"Unified Compliance" = 5 Steps + C^3

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI
Final Draft for June 2009 CSI Alert

To say information security and privacy practitioners are perplexed and overwhelmed by the growing numbers of compliance requirements is an understatement. There are well over one hundred international data protection laws, hundreds of U.S. state-level laws, and increasingly more information security and privacy standards. These often overshadow the just-as-important contractual requirements for data protection, along with organizations' own bevy of policies that must be followed.

For the past several years I've been teaching sessions and classes pointing out the benefits of addressing the growing number of legal, regulatory, and contractual information security and privacy requirements with "unified compliance" activities instead of in a "one-off" manner. It just makes sense when you think about it. If, by doing one thing, you can address the requirements of over a dozen compliance requirements while also mitigating risk, isn't that better than spending valuable time and resources laboring to implement a safeguard that complies with just one requirement and doesn't significantly mitigate risk?

A one-off approach also can quickly and easily undermine the integration of information security and privacy compliance activities throughout the enterprise by:

- Making it harder to monitor, document and measure compliance and the associated controls and their effectiveness; and
- Making it harder for business leaders throughout the enterprise to cooperate and support information security and privacy efforts; they don't want to feel like they are constantly answering the same types of questions over and over again, and re-doing the same tasks to meet yet one more singular requirement.

For just these couple of reasons, organizations should consider implementing a unified approach to information security and privacy compliance.

Five important steps

Let's assume you've signed on to this concept of unified compliance. Now what? There are five basic steps to make this initiative as successful as possible.

1) Determine the person or role that will ultimately be responsible for the unified compliance efforts, and ensure executives are providing strong and visible support for him or her. Unified compliance efforts will only be successful if you have a clear leader who is coordinating all activities.

2) Document the laws, regulations, industry standards, contractual obligations and policies with which your organization must comply. Big task? Yes, if you give it to just one person. Be sure to recruit help from all key stakeholders to be as comprehensive as possible. I've helped organizations to perform such tasks, so remember there is outside help available if you need it.

3) Do an information security risk assessment in conjunction with a privacy impact assessment (PIA) to determine and rank, as much as possible, identified risks. A

common link within most compliance requirements is to establish controls that are appropriate for the organization's identified information security and privacy risks.

4) Map the compliance requirements to the identified risks. It is typically best to use the most stringent of common compliance requirements topics when doing the mapping. As a very simplistic example, if you have ten different password length requirements that range from using a minimum length of five characters to using a minimum length of eight alpha-numeric-special characters, then it is usually best to go with the latter; it would then not only meet but exceed all the other less-stringent requirements.

5) Create a unified risk mitigation plan that protects information assets while also meeting core compliance requirements. Use standards, such as ISO/IEC 27001, the OECD privacy principles and applicable NIST publications, to identify controls that will address the risks and core compliance requirements in a unified way; this reduces costs and increases the effectiveness and scope of security and privacy programs.

Core compliance commonalities ($C^{\wedge 3}$)

There are significant common core requirements across the many laws, regulations and industry standards that organizations should recognize and use as keystones within their information security and privacy programs. Organizations can use internationally-accepted and industry standards to address the requirements in a unified way to reduce costs, save time and increase the effectiveness and scope of information security and privacy programs. A single, good, comprehensive plan will meet the following core requirements, within three broad categories, of most common compliance requirements.

Administrative compliance requirements

1) **Formally established information security and privacy management program**. Would include requirements for risk analysis, risk management, policies, roles and responsibilities, measuring effectiveness and so on.
2) **Assigned responsibilities**. Formally documented and assigned roles responsible for information security and privacy governance and compliance, as well as responsibilities for different positions throughout enterprise. Establish and document responsibilities and obligations for information security and privacy activities.
3) **Information security and privacy policies and procedures**. Documented policies and procedures establish enterprise expectations. For examples, plans for identifying and responding to security incidents and privacy breaches; directives for building security and privacy controls into the entire systems and applications development process, and so on.
4) **Workforce security**. Background checks, pre-employment vetting, access authorization, supervision, clearance, termination, separation of duties, considerations for outsourcing and consulting services, supervision strategies, team development and communication, exit procedures, budgeting, recruiting, job definitions, performance discipline, and so on.
5) **Access controls**. Determining access to information assets based upon job requirements and the "minimum necessary" concept.

6) **Contingency planning.** Requirements and procedures for data backups, business continuity and disaster recovery planning, emergency operations, testing and revising plans, business impact assessments, and so on.
7) **Evaluations**. Determining policy and controls effectiveness, awareness levels, compliance progress and so on.
8) **Contracts**. Including detailed information security and privacy requirements within contracts and other written agreements.
9) **Awareness and Training**. Providing effective regular information security training and ongoing awareness communications.

Operational and physical compliance requirements

10) **Facilities**. Establishing access controls to buildings, work areas and all types of information assets.
11) **Business Continuity**. Keeping business going and maintaining customer access to information as much as possible, regardless of adverse situations and conditions.
12) **Monitoring and Reporting**. A key regulatory compliance activity that's fundamental to being able to collect data and report on the condition and successes of the activities, applications, and other processes being monitored.
13) **Records Management**. Establishing procedures and processes to classify information, and then retain specific types for required specified periods of time. Covers all types of records, in hard copy as well as electronic forms. A task often overlooked.
14) **Workstation areas**. Securing confidential information and appropriately protecting authorization credentials and electronic access in employee work areas.
15) **Device and media controls**. Ensuring appropriate and secure storage, disposal, media reuse, accountability, and so on.

Technical compliance requirements

16) **Access controls**. Unique and non-shared user accounts, IDs and passwords, automatic account locks, encryption, firewalls, endpoint access and so on.
17) **Audit controls**. Establishing logs, monitoring activities, generating access and modification reports, flags for changed data, alarms for inappropriate changes and so on.
18) **Integrity controls**. Controls to allow only properly authorized accounts to make changes to personally identifiable information and other sensitive data.
19) **Identification and Authentication controls**. Establishing individual accountability through acceptable identification mechanisms and authentication technologies.
20) **Transmission security**. Appropriately using secured VPNs, SSL, HTTPS, and other types of encryption and controls to protect data in transit.
21) **Storage security**. Encryption, passwords, access controls, and other technologies to safeguard data in storage.

Generally, if organizations mitigate risks through implementing appropriate safeguards in these twenty-one areas, they will find most compliance requirements have been addressed.

Unified compliance is more effective and efficient compliance

Increasing numbers of laws, regulations, industry standards, contractual obligations and organizational policies requires information security and privacy practitioners to view their job responsibilities as also including compliance enforcement activities. Increasing fines, penalties and other types of sanctions make it increasingly important to implement comprehensive enterprise-wide information security and privacy practices.

By using a unified approach to information security and privacy compliance, organizations can more effectively manage the growing number of compliance requirements. A unified approach to information security and privacy compliance allows organizations to not only address identified risks, but also to comply with legal requirements.

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI, The Privacy Professor ®, is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. See more about her services and awareness and training products at http://www.privacyguidance.com. She can be reached at rebeccaherold@rebeccaherold.com. She will be giving her 2-day class which covers unified compliance at the CSI conference in October!