THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: RA-001.02-Risk Assessment Process	
Version 2	**Effective Date: 05/26/2021**

Responsible Office: Office of Cybersecurity	Last Review: 05/27/2021 Next Review: 05/27/2023
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

The purpose of this practice is to provide guidance to University stakeholders on how to perform a cybersecurity risk assessment.

Scope

The scope of this guidance focuses only on the areas of risk framing, identification, analysis, evaluation, and response. Areas such as risk monitoring and reporting are beyond the scope of this guidance.

Definitions

Risk - Risk is defined as the function of:

- The likelihood of a given threat source exploiting a vulnerability of an asset; and
- The resulting impact of the occurrence of the threat event

Threat Event - Threat event refers to any event during which a threat source, by means of a vulnerability, acts against an asset in a manner that has the potential to cause harm.

Threat Source – The agent or actor by which a vulnerability is compromised. This could be a malicious nation-state, an accidental insider, an environmental event, etc.

Vulnerability - A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. A vulnerability could also include any predisposing conditions.

Predisposing Condition - A condition that exists within an organization, a mission or business process, enterprise architecture, information system, or environment of operation, which affects (i.e., increases or decreases) the likelihood that threat events, once initiated, result in adverse impacts to organizational operations or assets. An office on the coast being susceptible to hurricanes would be a predisposing condition.

Likelihood - Likelihood refers to the probability that a given threat source is capable of exploiting a given vulnerability (or set of vulnerabilities). The probability can be derived based on factors namely, discoverability, exploitability, and reproducibility.

Impact - Impact refers to the magnitude of harm resulting from a threat source exploiting a vulnerability (or set of vulnerabilities).

Risk Tolerance – Risk tolerance is the level of risk the University is willing to tolerate to achieve University or Department objectives.

Responsibilities

Risk Approver - Senior stakeholder within the University with the responsibility and accountability to ensure risks are appropriately managed within the Universities tolerance level.

System Owner – Senior stakeholder of a University system responsible for ensuring that technology system functions meet University goals and adhere to University policies and standards. Working with the System Custodian, ITS Risk Management Function, and Cybersecurity Function, they should identify the potential threats to a system, conceptualize risk scenarios, and determine risk likelihood and impact.

Data Owner - A Data Owner has administrative control and has been officially designated as accountable for a specific information asset dataset. This is usually the senior most officer in a division. The Data Owner may or may not be the same as the system owner. For instance, the Registrar is the Data Owner for student data but may not be the System Owner for a specific system accessing that data. The same may be true for data that could include financial, employee, healthcare, etc.

System Custodian - An individual or group within the University that is responsible for the maintenance and operations of the technological infrastructure, including network or applications, to support the running of the system(s) supporting University activities. The system custodian should know the system assets and technical operations very well and be able to advise on the technical impact for a compromised system.

Data Custodian – Like the System Custodian, the Data Custodian is a person who has technical control over an information asset dataset. This person may or may not be the same as the System Custodian. For instance, the System Custodian may be responsible for the administration of a database server, while the Data Custodian would be responsible for the data within the database itself.

ITS Risk Management Function - An individual or group within the University responsible for the ITS risk management approach. They should serve as a bridge between the technical and business function during risk assessment process and provide oversight of the risk assessment activities to ensure consistent risk-based decisions.

Office of Cybersecurity - An individual or group within the University responsible for the implementation and maintenance of cybersecurity controls in systems supporting business activities. The Office of Cybersecurity should be able to advise the appropriate measures to address identified threats/attacks.

Practice

Risk Assessment Process

Risk assessment is about identifying risks that are specific to the environment and determining the level of identified risks. The main steps in a risk assessment are risk identification, risk analysis, risk evaluation, and risk response.

Step 1: Risk Identification

Task A: Identify Assets

The first task is to identify and create an inventory of all physical and logical assets that make up the system that is within the risk assessment scope. Each asset should be classified using the System/Data Classification Standard. Use this asset inventory to create a system diagram that provides a visual representation of the interconnectivity and communication paths between the assets that make up the system. See Figure 1 below.

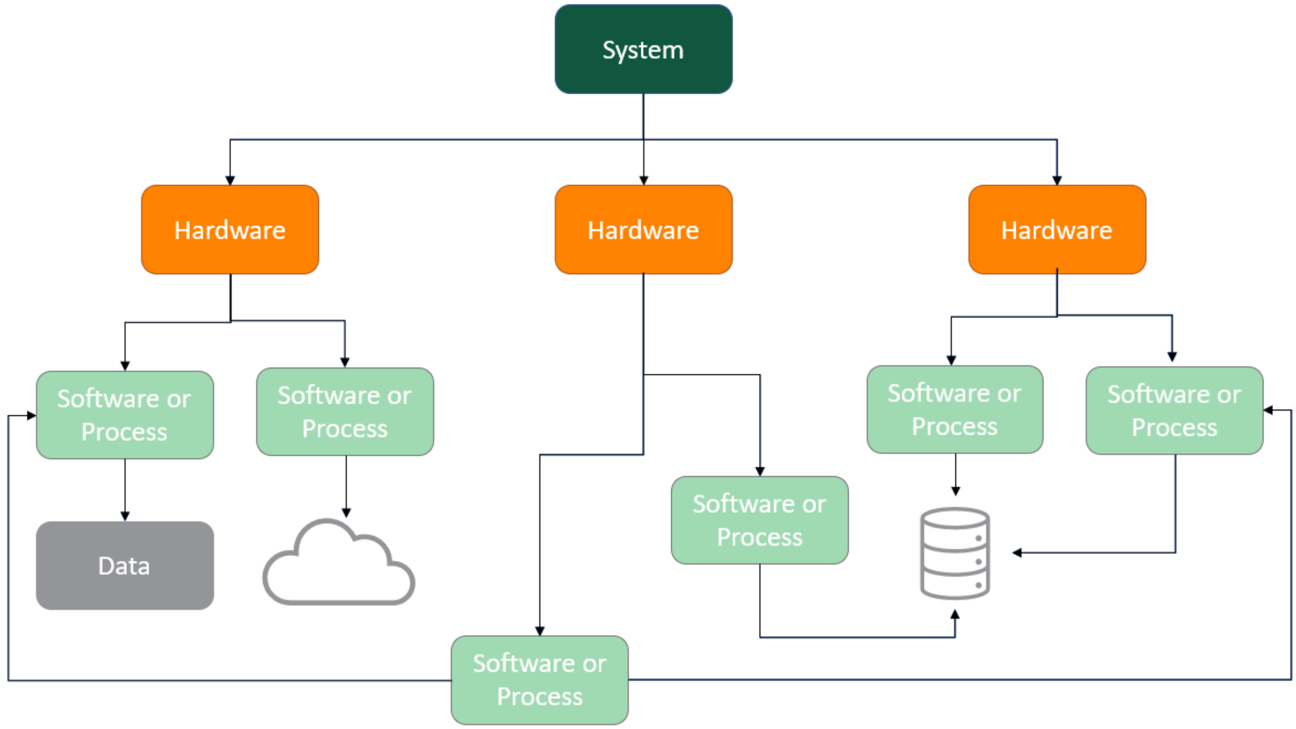


Figure 1

The authorization boundary defines the scope for a system to facilitate risk management and accountability. The system may be supported by one or more enabling systems that provide support during the system life cycle. Enabling systems are not contained within the authorization boundary of the system and do not necessarily exist in the system's environment of operation. An enabling system may provide common (i.e., inherited) controls for the system or may include any type of service or functionality used by the system such as identity and access management services, network services, or monitoring functionality. The connectivity (e.g., API) may need to be in the scope of the authorization boundary between the system and the enabling system. Finally, there are other systems the system interacts with in the operational environment. The other systems are also outside of the authorization boundary and may be the beneficiaries of services provided by the system or may simply have some general interaction.

Figure 2 illustrates the conceptual view of the system and the relationships among the system, system elements, enabling systems, other systems, and the environment of operation.

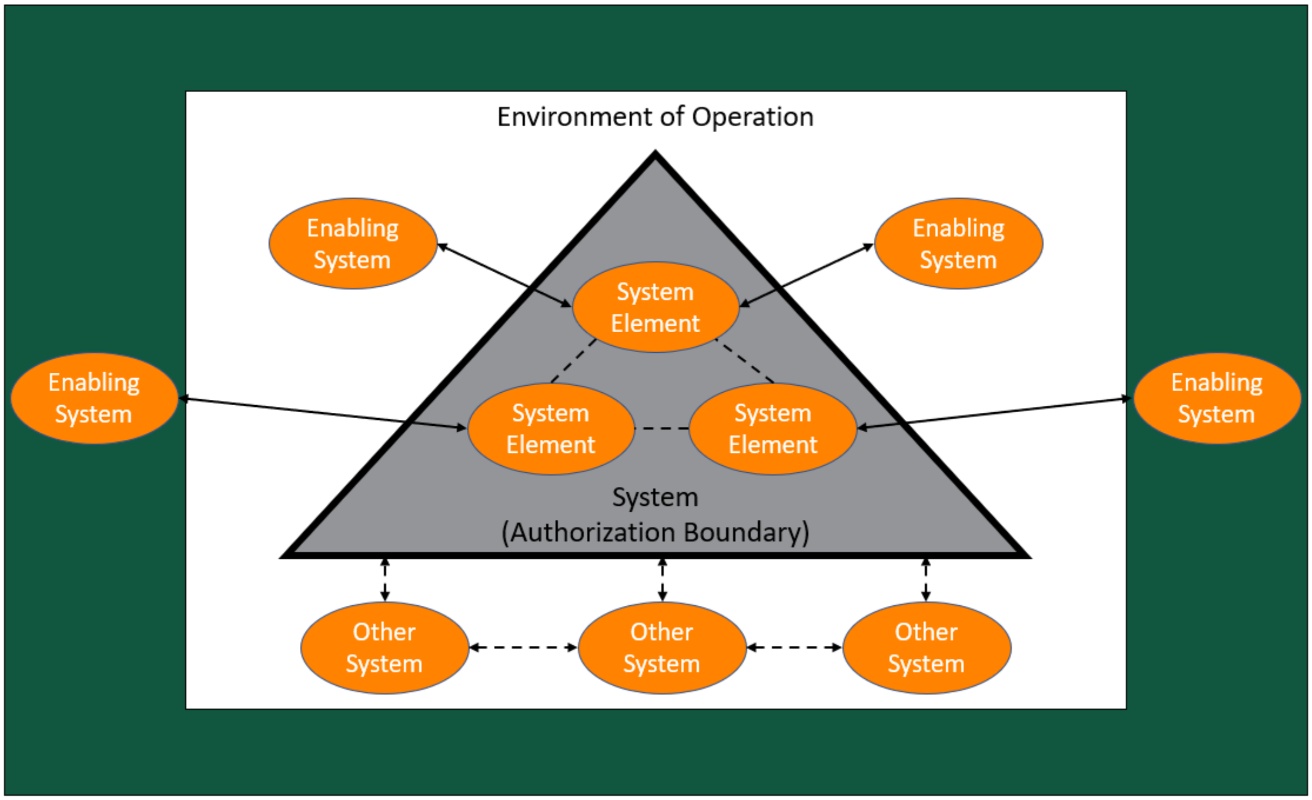


Figure 2

Task B: Identify Threats

With the asset inventory list, system diagram, and network architecture diagram, identify the threat events that could exploit vulnerabilities for each asset.

The MITRE ATT&CK Framework is a helpful tool in identifying these potential threats. It is a knowledge base of adversary tactics and techniques based on real-world observations and includes tactics such as initial access, lateral movement, and privilege escalation.

Task C: Construct Risk Scenarios

Constructing risk scenarios is the last task to complete the Risk Identification Step. This task aims to create “what could go wrong” scenarios that provide realistic and relatable view of risks based on the business context, system environment and pertinent threats.

A well-constructed risk scenario facilitates communication to stakeholders and allows for structured analysis of risks in subsequent steps. A risk scenario should articulate the following four (4) key elements:

- Threat Source - The agent or actor by which a vulnerability is compromised.
- Threat event - An attack event that has been identified in task B targeting an asset identified in task A.
- Vulnerability - A weakness in the asset or processes supporting the asset that can be exploited by the identified threat event.
- Consequence - The direct result of the threat event exploiting a vulnerability.

This is illustrated in the “Risk Scenario Model” diagrammed in Figure 3 below.

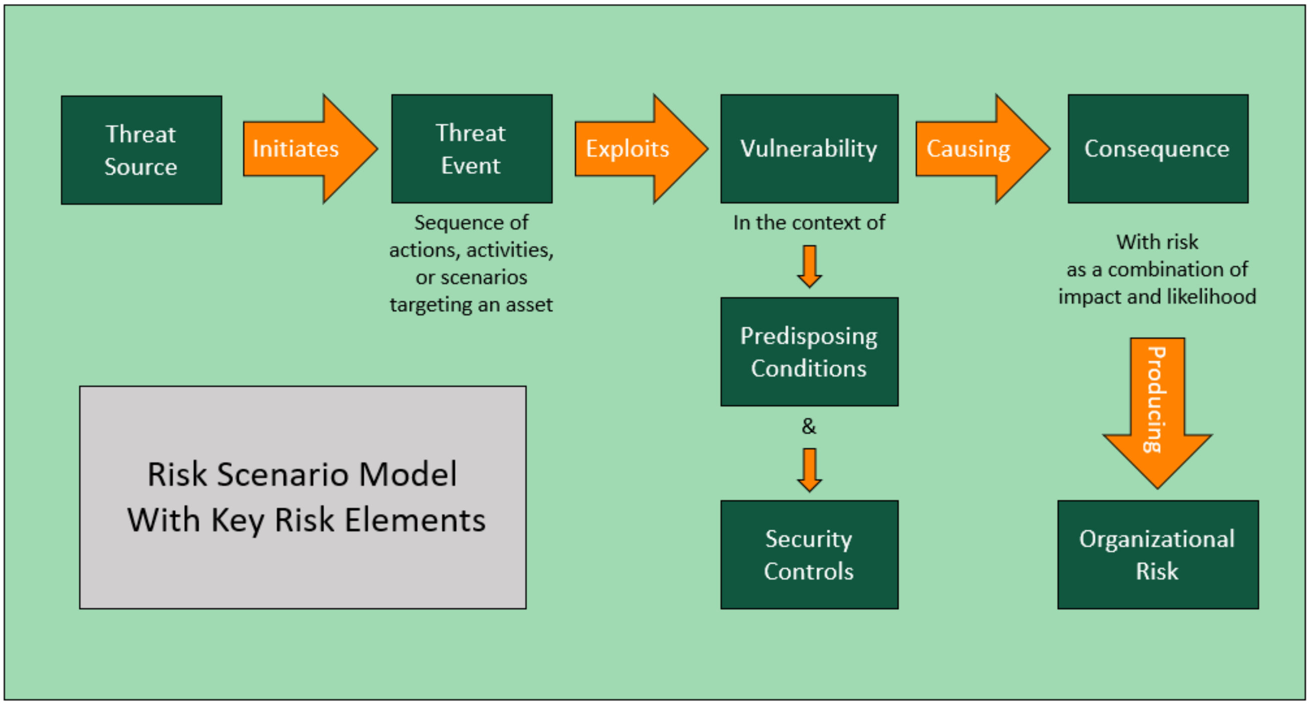


Figure 3

Some examples of well-constructed risk scenarios are illustrated below.

Legend: Threat Source | Threat Event | Vulnerability | Consequence

A malicious outsider could steal a laptop that has not be encrypted or properly secured leading to a breach of student data.

A clinic employee with a publicly visible computer monitor without a privacy screen could accidentally leave a patient record pulled up when helping another patient, exposing patient data.

A cloud service provider that cannot provide disaster recovery testing assurance documentation for a critical service could suffer an unexpected outage resulting in a loss of critical services.

Step 2: Risk Analysis

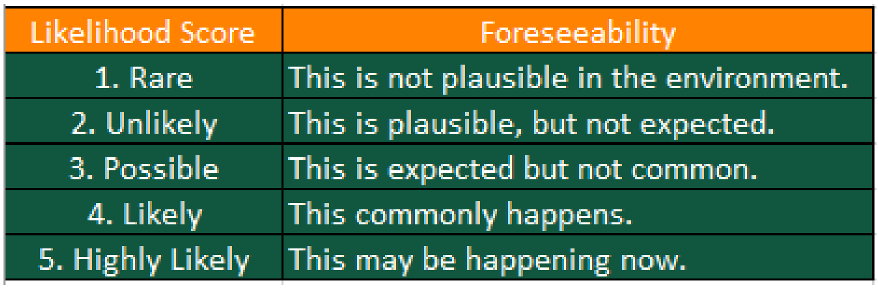
The goal of risk analysis is analyzing the elements that make up each risk scenario to determine:

- The likelihood of a risk scenario occurring; and
- The impact (i.e., magnitude of harm) resulting from the occurrence of a risk scenario

Task A: Determine Likelihood

Historical or expected occurrence of an event has traditionally been used as a metric to measure the risk likelihood (e.g., Event is expected to occur once every year or has occurred once in the past year). However, the use of such a metric to measure cybersecurity risk likelihood may not be appropriate due to the dynamic nature of cybersecurity threats. A system that has not been compromised previously does not mean it would not be compromised in the future.

As a general guidance, the likelihood of cybersecurity risks should be assessed from the perspective of threats and vulnerabilities. One method is to use a qualitative approach using a scale of 1-5 illustrated in Figure 4 below.

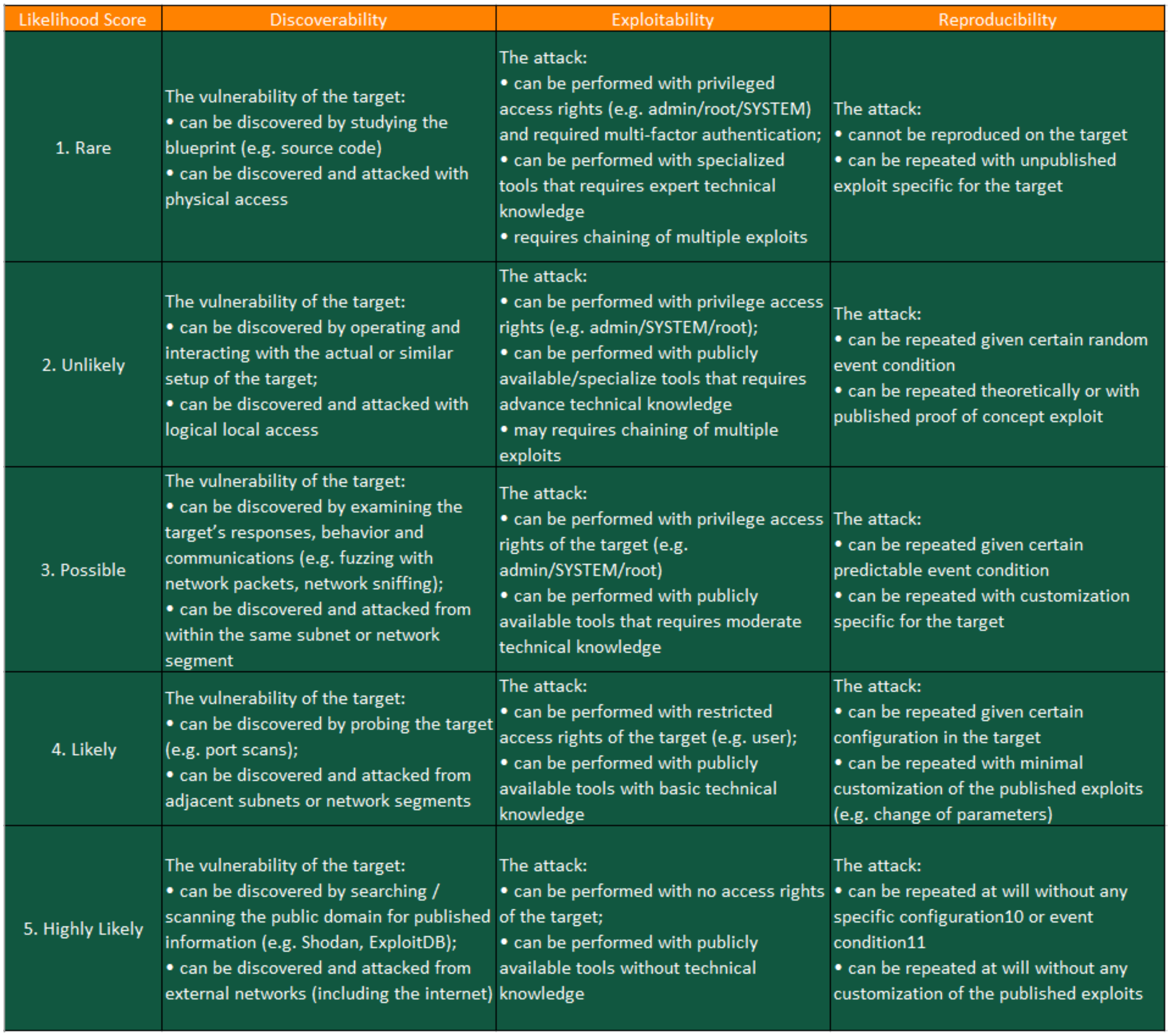


Likelihood Score	Foreseeability
1. Rare	This is not plausible in the environment.
2. Unlikely	This is plausible, but not expected.
3. Possible	This is expected but not common.
4. Likely	This commonly happens.
5. Highly Likely	This may be happening now.

Figure 4

Another method to determine the cybersecurity risk likelihood is to use a semi-quantitative approach illustrated in Figure 5 and consider the following factors:

- Discoverability - How easy would an adversary be able to discover the vulnerability of an asset? This is dependent on the availability of information about the vulnerability and the exposure of the vulnerable asset.
- Exploitability - How easy would an adversary exploit the vulnerability of an asset? This is dependent on the access rights, complexity of tools, as well as technical skills required to carry out the attack.
- Reproducibility - How easy would an adversary be able to reproduce the attack on the asset? This is dependent on the complexity of the exploit customization and the environmental conditions required to carry out the attack.



Likelihood Score	Discoverability	Exploitability	Reproducibility
1. Rare	The vulnerability of the target: • can be discovered by studying the blueprint (e.g. source code) • can be discovered and attacked with physical access	The attack: • can be performed with privileged access rights (e.g. admin/root/SYSTEM) and required multi-factor authentication; • can be performed with specialized tools that requires expert technical knowledge • requires chaining of multiple exploits	The attack: • cannot be reproduced on the target • can be repeated with unpublished exploit specific for the target
2. Unlikely	The vulnerability of the target: • can be discovered by operating and interacting with the actual or similar setup of the target; • can be discovered and attacked with logical local access	The attack: • can be performed with privilege access rights (e.g. admin/SYSTEM/root); • can be performed with publicly available/specialize tools that requires advance technical knowledge • may requires chaining of multiple exploits	The attack: • can be repeated given certain random event condition • can be repeated theoretically or with published proof of concept exploit
3. Possible	The vulnerability of the target: • can be discovered by examining the target's responses, behavior and communications (e.g. fuzzing with network packets, network sniffing); • can be discovered and attacked from within the same subnet or network segment	The attack: • can be performed with privilege access rights of the target (e.g. admin/SYSTEM/root) • can be performed with publicly available tools that requires moderate technical knowledge	The attack: • can be repeated given certain predictable event condition • can be repeated with customization specific for the target
4. Likely	The vulnerability of the target: • can be discovered by probing the target (e.g. port scans); • can be discovered and attacked from adjacent subnets or network segments	The attack: • can be performed with restricted access rights of the target (e.g. user); • can be performed with publicly available tools with basic technical knowledge	The attack: • can be repeated given certain configuration in the target • can be repeated with minimal customization of the published exploits (e.g. change of parameters)
5. Highly Likely	The vulnerability of the target: • can be discovered by searching / scanning the public domain for published information (e.g. Shodan, ExploitDB); • can be discovered and attacked from external networks (including the internet)	The attack: • can be performed with no access rights of the target; • can be performed with publicly available tools without technical knowledge	The attack: • can be repeated at will without any specific configuration10 or event condition11 • can be repeated at will without any customization of the published exploits

Figure 5

The following steps can be taken to derive the semi-quantitative likelihood score of a cybersecurity risk scenario:

1. Assign a score for each of the 3 likelihood factors (i.e., 1 – 5)
2. Average the score and round off to the nearest whole number

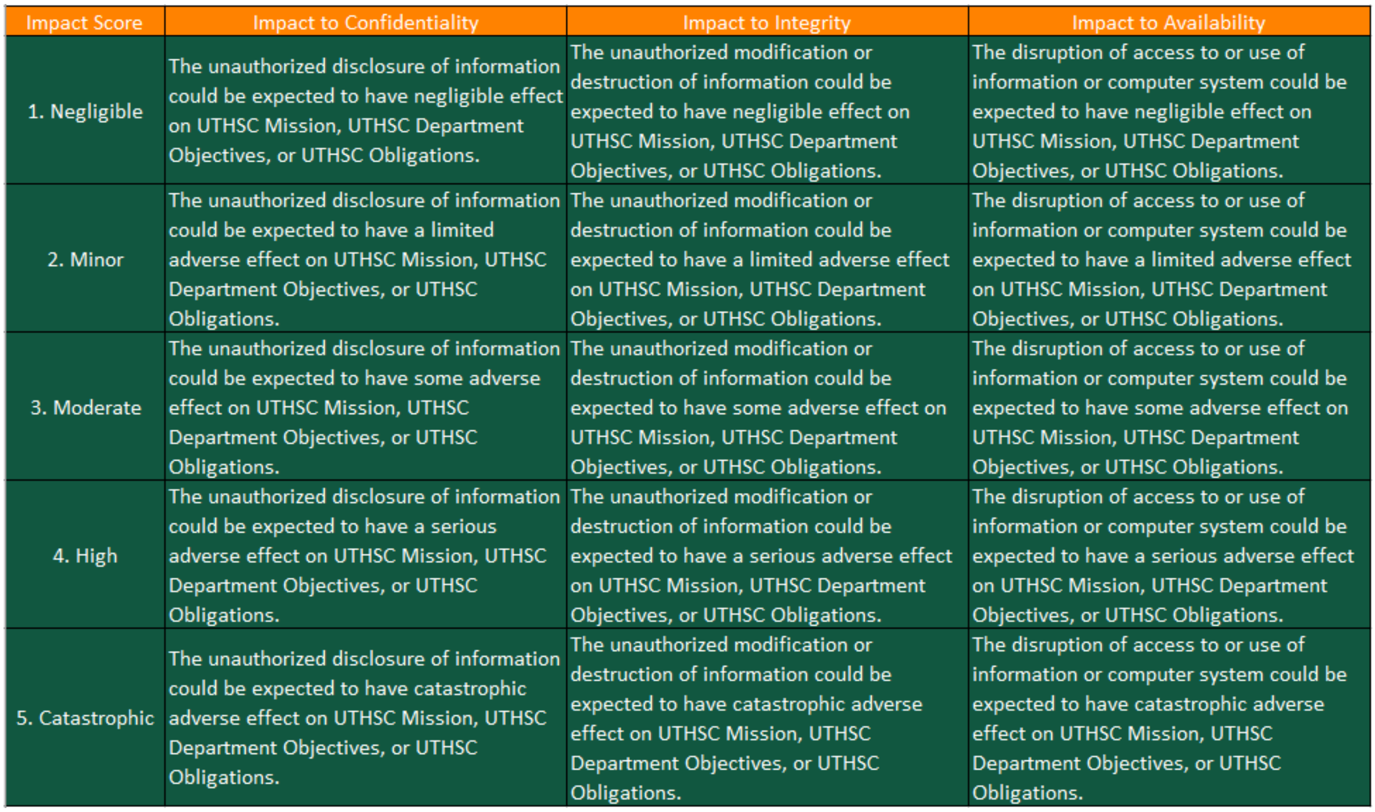
3. The final score will be the likelihood of the risk scenario; 5 being "Highly Likely" and 1 being "Rare"

Task B: Determine Impact

In general, the manifestation of a risk scenario can compromise the confidentiality, integrity and/or availability of assets (e.g., data, equipment, operations). Any compromise of the assets will translate to adverse impact at the following three (3) levels:

1. UTHSC Mission – The mission of the University of Tennessee Health Science Center is to improve the health and well-being of Tennesseans and the global community by fostering integrated, collaborative, and inclusive education, research, scientific discovery, clinical care, and public service.
2. UTHSC Department Objectives – The department objectives are defined by the department conducting the assessment.
3. UTHSC Obligations - UTHSC must protect our employee's, student's, and patient's interests, data, privacy, and financial future against misuse of their financial, medical, or personal information.

Each risk scenario may be assessed to have different impact ratings in areas of confidentiality, integrity, and availability as illustrated in Figure 6. The highest impact rating should be taken as the final "Impact" score.



Impact Score	Impact to Confidentiality	Impact to Integrity	Impact to Availability
1. Negligible	The unauthorized disclosure of information could be expected to have negligible effect on UTHSC Mission, UTHSC Department Objectives, or UTHSC Obligations.	The unauthorized modification or destruction of information could be expected to have negligible effect on UTHSC Mission, UTHSC Department Objectives, or UTHSC Obligations.	The disruption of access to or use of information or computer system could be expected to have negligible effect on UTHSC Mission, UTHSC Department Objectives, or UTHSC Obligations.
2. Minor	The unauthorized disclosure of information could be expected to have a limited adverse effect on UTHSC Mission, UTHSC Department Objectives, or UTHSC Obligations.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on UTHSC Mission, UTHSC Department Objectives, or UTHSC Obligations.	The disruption of access to or use of information or computer system could be expected to have a limited adverse effect on UTHSC Mission, UTHSC Department Objectives, or UTHSC Obligations.
3. Moderate	The unauthorized disclosure of information could be expected to have some adverse effect on UTHSC Mission, UTHSC Department Objectives, or UTHSC Obligations.	The unauthorized modification or destruction of information could be expected to have some adverse effect on UTHSC Mission, UTHSC Department Objectives, or UTHSC Obligations.	The disruption of access to or use of information or computer system could be expected to have some adverse effect on UTHSC Mission, UTHSC Department Objectives, or UTHSC Obligations.
4. High	The unauthorized disclosure of information could be expected to have a serious adverse effect on UTHSC Mission, UTHSC Department Objectives, or UTHSC Obligations.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on UTHSC Mission, UTHSC Department Objectives, or UTHSC Obligations.	The disruption of access to or use of information or computer system could be expected to have a serious adverse effect on UTHSC Mission, UTHSC Department Objectives, or UTHSC Obligations.
5. Catastrophic	The unauthorized disclosure of information could be expected to have catastrophic adverse effect on UTHSC Mission, UTHSC Department Objectives, or UTHSC Obligations.	The unauthorized modification or destruction of information could be expected to have catastrophic adverse effect on UTHSC Mission, UTHSC Department Objectives, or UTHSC Obligations.	The disruption of access to or use of information or computer system could be expected to have catastrophic adverse effect on UTHSC Mission, UTHSC Department Objectives, or UTHSC Obligations.

Figure 6

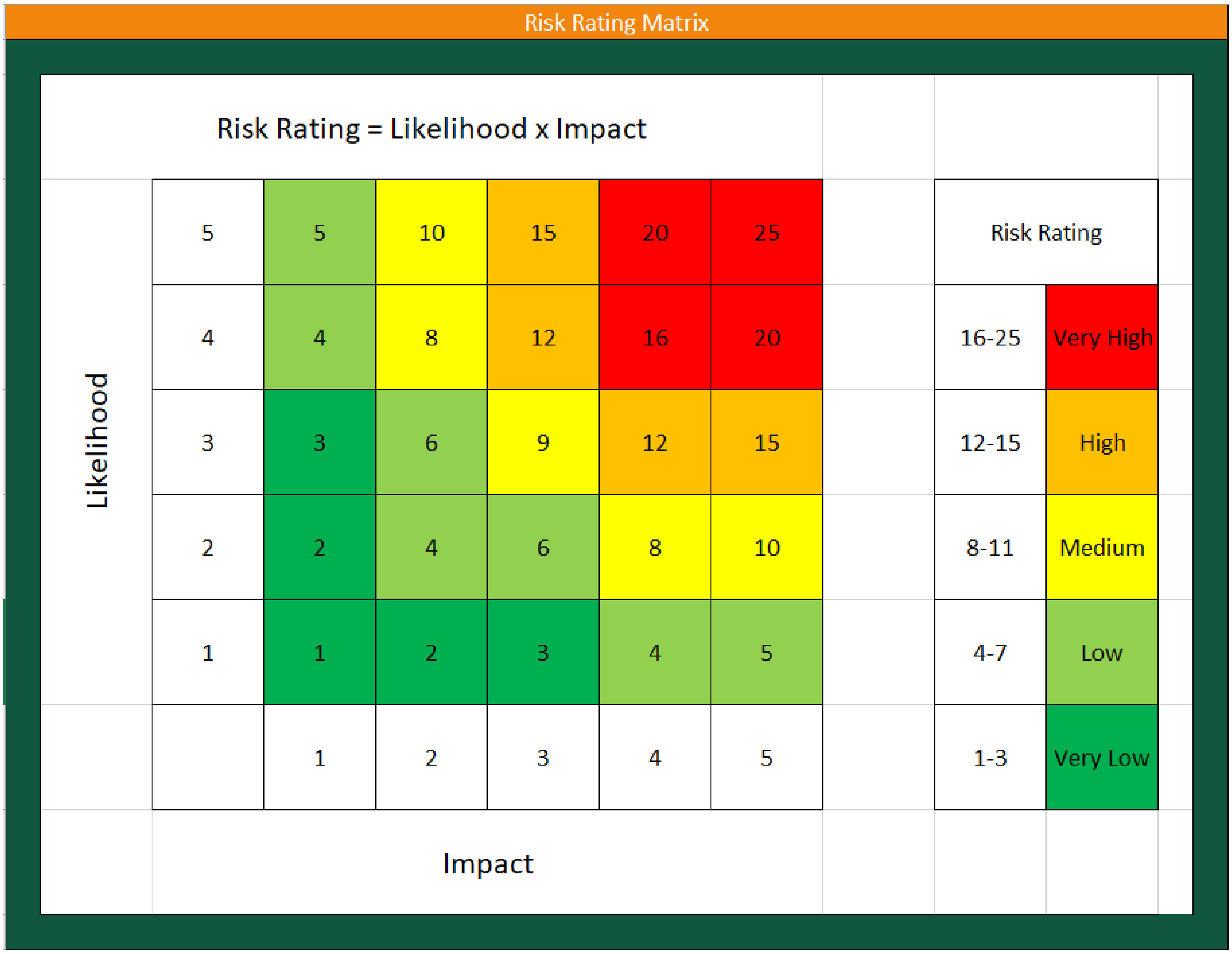
Step 3: Risk Evaluation

Risk evaluation is about determining and understanding the significance of risk level, and comprises the following tasks:

1. Determine Risk Rating
2. Document risk

Task A: Determine risk rating

Risk is a function of the likelihood of a given threat source initiating a threat event by exploiting a potential vulnerability of an asset causing a resulting impact. This can be illustrated using a risk matrix by multiplying the Likelihood and Impact to calculate the Risk Rating.



Risk Rating Matrix

Risk Rating = Likelihood x Impact

Likelihood	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Impact				

Risk Rating	
16-25	Very High
12-15	High
8-11	Medium
4-7	Low
1-3	Very Low

Figure 7

Task B: Document Risk

A risk assessment is incomplete without documentation. The outputs from previous steps must be clearly documented in a Risk Register for communication to stakeholders. A Risk Register is a record of all the risk scenarios identified, including their determined risk level. The Risk Register is a living document to be regularly reviewed and updated to ensure that the University's management has an up-to-date picture of the University's cybersecurity risks when making risk-informed decisions.

The Office of Cybersecurity maintains a Risk Register for use by University departments. Send an email to itsecurity@uthsc.edu for assistance documenting identified risks or accessing the Risk Register.

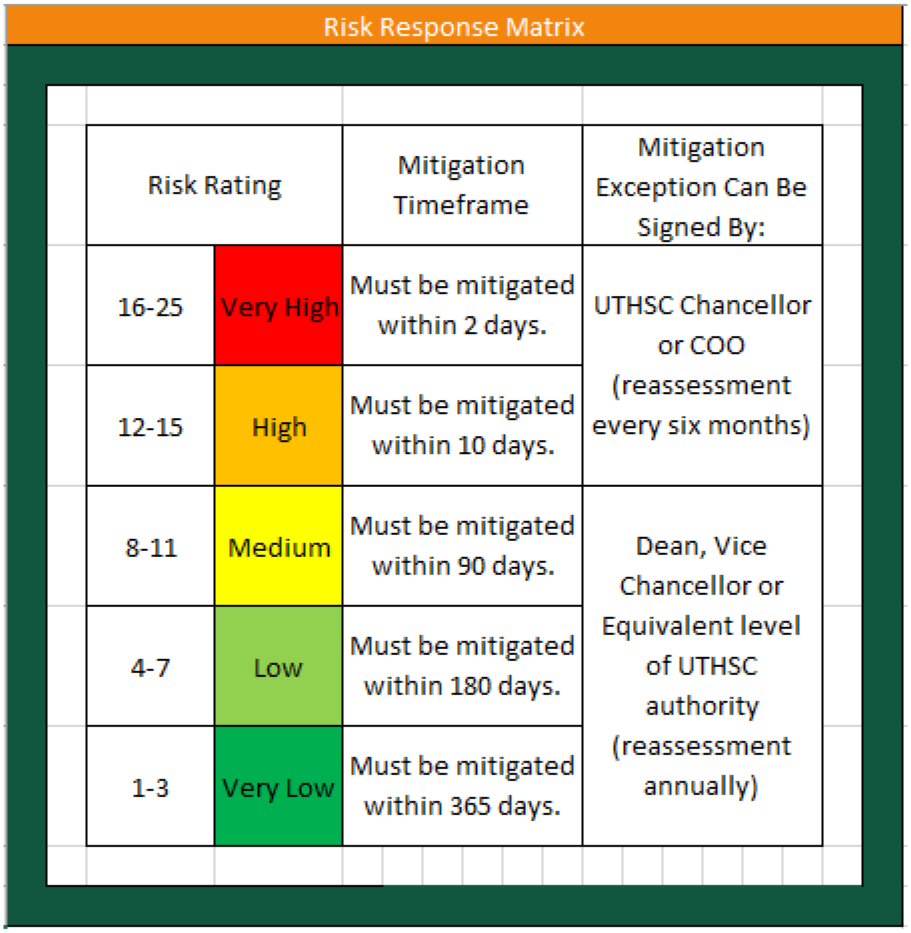
Having evaluated and documented the identified risks, the next step is to determine the appropriate risk response to keep identified risks within the University's risk tolerance level.

Step 4: Risk Response

The University standard for risk response is one of three options:

1. Avoid - Risk avoidance means discontinuing an action/activity that exposes the University to the identified risk. This may appear extreme but may be the best course of action if the risk outweighs the benefits. Example: Not conducting online payment transactions is an example of avoiding the risk of attackers hijacking the transaction to make fraudulent payments.
2. Mitigate- Risk mitigation means putting in place measures to reduce the risk level. This can be achieved through the deployment of security controls. Example: Implementing a firewall to restrict network traffic is an example to mitigate the risk of a system communicating with malicious external servers.
3. Exception/Exemption- A risk exception or exemption is when a system owner chooses not to avoid or mitigate the identified risk. Requests for exception from security controls, UTHSC IT/InfoSec Standards or Practices must be submitted in writing to the Office of Cybersecurity using TechConnect and the subsequent Security Exceptions and Exemptions to ITS Security Controls Request Form found therein. Identified risks using the Security Standards Exception/Exemption process must be periodically reassessed according to the timeframes illustrated in Figure 8 below. The Security Exceptions and Exemptions to ITS Security Controls Request Form must be signed by an authorized signer with the appropriate level of authority indicated on Figure 8.

As a general guidance, a control is considered appropriate and relevant to a risk when it reduces risk likelihood or reduces risk impact and the control itself does not generate more risk than the risk it is implemented to protect against. Mitigation efforts must be prioritized based on the level of risk to the University. The Risk Level and associated Mitigation Timeframe are illustrated in Figure 8 below.



Risk Response Matrix

Risk Rating		Mitigation Timeframe	Mitigation Exception Can Be Signed By:
16-25	Very High	Must be mitigated within 2 days.	UTHSC Chancellor or COO (reassessment every six months)
12-15	High	Must be mitigated within 10 days.	
8-11	Medium	Must be mitigated within 90 days.	Dean, Vice Chancellor or Equivalent level of UTHSC authority (reassessment annually)
4-7	Low	Must be mitigated within 180 days.	
1-3	Very Low	Must be mitigated within 365 days.	

Figure 8

Whichever risk response option is taken, senior management (with the appropriate level of authority and accountability) within the University must formally approve the selected risk response and monitor any remediation/mitigation activities.

References

1. GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices
2. Security Exceptions and Exemptions to ITS Security Controls Request Form
3. MITRE ATT&CK Framework
4. GP-002 Data & System Classification