



Project Name:		Project Number:
Enhancing Enterprise Security through ISO27002 Compliance		100709
Project Manager:	Project Sponsors:	Estimates (Hours & Cost):
< TBD >	Kathleen Starkoff Charles Morrow-Jones	2,850 hours,\$ 218,900
Prepared by:	Date Prepared or Revised:	Classification:
C. Morrow-Jones	February 12, 2009	3

Executive Summary

VISION: Create a secure information technology environment at The Ohio State University through the adoption of proactive projects, policies and practices. Replace fragmented central and distributed security efforts with coordinated efforts that are guided by a commonly agreed-on security framework.

OVERALL GOAL: Within 5 years, guide OSU’s information technology community into compliance with the 11 security domains and the associated controls that comprise the ISO27002 “Code of Practice for Information Security Management” security framework, in order to:

- Provide a framework that defines and prioritizes security projects
- Aid in the coordination of enterprise-wide efforts
- Aid in the development of appropriate IT security metrics
- Anticipate a State of Ohio rule requiring adoption of a security framework

Problem / Opportunity

Currently, the university faces unnecessary information technology risks due to fragmentation of security knowledge, practices and projects. Implementation of the ISO27002 standard provides an opportunity to coordinate projects and practices and to disseminate knowledge so that the university’s risk profile can be diminished.

Objectives

Begin the ISO adoption process by addressing the five high impact domains during calendar 2009 : **security policy, asset management, access control, business continuity, and compliance.**¹

Security policy – formulate, vet, adopt and communicate an overall IT security policy.

Asset management – Centrally inventory the critical servers that house restricted information; develop and distribute tools for inventorying other assets.

¹ See Appendix B for a description of the method by which high impact domains were selected.



Access control – Develop appropriate enterprise access control policies ; develop model unit access control policies; as identity management tools become available, assist in development /deployment of access management functionality

Business Continuity – work with current business continuity project to insure that IT security is being accounted for; assist in the development and execution of test plans that exercise the security component.

Compliance – discover, post and publicize the statutes and major contractual arrangements that affect the whole university; work with central and distributed units to help identify the applications that are affected by various laws and contracts; assemble an education campaign to boost compliance with these statutes and contracts.

In Scope

Work will be initiated and completed where possible, for the 5 domains described above. In addition, during the fourth quarter a process will be implemented to select the domains for the calendar 2010 focus.

Out of Scope

During the first year, no formal work is planned on these remaining six ISO27002 domains: Organization of security; Human resources; Physical and environmental security; Communications and Operations Management; System acquisition; and Incident management.

Success Criteria

OVERALL FIRST YEAR MILESTONES: make appreciable progress in meeting the controls in these five areas and increase the proportion of critical servers secured. “Appreciable progress” is defined as achieving 20 or more percent of the overall targets defined in the CIO metrics described below.

OVERALL ASSOCIATED METRICS: will be a count of the number of controls satisfied as a percent of the total number of controls, and the number of vulnerabilities mitigated as a percentage of total vulnerabilities identified.

Assumptions

1. No major changes in the ISO standards will occur during this phase of the project.
2. A staff member can be added who can assist distribute units with risk mitigation and ISO compliance.
3. The administration will continue to support Information Technology Security.



Major Risks

Description	How Likely	Impact	Score
	1=low, 2=med,3=hi	1=low, 2=med,3=hi	Likely x Impact
Budget cuts may lead to reduced available staff time	2	3	6
Lack of early availability of an IdM system may delay Access Control tasks	2	1	2
Lack of a data classification methodology may delay Asset Management tasks	3	2	6
A major breach could cause this approach to be questioned/repudiated	2	3	6

Obstacles/Constraints

- Limited availability/willingness of distributed staff to carry out their assignments
- Staffing limitations preclude more rapid compliance assistance to distributed units

Schedule Considerations/Related Projects

Proposed schedule depends on:

Schedule for the Identity Management Project

Schedule for the Data Classification Project(s)

Project Milestones and Major Deliverables

<The year-end milestones/deliverables are listed in the table below. Quarterly milestones for each objective are given in **Appendix C.**>

Milestone/Deliverable	Target Week	Responsible	M/D
Overarching Security Policy will be approved by community and management and will be communicated to the community.	52	Security/CIO/Communications/distributed units	D
Critical Servers will be registered by the distributed units, and tools to assist distributed units in asset management will be provided.	52	Security/distributed units/data management	M
Revised account management procedures will be put in place to gain major improvements in access control.	52	Security/operations (via identity management)	D
Business continuity planning will incorporate elements recommended by ISO27002, with revisions and testing as necessary.	52	Business Continuity, Security	M



Milestone/Deliverable	Target Week	Responsible	M/D
Compliance resources will be available to the OSU community including an inventory of applicable laws, regulations, etc. coupled with a major campaign to remind the community of compliance requirements.	52	Security, Privacy, OSU Legal, Office of Risk Assessment, Communications.	D
Project Complete – First year.	52	See Above	M

Project Resource Summary

Description	Hours	Rate	Cost	Notes
Internal staff	2,850	\$50.00	\$142,500	Assumes 1 dedicated FTE @ 1900 hours/year plus fractional assignments making up the other .5 FTE
External staff	0	0	\$ 0	
Software			\$ 50,000	Acquisition costs
Supplies & Services			\$ 5,000	Computer plus training costs, etc.
Maintenance			\$ 10,400	20% of SW+HW
Administrative Cost			\$ 9,000	Assumed at \$ 6,000/FTE/yr.
Hardware			\$ 2,000	To house software and data
Other			\$ 0	
Total	2,850		\$ 218,900	

Supporting Documents

Appendix A – Units Impacted and / or providing resources

Appendix B – Selection of the 2009 high impact domains

Appendix C – Quarterly milestones for each of the five objectives



Approvals

_____ (Project Manager)	_____ Date
_____ /s/ Keith Kidner Keith Kidner, PPMO (for CIO Sr. Leadership)	_____ 02/17/2009 Date
_____ /s/ Charles Morrow-Jones Charles Morrow-Jones, Director IT Security	_____ 02/17/2009 Date
_____ /s/ Kathleen Starkoff Kathleen Starkoff, CIO	_____ 02/17/2009 Date



Appendix A – Units providing resources to and/or impacted by project

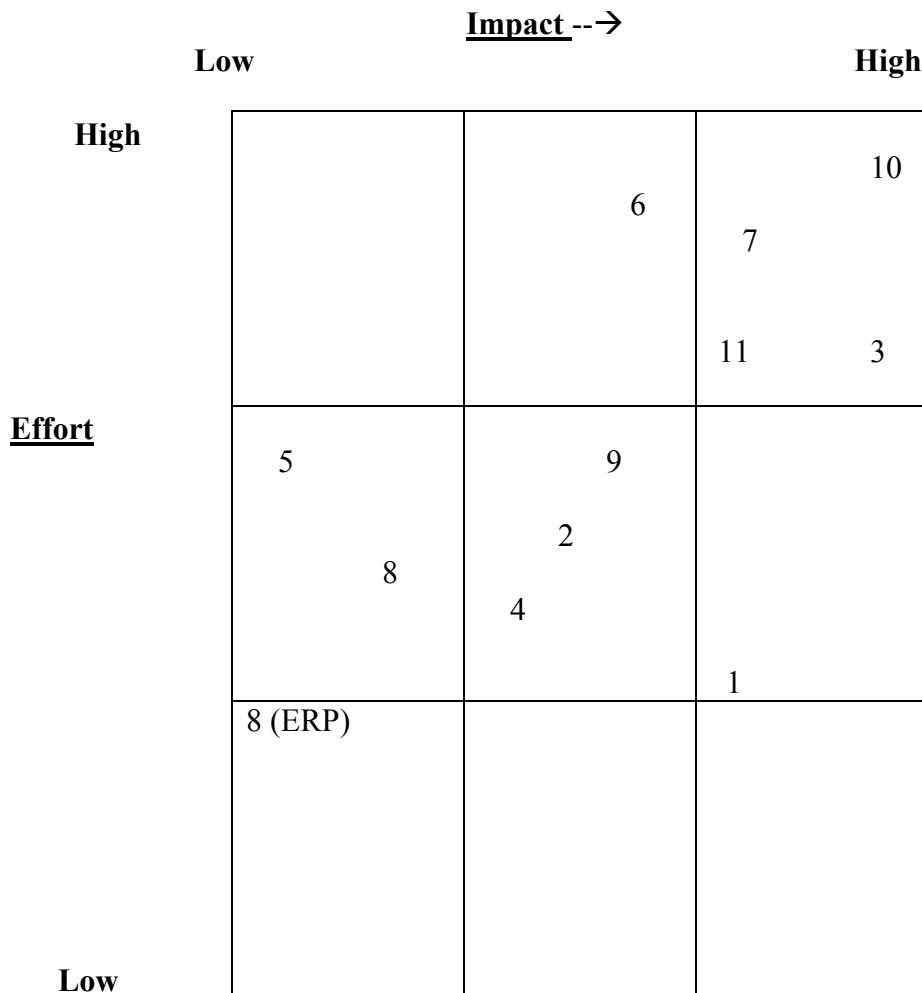
(A = Resources required if unit operates a critical server.)

CIO Unit	Team	Resources	Impacted
Enterprise Architecture	Security	X	X
	Emerging Technology		X
	Other		
Infrastructure	DBA	X	X
	Security	X	X
	PS Admin	X	X
	Operations	X	X
	BCP/DR	X	X
	Open Systems	X	X
	Batch	X	X
	T & N	X	X
	Other		
Applications	HR	X	X
	SIS	X	X
	Finance	X	X
	DW	X	X
	Univ Dev	X	X
	Remedy	X	X
	Training	X	X
	Documentation	X	X
	Other		
Customer Experience	Relationship Mgt	A	X
	Service Desk	A	X
	Processes	A	X
	Product Mgt	A	X
	Support	A	X
	Other		
Learning Technologies	Carmen	X	X
	Digital Union	X	X
	Classroom Services	X	X
	Tech Svcs	X	X
	eLearning Support	X	X
Communications		X	X
Human Resources			X
Finance			X
PPMO		X	X

Other University Units	Resources	Impacted
OSU Legal	X	X
Office of Risk Management	X	X



ISO 27002 DOMAIN EFFORT/IMPACT ANALYSIS



Numbers on the graph are ISO27002 domains.

The Critical Domains (High Impact spanning all efforts) were selected by a three step process: Two outside security experts gave their opinions about which domains were critical. A group comprised of security and privacy staff from the CIO organization examined each of the domains and the associated controls to determine which were operative in the OSU environment. Finally, the CIO Security group took this input, and positioned the domains on the graph using the input and the group’s security expertise and opinions.

The Eleven ISO27002 Security Domains (Numbers correspond to the graph above.)

1) Security Policy	6) Comm & Ops Mgmt	11) Compliance
2) Organization of Security	7) Access Control	
3) Asset Management	8) System Acquisition, etc.	
4) Human Resources	9) Incident Management	
5) Physical & Environ.	10) Business Continuity	



Appendix C – Quarterly Milestones For Each Of The Five Objectives

C = Activity performed by Central IT Security

D = Activity performed by Distributed IT and Central IT (other than Security)

DOMAIN: SECURITY POLICY – Objective: to provide management directive and support for information security in accordance with business requirements and relevant laws and regulations.

QUARTER 1 MILESTONE C - In concert with the CIO, draft a policy document that aligns security goals with OSU's business practices. This document could includeⁱ

- a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing;
- b) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;
- c) a framework for setting control objectives and controls, including the structure of risk assessment and risk management;
- d) a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:
 - 1) compliance with legislative, regulatory, and contractual requirements;
 - 2) security education, training, and awareness requirements;
 - 3) business continuity management;
 - 4) consequences of information security policy violations;
- e) a definition of general and specific responsibilities for information security management, including reporting information security incidents;
- f) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

QUARTER 2 MILESTONE: D - Communicate the draft policy to the relevant communities for feedback and to build support.

C -Revise the policy as appropriate to reflect community input. Begin moving it through the university policy process.

QUARTER 3 MILESTONE: C - get final approval of the Senior Management Council, reworking the policy as necessary to do so. In parallel, construct a communication plan. **D** -Once policy is approved, begin execution of the communication plan in order to make the entire community aware of the policy's existence and relevance.

QUARTER 4 MILESTONE. C - Complete initial communication about the policy. Construct a plan to do periodic reminders about compliance.

DOMAIN: ASSET MANAGEMENT – Objective: To achieve and maintain appropriate protection of organizational assets. An asset inventory is an important element in risk determination.



NOTE: because of the magnitude of the effort to comply with this domain, compliance has been divided into multiple parts. Inventorying and protecting critical servers is the first to be dealt with along with on-going data classification efforts as specified in the Institutional Data Policy.

QUARTER 1 MILESTONES – C - Construct web-based, authenticated data entry forms and accompanying database to enable construction of a centralized inventory of critical servers. Construct a communication plan aimed at the DNAs and others who will complete the form.

Determine whether any other asset information should be held centrally by IT Security. **D** - Coordinate data classification effort with relevant parties.

QUARTER 2 MILESTONES – D - Trial the data entry process to insure its success. Execute the communication plan. Toward the middle of the quarter, begin collecting data. If needed, establish a data collection mechanism for any other assets than need to be held by Security.

C - Make sure data classification is on track/meeting its timeline.

QUARTER 3 MILESTONES – C - Continue to collect data, with reminders to the submitters. Construct and publicize forms and other aids to the collection of asset information that will be held locally. Continue tracking data classification effort.

QUARTER 4 MILESTONES – C - Complete data collection for critical servers. Begin reminder program to change/update data as needed. Sample unit progress and problems with locally held data. Finalize data classification effort as appropriate.

DOMAIN: ACCESS CONTROL – Objective: access to information should be controlled.

QUARTER 1 MILESTONES - C - An access control policy should be established, documented, and reviewed based on business and security requirements for access. Review the status of access control mechanisms, including access control lists and identity management systems.

Coordinate adoption of stronger authentication controls, including two-factor authentication where appropriate. Coordinate password change plans for passwords associated with name.n accounts, including communication plans.

QUARTER 2 MILESTONES – C - put procedures in place for account management including provisioning/deprovisioning, password management, and privilege management. Put together a communication plan to inform users of impending changes. Formulate contingency plan if identity management system is not available in Q3.

QUARTER 3 MILESTONES – C - Prepare identity management system to manage accounts, password and privilege management. **D** - Communicate new processes to users and to user support groups (such as help desks). Test identity management system.

QUARTER 4 MILESTONES – D - Begin to utilize identity management system to manage all aspects of access to central systems. Communicate with users about policies that bear on access controls, such as the policy against shared passwords.

DOMAIN: BUSINESS CONTINUITY – Objective: To counteract interruptions to business activities



and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

QUARTER 1 MILESTONES – **C** - Coordinate with the current Business Continuity efforts, led by David Lindstedt, to be sure that they are including all of the IT elements recommended by the ISO27002 controls. Assemble a joint plan for including any that may be missing.

QUARTER 2 MILESTONES - **D** - Put together a joint testing plan for the BCP plans that are already in place, insuring that all appropriate IT elements are tested. Execute the test plan on several test cases. Return to any units that may have plans that omit IT, and add that element.

QUARTER 3 MILESTONES – **D** - Continue with joint testing according to plan. Revisit units that may have plans deficient in the IT elements. Confirm that new plans continue to include appropriate IT elements.

QUARTER 4 MILESTONES – **D** - Continue quarter 3 efforts, as necessary, to reach agreed on final levels of testing.

DOMAIN: COMPLIANCE – Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

QUARTER 1 MILESTONES – **C** - Work with OSU Legal and other appropriate parties (Registrar, Office of Risk, Internal Audit) to make sure that we have a complete inventory of laws, regulations, etc. Post all of these on the Buckeyesecure website. Create a publicity campaign that reminds people that compliance is required. Work with OIT Operations and Applications Development and Support to develop an inventory of the systems and applications that are in place.

QUARTER 2 MILESTONES – **C** - Construct an inventory of laws, regulations, etc. that pertain to each central system. Publicize to the Operations and AD&S groups, and others if appropriate. Working with Legal Affairs, develop a document that states the requirements for using intellectual property owned by others, including software. Formulate a communications plan to inform the appropriate groups of these requirements.

QUARTER 3 MILESTONES – **C+D** - Using the communications plan, inform campus of their responsibilities concerning intellectual property belonging to others. In conjunction with the records retention officer and legal affairs, assemble a campaign to publicize protection of the organization's records against loss, improper destruction or falsification.

QUARTER 4 MILESTONES – **C** - Conduct the campaign to inform campus of the need to protect records and consequences of not doing so. Conduct a "refresher" campaign that features data protection and privacy.

ⁱ From ISO27002, section 5.1.1, implementation guidance.