THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: RA-001-Risk Assessment	
Version 3	**Effective Date: 04/18/2016**

Responsible Office: Office of Cybersecurity	Last Review: 07/02/2020 Next Review: 07/02/2022
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

A risk assessment is used to identify security risks, examine threats to and vulnerabilities of systems, determine the magnitude of risks, and identify the proper security controls required to reduce the identified risk to an acceptable level defined by the business. This document provides guidance for data and system owners to conduct security risk assessments on their UTHSC resources for the purpose of determining areas of vulnerability, and to initiate necessary and appropriate remedies to the security of those resources.

Scope

This Standard applies to all UTHSC data and systems; regardless of technology, that transmits, stores, utilizes, or manipulates said data. This also applies to any and all computers, or other technology within in the UTHSC Enterprise. In short there are no exceptions nor exemptions of technology to this standard. This standard is applicable to all UTHSC employees, and students, as well as to third-party agents/vendors authorized to access UTHSC data.

Definitions

Data owner - The person who is ultimately responsible for the data and information being collected and maintained by his or her department or division

Risk Assessment - The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system

Risk - The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring

Security control - A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements

System owner - Person or organization having responsibility for the development, procurement, integration, modification, operation, and maintenance, and/or final disposition of an information system

Vendor - A commercial supplier of software or hardware

Vulnerability - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source

Responsibilities

Chief Information Security Office (CISO), is responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this standard.

Security Lead Analyst is responsible for providing security guidance for protection of PII, ePHI, and other sensitive information to the UTHSC community. This role along with the CISO is responsible for the adherence of this policy.

System/Data Owner is responsible for preparing the risk assessments. If a system contains HIPAA regulated data an annual risk assessment is mandated by the HIPAA Security Rule 45CFR164.308(a)(1)(ii)(A). The System Data Owners, or appointed delegate, are also responsible for performing the various steps related to identifying potential risks and threats and are required to ensure that identification of risks is properly categorized and documented in terms of their potential threat to their program area. The system and data owner(s) are then responsible to develop the risk mitigation plan and work towards complete mitigation of identified risks. All information regarding risks to the business systems will be the responsibility of the System Data Owner, or appointed delegate, to document, track and respond whenever appropriate.

Standard

1. **Risk Assessment**:

a. Data and system owners must complete a risk assessment in accordance with following parameters:
   - prior to a new implementation,
   - at the time of any major system changes, at least once annually.
   - in accordance with federal regulations, compliance requirements, state or local laws, or policies set by the University of Tennessee

b. Data and system owners should complete a risk assessment as part of best practices:
   - Prior to any activity or change to an activity that may have introduced new risk
   - Changes outside the system that may impact risk, i.e. third-party changes, or personnel changes

2. **Guidance for conducting the Risk Assessment** – UTHSC follows the National Institute of Standards and Technology (NIST) Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments or the latest version of the 800-30 . The general steps of conducting an RA shown in Figure 1

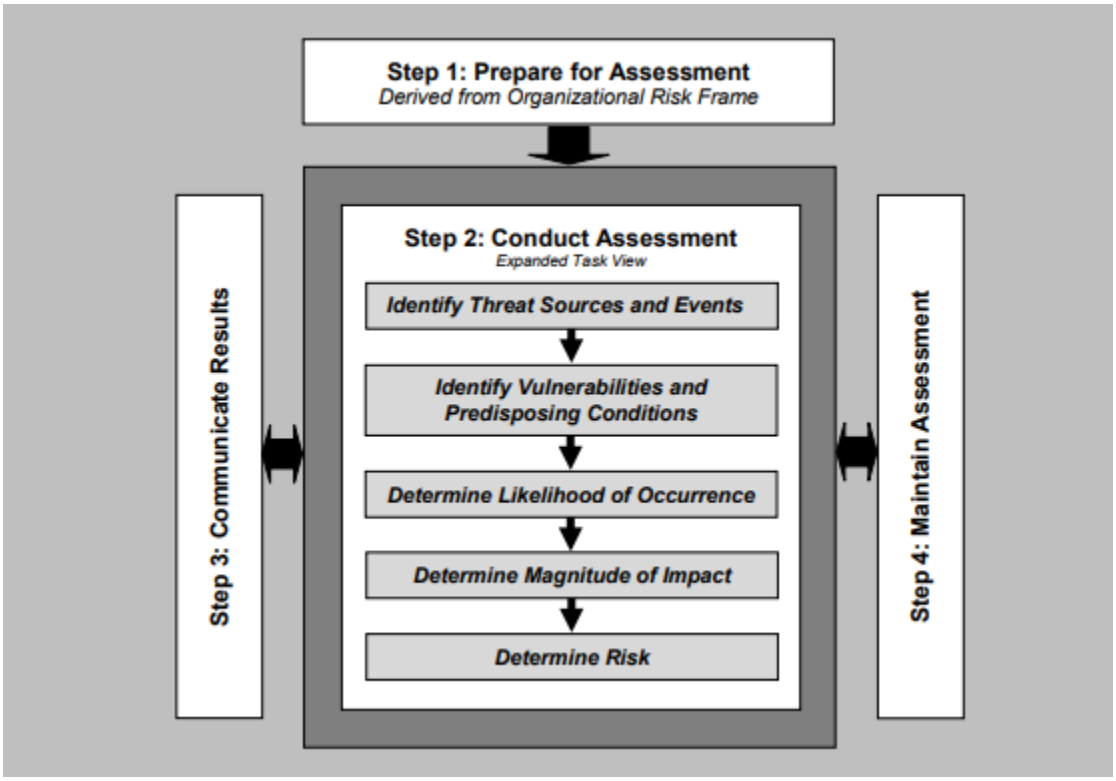

Figure 1: Risk Assessment Process

a. Prepare for the Risk Assessment
   - Identify the purpose of the assessment
   - Identify the scope of the assessment
   - Identify the assumptions and constraints associated with the assessment
   - Identify the sources of information to be used as inputs to the assessment
   - Identify the risk model and analytic approaches (i.e., assessment and analysis approaches) to be employed during the assessment.

b. Conduct the Risk Assessment
   - Identify threat sources that are relevant
   - Identify threat events that could be produced by those sources
   - Identify vulnerabilities that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation

- Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful
- Determine the adverse impacts to operations, assets, and individuals, resulting from the exploitation of vulnerabilities by threat sources (through specific threat events)
- Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations.

c. Communicate and Share Risk Assessment Information
- Communicate the risk assessment results
- Share information developed in the execution of the risk assessment
- Prepare and execute a mitigation plan to reduce risks found

d. Maintain the Assessment
- Monitor risk factors identified in risk assessments on an ongoing basis and understanding subsequent changes to those factors
- Update the components of risk assessments reflecting the monitoring activities carried out by organizations
- Ensure you know retention requirements of the RAs. i.e. HIPAA audits by Federal entities such as CMS or OCR may ask for up to three years of historical RAs

3. The risk assessment findings and remediation recommendations shall be reviewed with the Chief Information Security Officer (CISO) or Security Lead Analyst within one (1) month of completion of the risk assessment.
4. A mitigation plan shall be prepared to address the risk assessment findings.
5. **Annual Audit Process** - After the assessment is conducted, it is the sole responsibility of the System Data Owners to mitigate risks found. A mitigation plan strategy must be presented to the Office of Cybersecurity outlining what steps are being taken to eliminate the risk. All activity will be tracked, and an assessment completion record will be documented.

References

1. UTSA IT Policy [IT0124] Risk Assessment
2. HIPAA Security Rule 45CFR164.308(a)(1)(ii)(A)
3. -GP-002-Data & System Categorization
4. National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
5. National Institute of Standards and Technology (NIST) Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments.
6. NIST Glossary of Key Information Security Terms