Information Technology Security Program

Office of the CIO

December, 2008

IT Security Program

AGENDA

- What is it?
- Why do we need it?
- An international Standard
- Program Components
- Current Status
- Next Steps

What is It?

- A Policy Framework (an umbrella document)
    - An Information Security Policy Manual
    - aka Information Security Management System (ISMS)
    - See http://en.wikipedia.org/wiki/Information_security_management_system
- Documents management’s commitment to information security
- A risk-based approach
- Recognizes information as an asset!
- Specifies ownership and responsibility
- A Statement of Scope and Applicability

IT Security Program

Why Do We Need It?

- PWC (external auditors) recommendation
- Security consultants recommendation
- “Good practice” (documented policy)
- Communicates expectations
- Educates campus on risk management
- Auditable (formalizes current and required practice)

An International Standard

ISO/IEC

- International Organization for Standardization
- International Electrotechnical Commission
- The recognized system for worldwide standardization
- Information Security standard originated in U.K.
  - BS 17799
  - Became ISO/IEC 17799 (in 2000)
- ISO/IEC created an ISMS 27000 ‘family of standards’
- ISO/IEC 27001 -- for recognized certification “must do’s”
- ISO/IEC 27002 – code of practice “should do’s”
- See http://www.27000.org/iso-27002.htm

Information Security Definition and Focus

Information security is defined within the 27002 standard in the context of the C-I-A triad:

- *the preservation of **confidentiality** (ensuring that information is accessible only to those authorized to have access), **integrity** (safeguarding the accuracy and completeness of information and processing methods) and **availability** (ensuring that authorized users have access to information and associated assets when required)*.
- “Information security is the **protection of information** from a wide range of threats to **ensure business continuity**, **minimize business risk**, and **maximize return** on investments and opportunities.

IT Security Program

Security Program Components

- Will map to and be compatible with the ISO/IEC 27002 Standard's 'code of practice':
  - Based primarily on Risk Assessment/Risk Management; identification of critical business processes.
  - Security requirements also determined by regulatory and contractual provisions:
    - Data protection and privacy of personal information
    - Intellectual property rights
  - **N.B. Cost of implementing controls must be balanced against probability and impact of threats!**

IT Security Program

Eleven ISO 27002 Clauses (39 control objectives)

- 1. Security Policy
- 2. Organization of Information Security
- 3. Asset Management
- 4. Human Resources Security
- 5. Physical & Environmental Security
- 6. Communications/Operations Management
- 7. Access Control (incl. Networking)
- 8. Systems Acquisition, Development & Maintenance
- 9. Security Incident Management
- 10. Business Continuity Management
- 11. Compliance

Risk Assessment

- The Standard’s Eleven Clauses provide an organizational framework for the University’s IT security policies (i.e. controls).
- No organization implements all of the Standard’s 100+ controls!
- Policies/controls are only implemented when they are cost-effective and they reduce risk to an acceptable level.
- The major IT risks identified by the ERM-SC were:
  - Continuity of information management and technology
  - Management of Information and technology

Current Status

- Where to start?
    - Determine where we are!
- **Step One:**
    - PMO prepared a "**Report Card**" for the CIO
        - Assessed progress on implementing recommendations from a 2005 external security audit mapped to ISO 27002.
        - Grades:
        - A = Fully implemented; formally documented and approved
        - B+ = Implemented/operational; needs add'l. formalization
        - B = Substantially implemented; needs completed documentation and approval.
        - C = In-progress implementation; but not formalized
        - D = Only minimal reactive steps taken
        - E = No significant action or progress

IT Security Program

Current Status

- Report Card Summary:
  - Areas of Improvement (C's and B's)
    - Physical Security
    - Risk Assessment
    - Security Responsibilities
    - Network and Operational Security
    - Cryptographic Controls
    - Vulnerability Management
    - Systems Development/Change Management
    - Incident Management
  - Good work being done, but lacks formal documentation, procedural standards etc. which can be audited.

Current Status

- Report Card Summary:
  - Areas Needing Attention! (D's)
    - IT Asset Classification (and ownership)
    - Human Resource Security (before, during, after)
    - Business Continuity (probability planning; testing)
- **Step Two:**
  - Get management's attention!
  - Draft a Policy Framework (i.e. the Security Program).
  - Map existing approved and draft IT security policies to the Standard (and into the Program document).
  - Publish the draft Program.

IT Security Program

Next Steps

- The 27002 standard provides **guidance**!
    - **Essential Controls**:
        - Protection of privacy and organizational records
        - Intellectual property rights
    - **Common Best Practices**:
        - Allocate responsibility for IT security
        - Develop an information security policy document ☑
        - Manage information security events/incidents
        - Establish a vulnerability management process
        - Provide security awareness training
        - Develop a business continuity management process

Next Steps

- **Step Three:**
  - Introduce the Program!
    - CCS Council, ITSC, ISC, ITSIG
    - Solicit comment and feedback
  - Approval in Principle (by ITSC)
  - Confirm CIO ownership

IT Security Program

Next Steps

- **Step Four:**
  - Short-term policy priorities
    - IT Security: Roles and Responsibility Policy
    - IT Security Incident Management Policy
    - IT Security Awareness campaign
    - Network Infrastructure and Access Policies
  - **Longer-term priorities:**
    - Formalize business continuity planning
    - Review information management practice

IT Security Program

- Contact:
- Email: dbadger@uoguelph.ca
- Phone: Ext. 52830
- Websites:
  - www.uoguelph.ca/pmo
  - www.uoguelph.ca/itgov

  - Thank you!