



# A Unified Approach to Information Security Compliance

By M. Peter Adler

The information age has led to a heightened concern that personal information is not being protected. The high speed at which private information can be used and shared, often without permission, enables and increases the possibility of identity theft and other unauthorized uses of personal information.

Initially, self-regulation through the implementation of good security practices was thought to be the way to protect electronic personal information. In the latter part of the twentieth century, a sectoral approach to information security regulation started to gain favor with the passage of laws protecting health and financial information. However, between February 2005 and July 2006, there were 237 reported security breaches involving the compromise of more than 89 million records containing personal information.<sup>1</sup> Of these, 83 incidents involved institutions of higher education, including academic medical centers. The number of reported security incidents demonstrates that self-regulation has generally failed.

*M. Peter Adler, JD, LL.M., CISSP, CIPP, is President of Adler InfoSec & Privacy Group LLC and former Chief Information Security Officer at the University of Colorado.*

## A piecemeal approach may also undermine the integration of information security compliance into other institutional compliance programs.

As a result, controlling risks to personal information through enhanced information security has become the subject of state and federal laws. The recent upsurge in the number of state and federal laws and regulations represents an emerging legal standard that imposes obligations on colleges and universities to protect the data they collect, store, process, use, and disclose. These laws increasingly affect how higher education institutions, often operating in multiple jurisdictions, handle personal information, including sensitive health and financial data. Many of the new laws require disclosures to victims when there is unauthorized access to systems containing sensitive information. Failure to protect this type of information will inevitably result in public embarrassment and the financial costs associated with managing the response to incidents and may also result in investigations, fines, and other penalties.

Colleges and universities facing these growing legal obligations are often perplexed about how to comply with so many laws and regulations. Many do not approach information security compliance in an organized and integrated fashion. Some have permitted information security compliance to be handled by more than one department. For example, the health center or the university hospital may be tasked with Health Insurance Portability and Accountability Act (HIPAA) compliance, the registrar may be held responsible for the privacy of student educational records under the Family Educational Rights and Privacy Act (FERPA), while the financial aid office or departments using credit cards may focus on compliance with the Gramm-Leach-Bliley Act (GLBA) or the Payment Card Industry Data Security Standard (PCIDSS). Complicating these efforts are regulatory requirements affecting numerous institutional departments, such as research facilities, as well as external business partners. As a result, efforts are often incomplete, redundant, or inadequate and expensive.

A piecemeal approach may also undermine the integration of information

security compliance into other institutional compliance programs, such as information privacy and institutional governance. For example, a decentralized approach to information security could make it harder to monitor and report the controls that are increasingly a part of institutional audits. For all of these reasons, colleges and universities need to consider undertaking a unified approach to information security compliance.

### Information Security Laws and Regulations

A number of state and federal laws and regulations suggest or impose an obligation on colleges and universities to create and maintain an information security program.

#### *Family Educational Rights and Privacy Act (FERPA)*

The federal Family Educational Rights and Privacy Act of 1974 (FERPA) provides a postsecondary student the right to inspect his or her education records and establishes conditions concerning the disclosure of those records to third parties. Although the act does not specifically require that information security be implemented, the protection of electronic student records will require information security covering the student records subject to this federal law.

#### *Gramm-Leach-Bliley Act (GLBA)*

Under the Gramm-Leach-Bliley Act (GLBA), the Federal Trade Commission (FTC) has jurisdiction over the activities of higher education institutions. The FTC regulations contain both privacy and security requirements. Colleges and universities that comply with FERPA will be deemed by the FTC to be in compliance with its privacy provisions. However, educational institutions remain subject to the GLBA security provisions as found in the FTC safeguard regulations (“FTC Safeguards”), which became effective on May 23, 2003.

Under the FTC Safeguards, higher education institutions are to implement security measures to protect “customer

information” that is personally identifying—information such as names, addresses, account and credit information, and Social Security numbers. This most often applies to higher education in the area of student loans but may also apply when credit cards or other loans are issued directly to students.

The FTC Safeguards are aimed at ensuring the security and confidentiality of customer information. Higher education institutions are required to protect against any anticipated threats or hazards to the security or integrity of such records and to protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to the person noted in the record. To comply, colleges and universities must develop comprehensive information security programs, assess the need for employee training, and include obligations in their agreements with third parties that have access to the financial records covered by the rules. Although the FTC has not begun enforcement actions against higher education institutions, it demonstrated a willingness to pursue noncompliance when it charged three mortgage companies for not following the FTC Safeguards.<sup>2</sup> Among other things, the consent order in each of these cases requires the company to retain an independent professional to certify, within 180 days, that its information security program meets the standards listed in the order and also to make this certification every other year for ten years.

#### *The Health Insurance Portability and Accountability Act (HIPAA)*

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) contain both security and privacy provisions. HIPAA applies to covered entities that use certain electronic transactions—entities such as most health care providers, health plans, and health care clearinghouses. In the higher education arena, HIPAA most often applies to clinics used by both students and staff and to academic medical centers. The security

## Taking a unified approach to information security compliance would require an institution to adhere to the most stringent state law in order to comply with all of them.

regulations of HIPAA require covered entities to protect specific types of individually identifiable health information kept in electronic form, referred to as Electronic Protected Health Information (EPHI). To comply with the HIPAA security regulations, covered entities are to protect systems that store, process, and transmit EPHI. Entities must conduct periodic risk analyses to determine and implement reasonable and appropriate administrative, physical, and technical safeguards. The security regulations also require the implementation of risk-management processes, including policies and procedures and other documentation and training.

Although HIPAA does not allow individuals to sue covered entities that do not comply with the law, it does provide criminal and civil penalties for noncompliance.

### *The California Law on Notification of Security Breach (SB 1386)*

The California Law on Notification of Security Breach (SB 1386) applies to people, businesses, and government agencies, including colleges and universities. The law requires that whenever a security breach results in the potential compromise of certain personal information, notice must be given to any “data subjects” who are residents of California.

The type of personal information that triggers the notice requirement under this California law includes name (first name or initial and last name) plus any of the following:

- Social Security number
- Driver’s license or California Identification Card number
- Financial account number or credit/debit card number (along with any PIN or other access code where required for access to the account)

Notice must be provided as soon as possible. However, a delay in notifying may be permitted if legitimate law enforcement agencies determine that giving notice to the data subject would

impede a criminal investigation. Notice may also be delayed if the organization suffering the breach is taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system.

The California Office of Privacy Protection published recommended practices to comply with the California Law on Notification of Security Breach. The recommended practices are divided into three parts: (1) Protection and Prevention; (2) Preparation for Notification; and (3) Notification. The recommended practice of Protection and Prevention contains a number of best practices regarding information security and incident response, including most of the security practices and procedures required by GLBA and HIPAA.

Thirty-two states have passed similar legislation since California SB 1386 became law in July 2003.<sup>3</sup> Yet because most of the notice of security breach laws apply to a state’s citizens, colleges and universities have been required to respond to security incidents regardless of whether a local state law exists. Taking a unified approach to information security compliance would require an institution to adhere to the most stringent state law in order to comply with all of them. In addition, the federal government is contemplating a national notice of security breach law, which could preempt state law.

### *FDA Rule on Electronic Records and Electronic Signatures (21 C.F.R. Part 11)*

In 1997, the U.S. Food and Drug Administration (FDA) issued 21 C.F.R. Part 11, which consists of regulations that provide criteria for the acceptance of electronic records. These criteria include specific information security and electronic signature practices. Part 11 applies to electronic records that are created, modified, maintained, archived, retrieved, or transmitted under any FDA regulations. Part 11 also applies to electronic records submitted to the FDA under the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in

FDA regulations. Therefore, it applies to most aspects of research, quality assurance, clinical activities, manufacturing, and distribution of drugs, biologics, and devices. Virtually anything over which the FDA has jurisdiction, as well as some items subject to Public Health Service purview, is covered by the terms of Part 11. Therefore, higher education entities that conduct research under the jurisdiction of the FDA or the Public Health Service must comply with these regulations when submitting electronic records.

Organizations subject to these regulations are required to identify all information systems and applications covered by the regulations, develop a plan for bringing the systems and applications into compliance, and demonstrate that all of the items contained in the plan have been accomplished. The FDA recently issued guidance for organizations to follow when implementing compliance with 21 C.F.R. Part 11. Although the guidance contains only nonbinding recommendations, the FDA’s current approach is to interpret Part 11 narrowly and to use discretion in enforcing the requirements for validation, audit trails, record retention, and record copying. Enforcement discretion will also be applied to all organizations using “legacy systems,” which are those systems that were operational before the effective date of Part 11 (August 1997). However, the FDA guidelines state that the FDA intends to enforce all other provisions of Part 11, including the following controls and requirements:

- Limiting system access to authorized individuals
- Use of operational system checks
- Use of authority checks
- Use of device checks
- Determination that those who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks
- Establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures

## A close review of newer statutes, regulations, and cases demonstrates that this emerging legal standard for information security closely resembles other established information security standards.

- Appropriate controls over systems documentation
- Controls for open systems corresponding to controls for closed systems
- Requirements related to electronic signatures

Organizations that are not using legacy systems and that fail to comply with the above controls could be subject to an FDA enforcement action, including seizure, injunction, and debarment. For example, in a warning letter sent to a college that was found in violation of the Federal Food, Drug, and Cosmetic Act, the FDA Detroit District director wrote:

In addition to the above listed violations, our Investigator noted that the laboratory is using an electronic record system for processing and storage of data from the atomic absorption and HPLC instruments that is not set up to control the security and data integrity in that the system is not password controlled, there is no systematic back-up provision, and there is no audit trail of the system capabilities. The system does not appear to be designed and controlled in compliance with the requirements of 21 CFR, Part 11, Electronic Records.<sup>4</sup>

Compliance with this regulation can be achieved by following a unified approach to information security compliance.

### *The Payment Card Industry Data Security Standard (PCIDSS)*

In addition to the foregoing laws and regulations, the payment card industry recently created a private contractual compliance requirement: the Payment Card Industry Data Security Standard (PCIDSS). The PCIDSS requires that all merchants, including colleges and universities, that use credit cards comply with a number of technical, physical, and administrative requirements. Failure to comply with the PCIDSS could result in large penalties and suspension of the right to use credit cards for payment purposes.

### Putting It All Together

#### *The Emerging U.S. Legal Standard*

Although the laws and regulations noted above collectively represent an emerging legal standard, they rarely specify the information security measures that colleges and universities should implement in order to satisfy that standard. Most of the laws and regulations simply state that covered entities are to establish and maintain “reasonable” or “appropriate” security procedures, safeguards, or countermeasures. Further guidance or specific direction is not provided.

Yet a close review of newer statutes, regulations, and cases demonstrates that this emerging legal standard for information security closely resembles other established information security standards. One example of an established standard is the “800 series” issued by the National Institute of Standards and Technology (NIST). Another is the International Standards Organization (ISO) Framework of Security: ISO 17799. Under both the ISO standards and the NIST standards, management of information security requires the following:

- *Asset Identification and Assessment:* Identify the information and physical assets that must be protected within an organization
- *Risk Assessment and Analysis:* Conduct an assessment of the risks and analyze them against the probability of occurrence
- *Implementation of Safeguards to Counter Identified Risks:* For risks that are identified as having a high probability of occurring, implement reasonable and appropriate safeguards to lower the probability to an acceptable level
- *Addressing Third-Party Security through Contracts or Service Provider Agreements:* Control potential risks created by third parties through the use of contracts that require third parties to implement reasonable and appropriate safeguards when they process, store, use, or transmit organizational assets
- *Training:* Train students, faculty, staff, and third parties on policies and

procedures and other safeguards and security practices to protect organizational assets

- *Monitoring and Testing:* Regularly monitor and test the effectiveness of implemented safeguards against known or potential risks
- *Reviewing and Revising the Information Security Program:* Review and revise the information security program when safeguards are no longer effective against known or potential risks

The above steps represent a commonly accepted process for security of information and other assets within an organization. It is a process found in HIPAA and 21 C.F.R. Part 11 and GLBA. The process has been adopted in the consent orders issued as a result of FTC actions. It is also found in the contractually required PCIDSS. Rather than mandate specific security measures, each of these laws and regulations advocates the process of assessment and analysis and selection of safeguards that are appropriate for a set of potential risks.

The lack of hard-and-fast rules regarding which specific information security measures an institution should implement to satisfy its legal obligations has puzzled many lawyers and compliance officers. Security professionals are more comfortable with the emerging information security legal standard because for years, they have implemented measures that are reasonable when measured against identified risks to achieve the desired level of security. Since this process is the same under all U.S. information security laws and regulations, compliance with all may be achieved by undertaking a unified approach to information security compliance.

### *Meeting the Emerging Legal Standard through a Unified Approach*

Institutions that follow a unified approach to information security compliance will be ensured of an efficient and cohesive method to achieve and maintain information security protections. As mentioned above, a unified approach is effective

because HIPAA, the FTC regulations for GLBA, 21 C.F.R. Part 11, PCIDSS, and the laws on notice of security breach (e.g., California's SB 1386) specify or suggest many of the same security risk analyses and management practices (see Table 1).<sup>5</sup>

Again, by using a unified approach to information security compliance, institutions subject to multiple information

security laws, regulations, and guidelines will be able to comply with all of them at one time. This is accomplished by determining which laws and regulations are applicable, conducting a risk analysis that covers those laws and regulations, and then implementing at least the minimum level of required safeguards. When there are conflicting state laws, as found in the

notice of security breach laws, compliance should focus on the most stringent law applicable to the affected data subjects.

*A Typical Information*

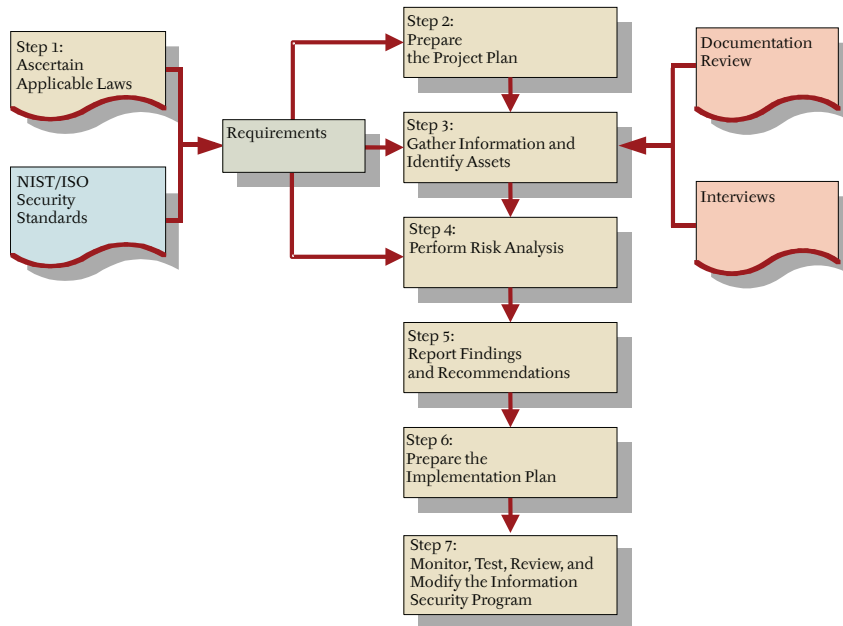
*Security Compliance Assessment*

To demonstrate how a unified approach works, this section describes the steps in a typical approach to conducting an

**TABLE I. SUGGESTED SAFEGUARDS**

SECURITY PRACTICE (E.G., ISO 17799 OR NIST 800)	HIPAA STANDARDS	GLBA (FTC REGULATIONS)	21 C.F.R. PART 11	PCIDSS	LAWS ON NOTICE OF SECURITY BREACH (GUIDELINES)
<b>ADMINISTRATIVE SAFEGUARDS</b>					
<b>Security Management Process</b> (e.g., risk analysis, risk management, periodic reviews of effectiveness)	✓	✓	✓	✓	✓
<b>Assigned Security Responsibility</b> (e.g., partial or complete assignment of responsibility for protection of information)	✓	✓	X	✓	✓
<b>Workforce Security</b> (e.g., authorization and/or supervision of workforce or contractors, clearance and termination procedures)	✓	✓	✓	✓	✓
<b>Management of Information Access</b>	✓	✓	✓	✓	✓
<b>Security Incident Procedures</b>	✓	✓	X	✓	✓
<b>Contingency Planning</b> (e.g., data backup plan, disaster recovery plan, emergency mode operation plan, testing and revision procedures, applications and data criticality analysis)	✓	✓ (in general terms)	X	✓	✓
<b>Evaluation</b> (e.g., opinion of compliance)	✓	X	X	✓	X
<b>Contracts</b> (e.g., extension of information security through contracts or other written arrangement)	✓	✓	X	✓	✓
<b>Security Awareness and Training</b> (e.g., security reminders, training on malicious software protection, log-in monitoring and password management)	✓	✓	✓	✓	✓
<b>PHYSICAL SAFEGUARDS</b>					
<b>Facility Access Controls</b> (e.g., contingency operations, facility security plan, access control and validation procedures, maintenance records)	✓	✓ (in general terms)	X	✓	✓
<b>Workstation Use and Security</b>	✓	✓ (in general terms)	X	✓	✓
<b>Device and Media Controls</b> (e.g., disposal, media reuse, accountability)	✓	✓	X	✓	✓
<b>TECHNICAL SAFEGUARDS</b>					
<b>Access Controls</b> (e.g., unique user identification, emergency access procedure, automatic logoff, encryption and decryption)	✓	✓	✓	✓	✓
<b>Audit Controls</b>	✓	✓	✓	✓	✓
<b>Integrity Controls</b> (e.g., mechanism to authenticate data)	✓	✓	✓	✓	✓
<b>Person or Entity Authentication</b>	✓	✓	✓	✓	✓
<b>Transmission Security</b> (e.g., integrity controls or encryption)	✓	✓	✓	✓	✓

**FIGURE 1. A TYPICAL INFORMATION SECURITY COMPLIANCE ASSESSMENT**



information security compliance assessment (see Figure 1).

**Step 1: Ascertain Applicable Laws and Regulations**

The first step in the process is to determine the laws, regulations, and guidelines applicable to the institution. As the foregoing discussion on the growing number of laws and regulations illustrates, this is an important preliminary step. This determination not only will assist in preparing the project plan but also will guide the person conducting the assessment in selecting the information to be collected and the type of risk analysis that should be performed.

Identifying the appropriate law is not always a straightforward process. Depending on their activities and operations, higher education institutions can be affected by a number of laws. In addition, some regulations apply only to specific departments or activities within an institution. In other cases, one or more state laws on the same subject may be applicable. Once the applicable law is determined, an appropriate information security risk analysis model, such as ISO 17799 or NIST 800 Series, should be selected. The model to be used will depend on the applicable laws and regulations, as well as the information security goals of the institution.

The following are some of the threshold questions that should be asked:

- Are student records kept electronically? What type of information is stored?
- Does the higher education institution provide health care services to students, faculty, and staff? Are electronic transactions used for payment or other purposes?
- Does the higher education institution use credit cards for payment purposes?
- What type of research information is stored on computer systems? Is this information centralized, or is it dispersed across the institutional system?
- Does the higher education institution conduct research that directly involves electronic filings with the FDA?
- What state notice of security breach laws may be applicable?
- Does the university or college have international campuses? If so, what types of personal information are transferred between the U.S. and foreign facilities?

**Step 2: Prepare the Project Plan**

After the legal and regulatory requirements are identified, a thorough project plan is prepared. This document is used to guide the project, providing schedules, tasks, and milestones. The project plan

will identify resources and include periodic briefings and reports to the administration and other stakeholders.

**Step 3: Gather Information and Identify Assets**

Information gathering includes the identification of assets to be protected, document review, and interviews with both management and other stakeholders. The individuals who are interviewed may be department personnel, IT staff, senior management, legal counsel, audit and compliance personnel, risk management staff, and facilities management personnel. The scope of the interviews will differ slightly, depending on the state, federal, and international laws and regulations that are applicable.

The discovery process will review technical, physical, and administrative security practices. Technical security includes vulnerability scanning and configuration analysis, as well as assessment of system policies and network architectures. Physical security includes the protection of information security facilities, the safeguarding of portable media and laptop computers, and media disposal practices. Administrative security includes information security infrastructure, governance, management effectiveness, policies and procedures, and existing compliance efforts.

Information gathered in this step also includes written policies and procedures, Internet policies and procedures, sanctions and disciplinary procedures, and other documents evidencing institutional efforts to protect personal information, documents such as business associate contracts, procedures for assigning, modifying, or removing access rights, and password-management policies.

In addition to the threshold legal inquiries stated above, the discovery process should, at a minimum, cover the following areas:

- The individual(s) responsible for information privacy and security within the institution
- Information and other assets that the institution needs to protect in order to ensure continued business operations
- How the information security function is structured within the institution;

## Students, faculty, and staff require training to be educated on their responsibilities concerning safe and secure information-processing practices.

how policies and procedures are to be implemented and integrated with current compliance activities

- How well departments work together to ensure that information security practices are uniform; which third parties have access to the institution's information system
- What type of personal information is used and disclosed by the institution
- What contractors and other organizations receive personal information from the institution
- The future plans and proposed budget for improving information security within the institution
- How change management methodologies can be optimized to implement a comprehensive information security compliance program

### Step 4: Perform Risk Analysis

In this step, the information gathered in Step 3 is integrated into the selected risk analysis. The quality and effectiveness of risk analysis results will depend heavily on how well Step 3 was accomplished. The risk analysis includes technical, administrative, and physical security including organizational considerations and third-party contracts (e.g., business associate contracts, service provider agreements). In this way, compliance requirements for third-party contractors are integrated into the overall information security compliance efforts. Current contracts are reviewed, and if necessary, model third-party contracts containing necessary safeguard provisions are provided.

### Step 5: Report Findings and Recommendations

The results of the risk analysis are documented in a risk analysis report in this step. The report should list identified threats and vulnerabilities, as well as the safeguard selection criteria. To demonstrate due diligence, the report should include and reference specific portions of the applicable security regulations. To maximize effectiveness, the risk analysis report should also contain a plan and a schedule for implementing the changes

necessary to enhance information security and to attain compliance with applicable laws and regulations.

### Step 6: Prepare the Implementation

#### Plan for Selected Safeguards

The implementation plan provided in the risk analysis report is put into effect in this step. The plan should encompass all the safeguards identified in the risk analysis and also include procedures for the selection of security system vendors and the installation of security equipment.

At this stage of the compliance process, it is important to integrate those measures implemented for information security compliance with other compliance efforts currently under way within the institution, including those required by other state and federal laws. The integration of compliance programs will ensure uniformity and avoid redundancy. For example, time, money, and other resources may be saved by using existing policies and procedures to comply with the information security regulations.

A key safeguard is information security training. Students, faculty, and staff require training to be educated on their responsibilities concerning safe and secure information-processing practices. Training should also include timely and periodic updates to emerging U.S. and state information security laws.

### Step 7: Periodically Monitor, Test, Review, and Modify the Information Security Program

Information security operations and management are ongoing processes. Given the changing nature of technology, institutions should regularly monitor and test the effectiveness of implemented safeguards against known or potential risks. Doing so involves testing areas of the network or applications against emerging risks and suggesting corrective action when vulnerabilities are discovered. Institutions should also perform periodic risk analysis to validate that safeguard selection and implementation features continue to be reasonable, appropriate, and effective.

### Special Considerations in Following a Unified Approach

The environment at colleges and universities has not been conducive to the centralized management of information security, due mainly to historical and practical considerations. This point is stated often in the 2003 EDUCAUSE Center for Applied Research (ECAR) study "Information Technology Security: Governance, Strategy, and Practice in Higher Education," which notes:

In many collegiate environments, particularly larger ones, a decentralized culture is the norm. As a result, individual schools, laboratories, and departments may control a portion of any or all of the previously mentioned IT assets, making the job of the IT security administrator much more difficult. Rather than being able to automatically push new security patches out to all devices on the network or mandate the use of security tools like virus protection software, many university IT security officers find they must educate and persuade their user community to keep their machines secure.<sup>6</sup>

Nevertheless, the only way toward an effective institution-wide information security program is to be certain that all system users understand and follow basic and sound information security practices. Rather than imposing a centralized information security model as found in corporate IT departments, many higher education institutions are following a model referred to as "embraced autonomy." Under the embraced autonomy model, campuses and other constituents work with an Information Security Officer (ISO) or other central authority to assess and implement reasonable and appropriate information security practices. This requires participation by campuses, branches, colleges, departments, and offices within the institution. Although the exact approach to be followed will depend on the organizational structure of each higher education entity, this model

often utilizes an information security committee comprising all key data holders, users, and processors.

Once the scope of the institution-wide information security program is identified, the standards to be implemented must be identified through a collaborative process, usually led by the ISO. In this way, all stakeholders will be more likely to accept the policies, procedures, and guidelines. Implementation of the standards is managed locally, with assistance from the ISO, who takes action only if the local implementation is not accomplished according to standards.

### Conclusion

The increased number of government-mandated and private contractual information security requirements has caused higher education security professionals to view information security as another aspect of regulatory or contractual compliance. The existence of fines, penalties, or loss (including bad

publicity) has also increased the incentive to implement comprehensive information security practices. By adopting a unified approach to information security compliance, higher education institutions will be able to effectively manage the growing number of information security compliance programs. This approach begins by reviewing all of the information security requirements imposed by the emerging statutory, regulatory, and contractual legal standards. These standards are then compared with the more established national and international information security standards. After a thorough risk assessment and analysis, the legal standards and the information security standards are blended to create a complete information security compliance program. A unified approach to information security compliance thus enables colleges and universities not only to address identified risks but also to comply with the law. *e*

### Notes

1. "A Chronology of Data Breaches Reported since the ChoicePoint Incident," Privacy Rights Clearinghouse Web site, <<http://www.privacyrights.org/ar/ChronDataBreaches.htm>>, July 25, 2006.
2. *In re Sunbelt Lending Services*, FTC, File No. 042-3153 (November 16, 2004); *In the Matter of Nationwide Mortgage Group, Inc., and John D. Eubank*, FTC File No. 042-3104 (April 15, 2005); *In re Superior Mortgage Corp.*, FTC, File No. 052 3136 (September 28, 2005).
3. These thirty-two states are Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Washington, and Wisconsin.
4. Warning Letter from the FDA Detroit District Office to Earlham College, July 29, 2002, <[http://www.fda.gov/foi/warning\\_letters/g3419d.pdf](http://www.fda.gov/foi/warning_letters/g3419d.pdf)>.
5. FERPA is not included in this table because it does not have any specific security laws or regulations and will default to the ISO 17799 or the NIST 800 series.
6. Robert B. Kvavik and John Voloudakis, "Information Technology Security: Governance, Strategy, and Practice in Higher Education," *EDUCAUSE Center for Applied Research (ECAR) Study*, vol. 5 (2003), <<http://www.educause.edu/LibraryDetailPage/666?ID=ERS0305>>, p. 25.