CHAPTER 19

Working with Compliance Auditors and Regulators

NOT ONLY DO YOU HAVE TO CONTEND WITH MEETing your own, internal IT-security standards, but you also have to face a wide array of government regulations and industry standards. Sometimes, it seems like you spend more time and resources on complying with these regulations and standards than on actually doing any business.

Regulations vary from country to country and from state to state within the U.S. On top of all that, additional, industry standards exist to be followed, such as the PCI DSS for companies that issue or accept credit cards (meaning almost every company today). Although it's not a government body, the PCI Security Standards Council wields as much power as one. In the worst-case scenario, it will ban a noncompliant company from using credit cards at all.

Furthermore, if you do business globally, you'll have additional sets of regulatory headaches.

Despite the thicket of different regulations, similar threads run throughout all of them. Organizing your security program along these lines will provide a good first step toward meeting any compliance mandate, even new ones that may arise.

Important

Bear in mind that compliance doesn't equal security. Some regulations do offer a good framework that, if followed to the letter, will take your company far on the road to achieving a high level of information security. However, checking off everything on someone else's checklist will not meet your internal IT-security requirements. You'll need to keep your eye on your own security program while making sure that it meshes with the compliance requirements — a delicate balance, indeed, at times.

Here is a sample of the most common government regulations and industry standards that you'll most likely face in the U.S.:

- *The Sarbanes-Oxley Act (SOX)*. Governs financial institutions and the financial controls that they use to ensure the accuracy of their accounting records. These controls include the IT-security controls that protect those records from unauthorized alteration or disclosure.
- *The Graham-Leach-Bliley Act (GLBA)*. Consists of regulations for protecting customer data in financial institutions.
- *The Health Insurance Portability and Accountability Act (HIPAA)*. Governs the protection of patient data in the health care industry.
- *The Federal Financial Institutions Examination Council (FFIEC) guidelines*. Regulates the financial industry and contains mandates for protecting online banking transactions. These guidelines are distributed by the Office of the Comptroller of the Currency (OCC), which regulates banks and reviews IT-security controls, among its other oversight functions.
- *California SB 1386*. Governs the privacy of customer information and the disclosure of breaches for any business that is operating in California.
- *The Payment Card Industry (PCI) Data Security Standard (DSS)*. Regulates companies that issue or accept credit cards. PCI is an

industry body that consists of the five largest credit-card companies (Visa, MasterCard, Discover, American Express, and JCB).

Outside the U.S., some of the most common regulations and regulatory bodies are

- In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA)
- In the EU, Directive 95/46/EC (governs the personal protection of data)
- In the EU, Basel II
- The Hong Kong Monetary Authority
- The Monetary Authority of Singapore

So, how do you comply with all these regulations but prevent your staff from trading other, productive work for the constant gathering of the information that keeps the regulators at bay?

One strategy is to implement an overarching security framework that covers all the bases. Three of the most common are ISO 27001, COBIT, and INFOSEC from the National Security Agency (NSA). These frameworks provide excellent guides for benchmarking an information security program, and strict adherence also ensures compliance with most of the elements of the regulations just cited.

But even if you use these frameworks, you'll still need to make sure that you're compliant with the fine points of each regulation that affects your company. Unfortunately, multiple regulations and overlapping requirements impact most companies. The good news is that these frameworks make it easier to sort out and simultaneously comply with the regulations and requirements.

Another strategy entails working with your internal auditors. Too often, an adversarial relationship exists between auditors and IT departments — particularly IT-security departments. Auditors are perceived as by-the-book nitpickers who interfere with daily operations and ask a lot of meddlesome questions. But, the reality is that auditors can be the allies who both work

with you to review your adherence to regulations and make sure that you're in top shape before the regulators come knocking on your door.

Here are the basics for preparing for auditors and regulators:

- Document everything. Auditors and regulators love documentation. Be prepared to produce documentation for all your security controls, processes, and activities. If you can't produce a document that proves something, you might find yourself up the creek.
- Document any deviations from regulations or standards. Explain why the exemption was granted; the business purpose; the effective dates; and the remediation plan, including implementation dates, that will be carried out when the exemption expires.
- Regularly audit your security procedures. Regulators tend to maintain regular audit schedules, even for reexamining systems that passed muster the last time around. The cycle for compliance with most regulations is annual, sometimes quarterly. Whatever it is, be proactive and audit yourself at least as often as the regulators will.

Rather than examine every regulation in detail, the following checklist contains the types of items that regulators and auditors generally look for — which correspond to some of the most-common points in many of the regulations.

1. Access management
    1.1. Reports of active user accounts
    1.2. Proof that inactive accounts have been audited and purged on a regular basis
    1.3. Logs of user access to systems
2. Data protection and privacy
    2.1. A privacy policy that is in place
    2.2. A demonstration of how customer data is secured
        2.2.1. Show that databases containing customer information have limited access and sensitive data encrypted.
        2.2.2. Explain how long data is kept for and how it's purged or destroyed after that.

3. Network security
   - 3.1. Details about how firewalls, routers, and gateways are secured
   - 3.2. Diagrams of all interfaces to third parties outside the company
     - 3.2.1. What data they carry
     - 3.2.2. How they're secured
   - 3.3. Details about how you monitor and test your network for vulnerabilities
     - 3.3.1. IDSs and IPSs
     - 3.3.2. Pen testing
4. Infrastructure and operating-system security
   - 4.1. Logs of the dates when every server and operating system has been patched
   - 4.2. An explanation of how the servers have been hardened and what services have been disabled
   - 4.3. Details about how antivirus and firewall protection is implemented
5. Web and application security
   - 5.1. Details about how security reviews are incorporated into the software-development life cycle
   - 5.2. Verification that software developers are following the OWASP guidelines for secure coding practices and that they have received training to that effect
   - 5.3. The results of Web and application server scans along with your testing schedule
   - 5.4. Evidence that your Web and application servers have been hardened and patched
6. Physical security
   - 6.1. Confirmation that all facilities containing IT equipment and sensitive data are properly locked down, guarded, and secured from malicious access by outsiders
7. Your information security policy
   - 7.1. An information security policy that can be produced on demand

8. Security awareness training
   8.1. Reports indicating that all employees have taken a basic security awareness training class every year

   8.2. Confirmation that the class covers the basics of both handling confidential information and protecting against social engineering

Note

The brief and succinct PCI DSS serves as a good guide to what is contained in the more lengthy and detailed regulations. For its requirements, see *https://www.pcisecuritystandards.org*. For particulars about the OWASP guidelines, see *http://www.owasp.org*. For a good reference book about the auditing process, see *IT Auditing: Using Controls to Protect Information Assets* (Chris Davis, Mike Schiller, and Kevin Wheeler; McGraw Hill, 2007).