-->

Risk Review Standard

Last Modified on 05/08/2025 9:35 am EDT

Table of Contents

For more details about the Information Security Office, **please visit our website**!

1. Introduction

This *Risk Review Standard* outlines the inputs, activities, decisions, and outputs for submitting and performing risk reviews of enterprise systems and third-party vendors at the Wharton School. Risk reviews are essential to understanding the risk associated with enacting significant changes and when introducing additional assets or vendors into the Wharton information technology (IT) environment. The purpose of this standard is to mitigate risk while enabling initiative success and supporting the business of the school.

This Standard describes the workflow for submitting, analyzing, and developing risk determinations. This standard includes italicized text when referencing documented policies, standards, and procedures (e.g., *Wharton Information Security Policy*).

1.1 Risk Review Standard Owner

The Chief Information Security Officer (CISO) is the lead of the Wharton Information Security Office (ISO). This role is accountable for the development and maintenance of this standard in accordance with both Penn and Wharton Information Security Policy. Additionally, the ISO is responsible for performing risk reviews as described in the Risk Review Process.

1.2 Purpose

In accordance with the *Wharton Information Security Policy*, the Risk Review Process scopes and assesses cybersecurity risks attributed to enterprise systems (existing and new) and third-party vendors within Wharton. The Risk Review Process establishes a standardized and risk-based analysis of the strength of the control environment and the adequacy of the related internal control frameworks.

Security risks are identified through an analysis of collected information/data regarding the intended use within the Wharton environment. The objective of these risk assessments is to understand how systems, assets, vendors, or initiatives may impact the design, security, or privacy of Wharton IT systems.

1.3 Scope

This standard applies to all enterprise systems (existing and new), third-party vendors, or contractors/consultants, or initiatives which may impact IT systems, components and services owned, or operated by Wharton. Interconnected systems and systems sharing data with Wharton systems are also in scope for this standard.

1.4 Compliance

This standard complies with the directives defined in the *Wharton Information Security Policy*. Wharton leveraged industry best practices and guidance (e.g., National Institute of Standards and Technology (NIST) 800-30 Rev. 1, Guide for Conducting Risk Assessments) in the development of the *Risk Review Standard*.

Top

2. Key Roles & Responsibilities

This section defines the roles and responsibilities for the *Risk Review Standard*.

2.1 Wharton Sponsor

The Wharton Sponsor is the requestor of the Risk Review and may be member of any Wharton department, center, or initiative (e.g. staff, faculty, or PhD student). The Sponsor and their designated Wharton Computing partner are responsible for completing a Scoping Document, clearly describing the proposed request, and submitting a Risk Request to initiate the Risk Review process. The Sponsor is also responsible for implementing any proposed risk mitigation defined by ISO.

2.2 Wharton Information Security Office

Wharton ISO is the receiver, assessor, and recommendation provider for Risk Review requests. ISO facilitates, and reviews collected artifacts/information and utilizes provided and independently researched information to complete risk dispositions and assessments.

2.3 University Procurement, Privacy, etc.

Penn Procurement is often responsible for completing the procurement process for Wharton initiatives, though exceptions occur. As such, Procurement is made aware by Wharton ISO of all proposed initiatives and Risk Review requests submitted by Wharton Sponsors. Procurement is responsible for ensuring that a Risk Review has been performed before proceeding with a review of initiative requests, and ultimately moving forward with procurement. Wharton ISO will also include the Office of Audit, Compliance, and Privacy (OACP), the department Business Administrator (BA), the Office of General Counsel (OGC), and/or the Office of Research Services (ORS) on communications as necessary.

Top

3. Risk Overview

Risk is determined by evaluating the potential impact imposed by a threat source acting on a vulnerability. This threat and vulnerability pair establishes a risk event that may impact Wharton business operations. Once identified, risk events are weighted based on the likelihood of the risk being realized and the impact of the risk if it were to occur.

Risk management is the total process of identifying, controlling, and eliminating or minimizing uncertain events that may adversely affect system resources. Wharton leverages the guidance within the National Institute of Standard

and Technology (NIST) Special Publication (SP) 800-30 and NIST SP 800-39 for identifying, assessing, and managing cybersecurity risks.

Wharton calculates risk using the following formula:

risk = (threat x vulnerability x probability of occurrence x impact)/controls in place

The following subsections provide an overview of key risk terms.

3.1 Threats

NIST defines threats as any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. Wharton leverages the NIST definition of threats to identify any circumstance that may adversely affect Wharton operations.

The first step in identifying risks is to define the threat sources. Threat sources are characterized as: (i) the intent and method targeted at the exploitation of a vulnerability or (ii) a situation or method that may accidentally exploit a vulnerability. Types of threat sources include adversarial (e.g., individual, group, organizational), accidental, structural (e.g., IT equipment, software) or environmental (e.g., natural or man-made disaster, unusual natural events, infrastructure failures).

Once threat sources that may adversely affect the operations of systems described in the Risk Request submission are identified, ISO consults with the Wharton Sponsor to quantify the threat using Figure 1 below.

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

Figure 1. Characteristics of Adversary Capability Assessment Scale (NIST SP 800-30)

3.2 Vulnerabilities

NIST defines vulnerabilities a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Wharton vulnerabilities may be security gaps or weakness in IT systems and networks. This includes missing patches, weak system configurations, lack of effective risk management strategies, etc. An exploitable vulnerability is any known vulnerability that can be leveraged by an attacker (i.e., threat source) to harm business operations. Effective Wharton vulnerability management involves the integration of different operational

and security focused areas to harden systems, track configuration changes, identify weaknesses, and remediate vulnerabilities across Wharton's environment.

Wharton ISO evaluates vulnerabilities of the systems identified in the Risk Request submission to quantify the vulnerability level using the definitions provided in Figure 2. below

Qualitative Values	Semi-Qualitative Values		Description
Very High	96-100	10	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
High	80-95	8	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.
Moderate	21-79	5	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.
Low	5-20	2	The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective.

Very Low	0-4	0	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective.

Figure 2. Vulnerability Severity Assessment Scale (NIST SP 800-30)

3.3. Likelihood

The likelihood of a risk impacting Wharton business operations is determined using qualitative analysis of the probability that a given threat is capable of exploiting a vulnerability based on existing security controls. While likelihood can be measured using many approaches, Wharton uses the qualitative values from Figure 3 below to assign a likelihood rating as part of the Risk Review.

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the treat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the treat event.

Figure 3. Likelihood Assessment Scale (NIST SP 800-30)

3.4 Impact

The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, loss of information or loss of information system availability. Similar to determining the likelihood of a threat source acting on a vulnerability, Wharton leverages the qualitative assessment from NIST SP 800-30 to determine the impact of the risk event occurring based on existing security controls.

Qualitative Values	Semi-Quantitative Values	Description

Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event 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.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event 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.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event 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.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Figure 4. Impact of Threat Events Assessment Scale (NIST SP 800-30)

3.5 Risk Level

The risk level is the overall measure of the effect a threat source has when acting on a vulnerability causing harm to business operations through a specific risk event. Cybersecurity risk events typically result in loss of confidentiality, integrity, or availability that affect Wharton business operations. Risk levels are calculated as the product of the likelihood and impact levels for the risk event. As with determining likelihood and impact, Wharton leverages the guidance provided in SP 800-30 for determining risk levels.

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	**Very high risk** means that a threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	**High risk** means that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Figure 5. Level of Risk (Combination of Likelihood/Impact Assessment Scale (NIST SP 800-30)

The Wharton ISO risk assessment approach is derived from the descriptions provided in SP 800-30, as shown in Figure 6, below, when describing the meaning of the risk level associated with a risk event.

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate

Very Low	Very Low	Very Low	Very Low	Low	Low

Figure 6. Level of Risk (Qualitative/Semi-Quantitative) Assessment Scale (NIST SP 800-30)

While Wharton ISO generally leverages the Risk Assessment Scale from NIST SP 800-30, the scale is normalized to align with the operational risk attribution scale defined in the Wharton Vulnerability Management Standard. Figure 7 below illustrates the alignment across scales.

NIST SP 800-30 Qualitative Values	Severity Risk Rating Matrix		Wharton Qualitative Values	Wharton Severity Risk Rating Matrix Risk Levels
Very High	96-100	10	**Critical/Out-of-Band** (Severe)	**9-10**
High	80-95	8	**High**	**7-8**
Moderate	21-79	5	**Moderate** (Elevated/Guarded)	**4-6**
Low	5-20	2	**Low**	**0-3**
Very Low	0-4	0		

Figure 7. Level of Risk (Qualitative/Semi Quantitative) Wharton Assessment Scale)

Top

4. Risk Review Overview

The Risk Review process covers distinct review types as described below. Risk reviews are conducted against enterprise systems, third-party vendors, consultants and contractors, and initiatives as required based on the Risk Review submission. The following subsections further describe these types.

4.1 Enterprise System

An Enterprise System Risk Review assessment is required when an enterprise system plans to undergo a change or a new enterprise system or component is planned for development/implementation. Enterprise systems are assessed through a risk-based analysis of the strength of the control environment and the adequacy of the related internal control frameworks. As part of this assessment, all relevant components to include infrastructure, software code, appliances, architecture/design changes, related data flows, including potential interconnections with other systems outside of the accredited authorization boundary, are considered. The goal of Enterprise System Risk Review's is to identify and quantify the potential risk to the system and/or the Wharton IT environment if the system is changed as defined in the Risk Review submission.

New and potential changes to system interconnections may also require an ISA (Interconnection Security Agreement) or MOU/A (Memoranda of Understanding/Agreement) to describe the rationale for the interconnection. This rationale becomes the basis for performing a risk assessment on potential changes, or new,

interconnections to systems.

4.2 Third-Party Vendor

A Risk Review assessment of a third-party vendor is required to identify risks and hazards associated with the vendor's processes, products, and solutions (e.g., external services), including associated consultants and contractors. The goal of this assessment type is to ensure that appropriate security controls are implemented to protect the confidentiality, integrity, and availability of data. Upon selection, Wharton ISO periodically monitors third-party vendor compliance throughout the vendor contract duration.

4.3 Consultant or Contractor

A Risk Review assessment of a consultants or contractor is required to identify potential risks and vulnerabilities associated with their involvement in organizational processes and projects. This assessment ensures that these external parties adhere to the organization's security policies and standards, safeguarding the confidentiality, integrity, and availability of sensitive data. Upon selection, Wharton ISO periodically monitors consultant/contractor compliance throughout their contract duration.

4.4 Initiative

An Initiative Risk Review assessment is required when a new initiative is proposed or an existing initiative undergoes a significant change in scope. This review ensures that all aspects of the initiative, including multiple systems and their interconnections, are thoroughly evaluated for potential risks. All relevant components, such as infrastructure, software, appliances, architectural and design changes, and data flows, are considered to identify and quantify potential risks. It is crucial to ensure that these initiatives comply with security standards and protect the organization's information assets. Any change in the scope of an initiative requires reassessment to ensure continuous protection and risk management throughout the initiative's lifecycle.

Top

5. Risk Review Process

As part of a comprehensive risk assessment and management process, Wharton leverages the following process to conduct risk reviews. **Risk reviews are required for all new Wharton services/systems/initiatives, any scope changes or contract renewals of current services/systems/initiatives, or when requested by ISO.**

5.1 Ideation

During the ideation process, the Wharton Sponsor and relevant stakeholders explore and identify potential solutions (e.g., new technology, third-party vendor solution) that may fulfill an identified business requirement. Once vetted by the relevant stakeholders, the Wharton Sponsor will submit the proposed solution in the form of a *Risk Review Request* along with a *Security and Privacy Scoping Document* to ISO for review. The scope should include elements such as: Problem Statement (E.g. Needs), Intended Use, Audience, Audience Use-How, Data Elements, etc.

5.2 Request Risk Review

For all risk reviews, a Wharton user submits the *Security and Privacy Scoping Form* to begin the process. The request should also include available documentation such as:

1. VSTAR

2. HECVAT

3. Supplemental Security & Privacy Information (e.g. security certifications – Soc 2 Type 2, ISO 27001, support documents for information security and privacy, cyber insurance, etc.)

While not all documentation listed above may be required for each review, additional information enhances Wharton ISO's ability to identify potential risks and recommend effective mitigation strategies. Any questions about documentation for a specific review can be answered by ISO.

NOTE: A data flow diagram is also required if available (particularly for the review of an application interacting with other systems/applications). The data flow diagram must illustrate intended system interconnections and dependencies. Additionally, impacted data types and how they are processed, stored, and shared should be included along with any implementation and rollout plans.

5.3 Review Risk Request

Upon receipt of a *Risk Review Request* and supporting artifacts, ISO uses the provided information as well as independent research, as appropriate, to review the request. Wharton ISO may also collaborate with the Office of General Counsel (OGC), and/or the Office of Research Services (ORS), and the Office of Audit, Compliance, and Privacy (OACP) as necessary. Once ISO has sufficient information, it will assess the potential risks to Wharton operations based on the *Risk Review Request*.

All relevant information for the Risk Review will be reviewed and may include:

- Independent analysis of open-source information
- Clarifications from the Wharton Sponsor based on the ISO's preliminary analysis
- Procedures or provided recommendations on alternative, security compliant acceptable processes and applications as appropriate
- Relevant existing security policies, architecture, standards, guidelines, publicly available security related documents and procedures
- Attestation certifications and documentation

5.4 Develop Assessment Report

ISO will produce a *Risk Review Disposition* resulting from the review of the completed *Security and Privacy Scoping Document*, and any additional security artifacts. Based on the findings in the report, a risk rating of **Low**, **Medium**, **High**, or **Critical** will be assigned for the assessment report. In addition, ISO may develop practical technical recommendations and recommend best practices to address the vulnerabilities identified with the goal of reducing the level of security risk.

5.5 Issue Risk Disposition

Based on the analysis, ISO will make a risk determination and provide recommendation to the Wharton Sponsor and Penn Procurement for review via email from security@wharton.upenn.edu. ISO will share the assessment report internally with relevant parties (e.g., Penn Procurement, OACP, etc.), provide recommendations for securely implementing the initiative, or provide alternative solutions, to minimize identified risk.

This report will outline any potential areas of risk and provides next steps:

- Proceed if willing to accept outlined risk,
- ISO will verify if a SIA (*Security Impact Analysis*) should be completed by the requestor in accordance with the *Change Enablement Standard*, or
- Recommend the initiative not proceed if risks cannot be appropriately mitigated to an acceptable level.

NOTE: A Security Impact Analysis (SIA) is required for significant changes to enterprise systems.

5.6 Review Risk Determination

The Wharton Sponsor will review the *Risk Review Disposition* and determine if the initiative will move forward by engaging Penn Procurement. Upon a decision not to proceed, the Wharton Sponsor may elect to conduct for further discussion with relevant stakeholders to develop a revised proposal for the initiative. The Wharton Sponsor would develop a new *Risk Review Request* if a revised proposed initiative is requested and reengage the Risk Review process from the beginning.

5.7 Review Initiative

Penn Procurement will review the *Risk Review Disposition* for compliance with their standards. If approved, Procurement will coordinate with the Wharton Sponsor to begin the procurement process for the approved initiative. If Procurement cannot approve the initiative, they will notify the Wharton Sponsor.

5.8 Initiate Change Planning

Once approved by Penn Procurement, the Wharton Sponsor may begin the Change Planning process in accordance with the *Wharton Change Enablement Standard*. Change planning must incorporate any required mitigations resulting from the risk assessment into the proposed change. For additional information regarding changes, refer to the *Wharton Change Enablement Standard*.

Top

Appendix A

The table below illustrates the responsibilities aligned with the relevant roles throughout the *Risk Review Standard*. Each step from is identified and aligned to the appropriate role that is either (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the *Risk Review Standard*. The overall standard is managed by Wharton ISO.

Process	Sponsor	Business Operation	Wharton ISO
Initiative Ideation	RA		
Request Risk Review	R	I	
Review Risk Review	C		R

Acknowledge Risk Request		R	
Provide Required Inputs	R		C
Analyze Request Package			R
Gather Additional Inputs	C		R
Develop Assessment Report			R
Issue Risk Disposition	C		RA
Review Risk Disposition	R		
Submit Initiative Approval Request	RA		
Review Initiative		R	
Begin Procurement Process		RA	I
Incorporate Required Mitigations into Change Planning	R		I
Begin Change Enablement Process	R		C

RACI Matrix Key

(**R**)*esponsible:* Person whose contributions and efforts results in a tangible deliverable or completed task - "**The Do'er**"

(**A**)*ccountable*: Person whose approval is required before the task or activity is considered completed - "**The Delegator**"

(**C**)*onsulted*: Person or role whose subject matter expertise is typically required in order to complete the item - "**The SME**"

(**I**)*nformed*: Person or role that needs to be kept informed of the status of item completion - "**Those kept up to date**"