THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: RM-001.01-Risk Assessment Process	
Version 5	Effective Date: 05/27/2021

Responsible Office: Office of Cybersecurity	Last Review: 11/28/2022 Next Review: 11/28/2024
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

A security 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 initiating necessary and appropriate remedies to the security of those resources. This standard is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but is not limited to, security requirements and safeguards for the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or Gramm-Leach-Bliley Act (GLBA).

Scope

This Standard applies to all UTHSC data and systems; regardless of technology, that transmit, store, utilize, or manipulate UTHSC data. This also applies to all computers or other technology within the UTHSC Enterprise. In short, there are no exceptions nor exemptions of technology to this standard. This standard is applicable to all UTHSC employees, students, and third-party agents/vendors authorized to access UTHSC data.

Definitions

Impact - Impact refers to the magnitude of harm resulting from a threat source exploiting a vulnerability (or set of vulnerabilities).
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.
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, results in adverse impacts to organizational operations or assets. An office on the coast being susceptible to hurricanes would be a predisposing condition.

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

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

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.

Threat Event – A 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.

Responsibilities

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

Data/System Custodian – An individual or group within the University that is responsible for the maintenance and operations of the technology asset/system. The asset custodian should know the asset and technical operations very well and be able to advise on the technical impact of a compromised system. The asset custodian coordinates with data owners and system owners to ensure data is properly stored, maintained, and protected. They are responsible for applying required security controls based on the classification, designated in GP-005-Data Security.

Note: Just like with owners, data and system custodians may be different groups or individuals. 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.

Data/System/Asset Owner – The owner is usually a senior stakeholder of a University asset/system and is responsible for ensuring that technology functions meet University goals and adhere to University policies and standards. The asset owner is ultimately responsible for ensuring the University security policies are followed and that risks associated with the asset/system are identified and managed to an acceptable level. The owner is ultimately responsible for the data and information being collected and maintained by their department or division. The owner shall address the following:

- **Review and inventory** — Review and inventory IT resources within their areas of responsibility
- **Assignment of data and or system classification labels** — Assign classification based on the system or data type and potential impact level
- **Approval and Review of Access Rights and Permissions** – Ensure that users, groups, and permissions are appropriate and limited to the least amount of privilege needed to perform necessary tasks
- **Risk Management** – Identification and management of risk associated with the data or asset to an acceptable level.

Note: An asset may have separate data and system owners. For instance, the Registrar is the Data Owner for student data but may not be the System Owner for a specific system accessing or storing that data. The same may be true for data that could include financial, employee, healthcare, etc.

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

Practice

Risk Assessment Process

Risk assessment is about identifying risks that are specific to the environment and determining the level of identified risks. 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 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 GP-002-Data & System Classification. 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. The ITS Infrastructure team can provide templates to assist in creating system diagrams.

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.

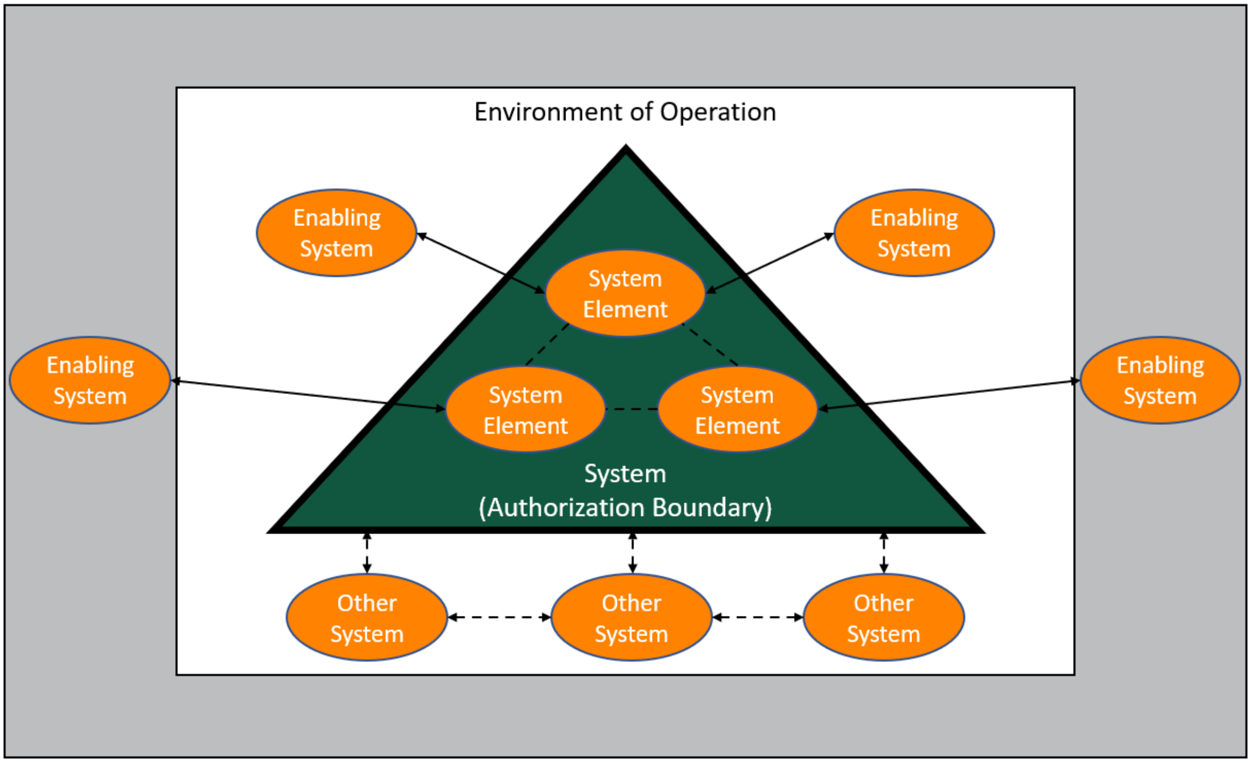


Figure 2

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.

There are many ways that threats and vulnerabilities can be identified for each system. One could start with a list of possible threats and assess each asset based on those possible threats. One could also start from a list of known vulnerabilities for each asset and assess threats associated with those vulnerabilities. There are many possible approaches to threat identification, and all have different pros and cons. To follow a standardized approach, UTHSC leverages the NIST Risk Management Framework (RMF) to manage the risk lifecycle including the identification of threats. This process starts by classifying each asset which results in a security categorization level. Based on that security level and the asset type, a tailored set of applicable controls can be applied to the system/asset. The risk assessment is then conducted based on the maturity level implementation of those tailored controls. Controls that have not been adequately applied to a system or asset may represent risk to those assets.

The MITRE ATT&CK Framework is another helpful tool in identifying 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. This can be used in conjunction with the NIST RMF.

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.

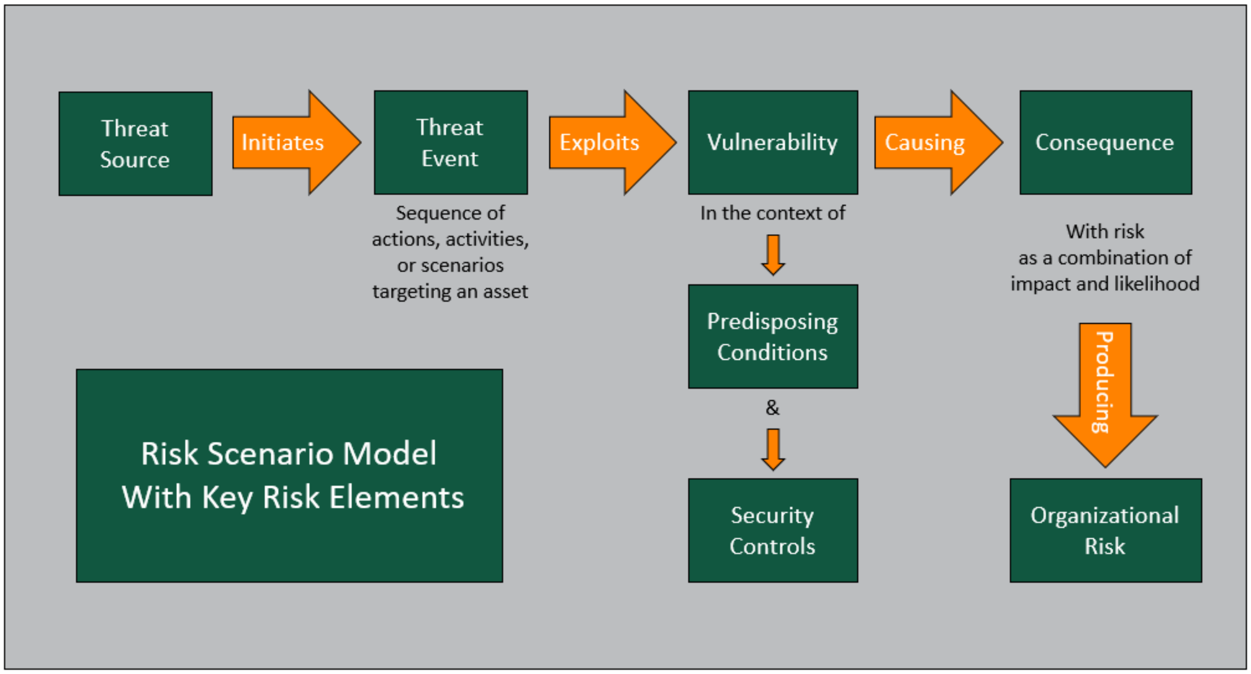


Figure 3

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

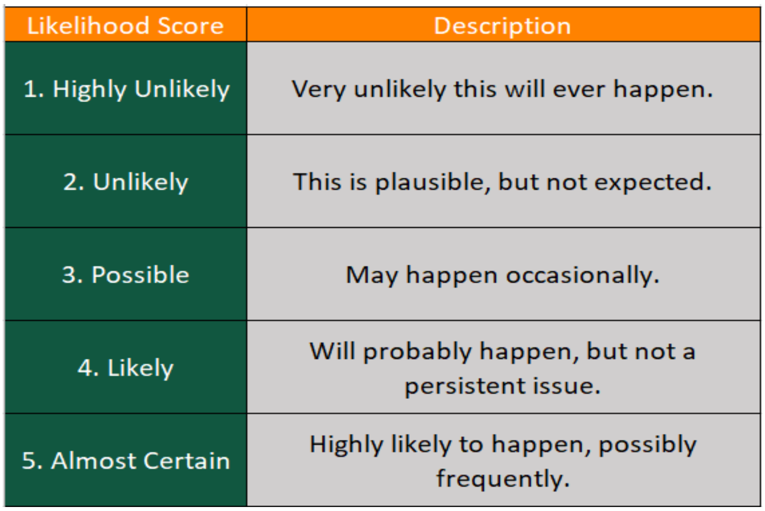
The goal of risk analysis is to analyze the elements that make up each risk scenario to determine:

- 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

The 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 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.

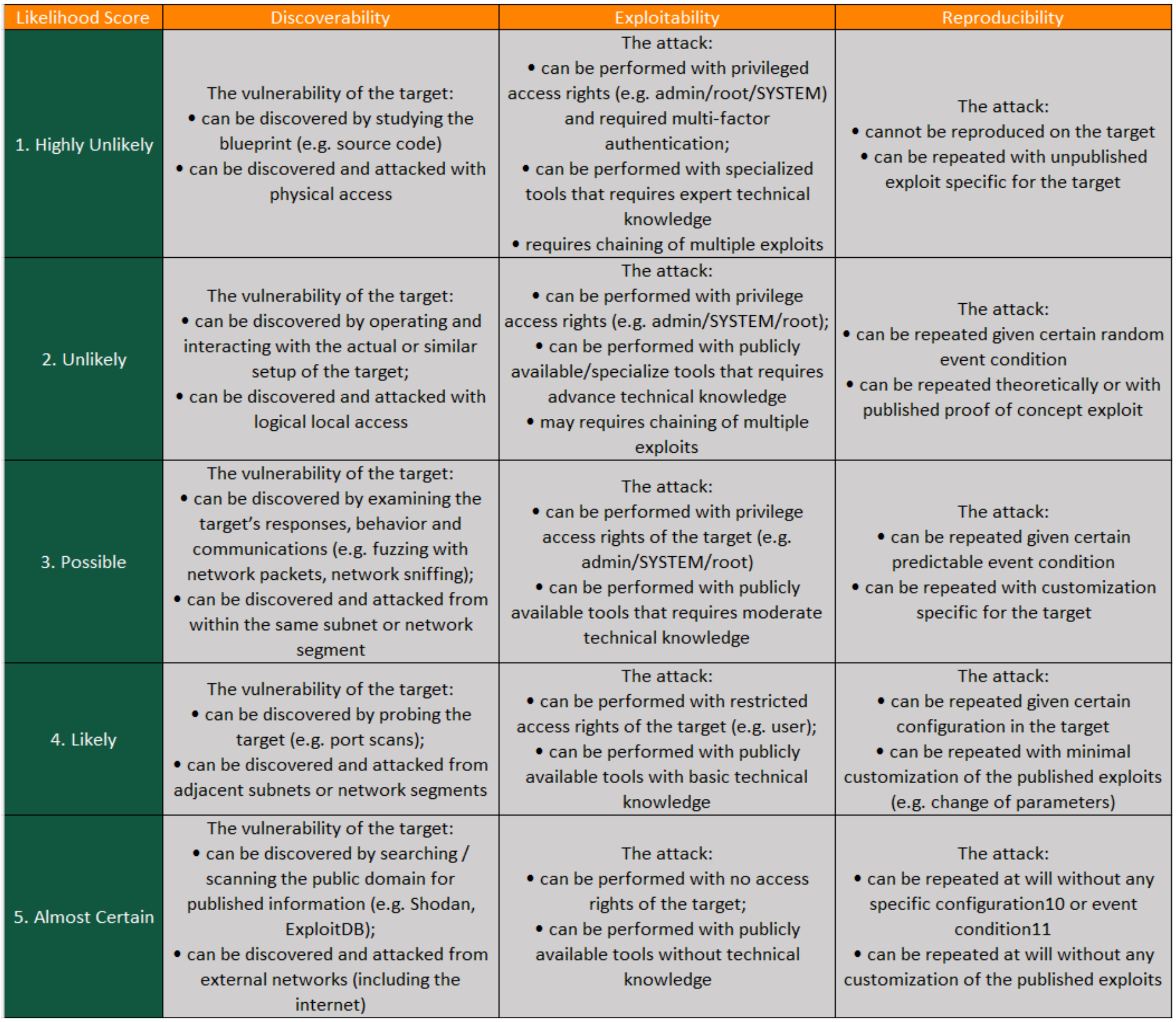


Likelihood Score	Description
1. Highly Unlikely	Very unlikely this will ever happen.
2. Unlikely	This is plausible, but not expected.
3. Possible	May happen occasionally.
4. Likely	Will probably happen, but not a persistent issue.
5. Almost Certain	Highly likely to happen, possibly frequently.

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. Highly Unlikely	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. Almost Certain	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:

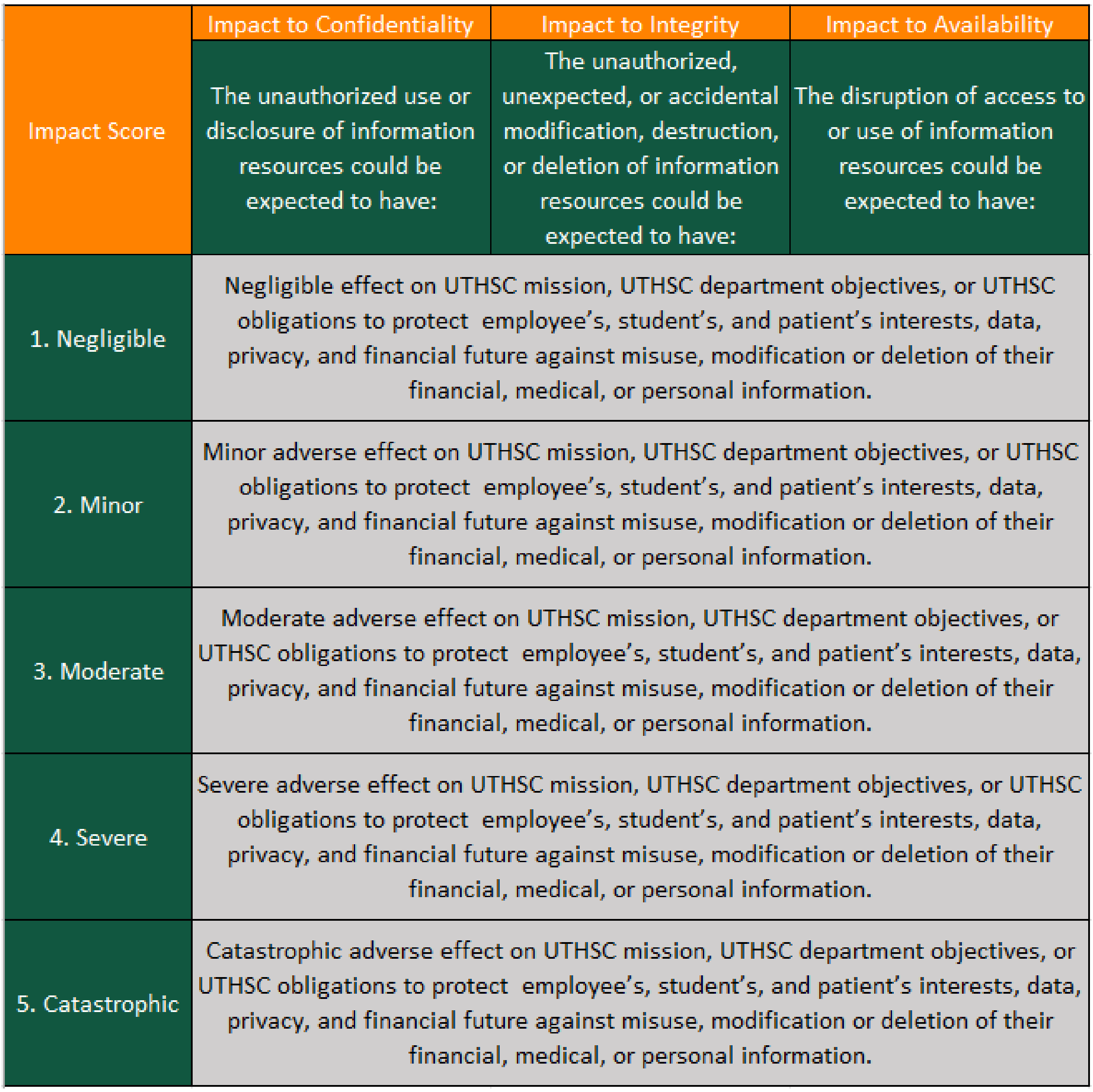
1. Assign a score for each of the 3 likelihood factors (i.e., 1 – 5)
2. Average the score and round off to the nearest whole number
3. The final score will be the likelihood of the risk scenario; 5 being "Almost Certain" and 1 being "Highly Unlikely"

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:

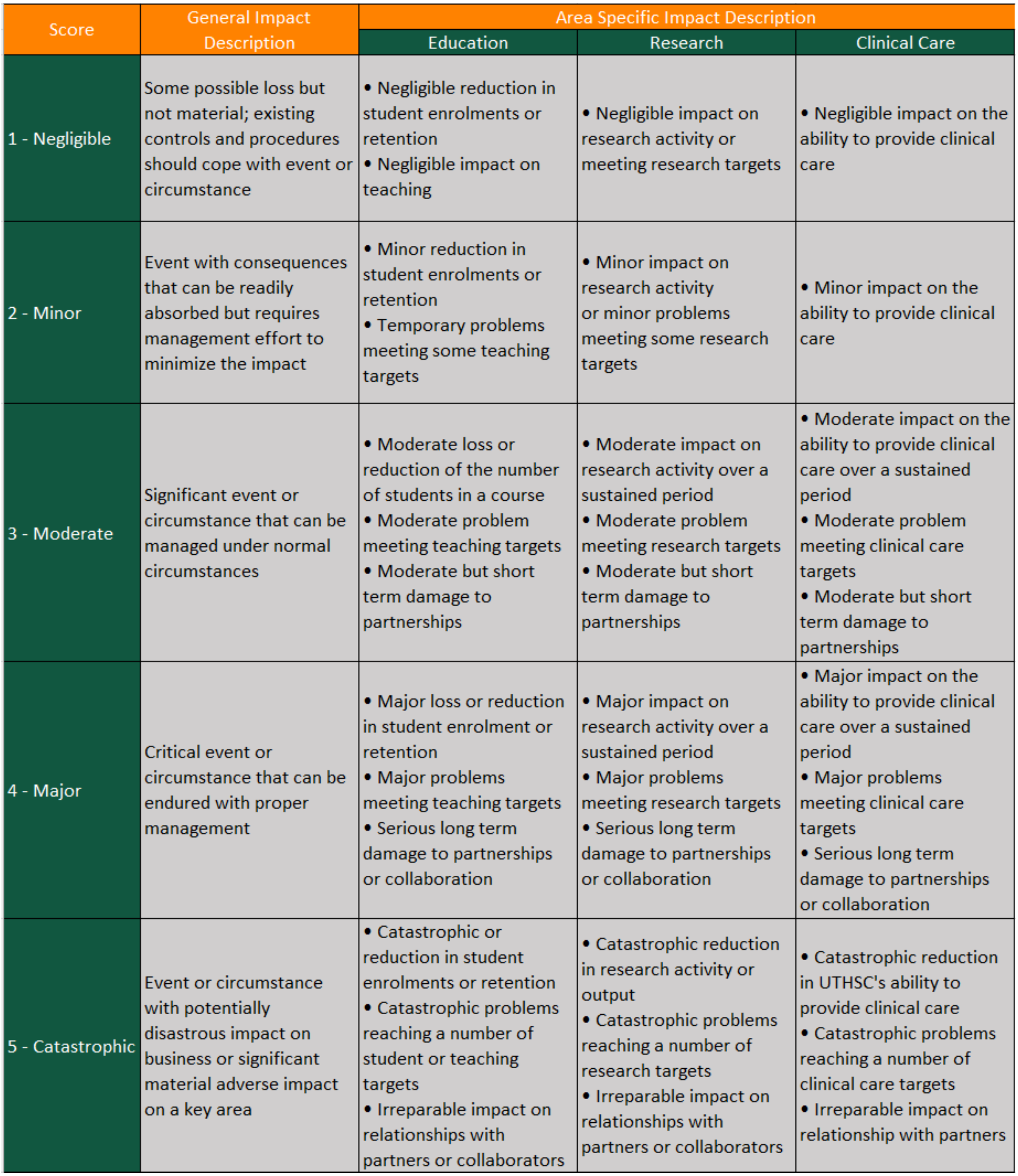
1. UTHSC Mission – The mission of the University of Tennessee Health Science Center is to improve the health and well-being of Tennesseans and the global community by fostering integrated, collaborative, and inclusive education, research, scientific discovery, clinical care, and public service.
2. UTHSC 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 well as other areas like brand, reputation, people, compliance, etc. as illustrated in Figures 6 through 9. The highest impact rating should be taken as the final "Impact" score.



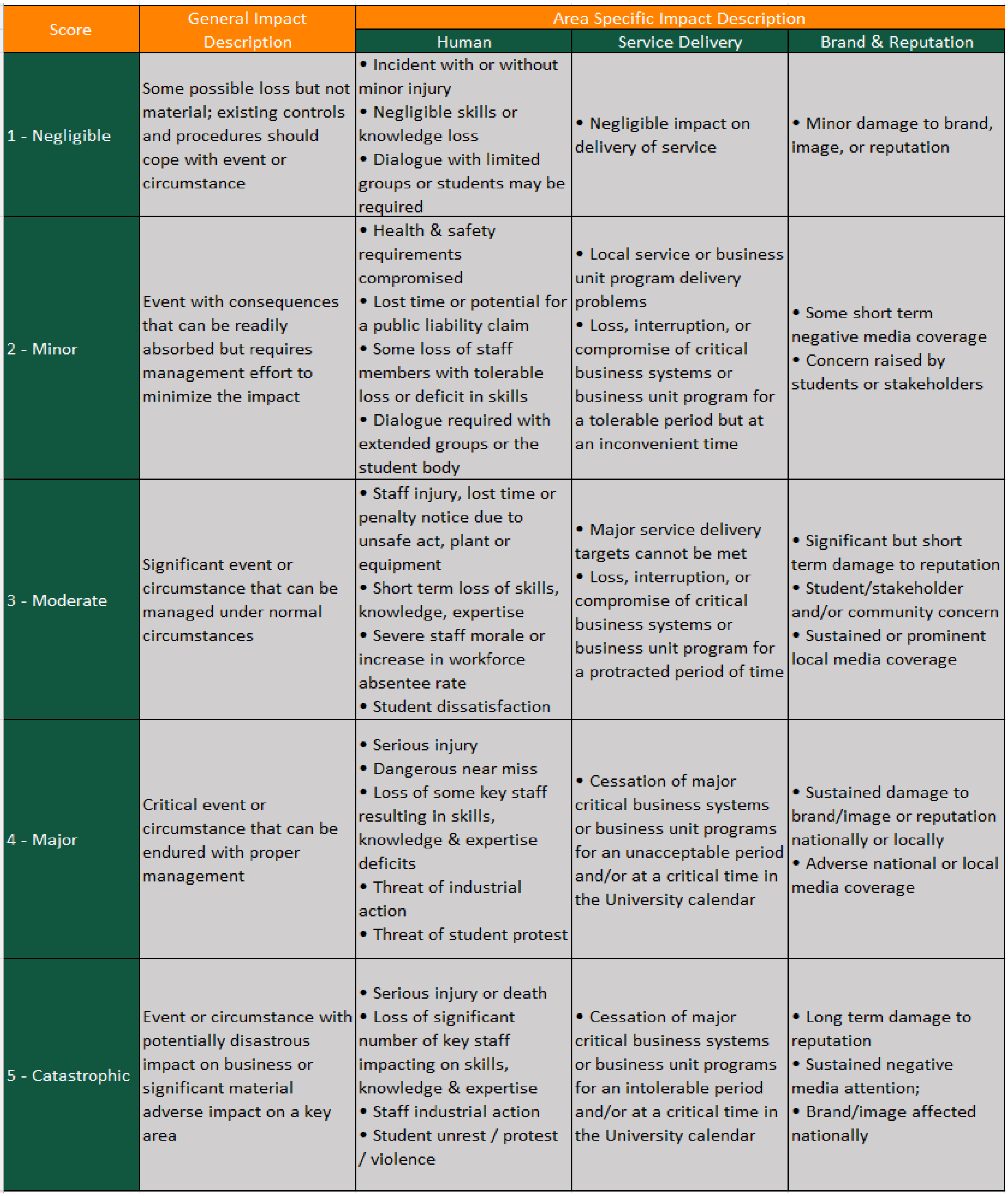
Impact Score	Impact to Confidentiality	Impact to Integrity	Impact to Availability
	The unauthorized use or disclosure of information resources could be expected to have:	The unauthorized, unexpected, or accidental modification, destruction, or deletion of information resources could be expected to have:	The disruption of access to or use of information resources could be expected to have:
1. Negligible	Negligible effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect employee’s, student’s, and patient’s interests, data, privacy, and financial future against misuse, modification or deletion of their financial, medical, or personal information.		
2. Minor	Minor adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect employee’s, student’s, and patient’s interests, data, privacy, and financial future against misuse, modification or deletion of their financial, medical, or personal information.		
3. Moderate	Moderate adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect employee’s, student’s, and patient’s interests, data, privacy, and financial future against misuse, modification or deletion of their financial, medical, or personal information.		
4. Severe	Severe adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect employee’s, student’s, and patient’s interests, data, privacy, and financial future against misuse, modification or deletion of their financial, medical, or personal information.		
5. Catastrophic	Catastrophic adverse effect on UTHSC mission, UTHSC department objectives, or UTHSC obligations to protect employee’s, student’s, and patient’s interests, data, privacy, and financial future against misuse, modification or deletion of their financial, medical, or personal information.		

Figure 6



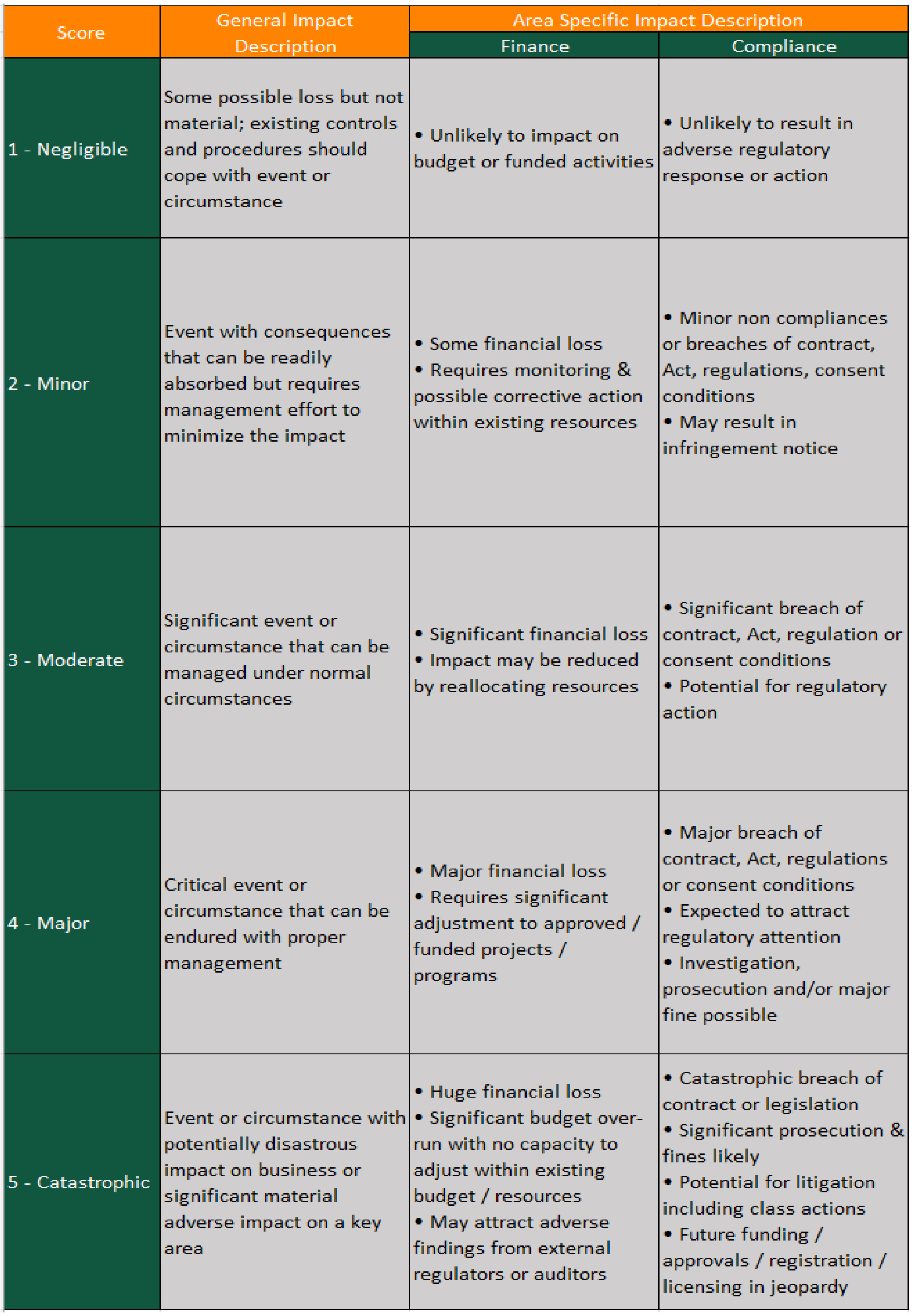
Score	General Impact Description	Area Specific Impact Description		
		Education	Research	Clinical Care
1 - Negligible	Some possible loss but not material; existing controls and procedures should cope with event or circumstance	• Negligible reduction in student enrolments or retention • Negligible impact on teaching	• Negligible impact on research activity or meeting research targets	• Negligible impact on the ability to provide clinical care
2 - Minor	Event with consequences that can be readily absorbed but requires management effort to minimize the impact	• Minor reduction in student enrolments or retention • Temporary problems meeting some teaching targets	• Minor impact on research activity or minor problems meeting some research targets	• Minor impact on the ability to provide clinical care
3 - Moderate	Significant event or circumstance that can be managed under normal circumstances	• Moderate loss or reduction of the number of students in a course • Moderate problem meeting teaching targets • Moderate but short term damage to partnerships	• Moderate impact on research activity over a sustained period • Moderate problem meeting research targets • Moderate but short term damage to partnerships	• Moderate impact on the ability to provide clinical care over a sustained period • Moderate problem meeting clinical care targets • Moderate but short term damage to partnerships
4 - Major	Critical event or circumstance that can be endured with proper management	• Major loss or reduction in student enrolment or retention • Major problems meeting teaching targets • Serious long term damage to partnerships or collaboration	• Major impact on research activity over a sustained period • Major problems meeting research targets • Serious long term damage to partnerships or collaboration	• Major impact on the ability to provide clinical care over a sustained period • Major problems meeting clinical care targets • Serious long term damage to partnerships or collaboration
5 - Catastrophic	Event or circumstance with potentially disastrous impact on business or significant material adverse impact on a key area	• Catastrophic or reduction in student enrolments or retention • Catastrophic problems reaching a number of student or teaching targets • Irreparable impact on relationships with partners or collaborators	• Catastrophic reduction in research activity or output • Catastrophic problems reaching a number of research targets • Irreparable impact on relationships with partners or collaborators	• Catastrophic reduction in UTHSC's ability to provide clinical care • Catastrophic problems reaching a number of clinical care targets • Irreparable impact on relationship with partners

Figure 7



Score	General Impact Description	Area Specific Impact Description		
		Human	Service Delivery	Brand & Reputation
1 - Negligible	Some possible loss but not material; existing controls and procedures should cope with event or circumstance	• Incident with or without minor injury • Negligible skills or knowledge loss • Dialogue with limited groups or students may be required	• Negligible impact on delivery of service	• Minor damage to brand, image, or reputation
2 - Minor	Event with consequences that can be readily absorbed but requires management effort to minimize the impact	• Health & safety requirements compromised • Lost time or potential for a public liability claim • Some loss of staff members with tolerable loss or deficit in skills • Dialogue required with extended groups or the student body	• Local service or business unit program delivery problems • Loss, interruption, or compromise of critical business systems or business unit program for a tolerable period but at an inconvenient time	• Some short term negative media coverage • Concern raised by students or stakeholders
3 - Moderate	Significant event or circumstance that can be managed under normal circumstances	• Staff injury, lost time or penalty notice due to unsafe act, plant or equipment • Short term loss of skills, knowledge, expertise • Severe staff morale or increase in workforce absentee rate • Student dissatisfaction	• Major service delivery targets cannot be met • Loss, interruption, or compromise of critical business systems or business unit program for a protracted period of time	• Significant but short term damage to reputation • Student/stakeholder and/or community concern • Sustained or prominent local media coverage
4 - Major	Critical event or circumstance that can be endured with proper management	• Serious injury • Dangerous near miss • Loss of some key staff resulting in skills, knowledge & expertise deficits • Threat of industrial action • Threat of student protest	• Cessation of major critical business systems or business unit programs for an unacceptable period and/or at a critical time in the University calendar	• Sustained damage to brand/image or reputation nationally or locally • Adverse national or local media coverage
5 - Catastrophic	Event or circumstance with potentially disastrous impact on business or significant material adverse impact on a key area	• Serious injury or death • Loss of significant number of key staff impacting on skills, knowledge & expertise • Staff industrial action • Student unrest / protest / violence	• Cessation of major critical business systems or business unit programs for an intolerable period and/or at a critical time in the University calendar	• Long term damage to reputation • Sustained negative media attention; • Brand/image affected nationally

Figure 8



Score	General Impact Description	Area Specific Impact Description	
		Finance	Compliance
1 - Negligible	Some possible loss but not material; existing controls and procedures should cope with event or circumstance	• Unlikely to impact on budget or funded activities	• Unlikely to result in adverse regulatory response or action
2 - Minor	Event with consequences that can be readily absorbed but requires management effort to minimize the impact	• Some financial loss • Requires monitoring & possible corrective action within existing resources	• Minor non compliances or breaches of contract, Act, regulations, consent conditions • May result in infringement notice
3 - Moderate	Significant event or circumstance that can be managed under normal circumstances	• Significant financial loss • Impact may be reduced by reallocating resources	• Significant breach of contract, Act, regulation or consent conditions • Potential for regulatory action
4 - Major	Critical event or circumstance that can be endured with proper management	• Major financial loss • Requires significant adjustment to approved / funded projects / programs	• Major breach of contract, Act, regulations or consent conditions • Expected to attract regulatory attention • Investigation, prosecution and/or major fine possible
5 - Catastrophic	Event or circumstance with potentially disastrous impact on business or significant material adverse impact on a key area	• Huge financial loss • Significant budget over-run with no capacity to adjust within existing budget / resources • May attract adverse findings from external regulators or auditors	• Catastrophic breach of contract or legislation • Significant prosecution & fines likely • Potential for litigation including class actions • Future funding / approvals / registration / licensing in jeopardy

Figure 9

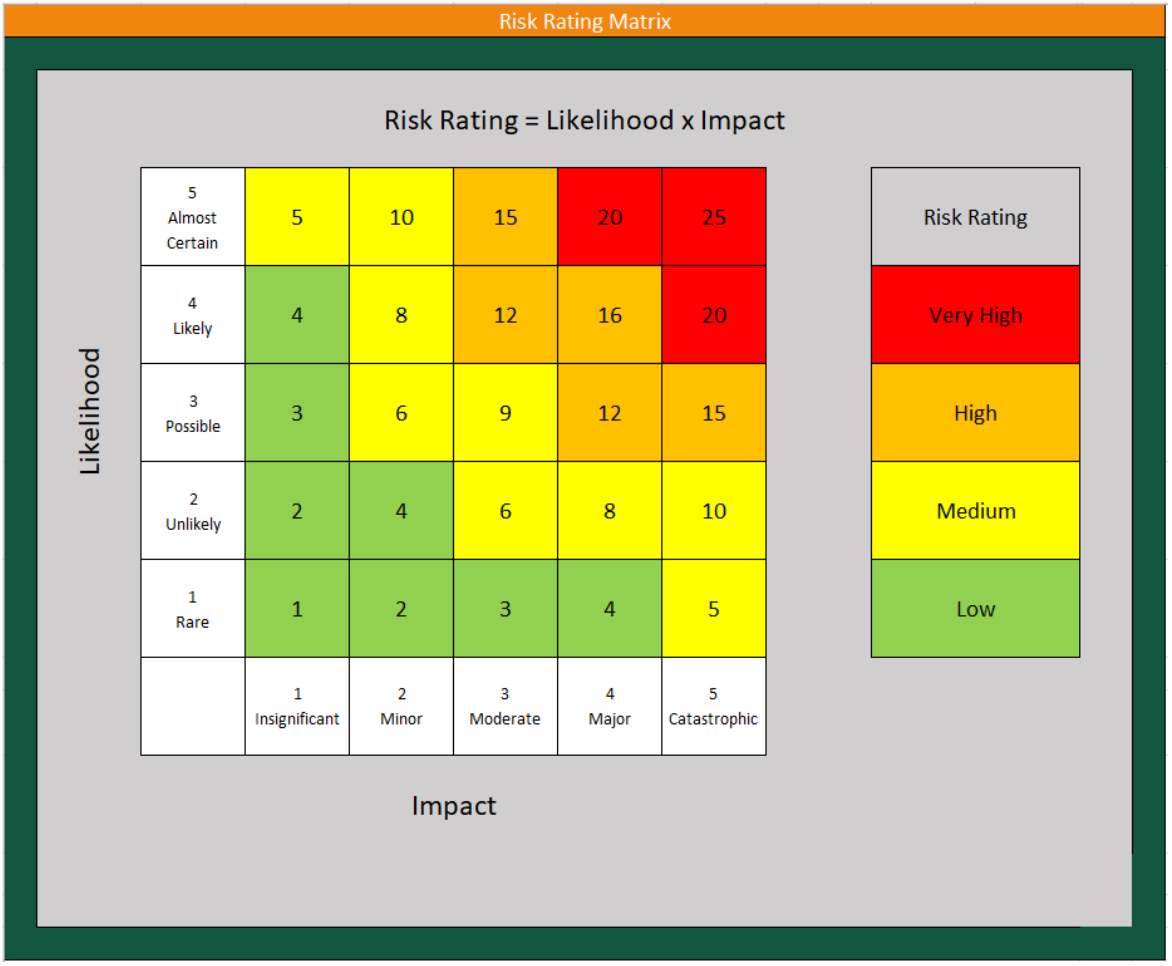
Step 3: Risk Evaluation

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 Almost Certain	🟨 5	🟨 10	🟧 15	🟥 20	🟥 25
4 Likely	🟩 4	🟨 8	🟧 12	🟧 16	🟥 20
3 Possible	🟩 3	🟨 6	🟨 9	🟧 12	🟧 15
2 Unlikely	🟩 2	🟩 4	🟨 6	🟨 8	🟨 10
1 Rare	🟩 1	🟩 2	🟩 3	🟩 4	🟨 5
	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophic

Impact

Risk Rating
🟥 Very High
🟧 High
🟨 Medium
🟩 Low

Figure 10

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

Risk appetite and tolerance:

The University of Tennessee Health Science Center has a low-risk appetite regarding cybersecurity-related risks impacting UTHSC's mission. In the pursuit of fulfilling its mission, the University will tolerate medium cybersecurity-related risks with appropriate approvals and monitoring.

The University of Tennessee Health Science Center has no appetite for compliance-related technology risks and will adhere to all laws and regulations regarding its operating environments.

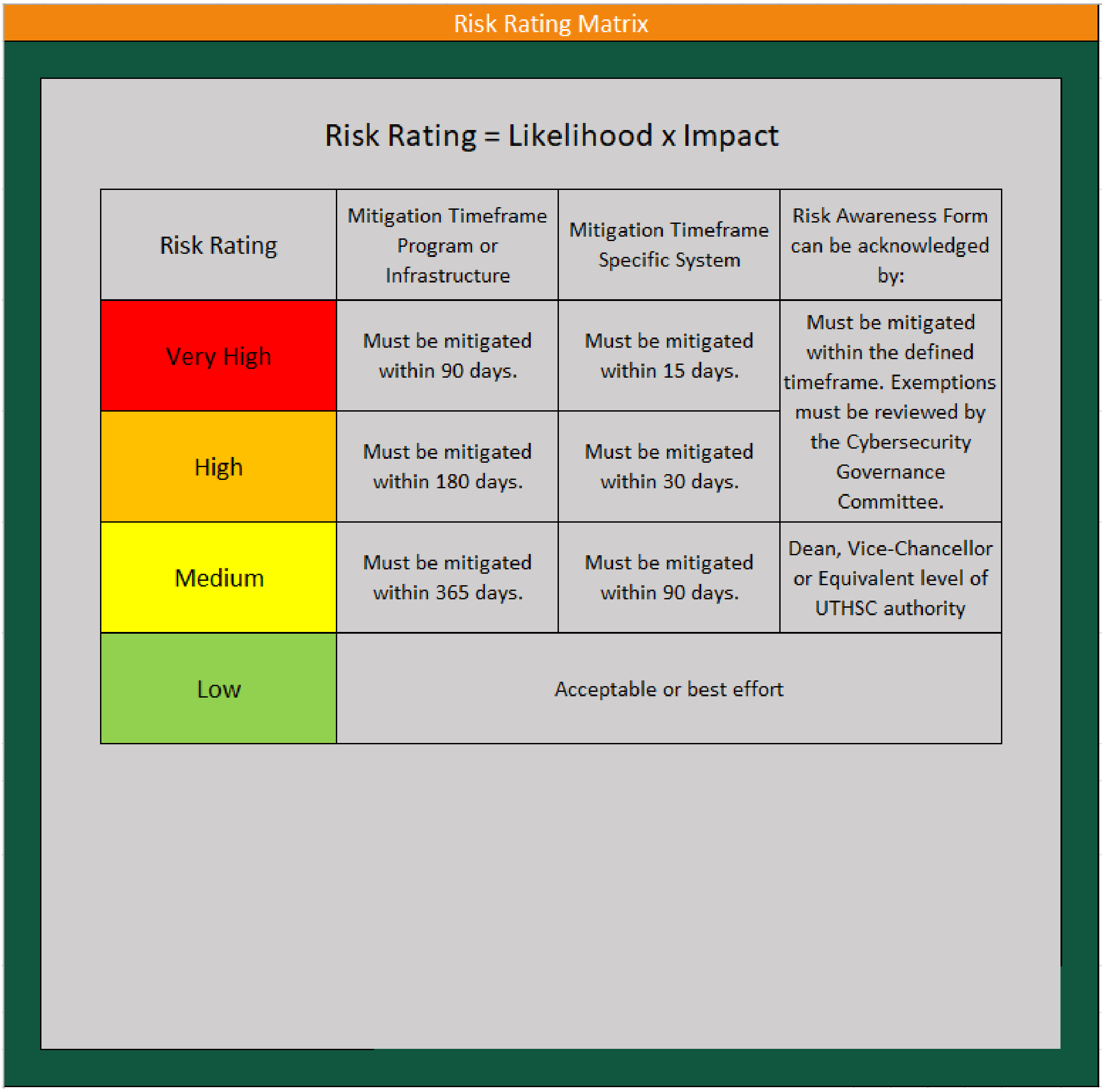
The University standard for risk response is one of three options:

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. Minimum security controls by classification level and asset type are published to provide guidance on risk mitigation. See also, GP-005-Data Security for additional guidance.
3. Acknowledge- If a risk owner chooses not to avoid or mitigate the risk, they must officially acknowledge the risk. This is accomplished with the "Risk Awareness Form" process. The form must be acknowledged by an approved authority illustrated in Figure 11 below. If the risk cannot be mitigated within

the "Mitigation Timeframe (Figure 11)," a Security Exception or Exemption should be requested and a Risk Awareness Form should be signed.

If the risk is a result of a deviation from UTHSC standards, an exception must be requested as well. Requests for exceptions 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 reviewed. 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 in Figure 11.

As general guidance, a security 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.



Risk Rating Matrix

Risk Rating = Likelihood x Impact

Risk Rating	Mitigation Timeframe Program or Infrastructure	Mitigation Timeframe Specific System	Risk Awareness Form can be acknowledged by:
Very High	Must be mitigated within 90 days.	Must be mitigated within 15 days.	Must be mitigated within the defined timeframe. Exemptions must be reviewed by the Cybersecurity Governance Committee.
High	Must be mitigated within 180 days.	Must be mitigated within 30 days.	
Medium	Must be mitigated within 365 days.	Must be mitigated within 90 days.	Dean, Vice-Chancellor or Equivalent level of UTHSC authority
Low	Acceptable or best effort		

Figure 11

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 Practices & Controls
2. Security Exceptions and Exemptions to ITS Security Controls Request Form
3. GP-002-Data & System Classification
4. MITRE ATT&CK Framework
5. 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