INFORMATION TECHNOLOGY SERVICES
George Mason University

IT Risk Assessment Procedure

Document Version Number:	2.0
Document Control Number:	ITS.ITRC-PROC004
Last Updated:	10/22/2025
FOIA Exempt?	No

Process Owner:

- IT Risk & Compliance

PURPOSE:

Brief Description of the Procedure:

This procedure provides step-by-step instructions for conducting risk assessments on systems to determine and evaluate their risk profiles. It utilizes National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 199 categorization, along with assessments of threats, vulnerabilities, likelihood, and controls status, to determine the residual risk of the system being assessed. Additionally, this procedure helps identify “Sensitive IT Systems”.

This procedure must be performed annually or whenever there is a material change in the design, architecture, contract, or usage of a system that could impact its risk profile. If there is no material change during the year, system owners may note that as ‘no change from prior status’ during the annual review. The procedure may also be performed on an ad-hoc basis.

NOTE TO ALL USERS: This procedure does not apply to third-party hosted service models. These are covered by the ITS.ITRC-PRS003 Third-Party Risk Management Process. For hybrid implementations, the on-prem component may be assessed using this procedure, and the components that are in the Cloud should be reviewed using the Third-Party Risk Management Process. The two records can be cross referenced within Archer, and a summary be provided for overall risk profile, in either record.

SCOPE:

This procedure applies to all new and existing IT systems where the system owner, process owner, risk and compliance teams, or any other stakeholders need to determine the system’s risk profile and classification as applicable to FIPS-199, Sensitive IT System, and Risk definitions.

COMPLIANCE AND STANDARDS:

- IT Security Standard
- University Policy Number 1311 Information Technology Security Program

Titles and department names are subject to organizational changes.

DEFINITIONS AND ACRONYMS:

Terminology or Acronym	Definition
30,000 records thresholds	The 30,000 records threshold is derived based on current level of cyber insurance per claim and current industry average cost of curing a data breach at the rate of $178 per record.
Availability	Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]
Catastrophic adverse impact	A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]
Critical Function	An operation or task that; (i) supports one or more of the mission essential functions (Public Safety, Education, or Research) or is required for compliance and (ii) without the operation or task continuing within 30 days there would be a cascading effect or detrimental harm to the institution.
Essential Component	Component that is absolutely necessary for the Critical Function to be operational, even if in a degraded state. Without this component the Critical Function will not be operational. The essential component is required to restore the Critical Function. “Essential Component” may also be referred to as “Critical Component”. These are or contain information and communications technology (ICT)—including hardware, software, and firmware—that **delivers or protects mission-critical functionality** of a system, or which, due to its design, may **introduce vulnerability** to the mission-critical functions of an applicable system. (Reference: *NIST SP 800-16. Additionally, it may also be referred to as Critical System Asset (Reference CP-2(8) of NIST SP 800-53)*
Exceptions	All exceptions must be reviewed and approved by the appropriate policy/standard/process owner (Sample in Appendix E).
Findings	Assessment results produced by the application of an assessment procedure to a security control, privacy control, or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a satisfied or other than satisfied condition.
Information	An instance of an information type.
Information system	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 U.S.C., SEC. 3502]
Integrity	Guarding against improper information modification or destruction and includes ensuring information about non-repudiation and authenticity. [44 U.S.C., SEC. 3542]

IT System	An interconnected set of IT resources under the same direct management control for the purpose of serving a set of the same business or functional needs. IT Systems in George Mason at a high-level may be: • George Mason University hosted (On-Premises/On-Prem) • In the Cloud (Software as a Service or SaaS, Platform as a Service or PaaS, Infrastructure as a Service or IaaS) • Hybrid (where some components of the system are On-Prem and others may be in the Cloud). This procedure does not apply to third-party hosted service models. These are covered by the ITS.ITRC-PRS003 Third-Party Risk Management Process. For hybrid implementations, the on-prem component may be assessed using this procedure, and the components that are in the Cloud should be reviewed using the Third-Party Risk Management Process. The two records can be cross referenced within Archer, and a summary be provided for overall risk profile, in either record.
ITRC	Information Technology Risk & Compliance
ITS	Information Technology Services
Enterprise Cybersecurity	Formerly known as the Information Technology Security Office (ITSO), led by the Chief Information Security Officer (CISO)
Light (Lite) Controls Set	Used in this risk assessment procedure is a subset of NIST SP 800-53 controls and derives from ITRM Risk Management Standard SEC520-05 (June 2024) Appendix A, Risk Management Framework Core. Based on technology and cyber threat trends, questions in the risk assessment may be updated to evaluate controls status.
Limited adverse impact	A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
NIST	National Institute of Standards and Technology
Mission Essential Function (MEF)	George Mason University has identified mission essential functions (MEFs) within its university-level Continuity of Operations Plan (COOP), based on the financial, economic, safety, or long-term effect of each function on the regional or state continuity and strategic plans. MEFs are comprised of critical functions that are detailed in the Unit COOP Plans.
Personally Identifiable Information (PII)	PII is any information about an individual maintained by George Mason University, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (Ref. definition from NIST SP 800-122). Email address by itself may not be PII, but when it uniquely identifies a person or combined with first name and/or last name or other attributes, can be considered PII.
Process Owner	May be a business or technology or functional process owner.

Recovery Time Objective (RTO)	The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes.
Recovery Point Objective (RPO)	The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage.
Risk Acceptance	The acceptance of risk is a deliberate decision to acknowledge and tolerate a certain level of risk without attempting to mitigate it further, implementing additional controls, or countermeasures to reduce the likelihood or impact. Departments should reach out to IT Risk & Compliance at itrc@gmu.edu for assistance regarding using the ITS Risk Analysis template which includes an option for Risk Acceptance (Sample in Appendix D). Risk acceptances must be documented and accepted by the appropriate George Mason leadership, usually the Vice-President of the appropriate department(s) or unit(s).
Risk Assessment Record	This is a digital record in Archer that contains product of a 'risk assessment' which is the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, George Mason community, resulting from the operation of an information system.
RMF	Risk Management Framework
Security objective	Confidentiality, integrity, or availability.
Sensitive Data	Is any data of which the compromise with respect to confidentiality, integrity, and/or availability could adversely affect George Mason's interests, the conduct of the University's programs, or the privacy to which individuals are entitled. At George Mason, these data fall into Protected categories (Highly Sensitive Data and Restricted Data) as defined in the Data Stewardship Policy.
Sensitive IT System	A "High" (as per FIPS 199 categorization criteria in Appendix A) category system that stores Protected data (as defined in the Data Stewardship Policy) and is an essential component of one or more Critical Functions. Appendix B can be used as a guide to identify Sensitive IT Systems and assign FIPS 199 categorization.
Serious adverse impact	A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
System Owner	A person who is responsible for the operation and maintenance of a George Mason IT system.
System Scope Boundary	When a set of system elements is identified as the scope boundary for a system, the elements are, • Generally, under the same direct management. • Support the same mission or business functions. • Have similar operating characteristics and security and privacy requirements. • Process, store, and transmit similar types of information (e.g., categorized at the same impact level).

	Reside in the same environment of operation (or in the case of a distributed system, reside in various locations with similar operating environments).

PROCEDURE:

Task 1: Categorize

Use Appendix A to establish an appropriate security category of an information by assigning the potential impact for each security objective associated with the particular information type. This information will be entered in the record in Archer at part of Task 2.

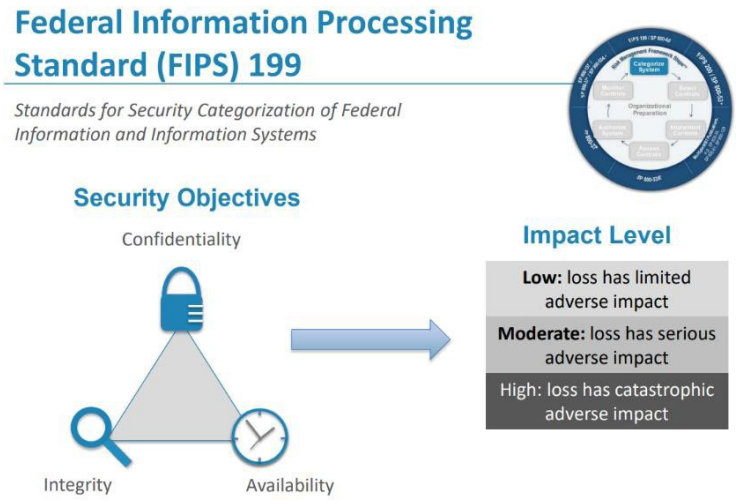
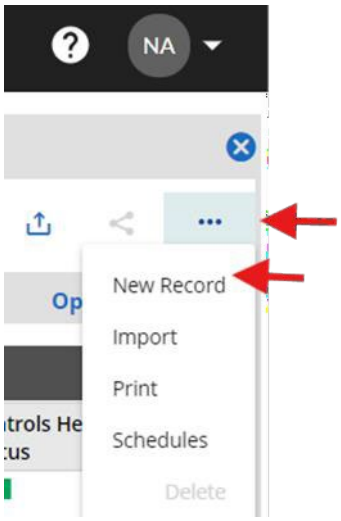


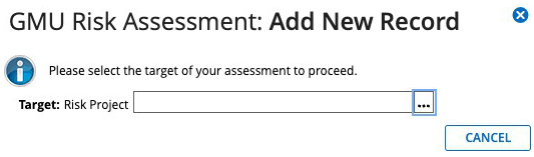
*Image courtesy NIST

Task 2: Select and Apply the Controls Set

1. Log into George Mason Virtual Private Network (VPN) using the AnyConnect client and Duo Multi-Factor Authentication (MFA).
2. In a browser, access the link for Archer production instance (https://gmu.archerirm.us/Default.aspx).
3. Login to Archer prod using enterprise Single Sign On (SSO).
4. From the menu options, select IT Security Risk Management > IT Risk Management > GMU Risk Assessment.
5. Create a new record.



6. Select the three (3) dots next to the field, and then choose "<CURRENT YEAR>_Risk_Assessment_Program" from the selection



7. Interview system/process owner to enter information on the profile of the system/process. The assessor may use the 'Information Gathering with Common Controls Worksheet' as a guide to gather and document information. Some examples of information that will be useful are as follows:
    - IP addresses
    - data classification
    - types of data stored, processed, or transmitted. The following table may be used.

	Stored	Processed	Transmitted
PCI DSS	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A
GLBA	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A
Federal Tax Information	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A
FERPA	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A
HIPAA	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A
PII	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A
Contract Restricted	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A
Research	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A
Other	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A	Yes/No/Maybe/N/A

    - upstream and downstream systems

- relationship to Critical Functions
- applications
- interconnections
- number of users
- types of users (employees, students, contractors, etc.)
- applicable regulatory requirements for data protection and system protection
- system owner, business owner
- upload any system or data diagrams that are available
- note any previous assessments (1-year timeframe) including audits or ASRB reviews
- submit date should not be more than 30 days from the day the current review is initiated
- next review date will be calculated to 334 days from submit date

8. Interview system/process/controls owners and/or implementers for answers to risk assessment questions. These can be answered as Yes, No, Partial, or Not Applicable (N/A). The score is to be disregarded at this time and analysis is to be subjective and qualitative.

9. Grade scale is as follows:

CONTROLS (LIGHT/LITE SET) SCALE	
All Yes	Low
One of more 'Partial' but none as 'No'	Medium
One or more 'No'	High

10. Any additional information about the context of the assessment should be entered in **Risk Assessment Comments.** The Information Gathering with Common Controls Worksheet may be used as a guide.

Task 3: Identity Threat Sources and Events

Threat evaluation is contextual and subjective, however NIST Special Publication (SP) 800-30 - TABLE E-2: REPRESENTATIVE EXAMPLES – ADVERSARIAL THREAT EVENTS and TABLE E-4: RELEVANCE OF THREAT EVENTS can be used as tools to assist this analysis.

THREAT SCALE	
Multiple Significant Threats (including Internet Facing Systems)	High
One or more Major Threats	Medium
No significant Threats	Low

Task 4: Identify Vulnerabilities and Predisposing Conditions

Use the 'ITRC Vulnerabilities by System Name' report in Archer to populate the following information in the record. Apply filter to select the appropriate System that is being assessed.

VULNERABILITES SCALE	
One or more Critical Vulnerabilities Past Due	High
One or more Critical Vulnerabilities Open but Not Past Due	Medium
One or more High Vulnerabilities Past Due	Low

Task 5: Determine the Likelihood of Occurrence

Based on discussion with the system owner and stakeholders, establish likelihood.

LIKELIHOOD SCALE	
Very Likely	High
Likely	Medium

Unlikely	Low

Task 6: Determine the Magnitude of Impact

1. Determined the magnitude of impact based on interviews with the stakeholders.
    - Organization Level: MEF Impact (Critical, High, Medium, Low)
    - Business Process Level: Critical Function Impact (Critical, High, Medium, Low)
    - System Level (Critical, High, Medium, Low)
2. Note the following:
    - Business Impact Analysis (BIA) statement
    - Privacy Impact Analysis (PIA) statement

Privacy Impact Assessments and criticality levels (when defined as part of contingency planning or Mission/Business Impact Analysis) indicate the adverse impacts of destruction, corruption, or loss of accountability for information resources to organizations.

Task 7: Determine Risk

1. George Mason uses a qualitative method (Figure 1: 3x3 matrix) to evaluate risk based on information collected in the prior tasks.

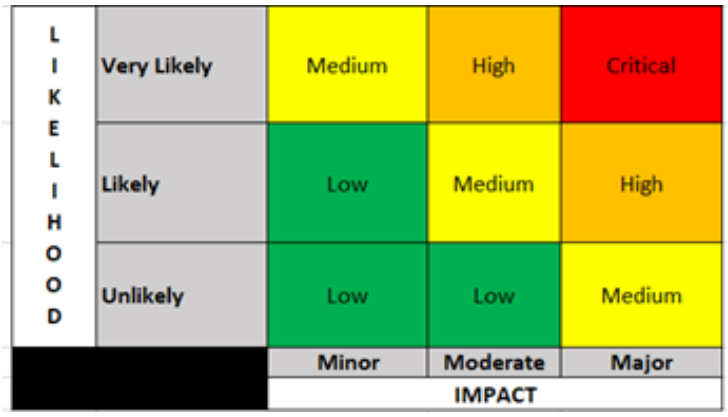


Figure 1

2. Use Appendix C during the calibration to evaluate information gathered in Tasks 2-6 and its effect the qualitative risk profile of the system.
3. At the end of this task, a Risk-based categorization of the system will be available. Use the following table to summarize:

Sensitive IT System	A High (as per FIPS 199 categorization criteria) category system that stores Protected data (as defined in the Data Stewardship Policy) and is an **essential** component of one or more Critical Functions.
FIPS 199 Category	High/Moderate/Low
Applicable GMU Security Baseline	High (248 controls)/Moderate (105), Low (49)

Risk Category	High Risk/Moderate Risk/Low Risk

4. Communicate the results of the Risk Assessment to all relevant stakeholders. In a calibration session, discuss the outcome of the assessment with IT Security Office, System Owner, Business/Process Owner and Office of Internal Audit (as needed) to arrive at agreement on risk rating and next steps.
5. Findings should be recorded in Archer and assigned to appropriate personnel for risk treatment.
6. For Systems tagged as 'Sensitive IT System', notify the System Owner to initiate the **Assessment and Authorization** process which includes the System Security Plan (SSP) and Plan of Action and Milestones (POA&M) record keeping.
7. Authorizing Official (Chief Information Officer) has the authority to overrule the analysis categorizations (Sensitive IT System, FIPS 199, Risk Rating).

INPUTS AND OUTPUTS:

Inputs:

- IT system

Outputs:

- Findings
- Risk Assessment Record

REVIEW SCHEDULE:

Annually

APPROVAL:

Title, Department Name	Name	Signature and Date
Director, IT Risk & Compliance	Noor Aarohi	DocuSigned by: Noor Aarohi D37A04E44AA04AD.. 10/24/2025

REVISION HISTORY:

Date	Version Number	Department or Author	Brief Description of Changes
10/31/2024	1.0	IT Risk & Compliance / Noor Aarohi	Initial release
3/28/2025	1.1	IT Risk & Compliance	Annual review – Reformatted content using the current procedure template.
4/9/2025	1.1	IT Risk & Compliance	Minor edits and errata
10/22/2025	2.0	IT Risk & Compliance / Noor Aarohi	Updates to reflect that the risk assessment questions can be updated to factor in current technology and threat trends.

Titles and department names are subject to organizational changes.

			Cost of data breach per record updated to $178 per 2025 IBM Data Breach report.

RELATED DOCUMENTS/REFERENCES:

- Information Gathering with Common Controls Worksheet (email itrc@gmu.edu for access)
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 199

APPENDIX A – Potential Impact Definitions for Security Objectives

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

APPENDIX B – Considerations and Criteria for Determination of 'Sensitive IT System'

Highest watermark for Information Type	Number of Records Threshold	Persistent Storage or Passthrough?	Function	Impact Assessment H, M, L			Highest watermark System Categorization	Follow up / Next Step
				C	I	A		
Highly Sensitive Data	>= 30,000 records	Persistent	Any	H	H	H	**High**	- Required to Apply/Assess against GMU High Controls Baseline. **-Evaluate against the 'Sensitive IT System' definition**
Highly Sensitive Data	< 30,000 records	Persistent	Any	H	H	H	High	- Required to Apply/Assess against GMU High Controls Baseline.
Highly Sensitive Data	N/A	Passthrough	Any	M	M	M	Moderate	
Restricted	>= 30,000 records	Persistent	Any	M	M	M	Moderate	
Restricted	< 30,000 records	Persistent	Any	M	M	L	Moderate	
Restricted	N/A	Passthrough	Any	M	M	L	Moderate	
Public Data	N/A	Persistent	Any	L	L	L	Low	
Public Data	N/A	Passthrough	Any	L	L	L	Low	
Public Data	N/A	Either	Emergency Management and Safety	L	H	H	High	- Required to Apply/Assess against GMU High Controls Baseline.
Highly Sensitive Data	N/A	Passthrough	Cyber-defense	H	H	H	High	- Required to Apply/Assess against GMU High Controls Baseline.

APPENDIX C – Risk Analysis Guide

	Vulnerabilities Grade	Threat Grade	Likelihood Grade	Controls Assessment
High	Increases the risk profile	Increases the risk profile	Increases the risk profile	May decrease or maintain current risk profile
Medium	May increase the risk profile	May increase the risk profile	May increase the risk profile	May increase the risk profile
Low	May decrease or maintain current risk profile	May decrease or maintain current risk profile	May decrease or maintain current risk profile	Increases the risk profile

APPENDIX D – Risk Acceptance Template

GEORGE MASON UNIVERSITY | Information Technology Services

ITS Risk Analysis Summary

*This template will be prepared by IT Risk and Compliance team in consultation with the technology team and/or department requesting for the solution/service.

Date: **Issue ID#:**
System Name:
Service Model:
Component:
System Security Level (FIPS-199 Categorization of the information system):
*Standards for Security Categorization of Federal Information and Information Systems

Requester:
Vendor Name:
Vendor Primary Contact: **Primary Contact Email:**
Vendor Secondary Contact: **Secondary Contact Email:**

Inherent Risk:
Residual Risk:

IT Risk Analysis

Determination

Applicable Policy/Standard (Include excerpt):

Business Justification for the Risk Acceptance:
What would be the impact (e.g., to the business or operations) of Denial of Authorization to Operate?

Justification for the Request: Operational: ☐ Technical: ☐ Other: ☐
Provide detailed explanation.

Risk Mitigation

1. **Describe the compensating controls that will be implemented.**

Page 1 of 2

2. **Describe how the compensating controls in Step 1 provide coverage to reduce the risk.**

3. **Additional Comments:**

Endorsement of Risk Analysis Understanding and Acceptance

Business Owner: _____ **Concurrence:**
Date: _____
Comments:

Information System Security Officer: _____ **Concurrence:**
Date: _____
Comments:

Authorizing Officer: _____ **Concurrence:**
Date: _____
Comments:

Please note: *If granted, this risk acceptance must be reviewed at least annually*

Risk accepted on: Same as date signed by Authorizing Officer
Next review due on (1-year from risk acceptance):

APPENDIX E – Exceptions Template

Exception Type		Exception ID	EXP-001		
Issue Sub-Type	Not Applicable				
Date Identified	2/1/2023				
Date Reported	2/1/2023	Requester			
Exception Expires		Control Owner	Noor Aarohi		
Requester	Noor Aarohi	Exception Extension Valid Thru			
Short Description		Notification to	ITS Senior Leadership Listserv		
Detailed Description		Program ID			
Asset (s) - attach list if needed	Attached list	Project ID			
Vendor Name	N/A	Project Priortization			
Criteria		Project Status			
Root Cause		Authority Document			
TCF Control ID	1.2.2	Control Objective	The governance of the Technology organization to policies, standards, and procedures is established through a formally defined program.	Control Sub-Objective	The governance of the Technology organization to policies, standards, and procedures is established through a formally defined program.
NIST 800-53 Control	RA-1				
Applicable Regulations					
Risk Statement					
Inherent Risk	Medium				
Residual Risk	Medium				
Direction of Risk	Stable				
Risk Treatment Decision	Remediate				
Remediation Plan	Risk and Compliance to work with the document owners to review and refresh				
Prioritization Decision					
Plan of Action and Milestones (POA&M) Status	In Progress				
Exception Approved by		Approver Comments			
Approver Signature					