

UT Space Institute Policy: IT0124-SI – Risk Assessment Plan	
Version: 1	Effective Date: 10/06/2019

Objectives

To establish a formal, documented plan to ensure the implementation of appropriate and effective Risk Assessment (RA) controls for information systems that host or contain sensitive University data.

Scope

This program applies to all users of and information technology (IT) resources owned, operated, or provided by the University of Tennessee Space Institute (UTSI) including its remote centers.

“Users” includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University’s information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

Principles

The University has chosen to adopt the policy principles established in the National Institute of Standards and Technology (NIST) 800 series of publications, and this program is based on those guidelines. This plan is based on guidelines in NIST Special Publication 800-53 Rev4 *Recommended Security Controls for Federal Information Systems and Organizations*.

The Chancellor or equivalent at each Campus must designate an individual or functional position responsible for information security at their Campus (Position of Authority and/or Campus Authority). The Position of Authority should be at a high enough organizational level to allow him/her to speak with authority on and for the Campus.

UTSI must develop or adopt and adhere to a program that demonstrates compliance with related policies and standards. This program is the responsibility of the Position of Authority.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of University policy is assumed if a User accesses, uses, or handles University resources.

Plan Details

Risk assessments identify and address potential risks and associated impacts to information systems and the information processed, stored, and transmitted by those systems (RA-3a). Risk assessment information is documented in the UTSI System Classification and Risk Assessment sheet. Risk assessments should be reviewed annually and updated whenever there are significant changes to critical information systems or their operational environment including new threats and vulnerabilities (RA-3b).

Roles and Responsibilities

Chief Information Officer (CIO): Has overall accountability of this Secure Network Infrastructure Program as the Position of Authority.

UT Space Institute Policy: IT0124-SI – Risk Assessment Plan	
Version: 1	Effective Date: 10/06/2019

IT Administrator: Responsible for conducting risk assessments for the system(s) for which they administer.

Applicable Systems:

This plan applies to all IT systems under the responsibility of UTSI personnel. A list of these systems can be found in the UTSI System Classification and Risk Assessment sheet.

Risk Assessment Process:

System Characterization

Business-critical systems are categorized for the information they store, transmit, or process. Information and guidance on system categorization can be found in IT0115-SI *Information and Computer System Classification Plan (RA-2)*.

Systems are characterized in order to establish the scope of the risk assessment activities. This information is part of the System Baseline

- General description/purpose
- Hardware
- OS and version
- Additional installed software and versions
- Connectivity with other systems

Threat Identification

Threat identification consists of identifying threat sources with the potential to exploit weaknesses in a system. The *Open Threat Taxonomy* should be used as a primer to help develop a comprehensive listing of potential threat sources.

Vulnerability Identification

Vulnerabilities can be identified using a combination of techniques and sources. UTM will primarily use vulnerability scans as detailed in IT0135-SI - *System and Information Integrity Program* to accomplish this (RA-5). Additional methods may be used in the process of vulnerability identification, if necessary.

Risk Analysis

Risk analysis is the determination (or estimation) of risk to a system through the consideration of factors, such as effectiveness of in-place controls, likelihood of attack, and the impact of an exploited vulnerability.

- Control Analysis
 - Analyzes in-place controls used to protect the system. This enhances the likelihood determination that a specific threat might successfully exploit a particular vulnerability.

UT Space Institute Policy: IT0124-SI – Risk Assessment Plan	
Version: 1	Effective Date: 10/06/2019

- Likelihood Determination
 - Considers a threat source’s motivation and capability to exploit a vulnerability, the nature of the vulnerability, the existence of security controls, and the effectiveness of mitigating security controls to describe how likely successful exploitation of a vulnerability by a given threat is to occur. This is expressed on a scale from 1 to 5 (see Appendix A).
- Impact Analysis
 - Considers impact to systems, data, and the University’s mission to develop the overall impact analysis. Criticality and sensitivity of the system and its data should also be considered to determine impact. This is expressed on a scale from 1 to 5 (see Appendix A).
- Risk Determination
 - Once the values for likelihood and impact have been determined, the overall level of risk can be calculated (see Appendix A).

Control Recommendations

Control recommendations are made to help reduce the level of risk to an information system and its data to an acceptable level. The following factors should be considered in recommending controls:

- Effectiveness of recommended options
- Legislation and regulation
- University policy
- Operational impact
- Safety and reliability

Results Documentation

The UTSI System Classification and Risk Assessment sheet is used to document the results of all risk assessment activities (RA-3c) and includes the following:

- Scope of the assessment based on the system characterization
- Methodology used to conduct the risk assessment
- Estimation of the overall risk posture of a system

Mandatory Controls

Mandatory security controls are University-wide controls that are required to be consistently designed, implemented, and monitored, and assessed.

UT Space Institute Policy: IT0124-SI – Risk Assessment Plan	
Version: 1	Effective Date: 10/06/2019

Risk management is an information systems lifecycle approach and not a single point of time evaluation. It is the responsibility of the information system and/or information owner to ensure risk is managed. All Campus Risk Assessment programs must include:

- Security Categorization (RA-2). Each Campus must categorize systems and information in accordance with University Policy IT0115 - *Information and Computer System Classification*, document the categorization and review security categorization bi-annually.
- Risk Assessment (RA-3). Each Campus must:
 - Conduct an assessment of risk, including the likelihood and impact of identified risks to the confidentiality, integrity, or availability of information and the information systems that process, store, or transmit that information;
 - Update the risk assessment annually or whenever there are significant changes to critical information systems or their operational environment including new threats and vulnerabilities.
 - Document and disseminate risk assessment results to appropriate management and system and information custodians.
- Vulnerability Scanning (RA-5). Each Campus must:
 - Scan critical systems and applications for vulnerabilities at least annually. Systems that require more frequent vulnerability scanning due to their risk profile or in order to comply with federal, state, or institutional regulations must be scanned accordingly.
 - Employ industry standard vulnerability scanning tools and techniques for:
 - Enumerating platforms, software flaws, and improper configurations;
 - Formatting checklists and test procedures; and
 - Measuring vulnerability impact;
 - Remediate legitimate vulnerabilities in accordance with organizational risk requirements.

References

IT0124 - *Risk Assessment*

IT0115-SI - *Information and Computer System Classification Plan*

IT0135-SI - *System and Information Integrity Program*

NIST SP 800-30 Rev1 - *Guide for Conducting Risk Assessments*

NIST SP 800-53 Rev4 - *Recommended Security Controls for Federal Information Systems and Organizations*

NIST SP 800-100 - *Information Security Handbook: A Guide for Managers*

Open Threat Taxonomy (Version 1.1) by James Tarala and Kelli K. Tarala, Enclave Security (October 2015)

Definitions

UT Space Institute Policy: IT0124-SI – Risk Assessment Plan	
Version: 1	Effective Date: 10/06/2019

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.

Impact - The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure, modification, destruction, or loss of information or information system availability.

Information Technology (IT) Risk Assessment - The process of identifying and measuring the factors that could negatively affect the security of information technology resources.

Likelihood - A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.

Risk - A measure of the extent to which an entity is threatened by a potential circumstance or event. Typically expressed as a function of impact and likelihood.

Risk Assessment - The process of identifying, estimating, and prioritizing information security risks through the analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact the University and the likelihood that such circumstances or events will occur.

Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation) or assets through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability - A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

UT Space Institute Policy: IT0124-SI – Risk Assessment Plan	
Version: 1	Effective Date: 10/06/2019

Appendix A – Risk Matrix

This table is used to help calculate the likelihood and impact of threats to IT resources.

Risk Matrix			
	Impact		
Likelihood	Low	Medium	High
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

Risk Matrix			
	Impact		
Likelihood	Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	High

These tables describe the different levels of likelihood and impact a threat might have.

Likelihood		
Low	0-32%	Unlikely to occur in normal circumstances but could occur at some point
Medium	33-65%	Likely to occur at some point
High	66-100%	Highly likely to occur at some time

Impact	
Low	Insignificant damage or harm to service users. Minor reputation impact. Possible financial loss for the campus.
Medium	Noticeable damage or harm to group of service users. Extensive reputation impact due to press coverage. External criticism likely. Moderate financial impact to campus.
High	Major damage or harm to service users. High reputation impact – national press and TV coverage. Minor regulatory enforcement. High financial impact to campus.