INFORMATION TECHNOLOGY SERVICES
George Mason University

Third-party Risk Management Process

Document Version Number:	2.3
Document Control Number:	ITS.ITRC-PRS003
Last Updated:	04/05/2025
FOIA Exempt?	No

Process Owner:

- IT Risk & Compliance (ITRC)

PURPOSE:

Brief Description of the Process:

This document provides an overview of the third-party risk management process for contracts with third-party providers that involve, or have the potential to involve, the exchange of George Mason University's Protected Data, as defined by University Policy Number 1114, Data Stewardship. These third-party providers consist of both those on rider contracts and those with direct contracts with the university and the Commonwealth of Virginia.

Objective of the Process:

- Supply Chain Risk Management
- System and Services Acquisition

Importance of the Process:

This process is to assess, monitor, and mitigate risks (cybersecurity, operations, legal, regulatory, and compliance) associated with working with third-party providers.

SCOPE:

1. This process is a requirement for third-party software applications and information services that are:
    a. New to the university. Or;
    b. Existing implementations that are planning significant changes to the implementation or scope.
2. The Risk Assessment stage (part of the ASRB process) of this process only applies to third-party software applications and information services that involve one or more of the following:
    a. Use of George Mason Protected data (as defined under University Policy 1114, Data Stewardship)
    b. Integration with George Mason's systems
    c. A user-interface
3. The Ongoing Monitoring stage of this process only applies to third-party software applications or information services that are currently in use by the George Mason community and are classified as high-risk for confidentiality, integrity, or availability. This categorization is assigned at the end of the ASRB review. High-risk systems are reviewed annually. These third-party providers include both those with rider contracts and those with direct contracts with the university or the Commonwealth of Virginia, in which the university is the user of the service. In these cases,

George Mason will make an attempt to obtain the documentation but accept that there is fidelity and trust in the processes in place for similar due diligence and compliance monitoring by the State.

4. This process may also cover any third-party hosted systems that the system owner or the Director of Financial Reporting identifies and requests to be monitored.
5. The Termination stage of this process only applies to third-party contracts with George Mason.

COMPLIANCE AND STANDARDS:

- IT Security Standard
- University Policy Number 1114, Data Stewardship
- University Policy Number 1307, Procurement and/or Development of Administrative
- Systems/Applications
- University Policy Number 1308, Electronic and Information Technology Accessibility
- University Policy Number 2106, Purchase of Goods and Services
- Data Security Addendum

DEFINITIONS AND ACRONYMS:

Terminology or Acronym	Definition
ASRB	A committee of university employees responsible for reviewing and approving proposed acquisitions of software applications and information services. The Board includes representatives from Information Technology Services, Purchasing, and the Assistive Technology Initiative.
Chief Data Stewards	The Chief Data Stewards for George Mason are the Senior Vice President and the Provost.
Data Custodian	An individual who has been authorized to be in physical or logical possession of data by the Data Owner. This individual is responsible for protecting the data in their possession.
Data Security Addendum	This addendum establishes terms and conditions to safeguard the university's protected data against security threats.
Data Owner	Deans, vice presidents, associate vice presidents, directors, managers, or others authorized by the Chief Data Stewards to manage a subset of data. This role is responsible for ensuring that university data security policies are followed and for developing internal controls to ensure data security and privacy.
Data Representative	Any university employee, contractor, affiliate, or duly authorized member of the community with the authority to request the procurement or development of information services or software applications.
Exception	An exception is a deviation from established policies, standards, procedures, or controls. Exceptions can arise when a risk control measure cannot be applied or is ineffective under certain conditions,

	leading to a temporary or permanent deviation from standard policies. Exceptions must be reviewed and approved in the context of the applicable Policy, Standard, Process, or Procedure. Departments should reach out to IT Risk & Compliance at itrc@gmu.edu for assistance regarding using the Exceptions template (Sample in Appendix B).
George Mason's Systems	They include applications, utilities, networks, storage, compute, database, and similar George Mason-owned and/or operated assets that are either on-prem or in the cloud.
Information Service	Refers to vendor-provided service employing a combination of information technology and people to store, process, and/or transmit university data.
Office of University Counsel	The Office of University Counsel assists the Purchasing Office with negotiating non-routine changes to standard terms and conditions and approves changes to George Mason's standard contract form and Data Security Addendum that address indemnification and/or limitations to liability.
Protected Data	Highly Sensitive Data or Restricted Data, as defined by University Policy Number 1114, Data Stewardship.
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 A).
Significant Change	Significant change refers to major changes such as in contract, architecture, implementation, subscription, adoption, number or type of users, etc., that involve a significant amount of preparation and work, evaluation, authorization, investments, and planning.
Software Application	Refers to computing software designed to carry out a specific task, or tasks, other than those related to the operations of the computer itself.
System Administrator	A System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Custodian.
System Owner	The System Owner is the person responsible for the operation and maintenance of a university system.

INFORMATION TECHNOLOGY SERVICES
George Mason University

PROCESS OVERVIEW:

The stages described here are tailored to George Mason's operating environment and security requirements.

Solution Selection

Requirements may enter the process via multiple pathways, with requests ranging from a loosely defined need to a specified off-the-shelf solution.

1. Contracts, technical compatibility, compliance with federal, state, and university policies, and security should all factor into the selection of a solution.
2. Business units are advised to consult with ITS early in the planning stage, e.g., utilizing the ITS Solution Request process to identify feasible alternatives and avoid potential stumbling blocks that could delay acquisition and/or implementation.
3. Per University Policy Number 1307, Procurement and/or Development of Administrative Systems/Applications, all procurement and/or development of software applications or information services of the dollar amounts greater than $5000 that will use George Mason data or integrate with George Mason's systems, or have a user interface, must be reviewed and approved by the Architecture Standards Review Board (ASRB) before finalizing the contract or procuring the software application or information services.
4. For the procurement of software applications or information systems of dollar amounts $5000 or less, PCard and eVA authorized approvers are required to ensure that potential purchases that meet the criteria for ASRB review, must be reviewed and approved by the ASRB before they approve the purchase.

Risk Assessment

Risk and security assessments are performed as part of the ASRB process for contractual arrangements of software applications or information services as per criteria defined in University Policy Number 1307, Procurement and/or Development of Administrative Systems/Applications.

Using the security and/or technical documents, as well as the current industry standard independent third-party audit reports provided by the third-party providers, ITRC collaborates with the IT Security Office (ITSO) to perform risk and security assessments on the requested software application or information services. The assessment results are then updated in the ASRB ticket.

Contract Negotiation

Depending on the contract's complexity and the perceived level of associated risk, negotiations may involve representatives from:

- Purchasing Office
- Office of University Counsel
- Information Technology Security Office (ITSO)
- Information Technology Risk and Compliance (ITRC)
- Assistive Technology Initiative (ATI) function of the Office of Compliance, Diversity, and Ethics[1]
- ITS operational units in scope for support or integration
- The university unit or department that initiated the request ("Sponsor")

1. **Exceptions:** All exceptions must be reviewed and approved by the appropriate policy/standard/process owner.
2. If the third-party provider will not agree to all the university's requested control(s), resulting in an elevated level of residual risk, risk must be documented and accepted by the appropriate George Mason leadership, usually the Vice-President of the appropriate department or unit.
3. The Data Owner(s) responsible for in-scope Protected Data must be informed of the contractual arrangement and any negotiated exceptions to the standard controls by the Purchasing Office or Office of University Counsel. Data Owner may require that specific data elements be excluded or not be used based on sensitivity and the results of the risk assessment.
4. The use of in-scope Protected Data must be approved by the responsible Data Owner as defined by University Policy Number 1114, Data Stewardship, or by a delegate assigned in writing.
5. The Purchasing Office must include a Data Security Addendum with the contracts or purchase orders of third-party products/services that have been identified to create, transmit, use, maintain, process, store, or dispose of university protected data by the ITRC staff in the Risk Assessment stage of this process.

Ongoing Monitoring

1. ITRC requests current industry-standard independent third-party certifications/attestations (e.g., SSAE 18 SOC 2 reports, ISO 27001/2, or equivalent) from third-party providers managing George Mason Protected Data. These requests follow the projected dates in the TPRM Module that specifies when these reports are anticipated to be released, with access limited to authorized users. A list calendar is displayed on the TPRM dashboard. These third-party providers consist of both those on rider contracts and those with direct contracts with the university and the Commonwealth of Virginia.
2. ITRC evaluates the certification/attestation and notes the following using the procedure called Entering the Due Diligence Review Process Results in Archer TPRM Module (ITS.ITRC-PROC002):
    a. Reporting Period of the independent third-party certification/attestation
    b. The auditor's overall status of the assessment
    c. Exceptions or deviations noted by the auditor
    d. If applicable, the third-party's management response to deviations or exceptions noted by the auditor
    e. Applicable Complementary User Entity Controls (CUECs), and a determination of whether they are being performed by the System Owner/Administrator or third-party provider that relies on its sub-service organization's industry-standard independent third-party certification/attestation.

[1] ATI performs accessibility reviews on applications intended for wide-scale use at the university, in accordance with University Policy Number 1308, Electronic and Information Technology Accessibility.

3. If the review indicates that the third-party provider is not maintaining compliance with the security controls specified in the contract, the ITRC staff notifies and forwards the information to the ITRC Director for potential escalation and/or risk treatment action. ITRC also confers with the System Owner, System Administrator, and ITSO to assess the impact on risk.
4. If the review reveals exceptions in the independent third-party attestation, the ITRC staff collaborates with the system owner to determine their relevance and impact. The system owner also evaluates the vendor's response and remediation efforts. If needed, additional controls will be implemented to mitigate the risks.
5. If the review indicates that the System Owner/Administrator or the third-party provider that relies on its sub-service organization's industry-standard independent third-party certification/attestations is not compliant with the CUECs, the ITRC staff works with them to address the non-compliance.

Termination

The termination stage of this process only applies to third-party contracts with George Mason.

1. At the end of the contract, the Department Representative arranges for any required transfer of data back from the third-party provider. *Note that the contract during the Contract Negotiation stage includes a termination clause that calls for the third-party provider to terminate or return all George Mason data.*
2. ITRC notes the termination date in the contract inventory.

INPUTS AND OUTPUTS:

Inputs:

- ASRB ticket
- Non-Disclosure Agreement between third-party and George Mason
- Security and/or technical documents from a third-party provider
- Current industry-standard independent third-party audit reports provided by the third-party provider

Outputs:

- ASRB ticket
- Contract with third-party provider (Riders and contracts between the vendor and the Commonwealth of Virginia are not owned by George Mason. The university will attempt to obtain a copy.)
- Risk treatment (if applicable)
- Engagement record in Archer TPRM Module

REVIEW SCHEDULE:

Annually

APPROVAL:

Title, Department Name	Name	Signature and Date
Director, IT Risk & Compliance	Noor Aarohi	DocuSigned by: Noor Aarohi 5/5/2025 D37A04E44AA04AD..

REVISION HISTORY:

Date	Version Number	Department or Author	Brief Description of Changes
1.0	12/8/2020	IT Process & Planning / Randy Anderson	Initial release
2.0	12/6/2023	IT Risk & Compliance / Cindy Kim & Noor Aarohi	Annual review with significant revisions (re-writing the entirety of the document and populating the Definitions table) including updating the DCN due to change in process ownership and reformatting content using the current template.
2.1	02/12/2024	IT Risk & Compliance / Noor Aarohi & Cindy Kim	Added appendices, definitions, and notes to users.
2.2	08/30/2024	IT Risk & Compliance / Cindy Kim	Updated section on exception review.
	03/03/2025	IT Risk & Compliance / Noor Aarohi	Added the Director, Finance Reporting as a source to request additional solutions/services to be included in the TPRM inventory for monitoring.
	03/04/2025	IT Risk & Compliance / Cindy Kim	Reformatted content using the current process template.
2.3	04/05/2025	IT Risk & Compliance / Cindy Kim	Updated sections to include data security addendum to contracts or purchase orders and to clarify the type of calendar maintained in the TPRM Module

RELATED DOCUMENTS/REFERENCES:

- Entering the Due Diligence Review Process Results in Archer TPRM Module Procedure (ITS.ITRC-PROC002)

APPENDIX A – Risk Acceptance Form 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.**

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):

INFORMATION TECHNOLOGY SERVICES
George Mason University

APPENDIX B – Exceptions Form 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					