regard to Sarbanes-Oxley compliance activities.
Increased leverage for information security and privacy professionals implementing security controls and practices.	A large increase in “snake oil” compliance-related vendor product solutions will be pushed upon organizations. Many of these products will likely be relabeled applications from existing “compliance” products. Using these will likely lead to gaps in compliance and a false sense of achieving compliance.

**Table 1: Benefits and detriments of privacy bills.**

## PDPSA Considerations

The specific requirements for the PDPSA will certainly help to beef up corporate information security and privacy programs, but will also create challenges for information security and privacy leaders:


Covered entities (CEs) would need to report each data breach of “personally identifiable information” to the U.S. Secret Service, credit reporting agencies, and consumers.

CEs would need to “implement a comprehensive personal data privacy and security program.”

CEs would be required to conduct risk assessments to identify all vulnerabilities that could potentially allow a data breach.

CEs would need to evaluate the sufficiency of policies, procedures, and security controls. For example, the PDPSA would require CE to make appropriate provisions for facility access, employee training programs, and the destruction of media or storage devices.

What is personally identifiable information? Within the PDPSA “the term ‘personally identifiable information’ means any information, or compilation of information, in electronic or digital form serving as a means of identification, as defined by section 1028(d)(7) of title 18, United State Code.”

 Section 1028(d)(7) of title 18 United State Code:

*“(7) the term “means of identification” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any -*


*(A) name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;*

*(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;*

*(C) unique electronic identification number, address, or routing code; or*


*(D) telecommunication identifying information or access device (as defined in section 1029(e))”*

The PDPSA would require that data brokers (defined by the bill as “a business entity which for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of collecting, transmitting, or otherwise providing personally identifiable information on a nationwide basis on more than 5000 individuals who are not the customers or employees of the business entity or affiliate”) and companies possessing databases with the personally identifiable information of 10,000 or more U.S. citizens would be covered entities (subject to the law). Civil and criminal penalties for violating the PDPSA are wide-ranging depending on the type of breach that has occurred and the number of personal records compromised. Businesses could potentially be fined as much as \$35,000 a day for each day the enterprise is in violation of PDPSA requirements.

 Unlike most of the state breach notification laws, the PDPSA does NOT include a provision to exempt encrypted data from the breach notification requirement; it applies to both encrypted and unencrypted data.

## Get Ready to Meet Compliance

Just before the Thanksgiving recess in November 2005, the Senate Judiciary Committee approved the PDPSA in a bipartisan vote. With the broad base of support from not only corporations but also from privacy groups, several legislative analysts expect the PDPSA to pass into law sometime during the last half of 2006 with little to no opposition. Organizations will then have one more regulation with which to comply. However, it is likely that with everything else on their compliance plates, most will take a wait-and-see attitude (much like most did with HIPAA and GLBA) before getting fired up to take compliance actions. Such lackadaisical attitude is risky and could be costly.

 According to the January 10, 2006 issue of the McLean Report “As with most new legislation, companies generally don’t begin compliance initiatives until 60 or 90 days before a legal deadline...each \$1 spent on compliance efforts pre-deadline will end up costing \$10 for the same activity if addressed post-deadline.”

---

Even without the passage of PDPSA, the U.S. government has already been finding businesses accountable for safeguarding personal information. Businesses will be impacted, with or without passage of the PDPSA, if an incident involving the breach of personal information occurs. It is wise to prepare now to respond to what seems to be the inevitable personal information breach. Think now about addressing the following issues:

Establish an area or position with accountability and responsibility for information security and privacy activities.

Define the personally identifiable information within your organization.

Identify where all the personally identifiable information is located.

Perform a privacy impact assessment (PIA).

Create a breach incident identification and response plan.

Create or review and update as necessary information security and privacy policies and procedures.


Implement an ongoing information security and privacy training and awareness program.

---

# The Evolution of BS7799 to ISO27001 and ISMS Certifications

*by Rebecca Herold, CISSP, CISM, CISA, FLMI*

The need to protect information has been following a crescendo of awareness over the past few years to climax with literally thousands of information security and privacy-related news reports during 2005. Consumers have become aware of the need for protection through cases of identity theft and fraud. Security incidents impact businesses in both the short-term and the long-term from the costs required to not only clean up incidents and implement better security controls to prevent similar incidents from recurring but also from diminished trust and lost business.

 According to an autumn 2005 independent survey of nearly 10,000 adults in the United States conducted by the Ponemon Institute:

- 20% indicated they terminated a relationship with a company after being notified of a security breach
- 40% say they are considering terminating the relationship
- 5% hired lawyers upon learning that their personal information may have been compromised

Growing numbers of laws and regulations are being passed and implemented throughout the world. Such legislation has justifiably captured the attention of business leaders who are now more seriously considering how to meet compliance regulations and perform information security due diligence than ever before. Establishing an effective information assurance program to incorporate information security into business activities is now high on the executives' to-do list.

## Information Security Management Systems Integrate Security into Business

A well-documented information security program will not be effective if it is not successfully integrated throughout the enterprise within all business practices. Information security practitioners are increasingly realizing that establishing a formal Information Security Management System (ISMS) will complement their existing information security efforts and work to effectively integrate information security throughout the enterprise business services, products, operations, and management. As a result, information security will truly become more effective and will more clearly support business success.

BS7799-2 specifically outlines and details the implementation and documentation requirements for an ISMS. In effect, an ISMS is the approach by which a BS7799-based information security program validates and documents its existence, documenting how information security processes must be implemented within a specified organizational scope. When an organization pursues certification, the ISMS is what is audited and ultimately certified.

BS7799-2 and the supporting ISO/IEC 17799 documents have evolved over the years. There was a major rewrite to ISO/IEC 17799 in 2005. ISO27001 is the new industry standard for an ISMS. It was formalized in October 2005 and replaces the previous BS7799 standard.

---

## What Is New About ISO/IEC 17799?

Over the years, many organizations have built their information security programs around the controls and domains listed in ISO/IEC 17799. A large number of organizations have written and organized their information security policies and procedures using the ISO/IEC 17799 as a model framework and to represent a leading international practice.


The revised version of ISO/IEC 17799 was published on June 15<sup>th</sup>, 2005, at which time the officially published 2000 version was withdrawn. The 2005 version contains 17 new controls, and a few of the old ones were merged, incorporated with others, or deleted. The 2005 version contains a total of 134 controls.

The 2005 version has 11 domains, or *clauses*; the 2000 version has 10 domains. The domains align pretty closely, however there were a few slight title changes as indicated in Figure 1. A few notable and definite improvements in the 2005 version include the addition of content addressing issues related to:

- Third-party and outsourcing security
- Managing systems updates
- Security following personnel termination
- Responding to incidents
- Ensuring appropriate mobile and remote computing device security

ISO/IEC 17799:2000	ISO/IEC 17799:2005
Security Policy	Security Policy
Security Organization	Organizing Information Security
Asset Classification & Control	Asset Management
Personnel Security	Human Resources Security
Physical & Environmental Security	Physical & Environmental Security
Communications & Operations Management	Communications & Operations Management
Access Control	Access Control
Systems Development & Maintenance	Information Systems Acquisition, Development and Maintenance
	Information Security Incident Management
Business Continuity Management	Business Continuity Management
Compliance	Compliance

**Figure 1: Mapping chapters from the 2000 version to the 2005 version.**

 ISO/IEC 17799:2005 is a code of practice for information security management and is not applicable for ISMS certification. BS7799 Part 2:2002 and ISO/IEC 27001 are currently used for ISMS certification.

---

## Certification Process

There are generally three phases in the ISMS certification process.

- First phase—The organization prepares for ISMS certification by developing and implementing the ISMS, integrating the ISMS into the enterprise business processes, training all personnel and creating ongoing ISMS awareness activities, and creating an ISMS maintenance process.
- Second phase—This step involves engaging an accredited certification body to audit the ISMS. Successful certification will last for 3 years, after which the ISMS must be recertified to maintain certification.
- Third phase—The certification body goes onto the ISMS site regularly, for example every 6 to 9 months, to perform surveillance audits.

## Benefits of Obtaining ISMS Certification

There are many business benefits for establishing an ISMS and pursuing certification. To consider just a few, an ISMS

- Can reduce liability risk and demonstrates due diligence as well as lower business insurance premiums
- Demonstrates credibility for, and trust in, how the organization protects information; this demonstration leads to increased satisfaction and confidence of stakeholders, business partners, and customers
- Demonstrates executive management support for internationally accepted security and privacy standards, principles, and practices
- Ensures that security and privacy controls and practices are built-in to all levels of an organization (at least within the ISMS scope) and that all personnel are educated on security and privacy as they relate to the business
- Establishes a holistic, quality management–based security and privacy program that also subsequently creates verifiable evidence of due care activities
- Helps to bring organizations into compliance with a wide range of legal, regulatory, and statutory requirements, such as the United States Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), 21 CFR Part 11, and the Sarbanes-Oxley Act (SOX), as well as California’s SB1386, the European Union Data Protection Directive, Canada’s PIPEDA, and Australia’s Federal Privacy Act
- Improves business continuity and availability by identifying threats and appropriately minimizing internal and external risks
- Is increasingly recognized worldwide as a security and privacy differentiator for regulatory oversight as well as competition
- Provides a documented, consistent, and repeatable process for enterprise information security and privacy governance

- 
- Provides an organization with market differentiation that creates a more positive company image that relays the importance of information security and privacy and could very well positively affect the revenues and asset or share value of the organization
  - Reduces operational risk by mitigating vulnerabilities and lessening risks through clearly defined and consistent activities
  - When implemented properly and successfully, an ISMS will significantly limit security and privacy breaches that can cost millions (through such things as lost or compromised information, fines and penalties, downtime, internal and external threats, consumer driven litigation, and so on)

## **Benefits of Requiring Business Partners to Have Certified ISMS Programs**

Many data breach and security incidents have actually been the result of mistakes and poor practices by third-party outsourced vendors who were performing activities for other companies. However, it was the primary company that ultimately made the headlines, and whose business was most impacted. For example, consider only incidents involving third-party backup tape handlers in just the United States:

- DHL Delivery Service lost an ABN Amro backup tape containing data on 2 million of their customers in November 2005; the tape was subsequently found December 19
- UPS lost Citigroup computer backup tapes containing information about 3.9 million individuals in June 2005
- Iron Mountain lost Time-Warner's computer backup tapes containing information about 600,000 current and former employees in May 2005
- Iron Mountain lost Bank of America computer backup tapes containing information about 1.2 million federal employees in February 2005
- Iron Mountain lost Ameritrade computer backup tapes containing information about 200,000 customers in April 2005

These are just a few of the hundreds of incidents that have occurred and been reported over the recent years involving organizations to whom businesses outsourced information handling, storing, transportation, or processing. Many organizations are outsourcing very specialized data processing and management activities in an effort to save money or because they just don't have the resources, experience, or capabilities to do it themselves. Organizations also commonly outsource to get specific expertise that their personnel may not possess, and which they cannot afford to hire or purchase. For example, if you outsource your applications programming activities, you will reasonably expect that the individuals doing this work know about application security issues and will incorporate adequate security controls into the product they create for you. You will also reasonably expect them to know how to protect information in a shared customer environment; making sure that the programming code they create for your organization does not get sent by accident to another customer, that the test data they use for your organization does not get used by another of their customers, and so on.



The National Association of Software and Services Companies, a New Delhi-based organization made up of 800 Indian IT and outsourcing companies, reported the business process outsourcing market in India alone grew 54 percent to \$3.6 billion during the first quarter of 2004, and by the end of March 2005, India controlled 44 percent of the global offshore outsourcing market for software and back-office services.

Outsourcing is becoming quite commonplace, particularly with many top financial, healthcare, tax reporting, and credit reporting companies. Even agencies within the United States government have outsourced processing of sensitive information. Chances are there are people within your organization considering outsourcing some of your data processing activities.



The United States Internal Revenue Service (IRS) has indicated that they will outsource private debt collection as part of their 2006 \$12 billion private debt collection initiative.

When entrusting third parties with your company's confidential data, you are placing all control of security measures for your organization's data completely into the hands of someone else. That trust cannot be blind. Many of the recent security incidents have resulted from loose security practices within outsourced third-party organizations that were custodians of another company's customer or employee personal information.

When you outsource critical data processing and management activities, how can you stay in charge of the security of the outsourced data and minimize your business risks? How do you know the third party is complying with your regulatory responsibilities? How can you demonstrate to regulators that you are in compliance with data protection requirements and promises when someone else possesses your data?

You need to hold such outsourced organizations to strict security standards. In many instances, the standards will be more stringent than your own organization's security requirements. Accordingly, requiring business partners to conform to ISO27001 or have a certified ISMS helps to protect your organization from business partner security and privacy incompetence.

---

## Challenges for Obtaining ISMS Certification

Although there are many significant benefits to implementing a certifiable ISMS, do not think that doing so will be a simple task that can be accomplished in a matter of a couple of months let alone weeks. There are many associated challenges. Consider them now so that you can plan accordingly when creating your own implementation plans. A few of these challenges include:

- Obtaining executive management commitment. Successful implementation of an ISMS is dependent upon visible and active executive management support. ISMS enforcement authority must come from executive management.
- Setting the ISMS scope. Organizations must understand that an ISMS typically governs multiple manageable security domains. Organizations often try to create a scope that is much larger than can feasibly be managed, or they do not create realistic security domains.
- Risk analysis. The basis for the ISMS controls must be risk. Organizations must identify risks to be able to prioritize and implement appropriate safeguards within the ISMS. Many organizations do not perform a risk analysis or do not truly understand the risks within their environment.
- Implementation flaws. An ISMS should leverage other existing business frameworks, such as ITIL and COSO. Without doing so, duplication of effort and implementation conflicts occur.
- Asset identification and classification. Organizations must know the information assets they are protecting and why they need to be protected. Unfortunately, most organizations lack or have a poor or inaccurate asset inventory and information classification system. These deficiencies lead to inconsistent and flawed implementation.
- Resources. Implementing an ISMS requires participation from everyone within the organization, including support from multiple business leaders and understanding from all personnel within the organization who must follow the policies and procedures.
- Personnel awareness and training. Organizations must communicate the ISMS information security policies, processes, standards, and responsibilities to personnel, otherwise they cannot expect them to know, understand, or follow the directives. Unfortunately, most organizations have grievously insufficient or ineffective awareness and training programs.
- No magic bullets. There does not exist one magic bullet product or system to implement an effective and certifiable ISMS. Beware of vendors who claim their products will do so. The specific environment and culture of each organization must be taken into account individually to create an effective ISMS.
- Ongoing evaluation and modification. Once an ISMS is launched, processes must be in place to continuously evaluate the effectiveness and feasibility of all components of the ISMS. When weaknesses, inefficiencies, or security gaps are discovered, the ISMS needs to be modified accordingly.

---

## ISMS Certification Facts

According to the International Register of ISMS Accredited Certificates (<http://www.iso27001certificates.com/>) there were 2017 actual ISMS certified organizations as of the end of December 2005. The ten countries with the most certifications at the end of 2005 were:

1. Japan: 1187
2. UK: 219
3. India: 139
4. Taiwan: 66
5. Germany: 49
6. Italy: 40
7. Korea (note, “South” or “North” was not indicated): 35
8. USA: 31
9. Hungary: 23
10. Netherlands: 22

## Certified ISMS Auditors

The International Register of Certified Auditors (IRCA—<http://www.irca.org/>) manages the certification for ISMS auditors. There are six types of auditor certifications:

- ISMS Auditors
- ISMS Internal Auditor
- ISMS Lead Auditor
- ISMS Principal Auditor
- ISMS Provisional Auditor
- ISMS Provisional Internal Auditor

IRCA evaluates certification applicants against requirements that reflect the key skills, knowledge, and experience that define competence and which the ISMS auditor needs to demonstrate during audits. The evaluation criteria include education, work experience, auditor training, and auditing experience for each of the types of auditor certifications. The details of all certified auditors are included within a register, which is published and made publicly available by IRCA.

---

It is interesting to note the number of IRCA ISMS-certified auditors within each of the countries that have a preponderance of ISMS certified businesses. According to IRCA, there were the following combined numbers of certified ISMS auditors as of January 2006 in each of the indicated countries:

- Japan: 12
- UK: 16
- India: 1
- Taiwan: 6
- Germany: 1
- Italy: 14
- South Korea: 3
- USA: 6
- Hungary: 1
- Netherlands: 0
- Canada: 4

It is important to keep in mind that although the number of certified ISMS auditors appears to be small, each of the at least 51 worldwide ISMS registrars (certification bodies) may have their own certifications available to allow consultants and auditors to participate within the ISMS certification process. For example, BSI Global (<http://www.bsi-global.com>) provides training programs for individuals who are on their way to becoming IRCA certified, which allows the individuals to participate within ISMS audits. There are likely hundreds more individuals worldwide who have some sort of registrar-specific certification or qualifications.

## ISMS Certification Trends

It is apparent from the previous statistics that United States' businesses have been slow to seek ISMS certified programs. Why? Ray Kaplan, a United States-based BSI Qualified BS7799 Auditor, Implementer, and Instructor points out an error many organizations make is considering that BS7799:2002 and ISO/IEC 27001 can be used as a checklist approach for grading their existing information security programs. "To use ISMS standards as mere checklists completely misses the main thrust of this important fabric: an ISMS is a process management system. The developing fabric of the ISO 27000 family of ISMS standards carries on the developing traditions of many process management systems. Some previous BS7799 certifications were conducted poorly, giving rise to the mistaken idea that ISMS certification was a sham. Some BS7799 certifications were issued on the flimsiest of grounds. However, as the fabric of national authorities square up to enforce rigor in formal certification to the developing ISO 27000 family of standards, rigor is becoming the rule. For instance, registrars are now requiring real, internationally recognized ISMS audit credentials for their auditors."

---

I anticipate that the growing number of security incidents coupled with the growing number of worldwide laws and regulations for protecting information will result in an increase in the number of organizations who establish formal ISMSs and subsequently seek ISMS certification; particularly as organizations begin to understand ISMS scope and certification processes.

#### Resources

The following list highlights a few good resources for you to check when considering ISMS implementation and certification:

- <http://27000.macassistant.com/>
- [http://dmoz.org/Science/Reference/Standards/Individual\\_Standards/ISO\\_17799](http://dmoz.org/Science/Reference/Standards/Individual_Standards/ISO_17799)
- [http://hotskills-inc.com/services\\_iso\\_17799.shtml](http://hotskills-inc.com/services_iso_17799.shtml)
- <http://www.17799.com/index.php>
- <http://www.irca.org>
- <http://www.iso27001certificates.com>
- <http://www.iso27001security.com>
- <http://www.standardsmark.com/Products/InformationSecurity.htm>
- <http://www.xisec.co>