University Technology Services May 5, 2015

Risk Assessment Checklist

What is Risk Assessment?

Information technology risk assessment involves identifying and assessing technical risks to:

- Confidentiality – Ensuring authorized access and restricted sharing activities meet the trust expectations of the information owner; the state of being secret.
- Privacy - Described by Professor Anita Allen, Professor of Law and Philosophy at the University of Pennsylvania, as:
  - Physical privacy: spatial seclusion and solitude.
  - Informational privacy: confidentiality, secrecy, data protection, and control over personal information.
  - Proprietary privacy: control over names, likenesses, and repositories of personal identity.
  - Decisional privacy: control of basic human decisions, protection from interference in personal and family decisions.
- Operations – daily routine academic, research, and business activities.
- Financial Management – fiduciary responsibilities and reputation.
- Regulatory Compliance – adherence to standards posed by regulations such as FERPA, HIPAA, and PCI.

UTS Participation in Risk Assessment

Each year UTS completes a risk assessment that is reviewed with the university external auditor. Additional risk assessments may be completed as required for compliance (i.e., PCI, HIPAA, etc.) or security.

The CIO represents information technology risk interests in auditor meetings and with the Vice President of Academic Affairs and Provost.

UTS holds a weekly Change Management meeting to review planned changes meeting the standards posted here: http://www.oakland.edu/uts/policies - change

Performing Detailed Risk Assessment

Please review the Detailed Risk Assessment checklist when:

- Evaluating the information technology risk for a department.
- Changing the data management or technology management of your operation.
- Considering purchase of a new information technology resource.
- Considering the outsourcing of an information technology or data management operation.
- Staff or processes change, or on a regular audit basis, periodically or annually.
- Processing Confidential Data per Policy #860 Information Security.

All statements are designed for an answer or YES or TRUE. If you

have answered NO to any question, or if you have any questions, please contact the CIO for assistance.

Action Plan

After completion of an assessment, an Action Plan will be created identifying detailed steps needed to mitigate or remove risk. If risk cannot be mitigated or removed, then the CIO will engage the area Vice President, Office of Legal Affairs, and Risk Management, as needed, to determine risk tolerance.

DETAILED RISK ASSESSMENT

Domain: Strategic

1. Key stakeholders include the President, Provost, Vice Presidents, Legal Counsel, Risk Management, Internal Audit, CIO, and subject matter experts. Consider how they are involved in the particular IT risk management process.

Domain: Personnel

1. Staff members have completed review of IT policies.

2. Staff members have completed security training on the UHR web site.

3. Staff members have completed required regulatory training.

4. Staff members are aware of appropriate SSL/https web site usage.

5. Staff members are trained on the Emergency Preparedness http://wwwp.oakland.edu/police/emergency-

preparedness/prepared/ information technology compromises and understanding reporting procedures.

6. Access to information technology resources and data are based on **need to know and job responsibilities**.

7. Passwords are protected, not written down, and kept confidential.

8. Staff members do not log on to any resource, and then turn that resource over to another individual for use.

9. Accounts are immediately deactivated for terminated or transferred employees.

Domain: Infrastructure Assets

1. Key or critical department functions are documented.

2. Hardware assets are documented in an asset database, including system administrator, model number, serial number, operating system, and purchase record.

3. Software assets are documented in an asset database, including license information, usage metrics, renewal date, and installation location. University retention policies are followed: http://www.oakland.edu/policies/481/ with Appendix A.

4. Systems are routinely backed up, with a verified and tested backup and restore procedure.

Domain: Data

1. Policy #860 Information Security has been reviewed and implemented.

2. All locations of Confidential Data used in departmental operations are known, documented and protected.

3. Confidential Data are removed from information technology resources prior to reassignment or disposal of equipment.

4. Faculty members conducting research have determined if their research data are confidential and have protected the data accordingly.

5. Faculty and staff participating in federal, state, or grant agency operations or projects have determined if related data are confidential and have protected the data accordingly.

Domain: Communications

1. Confidential Data are not distributed via email or instant messaging.

2. Secure file transmission or VPN are used for file transfer.

3. Cell phones have been purged of all data according to manufacturer's instructions prior to disposal or release.

4. Multi-function printer/copiers have been purged of all data according to manufacturer's instructions prior to disposal or release.

Domain: Physical Security

1. Servers are protected by environmental controls, such as uninterruptible power supplies (UPS), surge protection, smoke detectors, fire suppression systems, water sensors, and temperature sensors.

2. All computers are in locations not easily accessible to outsiders.

3. Systems storing Confidential Data as defined in university Policy #860 are kept in a locked location with access restricted to authorized personnel.

4. Physical security has been reviewed with OUPD and/or Facilities.

5. Department carefully tracks access to keys.

6. Monitoring and surveillance solutions have been implemented where appropriate and in compliance with university Policy #674 Surveillance and Monitoring Technology.

Domain: Desktops, Laptops and Client Computing

1. Password-protection screen saver is enabled.

2. Firewall is installed.

3. Anti-virus software is installed and virus definitions up-to-date.

4. Operating system updates are performed on a regular basis.

5. Faculty and staff are aware of personal computer backup requirements and options.

6. Systems, printer/copiers, and storage devices are formatted and degaussed according to policy prior to equipment disposal, sale, or donation.

7. Equipment is maintained to comply departmental standards.

8. Confidential Data are not stored on laptops, or are stored with encryption enabled.

9. Publicly accessible computers are installed with a locked image, inability to store or cache personal data, and posted with a reminder to log out.

Domain: Server Considerations

1. Policy #880 Systems Administration Responsibilities has been reviewed and implemented.

2. Systems are regularly backed up, with a back-up copy stored off site, and restore processes tested and verified.

3. Vendor default passwords have been changed.

4. Unnecessary services and features have been disabled.

5. Operating system updates are performed on a regular basis.

Domain: Software Applications

1. All software is used in compliance with licensing and copyright.

2. Vendor security strategy reviewed annually.

3. Vendor default passwords have been changed.

4. Passwords comply with UTS posted password recommendations.

5. Vendor patch releases are promptly applied.

Domain: Network

1. Policy #850 Network Policy has been reviewed and implemented.

Domain: Compliance (PCI, HIPAA, etc.)

1. Security audit completed with University Technology Services.

2. Related systems added to external vulnerability scanning agreement.

3. Identified systems added to the relevant secure network or VLAN.

4. Staff members have completed relevant security training:

    - Cash handling training from Student Business Services for PCI.

    - Online compliance training for HIPAA or PCI.

5. UHR has verified that the employees have signed an agreement verifying they have read and understood the security policies and procedures, and that a background investigation (such as credit and criminal record check) has been done prior to systems access.

6. Risk Management has verified that any contractors or temporary employees with access have appropriate contract protections in place.

7. Secure disposal of sensitive Confidential Data and the retention period of such data prior to disposal have been verified.

8. Verify access control logging on the desktop or servers, including security review, successful and unsuccessful login attempts, access to audit logs, and root / administration access, and that logs are kept for one year.

8. Access control is defined on desktop, with the desktop access limited so that only the defined individual can access the desktop and then by unique username and password. Similar limited access must be implemented on relative servers.

9. A password protected screen saver that is enabled at 10 minutes of inactivity is installed on all necessary desktops.

10. Verify that all passwords on critical and confidential systems meet strong password requirements; minimum length standard followed; mix of letters, numbers and special characters; password reuse limits; forced password change every 90 days; passwords stored in a hashed non-reversible form; account locked after 3 failed password attempts.

11. Confidential Data processing, storage and transmission must be approved by both the data steward and the employee supervisor.

12. Verify that no unapproved remote access is allowed.

13. Verify account removal strategy for employee termination or contractor termination with the employee's supervisor and department director.

14. Verify ongoing account review requirements to ensure that malicious, out-of-date, unused or unknown accounts do not exist.

15. Verify that system installation procedures are documented, all unnecessary tools and services are removed, and that vendor default accounts, passwords and security settings are disabled or changed.

16. Verify that account numbers are sanitized before being logged in the audit log.

17. Verify that account numbers are not transmitted via email.

18. Verify that secure, encrypted communications are used for remote administration of production systems and applications.

19. Verify that all desktop operating systems, desktop office applications and any other software are regularly updated with the latest security-related patches.

20. Verify that virus scanning is installed and regularly updated.

21. Verify backup procedures and that procedures are in place to handle secure distribution and disposal of backup media and other media containing sensitive cardholder data.

22. Verify that all changes to the computer are formally documented, authorized, planned, and logged before being implemented.

23. Verify that the system clock is synchronized, and that logs include data and time stamp.

24. If web applications are involved verify that the Open Web Application Security Project group (www.owasp.org) or similar guidelines were taken into account in the development of Web applications.

25. If web applications are involved verify that cookies are encrypted.

26. If web applications or database storage are involved, verify that UTS web servers are used, and if not, complete defined network and firewall assessments.

30. Verify that a security assessment, penetration test, or both

performed on all Internet-facing applications in use.

31. Verify that if production data are used for testing and development purposes, Confidential Data are sanitized before usage.

32. Verify that all but the last four digits of the account number are masked when displaying account data.

33. Verify that accounts in databases and in backup media are stored securely – for example, by means of encryption or truncation.

34. If an SQL database is used, verify that controls are implemented to prevent SQL injection and other bypassing of client side input controls.

35. Verify that multiple physical security controls (such as badges, escorts, or mantraps) are in place that would prevent unauthorized individuals from gaining access to the facility and to equipment (such as servers, workstations, laptops, and hard drives) and media containing cardholder data.

36. Verify that Confidential Data are deleted or destroyed before physically disposed (for example, by shredding papers or degaussing backup media).

37. Verify that all Confidential Data printed on paper or received by fax are adequately protected against unauthorized access.