Laws and Regulations and Standards… Oh My!

by Carol Woodbury

Oh my is right. When you look at all of the laws, regulations and standards that drive security and compliance requirements, your head can start to swim. How should these be used within my organization? Which ones does my organization need to be in compliance with? If my organization is compliant or has passed an audit, is our data secure? These questions and more are addressed as several of the more well-known laws, regulations and standards are described and contrasted.

First let's define two terms – *information security* and *compliance*.

> The generally recognized definition of **information security** is protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. (http://en.wikipedia.org/wiki/Information_security)
>
> According to Webster, **compliance** is conformity in fulfilling official requirements http://www.merriam-webster.com/dictionary/compliance

Keeping these definitions in mind, let's see how these laws, regulations and standards either drive or contribute to information security and compliance within your organization.

Payment Card Industry (PCI)

Every organization that stores credit card information has heard of the PCI's Data Security Standard (DSS). This standard was first developed by Visa and MasterCard and was known as Visa PCI. In 2006, Visa, MasterCard, American Express, Discover and JCB formed the PCI Security Standards Council and, with minor changes, adopted the Visa PCI standard and made it the PCI Data Security Standard. The Council has turned into a consortium that includes security experts, vendors and others interested in keeping cardholder data secure. The PCI DSS is updated at least every other year to address changes in technology and threats.

The reason PCI DSS exists is to reduce the risk to cardholder data. Why? Because the credit card companies and the banks that issue credit cards were losing too much money to fraud and theft. They felt that if they could get the merchants to secure the cardholder data, their losses would at least be slowed. While Level I (organizations with over 6 million transactions per year) and Level II (organizations with between 1 – 6 million transactions per year) merchants have had to be PCI compliant for several years, many merchants with fewer transactions are only now realizing that PCI DSS applies to them as well.

Although containing more specifics than ISO 27000+ standards (which we'll examine next), PCI DSS has to be interpreted for each operating system and technology to which it's being applied. For example, rather than specifically listing the settings for an AIX system running an Oracle or DB2 database it states that access to cardholder data be "deny by default." And, like the ISO standards, the DSS is very broad – addressing the need for an information security officer, security policy, network security, access controls, encryption, application development security standards, testing, monitoring, incident response and regular security assessments.

How PCI DSS can be used: Obviously, compliance with PCI DSS is a requirement of any organization that stores cardholder data – regardless of the organization's size, purpose or number of transactions. Should the PCI DSS be ignored if the organization doesn't store cardholder data? No. The PCI DSS provides a good example of one industry's view of security best practices. You may not follow all of the requirements, but it is a good reference point for all organizations.

Is the data secure if the organization is PCI compliant?
While compliance with PCI has caused card holder data in most organizations to be less vulnerable, several high-profile thefts (Hannaford and Heartland Systems) have shown that PCI compliance is not sufficient in all cases to ensure the security of cardholder data.

ISO 27000 Series

These standards first started out as a British Standard – BS7799 to be exact. BS7799 was adopted by the International Standards Organization (ISO) www.iso.org as ISO17799. ISO17799 then became ISO 27001. ISO17799 was renamed to allow for the sequential numbering of more security-related standards being developed (27001 – 27006). These are now known as the 27000 series. The intent of the 27000 series is to establish a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS).
These ISO standards place great emphasis on:

- the responsibilities of management and requirement for management involvement for a successful ISMS
- finding the balance between too much security and not enough. For example, it encourages expenditures to be meted out after appropriately weighing the risks to the business caused by the vulnerability against the likelihood of occurrence. The goal is to reduce the risk to an acceptable level.
- continual improvement. In other words, security management is not a one-time event. Security management is a process. Part of the ISO standard addresses the discovery of flaws and the need to continually seek ways to improve the security posture of the organization.

These security-related ISO standards provide broad and far-reaching guidance. ISO 27001 addresses all parts of the organization – security policy, organizing information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, information security incident management, business continuity management and compliance. Only 27001 and 27002 have been published. The others are placeholders for topics such as implementing an ISMS (27003), information security management and metrics (27004), information security risk management (27005) and guidelines for organizations offering accreditation (27006).

Because the ISO 27000 series is intended to provide guidance to every type of organization large or small, public or private, it doesn't address one specific type of data, such as cardholder data. Rather it recognizes and addresses the fact that information is an asset and needs to be secured according to its importance (value) to the organization.

The standards are written for all organizations. That's why you'll find it written as guidance rather than absolutes. About the most detailed you'll see as you read through the standards is for password use. PCI, for example, states that users must have "strong passwords" and goes

on to state the exact requirements (minimum length of 7 characters, require a digit, changed every 90 days, no default passwords) ISO's guidance is far more general:

> Select quality passwords with sufficient minimum length which are:
> 1) easy to remember;
> 2) not based on anything somebody else could easily guess or obtain using person-related information, e.g. names, telephone numbers, and dates of birth etc.;
> 3) not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);
> 4) free of consecutive identical, all-numeric or all-alphabetic characters;

How ISO 27000+ can be used: ISO27000 series should be used as a model for assessing and implementing your organization's Information Security Management System. At a minimum, your organization's security policy and practices should be reviewed against these ISO standards when you perform your annual policy review to ensure you are addressing all applicable areas of the standard.

Is the data secure if the organization is ISO compliant?
Possibly. The purpose of the ISO 27000 series is to provide guidance on best practices for securing all aspects of your organization. Because of the breadth of the standards, organizations' data is likely to be at less vulnerable than organizations that aren't ISO compliant. However, part of the decision in determining how to secure data is based on the perceived risk to the data. If the perceived risk of a particular vulnerability is low and that assumption is wrong, the organization may technically have been ISO compliant but the data wasn't secure. In addition, the ISO standards are a bit dated (updates are expected soon.) So while your organization may be ISO compliant, unless you're keeping up with the latest technology and addressing their associated security vulnerabilities, your organization could be at risk.

If an organization is ISO compliant are they PCI compliant?
Possibly. It depends on how the ISO guidelines have been implemented and whether they meet the specific requirements of PCI. For example, ISO doesn't voice specific requirements for encrypting data and encryption key management, but PCI does.

Control Objectives for Information and related Technology (COBIT)

COBIT is a set of best practices for Information Technology (IT) management. It was created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1996. COBIT is a methodology for evaluating and managing risk in the IT organization. It seeks to integrate this methodology into IT decisions, applying the same discipline (such as clear objectives and measureable benefits) as is applied to other areas of business. COBIT strives for appropriate governance and controls in organizations' IT departments. COBIT became popular when Sarbanes-Oxley audit requirements started to flow into IT organizations.

If you follow COBIT, are your systems and data secure?
Possibly. Anytime rigor and discipline is added to processes, there's less likelihood of missing something. So if your security policy is thorough and your COBIT process supports the requirements of your policy your organization has a better chance of having addressed the issues that may have caused a gap in your security scheme. For example, when IT is implementing a new technology or designing a new application, security can be an

afterthought. Following a well-disciplined process that includes a review of the security implications of each project will help ensure security is not ignored. Then, following rigorous testing and implementation processes will ensure security remains in focus for the entire project.

How COBIT can be used:
Few organizations follow the entire COBIT process because it does add significant overhead to every decision; however, even if you don't implement all aspects of COBIT, it can be helpful for all organizations. If most IT organizations were honest with themselves, they'd admit that they could use more rigor in their processes. Reviewing the COBIT control objectives can help identify gaps in your current processes.

Sarbanes-Oxley Act (SOX)

Of course everyone's heard about -and most of you have been affected by - the Sarbanes-Oxley Act. Japan even has its own version of SOX – fondly referred to as JSOX. SOX was enacted to make sure that there are sufficient controls and processes in place to ensure the corporate financial statements are accurate and reflect reality. Contrary to popular belief, SOX says absolutely nothing about IT security. However, it cannot be argued that the need for information security is at least heavily implied. How is that conclusion reached? Without proper access controls, data could be open to modification by unauthorized users. To ensure the integrity of the financial data, all databases used as input to the company's financial data must be set to a default access that allows no more than read-only access. And with the emphasis on separation of duties, a deny-by-default approach is the best way to ensure that only users with a business need to access the data can do so.

If your organization passes a SOX audit, is the data secure?
Since the purpose of a SOX audit is to ensure the integrity of the financial data, it's doubtful that the scope of the SOX audit is sufficient to ensure that the data is secure. Remember, integrity of data is achieved by ensuring no one but authorized users can modify the data. This implies read-only access. But some types of data, such as PII (Personally Identifiable Information) also need to be kept confidential. This implies preventing all access (deny by default) except to those users whose job responsibility requires access.

If your organization passes a SOX audit, is your organization in compliance with COBIT?
Not necessarily. As COBIT gained popularity during the height of the SOX compliance push, compliance with SOX - in some peoples' minds - became synonymous with being in compliance with COBIT. The other misconception is that you *had* to be in compliance with COBIT or follow COBIT to be in SOX compliance. Depending on what your SOX auditor felt was important, COBIT may have been a method used to help your organization come into and maintain SOX compliance. But COBIT is certainly not required by the Sarbanes-Oxley Act.

What are the benefits of SOX?
Despite the bad name SOX has attained in many IT departments, SOX has several benefits. One such benefit is that Sox has caused organizations to implement and document processes (such as change management) where none previously existed. In addition, the requirement for separation of duties causes more accountability throughout the organization.

Statement on Auditing Standards, No 70, Service Organizations (SAS70)

One requirement that more organizations are talking about is a SAS70 audit. This standard is defined through the American Institute of Certified Public Accountants (AICPA) and has been in existence for some time. Its official title is "Reports on the Processing of Transactions by

Service Organizations". SAS70 specifies audit requirements for organizations that either perform outsourced services or organizations that are using outsourced services. As more organizations outsource more services, the requirement for organizations to participate in a SAS70 audit grows. There are two aspects to a SAS70 audit. One is for the company using the outsourced service. They typically want a SAS70 audit to ensure that the internal controls within the outsourcer's organization are sufficient to ensure delivery of the service they're purchasing and that the outsourcer's internal controls support the requirements of their own internal controls. The other aspect of a SAS70 audit is for the outsourcer itself. They may be requested by their users to have a SAS70 audit of their internal controls to ensure that their policies and procedures represent the service they've said they're providing and that the policies and procedures were being followed.

If an organization has passed a SAS70 audit, it is secure?
Like SOX, the requirements for passing a SAS70 audit specify nothing specific about security requirements. While the requirement for good security practices may be implied by SAS70, (certainly, a good security scheme supports many of the SLAs outsourcers provide) it's really up to your organization's requirements of the outsourced service to impose security requirements on an outsourcer.

How a SAS70 audit can be used:
If your organization is considering using an outsource service, requiring the outsourcer to pass a SAS70 audit is a good idea. If you are using an outsourced service, undergoing a SAS70 audit will help provide peace of mind that the requirements of your internal controls are supported by your outsourcer.

The impact of these laws, regulations and standards

The impact of these and other laws, regulations, standards and audits is directly to your organization's security policy. Your organization's security policy should be developed and reviewed using the guidance and recommendations from the ISO 27000 standards as well as COBIT and address the requirements of all the laws and regulations with which your organization must comply. In addition, the policy should address the issues that are unique to your organization. Resist the temptation to have a security policy that is a generic template that could apply to any organization. In other words, make it meaningful for your organization so that it is an actual reflection of your organization's security requirements. Finally, it is essential that your policy be reviewed at least annually. Issues such as shifts in the organization's business plan and technology changes need to be considered for incorporation into the policy.

Bottom line

What do you need to be in compliance with? Your organization's own security policy. While your policy will document your organization's security requirements, it's in the implementation of this policy that will determine whether your organization is in compliance.

Carol Woodbury is President and co-founder of SkyView Partners, a firm specializing in security administration and policy compliance software and services. Carol is the former Chief Engineering Manager for IBM AS/400 in Rochester, MN and has over 20 years' experience in the field of computer security Her third book, IBM i and i5/OS Security & Compliance: A Practical Guide is available from amazon.com. For more information about SkyView Partners' products and services, visit www.skyviewpartners.com or contact us at info@skyviewpartners.com.

How SkyView Partners' Solutions Can Help

SkyView's software solutions will help you meet your compliance requirements when implementing your corporate security policy.

SkyView Risk Assessor for IBM i and i5/OS produces an unbiased security assessment. Risk Assessor examines over 100 'risk points' throughout the operating system and compares them to security best practices. The documentation and supporting reports describe:

- why the issue is considered a risk point
- recommended settings
- considerations to make before remediation

SkyView Policy Minder for IBM i and i5/OS is a policy compliance and security administration tool that allows you to automate processes. With Policy Minder you can:

- document your organization's policy implementation
- check for non-compliant items
- notify the appropriate individuals
- fix the issue that is out of compliance