

Virginia Tech IT Risk Management Standard

1. Purpose and Scope

This standard establishes the process for assessing and evaluating university IT assets, including university-owned technology resources and applications, for risks to systems and data; and documenting and communicating those risks to university stakeholders so decisions regarding the treatment or acceptance of those risks can be determined. The security and privacy of “High-Risk” university data will be a primary focus of IT risk assessments. This standard directly supports [University Policy No. 7010 - Policy for Securing Technology Resources and Services](#) and [University Policy No. 7105, Policy for Protecting University Information in Digital Form](#). The key objective of this standard is to ensure a periodic and comprehensive assessment of risks related to the university's information systems, and the processing, storage, and transmission of institutional data. These assessments include risks to university operations that could affect the institutional mission, function, or reputation or affect university assets and individuals. The assessment process is designed to help identify risks, document concerns, prioritize mitigations, implement actions, and monitor efforts on an ongoing basis in support of the comprehensive information security management program.

Key Program Principles:

1. Security is a shared responsibility and everyone has a role to play;
2. In continuous risk management, risk assessment is key;
3. Unit leaders have responsibility in managing their own information security risk; and
4. “Risk” and “Priority” classifications primarily inform risk level and security controls.

2. Standard

The IT Security Office (ITSO) administers Virginia Tech's IT Risk Management (ITRM) program and maintains our Governance, Risk Management, and Compliance (GRC) platform. University organizational units maintain IT asset inventories and complete periodic IT Risk Assessments (ITRA) for their units using the GRC platform. The Virginia Tech IT risk assessment process is based on information technology risk assessment methodologies documented in **NIST SP 800-30: Guide for Conducting Risk Assessments** ^[1].

2.1 GRC Roles and Responsibilities

Applicable personnel from university organizational units (“org unit”, OU) shall be enrolled in the GRC platform with permissions appropriate for their role:

- **Organizational Unit:** This is the level at which IT Risk Assessments are completed using the GRC platform. Org units can be managed at the Dean, Vice President (VP), or Associate/Assistant Vice President (AVP) level, or at the Department level, at the discretion of Deans, VPs, and AVPs. Risk assessments completed at the Department level will have higher fidelity than assessments completed at higher levels.
- **Org Unit Head:** Department Head, Dean/AVP, or Senior IT leader (if delegated by Department Head). This role is responsible for final acknowledgement of IT risk assessments representing the organizational unit.
- **Assessment Manager:** Responsible for managing assessments and ensuring accurate data entry into the system (inventories, asset classification, and overseeing IT risk assessment survey responses).
- **IT Staff:** Responsible for completing any assigned sections as delegated by the Assessment Manager(s).
- **User:** Responsible for *individual* assets inventoried in the GRC system. Those accounts with the “User” role will be able to manage any individual assets where they are identified as the “owner”. The IT risk assessment team may choose to enroll personnel from their organization with this role when appropriate

(i.e. an application developer that is not a part of the IT unit, or a part of the IT risk assessment team, but needs to be able to manage inventory records for their custom applications.)

2.2 GRC Asset Inventory

All university-owned technology resources (endpoints [laptops, desktops] & servers [physical, virtual, cloud], network infrastructure devices, multi-function printers/scanners, as well as special-purpose computing devices capable of storing or processing university data), aka “assets”, and custom software applications developed “in- house” by Virginia Tech resources, aka “applications/apps”, shall be registered in the ITSO GRC system for the purpose of IT risk assessment. GRC asset inventory records must include at a minimum (as applicable):

- **Assets:** asset name(s), description, IP address(es) (if static), MAC address(es), asset/system type, OS/platform version, inventory tag number (or serial number), owner (custodian), and responsible IT administrative support contact(s);
- **Applications:** application name, description, owner and/or responsible administrative support contact(s), data risk classification (if classified as high-risk, include data categorization), deployment details (URL(s), relationship to supporting infrastructure [from hosts inventory], etc.).

2.2.1 GRC Asset Classification and Categorization

All assets shall be classified according to the [Virginia Tech Risk Classification Standard](#) to include both “Risk” and “Priority” classification labels. Any asset(s) classified as “High-Risk” shall also be categorized by the “High-Risk” data type(s) handled by the asset(s) and/or the “High-Risk” function(s) performed by the asset. Any asset(s) classified as “High-Risk” and/or “Critical-Priority” must also designate and maintain appropriate contact information for use by the university’s 24x7 Security Operations Center (SOC).

Any server classified as “Critical-Priority” or “High Risk” must have a fully qualified domain name (FQDN) or static Internet Protocol address recorded in the inventory entry for that asset. The definition of “Server” is provided in Paragraph 4, below.

2.3 GRC Assessment Survey

IT risk assessment surveys are used to measure an organizational unit’s security posture scoped to that organizational unit’s IT operations, including the information technology assets cataloged in the OU’s inventory and the processes or functions carried out or supported by the organizational unit. The intent of the assessment surveys is to identify areas of weakness, vulnerabilities, or gaps in security controls, based on university security standards, for further analysis or evaluation (threats, impact, likelihood, etc.) and ultimately, for appropriate risk treatment (acceptance, avoidance, transference, or mitigation).

As cybersecurity is a rapidly evolving field, exact content and format of IT risk assessment surveys will vary based upon factors such as updates or changes to policies, standards, external regulatory compliance requirements, and/or other industry best practices. Generally, IT risk assessment surveys will evaluate the org unit(s) or individual application(s) adherence to the [Virginia Tech Minimum Security Standards v4.0](#) relative to the *effective scope* of the standard.

2.4 Risk Model and Risk Analysis

To evaluate information security risk, a qualitative, asset/impact-oriented risk model shall be used to analyze each residual risk identified to determine the severity of the risk based upon the combination of factors of **“Likelihood”** - *the probability that a given threat is capable of exploiting a given vulnerability*, and **“Impact”** - *the magnitude of harm that can be expected to result from the consequences of the risk event occurring*. The determination of the appropriate likelihood (figure 1) and impact (figure 2) values for a risk is typically based upon a threat assessment, whereby the nature of a threat is determined and the degree of threat to an asset or

organization is evaluated. A taxonomy of threat sources and list of representative examples of threat events that can be considered for this exercise are available in **NIST SP 800-30: Guide for Conducting Risk Assessments**.

Likelihood Factor Scale		
Rating	Value	Description
Highly Unlikely	1	Highly unlikely risks have a very low probability of occurring, 10% or less.
Unlikely	2	Unlikely risks have a relatively low chance of occurring – 11-35% chance of occurrence.
Possible	3	Possible risks may happen about half of the time, with a 36-60% chance of occurrence.
Likely	4	Likely risks have a 61-90% chance of occurring. These risks need regular attention, as they are bound to reoccur and therefore require a consistent mitigation strategy.
Highly Likely	5	Risks in the highly likely category are almost certain to occur. Risks with 91% or more likelihood fall into this category.

Figure 1: Likelihood Factor Scale

Impact Factor Scale		
Rating	Value	Description
Negligible Impact	1	Risk event would result in minimal or zero adverse consequences on university operations or resources. There would be negligible or zero disruption or loss, requiring almost no remediation efforts.
Low Impact	2	Risk event would result in minor disruptions with limited impact on a single department/organization. Remediation efforts are straightforward.
Moderate Impact	3	Risk event would result in some level of downtime/disruption in one or more university departments or orgs and may result in exposure of “Moderate-Risk” university data. Remediation efforts may require some additional resources and time.
High Impact	4	Risk event would cause significant disruptions or losses, negatively impacting university operations in multiple departments and potentially resulting in exposure of “High-Risk” and/or “Moderate-Risk” university data. Remediation efforts would be complex and may require substantial resources.
Catastrophic Impact	5	Risk event would have severe consequences, likely resulting in widespread (affecting most department or personnel) or irreparable damage to university operations/reputation, threats to human life/safety, or would cause extensive exposure of “High-Risk” university data. Recovery/remediation efforts would be extensive and very costly, if possible at all.

Figure 2: Impact Factor Scale

The function of the combination of likelihood and impact factors enables the prioritization of information security risks for prioritization and appropriate risk treatment. The risk analysis scoring matrix (figure 3) shall be used to determine the effective risk severity rating (figure 4) for the risk, where:

$$\text{Risk Severity Rating} = \text{Likelihood} \times \text{Impact}.$$

Risk Analysis Scoring Matrix					
Likelihood/ Impact	Negligible Impact (1)	Low Impact (2)	Moderate Impact (3)	High Impact (4)	Catastrophic Impact (5)
Highly Likely (5)	Low Severity	Moderate Severity	High Severity	High Severity	Major Severity
Likely (4)	Low Severity	Moderate Severity	Moderate Severity	High Severity	Major Severity
Possible (3)	Low Severity	Low Severity	Moderate Severity	High Severity	High Severity
Unlikely (2)	Negligible Severity	Low Severity	Moderate Severity	Moderate Severity	High Severity
Highly Unlikely (1)	Negligible Severity	Low Severity	Low Severity	Moderate Severity	High Severity

Figure 3: Risk Scoring Analysis Matrix

Risk Severity Rating Scale	
Negligible- Severity Risk	Highly unlikely and unlikely risks with negligible impact.
Low- Severity Risk	Possible, likely, and highly likely risks w/ negligible impact; highly unlikely, unlikely, and possible risks w/ low impact; or highly unlikely risks w/ moderate impact.
Moderate- Severity Risk	Likely and highly likely risks w/ low impact; unlikely, possible, and likely risks w/ moderate impact; or highly unlikely and unlikely risks w/ high impact
High- Severity Risk	Highly likely risks w/ moderate impact; possible, likely and highly likely risks w/ high impact; or highly unlikely, unlikely and possible risks w/ catastrophic impact.
Major- Severity Risk	Likely and highly likely risks with catastrophic impact.

Figure 4: Risk Severity Rating Scale

2.5 Reporting

Reports are generated from the GRC system for IT risk assessments targeted at OUs or individual applications. These reports summarize the OU's "assets" inventory by risk classification and the results of the assessment survey. The ITSO shall maintain up-to-date GRC metrics at <https://metrics.iso.vt.edu> for ad hoc inventory and assessment reporting.

2.6 Risk Ownership and Risk Acceptance

Figure 5 establishes the stakeholder responsibilities in ownership and/or acceptance of residual security risks

based upon the risk severity rating. Named data trustees and data stewards are listed in the [Standard for Administrative Data Management](#). Documentation of risk acceptance shall be maintained by the ITSO.

Risk Ownership and Risk Acceptance	
Negligible-Severity Risk	Negligible-Severity and Low-Severity risks are owned by the OU. These risks can be accepted by the OU Head(s) or Assessment Manager(s) if delegated by the OU Head.
Low-Severity Risk	
Moderate-Severity Risk	Moderate-Severity risks are owned by the OU and relevant data steward(s), if applicable. These risks can be accepted by the OU Head and/or relevant data steward(s), where applicable
High-Severity Risk	High-Severity risks are owned by the applicable data steward(s). Risk acceptance(s) shall be carefully considered among all relevant stakeholders and documented as necessary.
Major-Severity Risk	Major-Severity risks are owned by the VT IT Risk Governance Committee. These risks may potentially threaten the university's mission and cannot be accepted; these risks must be treated.

Figure 5: Risk Ownership and Risk Acceptance

2.7 Risk Treatment

Risk treatment efforts shall be undertaken to mitigate documented unaccepted residual risks, using appropriate administrative, technical, and/or physical security controls. Valid risk treatment options are:

1. **Mitigation** – Apply controls to reduce the impact of the risk event's potential consequences and/or the likelihood that it will occur.
2. **Avoidance** – Eliminate the conditions that allow the risk to exist.
3. **Transference** – Transfer liability (partially or wholly) of the risk event's potential consequences to another party.

Risk treatment decisions, including all related corrective action plans, shall be documented with the ITSO under the oversight of the IT Risk Working Committee of IT Governance. Treatment decisions should take account of the legal-regulatory and private certificatory requirements; organizational objectives, operational requirements, and constraints; and the costs associated with implementation and operation relative to the risk being reduced. Individual departments are responsible for addressing IT risks within their organizations. Compliance is monitored by the IT Security Office, and audited by Virginia Tech's Office of Audit, Risk, and Compliance (OARC), which completes departmental Policy Compliance Reviews on a three-year cycle.

2.8 Organizational Unit IT Risk Assessment Requirements

Figure 6 establishes the minimum organizational IT risk assessment requirements based on the highest level of "Risk" or "Priority" classification from the OU's GRC inventory. Higher-risk OUs will generally complete assessments more frequently than lower-risk OUs. Since risk level may change over time, the projected risk assessment cadence is also subject to change accordingly. The ITSO will contact university OUs to initiate and support this work using a risk-based approach.

OU IT Risk Assessment Minimum Requirements			
Risk Priority	High-Risk / Critical-Priority	GRC Inventory Updates	GRC Assessment Survey
	The Org Unit's GRC inventory includes one or more High-Risk or Critical-Priority assets	High-Risk/Critical-Priority asset inventory records must be documented <i>immediately upon deployment</i> and <i>kept up-to-date</i> by the asset owner whenever changes are made that impact the accuracy of the GRC asset inventory records(s). Inventories must be revalidated at least annually.	Annually
Moderate-Essential	Moderate-Risk / Essential-Priority	GRC Inventory Updates	GRC Assessment Survey
	The Org Unit's GRC inventory includes one or more Moderate-Risk or Essential-Priority assets, but no High-Risk assets and no Critical-Priority assets	Moderate-Risk/Essential-Priority asset inventory records must be documented and updated <i>at least quarterly</i> , as needed. Inventories must be revalidated at least annually.	Annually
Low-Non-Essential	Low-Risk / Non-Essential Priority	GRC Inventory Updates	GRC Assessment Survey
	The Org Unit's GRC inventory includes only Low-Risk and Non-Essential-Priority assets	Low-Risk/Non-Essential-Priority asset inventory records must be documented and updated <i>at least annually</i> .	Every two years

2.9 Related Requirements

[University Policy No. 7025 – Safeguarding Nonpublic Customer Information](#) specifies the roles, responsibilities and procedures for “facilitating compliance with the Gramm-Leach-Bliley Act (GLBA) and Standards for Safeguarding Customer Information (16 CFR, Part 314, aka “Safeguards Rule”) through developing, implementing, and monitoring policies and procedures that include specific requirements regarding the privacy of customer financial information.” This standard supports the required risk analysis process for the Office of University Scholarships and Financial Aid, the Bursar’s Office, and any other departments that collect nonpublic personal financial information from a customer seeking to obtain a financial product or service as described in GLBA by periodically assessing risk to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of nonpublic personal financial information that could result in the unauthorized

disclosure, misuse, alteration, destruction or other compromise of such information, and assessing the sufficiency of any safeguards in place to control these risks. The university's risk analysis activities related to GLBA and handling of nonpublic customer information will be described in an annual GLBA assessment also documented in the GRC system.

3. Compliance and Enforcement

It is the responsibility of organizational unit leaders to ensure that the controls described in this document are implemented. Department leaders are responsible for remediation of any findings of noncompliance with this standard. Failure to remediate or mitigate known risks in a timely manner could result in offending systems being removed from the university network.

4. Definitions

GRC. Governance, Risk, and Compliance.

Asset. Any university-owned technology resources (endpoints [laptops, desktops] & servers [physical, virtual, cloud], network infrastructure devices, multi-function printers/scanners, as well as special-purpose computing devices capable of storing or processing university data), aka "assets", and custom software applications developed "in- house" by Virginia Tech resources, aka "applications/apps".

Server. A host that provides network-accessible services. Server can be physical or virtual machines and may be hosted in-premises or with a cloud service provider (CSP).

5. References

NIST SP 800-30: Guide for Conducting Risk Assessments:

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

6. Maintenance of Standard

The IT Security Office is responsible for this IT Standard. Questions may be directed to itso@vt.edu.

7. Revision History

Version 1, published August 2024

Version 2, published February 2026

- Standard changed to IT Risk Management Standard from IT Risk Assessment Standard.
- Clarified organizational unit definition.
- Added requirement for fully-qualified domain name or IP address for university-critical systems.
- Added Risk Acceptance as a potential risk treatment.
- Edited for clear language and consistency with other IT security standards.