UF Risk IT Assessment Guidelines

Who Should Read This

All risk assessment participants should read this document, most importantly, unit administration and IT workers. A robust risk assessment includes evaluation by all sectors of an organization, so it is recommended that other relevant faculty, staff, and students also participate in risk assessment and read this document.

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.
Evaluation: To examine and judge carefully; appraise.
Criticality: Degree of importance.
Exposure: The potential for loss.
Control: Any protection measure that could directly 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 in individuals, assets, or operations making 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.

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.

These guidelines are intended to be comprehensive. Especially for the first risk assessment, it may not be practical for some units to rigidly follow these guidelines. Consider the following suggestions to help your unit prioritize and determine what is most meaningful to include in its risk assessment process.

- Resist the urge to be too comprehensive on the first assessment.
- Aggregate resources into similar groups and assess the group rather than individual resources. For example, rather than assess each workstation, aggregate similar workstations in to a group and assess them as a group.
- Avoid straying from the process. Resist mission creep.
- Focus on most critical assets.
    - Those used for Restricted and Sensitive data.
    - Those critical to the mission and function of the unit.
    - Those not easily replaced.
- Focus on most probable threats.
- Balance mitigation strategy with risk, cost and usability. Keep it doable.

Guidelines

Below are suggested steps for a comprehensive risk assessment. There is no such thing as perfect IT security. IT security is ongoing process of improvement. Also, security must be balanced with cost and usability. Your unit will be best served by a candid risk assessment process. Avoid answering questions as if this were a job performance evaluation.

The risk assessment process outlined below consists of twelve steps that are organized into four phases.

I. Assessment planning

1. Organize the team: With assistance from unit administration, create and convene a risk assessment team (See Appendix A for suggestions)
   - a. Assessment Manager
   - b. Administrators
   - c. IT Workers
   - d. Users
2. Document a project plan
   - a. Define the goal
   - b. Establish the scope
   - c. Establish a schedule of one to three months

II. Data collection

3. Gather documentation
   - i. Asset classifications
   - ii. Security roles
   - iii. Policies
   - iv. Incident reports
   - v. Audit findings
   - vi. Appetite for risk (Educause provides a MS Excel tool for determining risk tolerance at http://connect.educause.edu/Library/Abstract/InformationSecurityGovern/43206)
   - vii. Other relevant information (See Appendix B for more suggestions)
4. Convene a kick-off meeting and begin assessment (Achilles can be used for this step, https://infosec.ufl.edu//cgi-bin/achilles/index.cgi)
   - a. Identify critical assets and related infrastructure (Appendix C)
   - b. Evaluate threat probability and threat impact. Consider potential consequences (Appendix D)
     - 1) Malfunctions
     - 2) Malicious threats
     - 3) Human errors
     - 4) Environmental threats
5. Conduct control survey. Identify vulnerabilities and controls. Evaluate the extent to which controls exist (e.g. implemented, needed, not applicable, or don't know). (See http://www.it.ufl.edu/policies/security/documents/risk-assessment-controls.pdf for list of controls or use Achilles, https://infosec.ufl.edu//cgi-bin/achilles/index.cgi)
   - a. Strategic controls and vulnerabilities
     - 1) Policy
     - 2) Communication

        3) Records
        4) Contingency
        5) Risk
    b. Operation controls and vulnerabilities
        1) Access
        2) Change management
        3) Environmental
        4) Incident response

6. Conduct technical evaluation. Assistance with technical risk analysis can be requested from the UF IT Security Team by contacting ufirt@ufl.edu . A self-scan interface is available at https://infosec.ufl.edu/cgi-bin/newscan/.
    a. Port scans
    b. Vulnerability scans
    c. Application audits
    d. Penetration testing

III. Data analysis

7. Review documentation
    i. Are assets classified and documented?
    ii. Are security roles documented and current?
    iii. Are lessons learned from incidents?
    iv. Are audit comments addressed?
    v. Are other issues addressed?

8. Review technical results
    i. Are ports unnecessarily exposed?
    ii. Are vulnerabilities patched?
    iii. Are applications robust against attack?
    iv. Are systems robust against attack?

9. Analyze assets, threats, vulnerabilities and controls to build risk profiles (See Appendix E or, if you're using Achilles, see review the Achilles reports, https://infosec.ufl.edu//cgi-bin/achilles/index.cgi)
    i. For the most valuable assets, consider which vulnerabilities are most likely to be exploited and by which threats.
    ii. Rank the threat-vulnerability pairs according to the impact that would result if the vulnerability was exploited.
    iii. For the threat-vulnerability pairs that will have the largest impact, create risk profiles
    iv. For each risk profile, write a risk statement.

IV. Mitigation (See Appendix F)

10. Write and submit a mitigation report
    a. Decide which risks to address
    b. For each risk, evaluate mitigation options
    c. For each mitigation recommendation, document:
        1. Person responsible for mitigation
        2. Implementation schedule
        3. Cost estimates
        4. Metrics to evaluate mitigation success
    d. Convene DDD exit briefing
    e. Obtain DDD approval

f. Submit report
   1. Level 3 Departments submit to Level 2 ISM
   2. Level 2 ISMs submit to UF ISM, http://infosec.ufl.edu/achilles/mitigation

11. Implement mitigation
    a. Allocate resources to implement mitigation
    b. Do the work
    c. Monitor progress
12. Evaluate mitigation implementation progress annually and submit progress report

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 Environmental Health and Safety, Risk Management, Insurance, http://www.ehs.ufl.edu/RiskMgmt/insure2.htm

[7] Educause risk assessment framework, http://www.educause.edu/LibraryDetailPage/666?ID=CSD4380

[8] Educause Information Security Governance Assessment Tool for Higher Education, http://www.educause.edu/ir/library/pdf/SEC0421.pdf

[9] Educause Effective Practices and Solutions in Security, http://www.educause.edu/EffectivePracticesandSolutionsinSecurity/1246

Appendix A: Suggested Roles to Include on the Risk Assessment Team

Many aspects of risk assessment are subjective. It is important to get the perspective of relevant staff throughout the organization. Within a manageable limit, the more individuals included in the assessment, the more the results will be.

- ISA
- ISM
- IT workers
- Faculty
- Staff
- Students
- Representative from the Office of Audit and Compliance Review
- Representative from the UF IT Security Team
- Representative from the Office of General Council
- Representative from Computing and Networking Services, Infrastructure Group
- Representative from Computing and Networking Services, Network Services
- Representative from Property Services
- Representative from Environmental Health and Safety
- External IT security consultant

Appendix B: Documentation to Review for Risk Assessments

Depending on the scope, following are examples of information that might be helpful for conducting a risk assessment.

- Organizational chart showing where IT security fits
- Policies, standards, procedures and guidelines
- Inventory, diagrams and other similar documentation
- Software licenses
- Accounts and access privileges
- Data security roles and classifications
- Positions of Special Trust agreements audit
- Awareness program review
- Network access control review
- Security zones (private IP, network and host firewalls, acls)
- IT Continuance of Operations Plan
- Incident prevention (endpoint, access policies, malware protection, etc.)
- Incident detection (host and network ids, log monitoring)
- Incident history

Appendix C: Identifying Critical Assets

An asset is any intellectual or physical entity deemed important for doing or continuing business.

Types of assets that should be considered

- Information
- Software
- Systems
- Network
- Physical

Considerations for determining asset value

- Which assets will have a large adverse impact if they are exposed to unauthorized individuals?
- Which assets will cause a large adverse impact on the unit if they are modified without authorization? Are authenticity, accuracy, and completeness important?
- Which assets will cause a large adverse impact on the unit if they are lost or destroyed?
- Which assets will cause a large adverse impact on the unit if access to them is interrupted?
- Which assets are mission critical?
- Which assets are difficult to replace?
- Which assets are costly to replace?
- Which assets are proprietary?
- What legal requirements impact the asset?
- How will the unit's reputation be impacted?
- Are there dependencies critical to the proper function of identified assets?

Examples of critical assets

- Student data systems
- Medical data systems
- Financial data systems
- Human Resources systems
- Critical enterprise systems
- Donor systems
- Systems under contract and used for collaboration
- Certain intellectual property

Appendix D: Threat Probability and Threat Impact

Categories of Threats

Malfunction

- Software malfunction
- Hardware malfunction
- Process malfunction
- Power disruption
- Power surge

Malicious

- Physical break-in
- Equipment theft
- Process violation
- Eavesdropping
- Malicious authorized user
- Social engineering
- Self replicating malware
- Malware that requires user interaction
- Malicious scan
- Malicious unauthorized access

Human error

- Equipment loss
- Miscommunication
- Implementation error

Environmental

- Electronic emanation/electro-magnetic pulse
- Hazardous materials
- Fire
- Flood
- Lightning
- Damaging Wind
- Temperature/humidity extremes

Considerations for assessing threats impact

- Confidentiality
- Integrity
- Availability
- Reputation/customer confidence
- Safety/health issues
- Fines/legal penalties
- Financial impact
- Productivity
- Historical data such as incident response report

Appendix E: Building Risk Profiles

Considerations for building risk profiles

- Which are the most critical assets? Select a few of the most critical assets.
- What vulnerabilities are most likely to be exploited by threats? Select a few of the vulnerabilities most likely to be exploited.
- What are the missing protection measures? Select a few of the most needed protection measures.
- Which threats would cause the largest impact? Select a few of the highest impact threats.
- Which threats are most likely to impact the unit? Select a few threats that are mostly likely to occur.
- What is the risk from dependent assets? For example, do systems depend on GatorLink authentication?

Document the risk profiles based on priorities identified above. Each risk profile should include the following.

a. Identify the assets affected and their criticality.
b. Identify vulnerabilities associated with assets
c. Identify threats likely to exploit assessed vulnerabilities.
d. Estimate likelihood that threats will exploit vulnerabilities.
e. Quantify the impact significance if threats exploit the vulnerabilities.
f. Recommend controls to mitigate the risk.

Appendix F: Mitigation Considerations

Mitigation considerations

- What can be done to improve the way in which security issues are integrated with the unit's business strategy?
- What funding level is appropriate to support the unit's security needs? What solution is most cost effective?
- How will the strategy impact usability?
- Is insurance needed to mitigate risks?
- Is unit administration willing to assume responsibility for some risks?
- What measures will be used to verify that this mitigation plan works and is effective?

Suggested content for mitigation strategy document

A. Introductory summary
B. The risk statements.
C. Mitigation recommendations
    a. Enumerate risks for which no mitigation is planned. Provide justification.
    b. Enumerate risks that will be monitored or studied for possible future action.
    c. For risks that will be mitigated, enumerate a prioritized list of recommendations.
    d. For each recommendation, estimate cost.
        i. Financial
        ii. Staff
        iii. Software
        iv. Hardware
        v. Space
        vi. Other
    e. An implementation schedule for each recommendation.
    f. Identify performance metrics that can be used to evaluate the effectiveness of each recommendation.

Consideration for management

A. What refinements, modifications, additions, or deletions must be made to the protection strategy?
B. What will the unit do to build on the results of this evaluation?
C. What else will management do to ensure that the unit improves its information security?
D. What can management do to support this security improvement initiative?
E. What are management's plans for ongoing security evaluation activities?