Global Information Assurance Certification Paper

Using ISO 17799 as a Framework for Improving Data Management and Creating a Culture of Information Security in Higher Education

Christine Miller
SD Number: 719059
Certification: G7799
Version 1.1
NS 2004
March 21, 2005

Abstract

The following document describes the development of an ISO 17799 Information Security Management System (ISMS); goals include improving data management policies and procedures and integrating information security into the culture of Mead College. Mead College is a college of arts and sciences at a large, public university. Information security is about ensuring the confidentiality, integrity and availability of information. Data is pervasive, and developing an ISMS with an emphasis on information assets provides an opportunity to engage all personnel at all levels of the organization. In public universities, shrinking state budgets have resulted in greater financial accountability and increased emphasis on data and data driven decision-making. Therefore, an ISMS with a focus on data management will align with the mission and goals of the university and the college. The project will encompass policy development, asset classification, training and security awareness, risk analysis, risk management and auditing strategies. Identifying and mitigating human threats to information assets will be the primary focus of the project.

Part One: Define the System

Introduction

Information security could be defined as the art and science of securing information. Information assets such as data, applications and intellectual property are core assets. Without information, infrastructure, such as servers and networks, is reduced to property. Information assets make infrastructure mission critical. The ISO 17799 standard provides a flexible framework of best practices that will help any organization identify their information security strengths and weakness and begin a process of continuous improvement. Information security is not another information technology problem. Information security encompasses the entire organization: all internal and external entities, those that are authorized and those that are unauthorized. Information Security truly is everyone's job. Even in an organization with unlimited resources, creating a culture of information security will not occur overnight. The ISO 17799 standard provides a great place to start. The framework is one size fits all; implementation can be one size fits one.

Focus on Data Management and Information Assets

Information is a core asset, and every person or entity that interacts with an organization interacts with information. The development of an ISO 17799 Information Security Management System (ISMS) with a focus on data management presents a high impact opportunity for an organization with adequate, existing infrastructure controls. This ISO 17799 initiative will engage personnel at all levels of the organization and will begin the process of creating a culture of information security.

Organizational Overview

The ISMS for data management will be developed for a college of arts and sciences within a large, public university classified as a 'Doctoral/Research – Extensive' institution by the Carnegie Foundation. The college includes about 700

faculty, 300 staff members and 14,000 students. For the purposes of this exercise, the name of the college is Mead College, and the scope of this initial project will be limited to the administrative offices within the college including the Dean's Office. The college includes about 30 academic departments as well as a number of centers and programs encompassing the arts and humanities, social sciences, biological sciences and physical and mathematical sciences; the departments, centers and programs reside in 30 sites.

Mead College utilizes a distributed organizational model. The Dean's Office provides an oversight role and controls budgets as well as approvals for new and vacant state-funded positions and major acquisitions within the departments. Departments that earn grants have discretion over their grant funding. In many ways, the college represents a microcosm of the university at large. The university utilizes a federated model; some resources are centralized, some are decentralized and others are shared. The university includes both an Office of Information Security and a Chief Information Security Officer. These assets are still somewhat new to the environment; roles and responsibilities continue to evolve. Mead College plans to adopt and/or extend the policies and procedures defined by the university-level Office of Information Security. The plan will be developed with a specific environment in mind; at the same time, the system is based on a standard, and the principles and procedures should transfer to other environments.

Climate and Culture

Reductions in state funding have transformed public universities. Public research universities now place even greater emphasis on fund raising and external research funding. In many cases, public universities are doing as much or more with less. On the plus side, having less has made universities better stewards of state funds. Data integration and data driven decision-making have become preeminent concerns. This focus on data creates an opportunity to align the ISO 17799 initiative with institutional priorities that are relevant to senior management.

Traditionally, universities encourage the open exchange of information and ideas. In the information security age, this tradition creates lots of risks. Information security can be a hard sell in higher education. Universities often want to cling to a way of life that no longer exists. At the same time, universities are becoming more entrepreneurial. They want to protect the privacy of their consumers (students) and personnel (faculty and staff); they also want to protect their products (intellectual property and reputation). The current climate of reduced funding, greater entrepreneurialism and data-centricity provide fertile soil for information security in higher education.

Mead College Office of Information Technology (OIT)

Mead College Office of Information Technology includes five information technology professionals; each group member has a primary focus area and serves as a backup for one or more co-workers. The focus areas include leadership, desktop support, server and network administration, web design and web development.
Sidebar: Achieving separation of duties in a small group presents challenges. At some point, the university-level IT organization may provide resources such as central

logging. Most group members have attended some information security training such as Security+, SANS Security Essentials, SANS Security Leadership Essentials for Managers and SANS 17799 Security and Audit Framework. The system and network administrator currently serves as the primary unit-level information security officer.

Mead College Office of Information Technology serves as a source of leadership and sets standards and guidelines for technical support staff in academic departments. Within a year, OIT hopes to create a position that will allow the group to supply our academic departments with basic information security services such as awareness training and risk analysis/management. Most departments have one or two generalists who provide all technical support services within in the department. Most positions in the Mead College OIT have some college-level and some college-wide roles. Two group members participate in the campus-wide security committee that advises the Chief Information Security Officer. Another group member participates in an ad hoc committee with the charge to define best practices for developing secure applications.

At Mead College, the Office of Information Technology has built a positive relationship with the Dean's Office, and the Dean's Office traditionally supports OIT initiatives. In about a year Mead College administration will be moving to a new building which offers very little space for paper-based file storage. The Dean's Office is very likely to support the ISMS for data management because the need for an electronic document management system is self-evident, and the other provisions of the ISMS will be bundled with the document management project.

Scope

ISO 17799 isn't an all or nothing approach; as Hoelzer (2004b) says it allows an organization to take 'baby steps (p. 33).' Mead College already utilizes a number of best practices such as layered anti-virus, on and off site backups and vigilant patching of desktops and servers. At this time, clients perceive information security as OIT's responsibility. The purpose of this ISO 17799 initiative is two-fold: 1) begin the process of creating a culture of information security and 2) establish better policies and procedures for data management. Fortunately, these goals are complementary. In this initiative, information assets will be the primary information system, and identifying and mitigating human threats, intentional and unintentional, will be the primary focus of the project. The project will encompass policy development, asset classification, training and security awareness, risk analysis, risk management and auditing; all twelve steps of the ISO 17799 framework will be addressed.. At Mead College, the ISO 17799 framework will be used as a best practices framework; pursuing ISO 17799 registration is unnecessary for the organization at this time.

In the long-term Mead College OIT will rollout tested plans, policies and procedures that will help academic departments elevate the priority of information security within their units and begin the process of engaging in continuous information security improvement. *Caveat: A department such as Dance will have very different requirements than a department such as Biochemistry.* The recommendations in this document will give departments a starting point; some will need to do more.

Part Two: Plan

ISO 17799: A Twelve-Step Program

Every journey starts with a single step, and the ISO 17799 standard is no exception. The project will be completed during the next eighteen months.

Establish Importance

Based on the current climate and culture, the work of establishing the importance of planning an ISMS for information assets has already begun. Data-driven decision making is an institutional priority, and decision-makers have seen enough headlines in *The Chronicle of Higher Education* to recognize that the playing field has changed, incidents happen and incidents can create bad perceptions. No college wants to lose grant funding because research data becomes invalidated due to security issues. No college wants to be in the headlines as a result of FERPA (Federal Educational Rights and Privacy Act) or other privacy violations. *Sidebar: For more information on FERPA, visit http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.*

High Level Policy

The high level policy will establish senior management support for the ISO 17799 data management initiative. After ratification, the Dean's Office will kickoff the initiative and deliver a proclamation to all clients.

Draft: To ensure security of information assets and comply with legislation and university policy, Mead College shall adopt a holistic approach to data management. Policies, procedures, controls and audit strategies will be implemented to accomplish goals and facilitate data-driven decision making. Major initiatives will include document management, asset classification and awareness training.

Establish Security Organization

OIT will be the primary security organization. Each team member will take the lead within his/her focus area. Existing client groups will provide opportunities to create and maintain linkages with clients. The Dean's Office will have the role of sanctioning policy. Legal Affairs and other university-level offices will be consulted as necessary. The Mead College security organization will oversee future information security initiatives; therefore the mission and charter are general.

Mission: The Mead College security committee will support the mission of Mead College by serving in a leadership role and fostering a culture of information security and awareness.

Charter: The responsibilities of the security committee shall include the following:

- Protecting intellectual property and the privacy of our faculty, staff and students
- Engaging in continuous communication with clients and the broader community
- Developing policies, procedures and controls based on best practices and helping ensure compliance with federal, state and local legislation as well as university policies
- Conducting regular internal audits to assess the effectiveness of our policies, procedures and controls
- Creating opportunities for continuing education in the area of information

security for clients as well as technical support staff.

Policy Summary

Using the SMART methodology policies will be developed to address the identified risks. As per Hoelzer (2004a), SMART stands for specific, measurable, achievable, realistic and time-based (pp. 138 – 140). A policy summary table appears on the following page.

Table 1: Policy Summary					
All policies that apply to clients will include the development of documented procedures and/or training.					
All tasks assigned to Mead College OIT; a 'train the trainer' approach may be used in some areas.					
Policy	**Purpose**	**Audience**	**Areas**	**Status**	**Notes**
Access	Implement principle of least privilege for information assets in all forms. Create legal basis for internal and external unauthorized access. Physical access will also be addressed.	All Clients	Risk Mitigation	In progress	See also password management.
Code of Ethics	Encourage a culture of integrity.	All Clients	Risk Mitigation, Training and Awareness	In progress	Mandatory training and endorsement
Data Classification	Create awareness that we process and access different types of data; some data will require additional safeguards to protect privacy and comply with federal legislation.	All Clients	Identify and Classify Assets, Training and Awareness	In progress	Will adopt document management system to facilitate storage, retrieval and labeling of information assets.
Digital Storage	Address vulnerabilities of data stored or maintained on optical and magnetic media; address issues such as physical location and encryption as necessary.	All Clients	Risk Mitigation, Training and Awareness	In progress	
Digital Transmission	Address transmission of all data types in digital formats: Email, phone, fax, internal and external network.	All Clients	Risk Mitigation, Training and Awareness	In progress	
Media Sanitization	When media is transferred or sent to surplus, ensure sanitization. Comply with federal legislation; protect privacy of faculty, staff and students; protect research data and intellectual property.	System Administrators and Clients	Risk Mitigation	Complete; waiting for ratification by Dean's Office	
Non-digital Storage	Address vulnerabilities of data stored or maintained in paper format.	All Clients	Risk Mitigation, Training and Awareness	In progress	
Non-digital Transmission	Address transmission of all data types in non-digital formats: US mail, campus mail and hand delivery.	All Clients	Risk Mitigation, Training and Awareness	In progress	
Password Management	Implement password standards. Reduce the risk that passwords will be compromised.	All Clients	Risk Mitigation, Training and Awareness	Have informal standards	Need to formalize.

Patch Management	Reduce risk that OS and application vulnerabilities will be exploited.	System Administrators	Risk Mitigation	Standards exist	Need to audit standards periodically.

Identify and Classify Assets

At this time, Mead College does not have a classification system for information assets. The scope of this initiative will include data residing on both magnetic and optical storage media and paper as well as data transmitted via voice and data networks and 'snail mail.' All data qualifies as an information asset.

Table 2: Information Asset Classification System		
Label	Priority	Definition
Public	Low	All content published to our publics
Internal	Medium	Data subject to open records but intended for a specific individual or target audience
Protected	High	Private data such as student records that is not subject to open records

Mead College is located in Georgia, a state with open government and open records. State universities are subject to the open records act. As per the official codes of the state of Georgia posted at http://www.ganet.org/cgi-bin/pub/ocode/ocgsearch?docname=OCode/G/50/18/70:

> "All public records of an agency as defined in subsection (a) of this Code section, except those which by order of a court of this state or by law are prohibited or specifically exempted from being open to inspection by the general public, shall be open for a personal inspection by any citizen of this state at a reasonable time and place; and those in charge of such records shall not refuse this privilege to any citizen."

Identify and Classify Risks

In this phase, the ISO 17799 initiative will focus on human threats to information assets. A modified version of FMEA (Failure Mode Effects Analysis) will be used to conduct a risk analysis. According to http://www.fmeainfocentre.com/standards.htm, FMEA was originally developed by the auto industry. FMEA can be adapted to a variety of organizations. Appendix A includes the FMEA severity, probability and detection/prevention rankings used by a university-level security committee. For more information on FMEA, visit http://www.semiconfareast.com/fmea_quickref.htm#table. A risk analysis table appears on the following page.

Table 3: Risk Analysis					
Information Asset	**Threat or Vulnerability**	**Severity**	**Probability**	**Prevention /Detection**	**Score (multiply values)**
Public Data	unauthorized editing/defacement (internal or external)	2	4	3	24
	improper storage (digital or paper)	2	2	4	16
	improper transmission (digital and sneaker-based)	1	2	4	8
	data misclassification	5	2	3	30
Internal Data	unauthorized access (internal or external)	3	4	4	48
	improper storage (digital or paper)	3	3	4	36
	improper transmission (digital and sneaker-based)	3	3	4	36
	data misclassification	5	2	3	30
Protected Data	unauthorized access to private/protected data (internal and external)	6	2	4	48
	improper storage (digital or paper)	6	2	4	48
	improper transmission (digital and sneaker-based)	6	2	4	48
	data misclassification	4	2	3	24

Plan for Risk Management

As illustrated below, primarily preventive controls will be developed to address known human threats and ensure the confidentiality, integrity and availability of information assets. Some preventive controls such as training may also be used as corrective controls depending on the severity of the incident. In all cases, multiple controls will be applied to achieve defense in depth. A number of detective controls, such as logging, already exist. After controls are implemented, risk should be reduced to acceptable levels. A risk management table appears on the following page.

Table 4: Risk Management								
Information Asset	**Threat or Vulnerability**	**Score**	**Priority (Arbitrary: High = 36 and up)**	**Access Controls**	**Patch Management**	**Policy**	**Procedure**	**Training**
Public Data	unauthorized editing/defacement (internal or external)	24		X	X	X	X	X
	improper storage (digital or paper)	16		X		X	X	X
	improper transmission (digital and sneaker-based)	8		X		X	X	X
	data misclassification	30		X		X	X	X
Internal Data	unauthorized access (internal or external)	48	High	X	X	X	X	X
	improper storage (digital or paper)	36	High	X		X	X	X
	improper transmission (digital and sneaker-based)	36	High	X		X	X	X
	data misclassification	30		X		X	X	X
Protected Data	unauthorized access to private/protected data (internal and external)	48	High	X	X	X	X	X
	improper storage (digital or paper)	48	High	X	X	X	X	X
	improper transmission (digital and sneaker-based)	48	High	X		X	X	X
	data misclassification	24		X		X	X	X

Part Three: Do

Expectedly a number of high level risks involve protected data. Procedures and training that align with policy will be developed to mitigate risks. Mitigation strategies will address risks to all types of data. The table on the following page provides a summary of action items.

Table 5: Risks to Information Assets		
Problem	**Actions**	**Steps**
Unauthorized Access	***Develop and implement policies, procedures and training to address risk***	Develop and Implement Access Policy
		Formalize Password Management Standards
		Audit Access Controls including Password Management
		Audit Patch Management
		Audit Detective Controls e.g. logging
		Develop and Deliver Awareness Training to Ensure that Clients Conform with Relevant Legislation and Policy
		Adopt Code of Ethics (long-term: college-wide)
		Develop and Implement Physical Access Controls
Improper Storage		Develop and Implement Storage Policy for Digital and Paper Information Assets
		Develop Storage Procedures for Digital and Paper-based Information Assets
		Implement Media Sanitization Policy
Improper Transmission		Develop and Implement Transmission Policy for Information Assets
		Develop Transmission Procedures -- ssh, ssl and encryption will be used as necessary
Data Misclassification		Implement Information Asset Classification System
		Facilitate Classification via Document Management System such as Doculex
		Deploy Document Management System
		Develop Training on the Use of the Document Management System
		Train Clients to Use Document Management System
		Develop and Implement Controls to Audit Information Asset Classification System

Statement of Applicability

The implementation phase will provide an opportunity to identify gaps in the in the policy, procedures and training initiatives. As stated previously, Mead College does not plan to pursue certification as an ISO 17799 organization. Natural and environmental risks will be addressed in phase two. The priorities for phase one are increasing client/management awareness and improving data management practices. Existing patch and password management controls are deemed adequate; they will be audited thoroughly in phase two.

Training & Security Awareness

Training and security awareness is a core component of this initiative as well as a risk management strategy. Awareness training will be designed for staff and management. Staff and management will also receive training on new procedures. A code of ethics will be adopted organization-wide. Hopefully, the university will provide information security awareness training as part of new employee orientation at some point. Relevant training for technical staff will continue to be a priority.

Part Four: Check

The following checklist will give Mead College OIT a means to audit the implementation of the ISMS for data management. The checklist reveals weak auditing procedures in some areas. These weaknesses create opportunities to identify more effective auditing procedures. Higher education sometimes views policies, procedures and controls as bureaucratic. The code of ethics may be a particularly hard sell in the environment. Mead College employees are accustomed to approaching others with trust and acting on faith. As a result, the culture is particularly vulnerable to social engineering. Awareness training should make clients savvier. In spite of due diligence, incidents will still occur, and incident handling procedures will need to be developed. An audit checklist appears on the following page.

Table 6: ISMS Data Management Audit Checklist		
Control	**Objective**	**Audit Steps**
Access Policy	Prevent unauthorized access to data.	Check paper-trail for paper-based data; check logs and storage for digital data.
Password Management	Prevent unauthorized access to data.	Verify effectiveness of passwords with a tool such as L0phtcrack.
		Check for passwords in plain sight.
Patch Management	Prevent unauthorized access to data.	Personnel will be assigned to audit each other to ensure that patches are up-to-date on all systems.
Classification System for Information Assets	Create awareness that not all data is equal; avoid misclassification of data.	Spot check data to ensure proper classification.
		Find a fun way to quiz clients on classification system.
Code of Ethics	Encourage integrity; create a culture of personal responsibility.	Employees will be asked to endorse the code of ethics.
Awareness Training	Ensure that clients are informed about relevant legislation and polices; avoid ignorance;make the initiative relevant	Training will be mandatory and attendence will be logged.
Storage Policy	Expand client thinking about storage - it's not just servers and desktops, it's also handhelds and laptops and media; prevent improper storage.	Spot check paper and digital storage.
		Devices like laptops and handhelds will be challenging. The policy may be the only control until the item is returned or brought in for service. To-do: Search for technologies that will make it easy for clients to comply and/or IT professionals to audit
Media Sanitization Policy	Completely wipe or destroy media prior to surplus or transfer	OIT is already in charge of surplus/transfer -- wiping or destroying magnetic media housed in computers and servers will not be a problem.
		Media like floppy disks and CDs may be more of a challenge. Provide secure one-way mailboxes for clients to deposit used media.
Transmission Policy	Part of developing a data-centric culture; think before you share.	Scan for 'protected' label to determine if protected data is sent in the clear.
		Detective work may be the best control for paper-based transmission.

Part Five: Act

The ISO 17799 framework provides opportunities to assess and revise the ISMS on a periodic basis, and the review process will identify emerging issues and weaknesses in the ISMS. Mead College plans to conduct an annual internal audit after implementation. Training materials, documentation and procedures will be updated more frequently. In phase two, natural and environmental risks will be considered;

patch and password management strategies will be audited.

Conclusion

Implementing an ISMS for data management will be a giant leap for Mead College and should accomplish the goals of enhancing information security awareness at all levels, improving the security and management of information assets and beginning the process of developing a culture of information security. Ultimately, practice and continuing education will guide the improvement process. In subsequent phases, Mead College will become more comfortable with the ISO 17799 framework and the process will be fine-tuned prior to department-level rollouts.

Appendix A – FMEA Rankings Used by University-level Security Committee

Assessment Ranking Definitions

The following definitions of Severity, Probability, and Detect-ability/Prevention were adopted for use with the Failure Mode and Evaluation Assessment (FMEA) risk profile exercise. Gaps in definitions are intended to provide flexibility for interpretation and judgment.

Ranking	Severity	Loss of Confidentiality, Integrity, or Availability
10	Human Safety at Risk	Life threatening, severe injury, medical or emergency services shutdown.
9	High	24 hour outage of core enterprise system. $1,000,000 legal or financial impact. Initiates notification of federal or state authorities. Is reported in national news.
5	Important	One hour outage of core enterprise system. $100,000 legal or financial impact. Initiates notification of institutional authorities (Senior VPs, President). Is reported on regional television news.
1	Annoyance	Less than one hour outage of core enterprise system. $10,000 legal or financial impact. Colleagues/bosses are informed.

Note: Severity is a function of impact based on financial, legal, reputation, health & safety, and operations.

Ranking	Probability	Probability that a Vulnerability will be Exploited by a Threat
10	Constant Attempts	There are constant attempts to exploit vulnerabilities
9	Happening Elsewhere	Attempts are happening elsewhere now
8	Multiple Attempts	There have been more than one attempt in the past year
5	Has Happened Here	Attempts have happened here more than a year ago
4	Has Happened Elsewhere	It has happened elsewhere, but not currently
2	Possible	It is possible, but no attempts have been recorded
1	Emerging	Emerging possibilities

Ranking	Detection/Prevention	Likelihood of Detection and Prevention
10	Absolute Uncertainty	Design control cannot detect potential cause/mechanism and subsequent failure mode
9	Very Remote	Very remote chance the design control will detect potential cause/mechanism and subsequent failure mode
8	Remote	Remote chance the design control will detect potential cause/mechanism and subsequent failure mode
7	Very Low	Very low chance the design control will detect potential cause/mechanism and subsequent failure mode
6	Low	Low chance the design control will detect potential cause/mechanism and subsequent failure mode
5	Moderate	Moderate chance the design control will detect and prevent potential cause/mechanism and subsequent failure mode
4	Moderately High	Moderately High chance the design control will detect and prevent potential cause/mechanism and subsequent failure mode
3	High	High chance the design control will detect and prevent potential cause/mechanism and subsequent failure mode
2	Very High	Very high chance the design control will detect and prevent potential cause/mechanism and subsequent failure mode
1	Almost Certain	Design control will detect and prevent potential cause/mechanism and subsequent failure mode

Resources

FERPA (Federal Educational Rights and Privacy Act)
http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

FMEA (Failure Mode Effects Analysis)
http://www.fmeainfocentre.com/standards.htm
http://www.semiconfareast.com/fmea_quickref.htm#table

Hoelzer, David. (2004a). *Introduction to BS ISO/IEC 17799: Policy, ISMS and Awareness*. SANS Institute.

Hoelzer, David. (2004b). *SANS 17799 Controls and Process Improvement I.* SANS Institute.

Official Codes of the State of Georgia
http://www.ganet.org/cgi-bin/pub/ocode/ocgsearch?docname=OCode/G/50/18/70