Compliance Management

Table of Contents

Getting Started

The initial process in developing compliance initiatives is to identify which laws, regulations, and policies are applicable to your institution. To that end, confer with your legal and/or audit departments, and review the Higher Education Compliance Alliance Matrix, our brief list of the most common federal data protection laws, and the EDUCAUSE Library Compliance page for additional guidance and resources.

1. **Identify** key stakeholders and/or partners across the institution who regularly deal with institutional compliance issues (e.g., legal, risk management, privacy, audit). Key stakeholders may vary from campus to campus.
2. **Perform** a high level gap analysis of each compliance requirement that is applicable to determine where progress needs to be made.
3. **Develop** a prioritized action plan that will help you organize your efforts (one section of your Information Security plan).
4. **Develop** a policy, standard, roles and responsibilities, and/or procedures in collaboration with other key stakeholders at your institution.
5. **Take advantage** of resources in the Guide such as the Information Security Policies, Privacy, and Risk Management chapters, as well as the HEISC GRC FAQ.
6. **Familiarize** yourself with common standards and regulations that address specific requirements (e.g., PCI DSS, HIPAA, GLBA, NIST).
7. **Determine** whether Governance, Risk, and Compliance (GRC) solutions can assist you with managing compliance. Visit the EDUCAUSE IT GRC Program for additional resources.

Learn more about the General Data Protection Regulation (GDPR) and how it may affect your institution starting in May 2018.

- The General Data Protection Regulation Explained (August 2017 *EDUCAUSE Review* article by Barmak Nassirian)
- GDPR: A Data Regulation to Watch (August 2017 *EDUCAUSE Review* blog by Jaime Tuttle-Santana)
- GDPR: Twelve Steps, Sorted (Jisc blog post)
- Data Protection Reform website (Information Commissioner's Office)
- EU GDPR (EDUCAUSE Library resource page)

Top of page

Overview

Higher education institutions are subject to numerous laws, regulations, and contractual obligations that specify requirements related to the appropriate management and protection of diverse information sets.

Understanding and maintaining compliance with these different requirements is sometimes a difficult road. The path to establishing compliance takes a complete look at the areas in which your institution has responsibilities, whether legal, regulatory, contractual, or self-imposed.

This section of resources is intended to serve as a roadmap in an institution's quest for compliance. This resource is *not* intended to serve as legal advice. Specific guidance for specific institutional issues should be sought from campus legal counsel.

Important elements to consider when developing a plan for compliance management include the following:

- Awareness of relevant regulations/laws. (Do you know what you need to follow?)
- Awareness of relevant policies. (Do you know what institutional policies apply to information use?)
- Awareness of relevant contractual agreements. (Do you know what agreements your institution has made that impose conditions on the use of data?)
- Awareness of relevant standards or best practices. (Do you know what standards or best practices your institution chooses to follow with respect to information use?)
- Management of institutional records. (Do you know what you need to keep and for how long?)
- Awareness of how records are managed by your institution.
- Approach to complying with each item. (Do you know what your organization is doing to follow the law?)
- Awareness of internal and/or external audit activities. (Do you know what internal/external audits exist and what is required to meet or pass these reviews?)

Top of page

Compliance with Legal and Contractual Requirements

Objective: The goal of this section is to help outline effective practices for identifying compliance obligations, as well as the roles and responsibilities, activities, and controls needed to manage all of the institution's legal, contractual, and records management requirements.

Identification of Applicable Legislation and Contractual Requirements

Legal requirements need to be explicitly identified and recognized and a plan in place for meeting applicable requirements.

To meet this part of compliance, controls should be developed which:

1. Identify the persons or person responsible for ascertaining the legal requirements. Those requirements should then be placed against the other controls that exist in some sort of matrix which shows controls in place to meet the requirements.

EDUCAUSE has identified a group of federal laws and sample contract clauses to help start you on this task:

- Family Educational Rights and Privacy Act (FERPA)
- Human Subjects Research, including the Federal Policy for the Protection of Human Subjects ("Common Rule"). *Note that different federal agencies may have slightly different rules regarding human subjects research. Always check with your institutional research review board for additional guidance in this area.*
- Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. *Note that HHS developed a free security risk assessment tool.*
- Payment Card Industry Data Security Standards (PCI DSS)
- Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act; GLB Act; GLBA) Safeguards Rule
- Fair and Accurate Credit Transactions Act of 2003 (FACT Act; FACTA) which amended the Fair Credit Reporting Act (FCRA), and amendments thereof, including Red Flags Rule (Identity Theft Prevention Program)
- Standard Confidentiality Agreement or Statement
- Higher Education Opportunities Act of 2008 (HEOA) Technology Mandates (Including: illegal peer-to-peer file sharing, emergency notification, and distance education student verification.)
- International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) (e.g., Baylor University's Export Compliance Policy and Purdue University's Export Control Regulations)
- Digital Millennium Copyright Act (DMCA)

Additionally, nearly each state has breach laws, personal information protection laws, social security protections laws, or other laws related to technology furnished at every institution. Each state must be taken as its own legal island and an institution must know if any of the following impact or enhance security efforts. The National Conference on State Legislatures Privacy and Security site is a good starting place to research the laws relating to your state (including the latest on state security breach legislation).

2. Identify the persons or person responsible for reviewing contracts to determine any information security requirements, whether they are requirements of the institution or requirements of the vendor. Those requirements should then be placed against the other controls that exist in some sort of matrix which shows controls in place to meet the requirements.

Every contract that involves institutional data must be documented and any controls specified in that contract must also be documented. It is crucial to know what your institution's contractual responsibilities are so that you can look at the physical and technical controls you have in place and determine if they are adequate for the assumed contractual liability. In instances where contracting parties have access to institutional data, you want to be sure that you can audit the contractual controls and protections that the other party has agreed to follow.

Reference: Data Protection Contractual Language

Top of page

Intellectual Property Rights

Intellectual Property (IP) rights are a dominant issue at any institution of higher education. Institutions have many different types of research and proprietary information that can be protected via these rights. These rights are also attached to the different technologies that an institution might buy or license from others (and the rights are then protected via contract provisions). Appropriate controls to identify and protect intellectual property include:

- An intellectual property rights compliance policy (which meets copyright policy requirements of certain laws);
- Ensuring proper use of software and other technology licenses;
- Education and awareness on respecting IP rights;
- Keeping track of IP assets.

EDUCAUSE has significant IP and Copyright resources:

- Copyright Support and Guides
- Copyright Act of 1976
- Copyright and Intellectual Property Policies
- Copyright Infringement
- Copyright Term Extension Act (CTEA)
- Digital Millennium Copyright Act (DMCA)
- Fair Use
- Intellectual Property
- Licensing

Top of page

Protection of Organizational Records (Records Management)

Every institution deals with the issues inherent in managing organizational records and data, whether electronic or in paper. As part of the compliance controls at every institution, important records as well as records we are legally obligated to retain need to be protected from loss, destruction, and falsification.

ISO has a separate standard, ISO 15489, "Information and Documentation — Records Management." This standard goes into greater detail about how an institution recognizes the context in which records are created, received, used, stored, and destroyed as an implicit part of the data governance process.

This records management function may be placed anywhere in an institution, and sometimes it is part of an institution's IT structure. Regardless, records management has components of compliance that are unavoidable.

EDUCAUSE has excellent materials on records management, including an Electronic Records Management Toolkit. Regardless of the ownership of this function at your institution, as part of your information security purview there are information security considerations you need to be aware of:

- Your institution's policies and guidelines on retention, storage, handling, and disposal of records should be reviewed. Oftentimes this will require a security control to ensure that these policies and guidelines are carried out properly. (Refer to the Records Retention and Disposition Toolkit for additional information and templates.)
- Policies that protect records from loss, destruction, or falsification.

Top of page

Regulation of Cryptographic Controls

Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations. For more on this topic, visit the Encryption chapter.

Top of page

Information Security Reviews

Objective: Ensure that information security compliance requirements are effectively addressed and maintained over time.

In order to meet compliance requirements, it is necessary to continually review compliance methods, systems, and processes of departments that are affected by various policies, regulatory requirements, and laws to ensure that their approach to compliance is effective. For example, a particular credit card Point of Sale system (POS) can be implemented at a point in time on your campus, and your reviews may indicate that the application is in full compliance with PCI DSS. However, two years later, the payment application may no longer be considered fully compliant by the PCI SSC and if reviews aren't conducted on a recurring basis, this could result in noncompliance with PCI DSS requirements.

Top of page

Independent Review of Information Security

It is important to have unbiased reviews of information security organization programs and initiatives on a recurring basis in order to measure and ensure effectiveness. Often, these reviews are carried out by multiple parties: internal audit departments, external auditors, and assessments performed by contractors or consultants. It is also important that individuals performing reviews and assessments are qualified to do so. The primary objective of independent reviews is to measure effectiveness and ensure continuous improvements are made. In the event that your campus does not have an internal audit function, you may be able to develop a cooperative agreement with another campus or hire a consulting firm to conduct an audit and/or assessment of specific areas you need to have assessed. Note: For some institutions, an independent review may include representatives from legal counsel, an executive leadership team, and/or a system office.

Top of page

Compliance with Security Policies and Standards

Managers have compliance responsibility to make sure that applicable security procedures related to their area of control are implemented and performed correctly to achieve compliance with internal security policies and standards. Many campuses are considering the implementation of Governance, Risk, and Compliance (GRC) solutions to automate compliance reviews and reporting, as well as assisting with determining corrective actions that need to be managed. Take a look at the resource Frequently Asked Questions about Governance, Risk, and Compliance (GRC) Systems to help you determine if a GRC system is a good investment for your information security program. EDUCAUSE has additional resources on IT GRC.

Technical Compliance Reviews

Technical compliance reviews are also performed by many campuses. From vulnerability and DLP (data loss prevention) assessments to penetration testing, there are a number of technical solutions available to help information security teams conduct effective reviews of IT infrastructure and the information lifecycle (processing, transmitting, storing). Some of these tools can disrupt business and IT operations if used by untrained individuals, which leads some campuses to use third parties for these purposes. However, these examinations are just a 'snapshot' at a point in time and must be repeated at recurring intervals in order to become an effective method or process.

Top of page

Resources

Campus Case Studies On This Page
Identity Finder at The University of Pennsylvania

HEISC Toolkits/Guides

- Data Classification Toolkit
- Data Protection Contractual Language
- Electronic Records Management Toolkit
- List of Common Federal Data Protection Laws
- Records Retention and Disposition Toolkit

EDUCAUSE Resources

- Digital Millennium Copyright Act (DMCA)
- EDUCAUSE Policy
- Fair Use
- Federal Privacy Law
- FERPA
- Gramm-Leach-Bliley Act (GLBA)
- Higher Education Opportunity Act
- HIPAA
- ID Theft Red Flags
- PCI DSS
- Sarbanes-Oxley Act of 2002 (SOX) (*financial records*)
- Policy and Law (EDUCAUSE Resource Center)
- Campus Policy and Law (EDUCAUSE Resource Center)
- Licensing (EDUCAUSE Resource Center)
- State Policy and Law (EDUCAUSE Resource Center)

Initiatives, Collaborations, & Other Resources

- Export Control: Trade Compliance Basic Awareness presentation by Baylor University
- Higher Education Compliance Alliance Matrix
- Treasury Institute for Higher Education

Top of page

Standards

ISO	NIST	COBIT	PCI DSS	2014 Cybersecurity Framework	HIPAA Security
27002:2013 Information Security Management **Chapter 18**: Compliance **ISO 27799:2008** **ISO/IEC 27007:2011**	**800-100**: Information Security Handbook: A Guide for Managers **800-53**: Recommended Security Controls for Federal Information Systems and Organizations **800-14**: Generally Accepted Principles and Practices for Securing Information Technology Systems	**APO12.01** **APO12.02** **APO12.03** **APO12.04** **MEA03.01** **MEA03.04**	**Req 3** **Req 9** **Req 12**	**ID.GV-3** **ID.RA-1** **PR.IP-4** **PR.IP-12** **DE.DP-2**	None

Top of page

Questions or comments? Contact us.