UF IT Risk Assessment Standard

Authority
This standard was enacted by the UF Senior Vice President for Administration and the UF Interim Chief Information Officer on July 10, 2008 [7]. It was approved by the UF General Counsel.

Who Should Read This
This document should be read by all Deans, Directors, Department Chairs and IT workers. A robust risk assessment includes evaluation by all sectors of an organization, so it is recommended that relevant representative group of faculty, staff, and students participate in risk assessment.

Purpose
Risk assessments are conducted to bring sense, order, and boundaries to the mitigation strategies needed to protect the mission, operation, and reputation of the University of Florida. They inform the judgments of decision makers about how risks should be managed.

Definitions
Audit: An independent unbiased examination of a system or organization to verify that it is in compliance with its own rules.
Risk Analysis: The study of criticality, exposures, threat impact and threat probability to determine the potential for security problems.
Risk Assessment: Identification and analysis of factors that might negatively influence operations.
Exposure: The potential for loss.
Protection measure: Any control that intended to minimize the likelihood and/or reduce the impact of threat exploitation. Protection measures are also referred to as safeguards or countermeasures.
Vulnerability: Any information system weakness or flaw attributed to individuals, assets, or operations that make them susceptible to exploitation.
Threat: The presence of dangerous or adverse circumstances or events with the potential to impact operations, assets, or individuals via disclosure, modification, destruction, or disruption of service.

Standard
The Level 2 Unit Information Security Administrator (ISA) must ensure that IT risk assessments are performed for their unit. The purpose is to determine protection level commensurate with resource value and exposure to threats. Units may use and document their own comprehensive risk assessment process provided it accomplishes the equivalent results as the “Risk Assessment Guidelines” [6]. A comprehensive risk assessment must be done at least once every five years.

The resulting risk mitigation strategy report (see example in Appendix A) must be provided to the UF Information Security Manager (ISM). The report must be protected from unauthorized access. The report to the UF ISM must cover at least the top 3-5 critical risks. For each risk:

1. Identify contacts responsible for the assessment and provide their contact information.
    a. ISM
    b. ISA
    c. Assessment Manager (if not ISA or ISM)
2. Risk statements (See Appendix A for examples). Risk statements should include:
    a. Identify the assets affected and their criticality.
    b. Identify threats likely to exploit assessed vulnerabilities.
    c. Estimate likelihood that threats will exploit vulnerabilities.
    d. Quantify the impact if threats exploit the vulnerabilities.
    e. Recommend controls to mitigate the risk.
3. For each risk statement, describe actions and resources required to mitigate or accept risk.
    a. Name, title, phone, and email address of person responsible for mitigation.
    b. Resources needed for the mitigation.
    c. Scheduled date of completion.
    d. Metrics that will be used to evaluate success of the mitigation.

Progress on the risk mitigation strategy should be reported to the UF ISM annually (see example in Appendix C).

The UF ISM must incorporate Level 2 Unit risk mitigation strategy reports into a university-wide risk framework that must be formally acknowledged by the UF ISA and university administration. The framework must include risk factors and vulnerabilities, approved mitigation measures and resources, and accepted and assumed accountability for residual risk.

Bibliography

[1] Security Self-Assessment Guide for Information Technology Systems, http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf
[2] OCTAVE, http://www.cert.org/octave/
[3] An Overview of Threat and Risk Assessment, http://www.sans.org/rr/whitepapers/auditing/76.php
[4] An Introduction to Information Risk Assessment, http://www.sans.org/rr/whitepapers/auditing/1204.php
[5] CACI Computer Security Threats, http://www.caci.com/business/ia/threats.html
[6] UF Risk Assessment Guidelines, http://www.it.ufl.edu/policies/security/risk-assessment-guidelines.pdf
[7] DDD announcement of this standard, http://lists.ufl.edu/cgi-bin/wa?A2=ind08&L=DDD-L&P=R35323&I=-3

Appendix A: Sample Mitigation Strategy for Unit ABC

Unit: Unit ABC
Date: March 30, 2008
ISA: Mary Johnson, mjohnson-abc@ufl.edu
ISM (Assessment Manager): Joe Smith, jsmith-abc@ufl.edu

1. Risk statement: There is a high risk of confidential information exposure when stored on personally managed computers.
   A. Mitigation: New policies and procedures will be created to discourage access of confidential data from personally managed computers. Unit administration and supervisors will authorize and document users allowed to access confidential data from personally managed computers and they will limit the amount of data allowed to be accessed. IT workers will verify personally managed computers are securely maintained with current anti-virus protection, current updates, and facilities for encryption. User compliance will be periodically verified.
      a. Responsible Contact: Jane Edwards
      b. Resources: 120 man hours
      c. Deadline: March 30, 2009
      d. Metrics: Users who access confidential data on personally managed computers and the computers they use to access confidential data will be counted and documented prior to the implementation of new policies. The security posture of the personally managed computers they use to access confidential data will be evaluated. One year after the implementation of new policies, the users will be counted again to determine if the number is reduced. The security posture of the personally managed computers still used to access personal data will be evaluated to assess their security posture and this will be compared to their posture before the implementation of the new policies.

2. Risk statement: There is a high risk of confidential data exposure when stored on mobile devices (such as laptops and PDAs) since, due to their mobility, they might be lost or stolen.
   A. Mitigation: Policy will be implemented to minimize the number of laptops authorized for use with confidential data. Full disk encryption will be required on all laptops used with confidential data. Remote data destruction and tracking software will also be required. Policy implementation will be verified at least annually.
      a. Responsible Contact: John “IT Worker” Doe
      b. Resources: $10,000
      c. Deadline: March 30, 2009
      d. Metrics: The security posture of laptops used with confidential data will be evaluated and documented prior to the implementation of the new policy. Laptop incident number and severity for one year prior to the policy implementation will be evaluated and compared to incidents during the year after the policy implementation.

3. Risk statement: There is a high risk of confidential information exposure due to inadequately trained users.
   A. Mitigation: All users will be required to attend data security training before they are granted access to confidential information.
      a. Responsible Contact: Jane Edwards
      b. Resources: 120 man hours
      c. Deadline: March 30, 2009
      d. Metrics: Number of users completing training will be compared to those authorized. Number of violations will be evaluated before and after training.

4. Risk statement: There is a high risk of confidential data exposure due to inadequate authorization and documentation of users and workstations authorized to use it.
   A. Mitigation: Unit administration and supervisors will formally authorize individuals and groups allowed to access confidential data and the workstations they can use. A database will be created to document them.

a. Responsible Contact: Jane Edwards
b. Resources: 120 man hours
c. Deadline: August 30, 2008
d. Metrics: Incident number and severity prior to authorization and documentation will be compared to incidents after authorization and documentation.

5. Risk statement: There is a high risk of confidential data exposure due to inadequate software testing.
   A. Mitigation: Procedures will be documented and implemented for vulnerability analysis and penetration testing of all software (written internally or obtained from an external source) before it is used with confidential data.
      a. Responsible Contact: John “IT Worker” Doe
      b. Resources: 1 FTE
      c. Deadline: March 30, 2009

Metrics: Severity of vulnerabilities found during the analysis will be documented and reported. Incident number and severity will be compared before and after the analysis.

Appendix B: Sample Risk Profiles Used to Develop Mitigation Strategy for Unit ABC

The Unit risk profiles are not provided to the UF ISM, only the mitigation strategy. These example risk profiles are intended only to demonstrate how the mitigation strategies can be developed from the risk profiles.

Risk Profile #1
Asset: Confidential Data

Needed Control: Some method is used to ensure that personally managed hosts comply with minimum security requirements (such as current software and operating system updates and malware protection) before they are allowed to access the network. Requirements are documented and readily available to users.

Needed Control: Unit administration authorizes and documents all personally managed computers used with confidential data. Such use is discouraged and should be the minimum necessary for accomplishing the purpose of using the data. Where no reasonable alternative exists, some method is used to ensure that these hosts comply with minimum security requirements.

- Encryption of the confidential data stored on personally managed computers is required. Full disk encryption is required on personally managed mobile computing devices such as laptops and PDAs
- Current software and operating system updates
- Current malware protection
- Appropriate and secure backups

Needed Control: Storage of confidential data is not permitted on personally-managed mobile computing devices such as laptops and PDAs.

Use: Storage on personally managed workstations

Vulnerability: Poor anti-virus protection
Threat: Malware
Threat Probability: Likely
Threat Impact: High

Vulnerability: Poor patch management
Threat: Malware
Threat Probability: Likely
Threat Impact: High
Threat: Malicious unauthorized access
Threat Probability: Likely
Threat Impact: High

Vulnerability: Poor access control
Threat: Malicious unauthorized access
Threat Probability: Likely
Threat Impact: High

Risk Profile #2
Asset: Confidential information

Needed Control: Storage of confidential data is not permitted on personally managed mobile computing devices such as laptops and PDAs.

Needed Control: Before users are authorized to use confidential information on mobile devices (laptops, PDAs, etc.) or removable media (CDs, thumb drives, etc.), they are informed of the authorized locations where the device or media can be used. Authorized locations are documented and users know that special permission is required to use the device or media in different locations. They also know that permission must be obtained from the Dean, Director, or Department Chair if confidential data will be moved from secure campus locations.

Needed Control: IT workers provide facilities such as encryption to properly secure storage and transmission of confidential data. Users employ these facilities to protect confidential information. The facilities are documented, reviewed, updated and verified. Example include:

- Encryption during transmission
- Encryption when writing to disk
- Virtual Private Network (VPN)
- Secure Socket Layer (SSL)

Use: Storage on laptops

Vulnerability: Easily removed from known-secure locations
Threat: Theft
Threat Probability: Likely
Threat Impact: High
Threat: Loss
Threat Probability: Likely
Threat Impact: High

Risk Profile #3
Asset: Confidential information

Needed Control: Before given access, new employee procedures for all staff include formal training regarding their responsibility to protect confidential data. Training material is readily available to its intended audience and is periodically reinforced. Training procedures are documented and followed. Some method such as a quiz is used to assure that users understand the procedures and their responsibility to comply with policies and procedures. Compliance is periodically verified. Training topics includes:

- Authentication requirements
- Strong passwords and secure password management
- Authorization requirements
- Encryption requirements

- File permissions restrictions
- Document labeling requirements
- Mobile device and removable media restrictions
- Screen lock requirements
- Social engineering
- Physical location restrictions
- Physical access procedures
- Disposal requirements
- Secure use of email
- Secure use of instant messaging
- Secure use of the web
- Secure use of software used to store and transmit confidential information
- Recognizing and reporting violations
- Sanctions for violating these requirements

Needed Control: Before given access, new employee procedures for all staff include the following steps. Some method such as a quiz is used to assure users understand their responsibilities. Training and awareness is periodically reinforced.

- Provide UF AUP instruction and obtain agreement to comply
- Provide sensitive data protection training and obtain signed agreement to comply
- Inform that bypassing security controls may result in sanctions
- Provide IT orientation
- Provide malware prevention instructions
- Provide legal software use instructions

Needed Control: Unit administration ensures that appropriate training and awareness material is available to users explaining their responsibility to protect confidential data.

Use: Any

Vulnerability: Inadequately trained users
Threat: Process violation
Threat Probability: Likely
Threat Impact: High
Threat: Implementation error
Threat Probability: Likely
Threat Impact: High
Threat: Malware that requires user interaction
Threat Probability: Likely
Threat Impact: High

Risk Profile #4
Asset: Confidential information.

Needed Control: Unit administration has authorized roles and assigned responsibilities to employees for protecting the confidentiality, integrity and availability of sensitive data. The role assignments and responsibilities are documented. Staff at all levels understand their roles and their responsibilities are executed. Compliance with roles and responsibilities is periodically verified.

Use: Authorization and documentation.

Vulnerability: Improper incident response might destroy evidence due inadequate authorization and documentation of users and workstations authorized to use confidential information.

Threat: Implementation error

Threat Probability: Likely

Threat Impact: High

Vulnerability: Improper data sanitization or destruction due inadequate authorization and documentation of users and workstations authorized to use confidential information.

Threat: Implementation error

Threat Probability: Likely

Threat Impact: High

Risk Profile #5

Asset: Confidential information

Needed Control: Prior to installation, procedures are documented for IT workers to plan, select and install all software, hosts and network equipment with consideration for the items listed below. Compliance is audited.

- Data protection - Security strategies, policies and procedures
- History of security compromises
- Results of security risk assessments
- Protections against compromise

Needed Control: Procedures are documented for testing software used with confidential data and they include:

- Testing by people that did not contribute code to the project
- Subjecting code to internal peer review or trusted external third party assessment
- Penetration testing of software and testing for vulnerabilities at every stage of development
- Testing includes attempts to compromise data, compromise the server, impersonate users or servers, perform fraudulent transactions, send junk data, and deny service
- Ensuring software is robust against unauthorized use or attack

Needed Control: Procedures are documented to ensure that software uses secure memory handling procedures. Code is tested for secure memory handling.

- Variables that index memory are within bounds
- Software code checks buffer sizes to prevent writing data that is larger than the buffer size
- Software code frees allocated memory when no longer needed

Needed Control: Software design and function are documented and tested thoroughly.

- A formal programming methodology is used to develop software
- Professional programmers write all software
- Software code is well documented
- Software code review is conducted at every stage of development

- Input characters are limited to prevent entry of information that could jeopardize the security of software

Use: Software

Vulnerability: Inadequately tested software.
Threat: Software malfunction
Threat Probability: Likely
Threat Impact: High
Threat: Malicious unauthorized access
Threat Probability: Likely
Threat Impact: High

Appendix C: Sample Risk Mitigation Progress Report

Unit: Unit ABC
Date: March 30, 2009
ISA: Mary Johnson
ISM (Assessment Manager): Joe Smith

1. Risk statement: There is a high risk of confidential information exposure when stored on personally managed computers.
   A. Mitigation: New policies and procedures will be created to discourage access of confidential data from personally managed computers. Unit administration and supervisors will authorize and document users allowed to access confidential data from personally managed computers and they will limit the amount of data allowed to be accessed. IT workers will verify personally managed computers are securely maintained with current anti-virus protection, current updates, and facilities for encryption. User compliance will be periodically verified.
      a. Responsible Contact: Jane Edwards
      b. Resources: 120 man hours
      c. Deadline: March 30, 2009
      d. Status: 20 users accessed confidential data from personally managed computers prior to the new policies. Of those, 16 of the computers had inadequate security protection. After the implementation of the new policies, the number of users authorized to access confidential data from personally managed computers was reduced to nine. They were documented and all of the computers had adequate security protection.

2. Risk statement: There is a high risk of confidential data exposure when stored on mobile devices (such as laptops and PDAs) and portable media (such as cdroms and thumb drives) since, due to their mobility, they might be lost or stolen.
   A. Mitigation: Policy will be implemented to minimize the number of laptops authorized for use with confidential data. Full disk encryption will be required on all laptops used with confidential data. Remote data destruction and tracking software will be also be required.
      a. Responsible Contact: John “IT Worker” Doe
      b. Resources: $10,000
      c. Deadline: March 30, 2009
      d. Status: 23 laptops were used with confidential data prior to the new policy. There were 3 incidents prior to the new policy and each incident resulted in privacy violations and notifications. One year after the new policy, 14 laptops are used with confidential data. There were two incidents and, due to encryption, neither resulted in a privacy violation, so notifications weren’t required. One stolen laptop was recovered as a result of new tracking software that was installed.

3. Risk statement: There is a high risk of confidential information exposure due to inadequately trained users.
   A. Mitigation: All users will be required to attend data security training before they are granted access to confidential information.
      a. Responsible Contact: Jane Edwards
      b. Resources: 120 man hours
      c. Deadline: March 30, 2009
      d. Status: In progress, but not complete. Revised deadline is August 30, 2009.

4. Risk statement: There is a high risk of confidential data exposure due to inadequate authorization and documentation of users and workstations authorized to use it.
   A. Mitigation: Unit administration and supervisors will formally authorize individuals and groups allowed to access confidential data and the workstations they can use. A database will be created to document them.
      a. Responsible Contact: Jane Edwards
      b. Resources: 120 man hours

c. Deadline: August 30, 2008
d. Status: There were 7 incidents in the year prior to the user authorization and documentation. Four resulted in privacy violations and notifications. There were 3 incidents in the year after user authorization and documentation was implemented. None resulted in privacy violations.

5. Risk statement: There is a high risk of confidential data exposure due to inadequate software testing.
   A. Mitigation: Procedures will be documented and implemented for vulnerability analysis and penetration testing of software before it is used with confidential data.
      a. Responsible Contact: John “IT Worker” Doe
      b. Resources: 120 man hours
      c. Deadline: March 30, 2009
      d. Status: In progress, but not complete. Revised deadline is August 30, 2009.