

Third Party Risk Management

Guide to Vendor Risk Assessments (Cyber)

January 23, 2023

Version 1

Contents

Contents **2**
1 About This Document **4**
History 4
2 Introduction **5**
2.1 Purpose 5
2.2 Audience 6
3 General Guidance and Recommendations **7**
3.1 Overview 7
3.2 Maintain Awareness of Vendor Relationships 7
3.3 Determine Inherent Risk and Tier Vendors 7
3.4 Review Vendor Documentation/Questionnaires 8
3.5 Assign Risk Exposure Rating (Score) 8
3.6 Address Risks and Monitor 8
4 Conducting Vendor Risk Assessments **9**
4.1 Scope 9
4.2 Overview of Process 9
4.3 Intake Process 9
4.4 Initial Questionnaire 10
4.5 Factors Used to Determine Inherent Risk, Tier, and Assessment Type 10
4.6 Assessment Types 10
4.7 Prioritization of Assessments and Stakeholder Communication 11
4.8 Documentation Request 12
4.9 Evaluation Process 12
4.10 Reporting and Stakeholder Engagement 13
5 Vendor Risk Assessment Capability Maturity Model **14**
5.1 Initial 14
5.2 Repeatable 14
5.3 Defined 15
5.4 Managed 15
5.5 Optimizing 15
APPENDIX A Definitions **17**
APPENDIX B Standards and Regulations **18**
APPENDIX C Security Rider Example **19**
APPENDIX D Additional Resources **20**

1 About This Document

Author UWSA Governance, Risk and Compliance Team

Change Authority UW System Office of Information Security

History

Version No.	Issue Date	Status	Reason for Change
1.0	01/23/2023	Published	Initial Publication

2 Introduction

The University of Wisconsin (UW) System purchases hardware, software, and services from third-party vendors, to meet ongoing business needs. The use of third-party vendors allows UW System to obtain specialized expertise, offer expanded products and services, and/or realize economies of scale not otherwise possible through purely internal information technology systems and operations. UW System is expected to continue to rely on third party Information Technology (IT) services as our reliance on technology to support academic programs grows.

UW System senior leadership is ultimately responsible for managing activities conducted through third-party relationships and identifying and controlling the risks arising from such relationships to the same extent as if the activity were handled internally within UW System. Reviews should be performed of vendors prior to engaging their services to gain a better understanding of the risks they may introduce to our organization.

This document provides general guidance and recommendations for performing information security reviews of third-party IT service providers, prior to purchase or renewal of software or IT services, to gain insight into vendor's security practices and the underlying exposure of information security risks presented by those vendors. This document also provides an overview of the assessment procedures used by UW System Administration (UWSA) that may serve as an outline and adopted by institutions to their liking. Finally, a capability maturity model is provided that illustrates 5 different levels of vendor risk assessment practices. This model can assist in conversations with institutional leadership to help identify where institutions are currently at, and where they would like to be.

Third Party Cybersecurity Risk Management isn't simply a security tactic, nor is it simply a compliance requirement. It's a key cornerstone of a solid modern security foundation.

2.1 Purpose

The main purpose of this document is to assist institutions in understanding the risks involved in partnering with a vendor for IT software or services. General guidance and recommendations highlight what high-level efforts should be made to manage the third-party information security risk landscape.

Further, processes are outlined that illustrate how UWSA performs vendor risk assessments in a flexible and resource-friendly way. Institutions are not required to follow the processes outlined in this document, however, may adopt some or all the processes outlined to supplement their own vendor risk assessment processes and programs. The processes in section four attempt to answer the following questions:

1. Does the vendor employ reasonable security practices and safeguards to protect UW System data and operations?
2. What precautionary measures should be taken if a partnership with a vendor for IT software or services is initiated?
3. What is the overall risk of partnering with this vendor?

No matter how many questionnaires a vendor fills out or how detailed of a review is conducted on their security practices, there is always a chance that the vendor could be compromised using a sophisticated attack that would not have been uncovered by the assessment. The main point of conducting pre-purchase assessments it to gain a reasonable assurance that the vendor takes security seriously and makes a reasonable effort to protect their systems and our data.

2.2 Audience

This document is intended for information technology/security personnel involved in reviewing the cybersecurity practices of third-party vendors. This document may also be used by other stakeholders and risk executives to gain an understanding of the processes used to assess vendor's information security practices at UW System Administration, and for institutional leadership to determine what level of assessment practices would be appropriate in their environment based on available resources.

3 General Guidance and Recommendations

3.1 Overview

The following is general guidance and recommendations for third party risk management as it relates to understanding your cyber risk landscape with your third parties. This does not cover other third-party risk management practices such as fiscal health of companies or the risk of vendors not being able to fulfill functional requirements.

3.2 Maintain Awareness of Vendor Relationships

Recommendation: Create an inventory or central repository of all your third-party vendors. Start with those that provide core/critical IT services and then move to other vendors that provide support services. Work with your procurement department(s) to stay abreast of any new purchases or renewals of software and/or IT services.

Considerations

1. It is important to account for all IT vendors used by all departments because even one can put the entire institution at risk. However, this does not mean every vendor needs to be reviewed.
2. Focus on vendors whose software or services are purchased through your own institution. Your procurement team may be in the best position to maintain these inventories. UWSA conducts vendor risk assessments for most enterprise technology purchases.

Applicable Resources: Institution's Procurement team

3.3 Determine Inherent Risk and Tier Vendors

Recommendation: Work with employees who administer or own vendor relationships to gain an understanding of the inherent risk the vendor poses to the organization. Understanding this inherent risk will further allow you to tier your vendors to help understand the level of attention and/or security review each vendor should receive.

Considerations:

1. Create a standard questionnaire that can be completed by employees or teams looking to purchase IT software or services. The questionnaire should capture vital information regarding the service being offered, the location and level of data being accessed, stored, or processed, and other factors that indicate what kind of security assessment may be needed.
2. Tier your vendors based on the level of inherent risk they introduce to your institution. Recommended tiers include Tier 1 (High Risk), Tier 2 (Moderate-Risk), and Tier 3 (Low-Risk). However, exact tiers used may depend on your environment.

Applicable Resources: Vendor Risk Assessment Processes: Tiering Vendors

3.4 Review Vendor Documentation/Questionnaires

Recommendation: Review vendor security documentation and questionnaires for vendors. Establish expectations when and to what extent vendors are reviewed during the procurement process and on a recurring basis thereafter.

Considerations

1. Every vendor presents a different level of inherent risk and review of a vendor's security practices should align with the level of risk presented. For example, a vendor that provides critical services and/or has access to large amounts of sensitive information poses a larger threat to the institution than a vendor that provides translation of course content. The level of review can be directly linked to the tier the vendor falls within as described in section 2.3.
2. Use a standard template to document the review. This will ensure consistency across reviews and allow for easy comparison and review at later dates.
3. If specific risks related to security controls are identified at this point, these risks should be noted and added to the institution's risk register if the institution enters into contract with the vendor.

Applicable Resources: Vendor Risk Assessment Processes

3.5 Assign Risk Exposure Rating (Score)

Recommendation: Assign a risk exposure rating to vendors based on their level of threat to the organization. The risk exposure rating should take into consideration the inherent risk identified in step 2, adjusted for mitigations (residual risk) identified during review of a vendor's security documentation and practices.

Considerations

1. Determination of risk exposure ratings for vendors is often subjective and may vary from analyst to analyst based on their knowledge of security standards and practices.
2. Start with determining the risk exposure rating for availability as well as confidentiality and integrity. The combined risk exposure ratings make up the overall risk exposure rating for the vendor.
3. Risk exposure ratings should align with the risk matrix identified in SYS 1039.

Applicable Resources: Vendor Risk Assessment Processes

3.6 Address Risks and Monitor

Recommendation: Specific risks identified with vendors should be addressed in order of priority and consistent with the institution's risk appetite. Continuous monitoring at regular intervals should be considered for the institution's highest risk vendors to keep risks in check, safeguard student and staff information, meet regulatory requirements, and maintain overall health of the institution.

Considerations

- Some risks can be mitigated by requiring controls and requirements in your contracts with vendors, so they understand expectations and act accordingly.

4 Conducting Vendor Risk Assessments

The following represents the processes developed by UWSA in their pursuit to evaluate information security risk of third parties IT vendors. Institutions may adopt these processes, in part or in whole, to supplement their own information security reviews of vendors.

4.1 Scope

The scope of these vendor risk assessments is limited to a review of the vendor's security practices to provide an opinion on the risk exposure of partnering with the particular vendor. The assessments also provide limited review of the proposed solution's security settings and whether security settings for the solution meet the expectations and level of quality that UW expects.

UWSA's review does not evaluate how the solution is potentially implemented by the UW and whether or not the architecture, deployment and day to day operations of the solution are secured appropriately. The information security of UW System's specific architecture, deployment and operations of a given solution are encouraged to be reviewed by a separate Implementation Risk Assessment, if warranted.

Pre-purchase assessments are not intended to be an approval to purchase, nor are they comprehensive audits. UWSA does not currently conduct privacy reviews as part of these security reviews.

4.2 Overview of Process

The following represents a high-level overview of the intake and assessment processes used by UWSA for conducting vendor information security risk assessments. We note that UWSA's intake process is currently transitioning to using Ivanti and OneTrust, and the forthcoming workflow has been captured here.

Intake: Ticket created in Ivanti → Ticket assigned to GRC Team → GRC Team emails initial questionnaire to requestor (link to OneTrust) → Questionnaire reviewed by GRC team and assessment prioritized → Estimated completion date, recommended template/assessment type communicated to requestor

Assessment and Reporting Process: Initial documentation request submitted to vendor → Continuous effort to obtain documentation prior to scheduled review of vendor → Review security documentation → Develop Report → Communicate results to stakeholders

4.3 Intake Process

The following represents an intake process that may be used by stakeholders to initiate a vendor information security review. The requestor may be a representative from the procurement department or the individual looking to purchase the vendor's solution. The process for requesting

a vendor information security review should be advertised to both the procurement team and on the institution's intranet.

1. Requestor submits ticket in Ivanti requesting an assessment
2. Ticket assigned to GRC Team
3. GRC Analyst responds with link to OneTrust to begin initial questionnaire (next section)

4.4 Initial Questionnaire

The following represent questions that are included in the initial questionnaire, which is filled out by the requestor or designee:

- Scope of purchase (department, institution, systemwide, etc.)
- Description of the vendor's solution(s) that will be used
- Will the solution incorporate SSO if available?
- Number of core users for the proposed solution
- Number of end-users or data subjects
- Length the system could be down or experience an interruption
- Type of data and amount of data
- Criticality of the system to ongoing operations
- Estimated amount of annual cost, if known (initial and ongoing)
- Point of contact at the vendor's organization for requesting security documentation and answering any follow-up questions

4.5 Factors Used to Determine Inherent Risk, Tier, and Assessment Type

The questions answered in the initial questionnaire are used to gain an understanding of the inherent risk that the vendor brings to the organization. Once inherent risk is identified, the vendor can be tiered and the level of information security review of the vendor should align accordingly. For example, a vendor in a high-risk tier should receive more scrutiny than a vendor in a low-risk tier, who may only receive a cursory review.

Vendors are recommended to be tiered into the following categories:

- Low-Risk
- Moderate-Risk
- High-Risk

4.6 Assessment Types

Every vendor presents a different level of inherent risk and review of a vendor's security practices should align with the level of risk presented. Each level of assessment has its own reporting template. The following assessments follow a general recommendation based on the inherent risk and tier of the proposed solution (see section 4.5):

Express Assessment
These assessments are typically used for inherently low-risk applications or services. These cursory assessments may also be used in cases where other assessments are recommended, but either the requested turnaround time is unreasonable or documentation from the vendor is limited or not available. Documentation recommended to be reviewed includes:

- BitSight Profile Review
- Review of publicly available information, including searches for previous security breaches

Standard Assessment
This assessment is the default assessment used for inherently moderate-risk applications or services. Documentation recommended to be reviewed includes:

- BitSight Profile review
- Review of publicly available information, including searches for previous security breaches
- Review of SOC 2 Type 2 or HECVAT 3.0+. Other security questionnaires may be substituted in place of these documents at the discretion of the analyst. For example: SOC 2 Type 1, HECVAT Lite, SIG, SIG-Lite, VSA, or CAIQ questionnaires.

Full Assessment
These assessments should be used for our more critical data sharing agreements, services, or software essential to ongoing business operations, or systems that will host large amounts of high-risk data. Documentation recommended to be reviewed includes:

- BitSight Profile review
- Review of publicly available information, including searches for previous security breaches
- SOC 2 Type 2 Report and/or HECVAT 3.0+. Other security questionnaires may be substituted in place of these documents at the discretion of the analyst. For example: SOC 2 Type 1, HECVAT Lite, SIG, SIG-Lite, VSA, or CAIQ questionnaires.
- The vendor's internal information security policies

4.7 Prioritization of Assessments and Stakeholder Communication

Determine the priority for completing the assessment as it relates to other active requests and ongoing initiatives. Assessments will typically be performed on a first in-first out basis in conjunction with inherent risk and requested completion date, subject to available resources and availability of documentation from the vendor. For example, assessments with a higher inherent risk may take priority when competing for resources and timelines with a lower-risk assessment request, even if the lower-risk assessment was requested first.

While the standard turnaround time for completing vendor risk assessments varies on the factors noted above, UWSA aims to have all vendor risk assessments completed within two weeks *of receiving the necessary documentation from the vendor*.

At this point, communicate with the stakeholder the inherent risk and tier of the vendor, the expected assessment type to be performed, and a rough timeline to complete the assessment. Make sure the requestor is aware timelines are largely dependent on the vendor and their ability to provide security documentation with a reasonable timeframe.

4.8 Documentation Request

Requests for security documentation should be made to the vendor point of contact identified in the initial questionnaire. Documents should be requested immediately regardless of the timeframe for completing the assessment as the vendor needs time to gather relevant information.

Non-Disclosure Agreement

At times, the analyst may be asked to sign a Non-Disclosure Agreement (NDA) with the vendor on behalf of UW System or the institution prior to the vendor sharing sensitive security documents with the analyst. The analyst should review the NDA and if reasonable, sign and return the NDA to the vendor. Note that documents shared under the purview of an NDA shall not be distributed further unless specifically authorized by the vendor's NDA.

4.9 Evaluation Process

The assessment process used will vary from assessment to assessment based on available documentation. In general, the analyst should review the available documents, the vendor's stated security practices, and document strengths and concerns within said practices. Recommended areas to be reviewed include:

- Where the vendor will store UW's data. This should be limited to within the borders of the United States when possible.
- Whether the vendor has a Disaster Recovery Plan and Business Continuity Plans
- Whether the vendor employs data encryption standards for data at rest and in transit
- The size of the vendor's security team
- Whether the vendor has patch and vulnerability management practices
- Whether the vendor has policies and procedures for information security
- The vendor's security awareness practices. For example, do they train their employees at hire and on an annual basis? Do they conduct phishing exercises?
- Solution specific:
    - Does the proposed solution have adequate security controls available for UW?
        - SSO capabilities
        - RBAC
        - MFA
        - Complexity for passwords for local/admin accounts (Non-SSO)
        - Audit logs
        - Logoff capabilities
        - Other access controls, such as account lockouts or timeouts (not applicable if SSO is used)

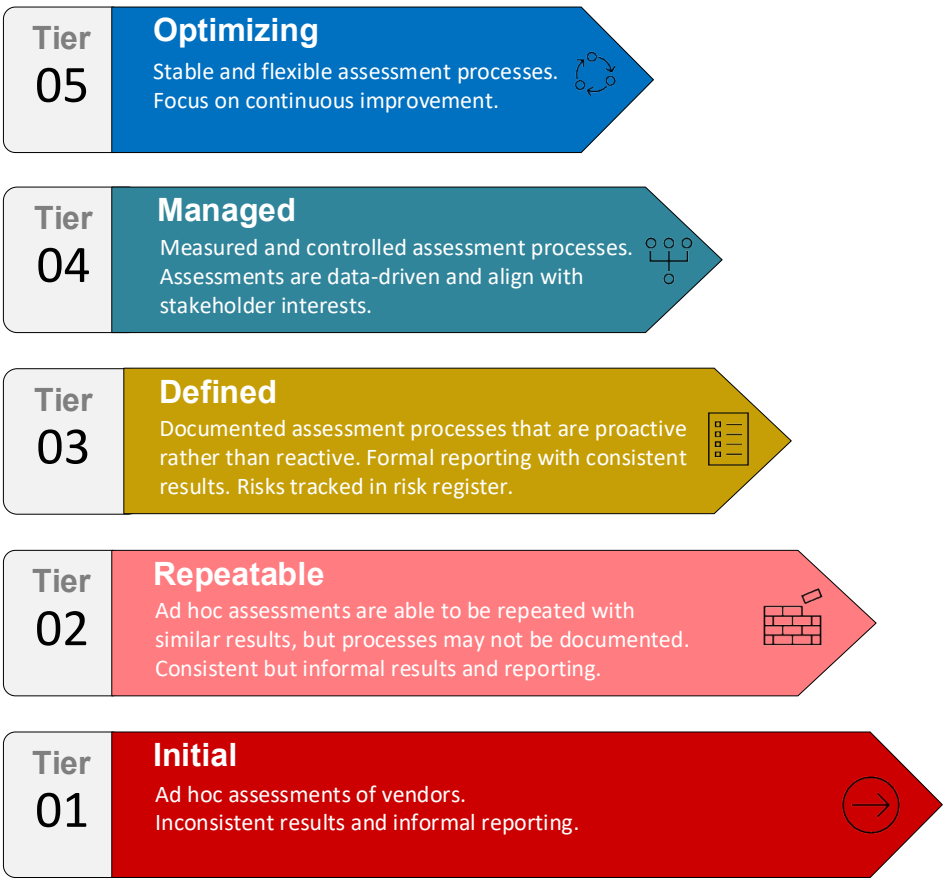
It is recommended to give the vendor a risk exposure score, taking into consideration availability, confidentiality and integrity risk based on the observations made in these areas during the review.

4.10 Reporting and Stakeholder Engagement

Once a review is performed of a vendor and the proposed solution, it is recommended to document the review in a report that includes an overview of documentation reviewed, notable strengths, observed concerns, and recommendations for the stakeholder if the solution is procured. The report should be discussed with relevant stakeholders after they've had a chance to review to ensure they understand the risk involved in partnering with the particular vendor. If warranted, an implementation risk assessment can be performed by reviewing the implementation and configuration of the solution. Specific risks identified with solutions should be further added to the institution's risk register.

5 Vendor Risk Assessment Capability Maturity Model

The following represents a 5-tier capability maturity model for third party cyber risk management and can be used to assist institutions in identifying their current state and desired future state.



5.1 Initial

Institutions in this tier may exhibit the following practices related to vendor risk assessments:

- Ad hoc reviews of vendors. Not injected into the procurement pipeline but may be informed of certain procurement efforts
- No continuous reviews or monitoring of vendors outside of the procurement process
- No formal process followed or formal report used. Reviews are inconsistent and results vary
- Identified risks are communicated to stakeholders
- No metrics on the vendor risk assessment process are gathered

5.2 Repeatable

Institutions in this tier may exhibit the following practices related to vendor risk assessments:

- Security is informed of the most critical data sharing agreements and central purchases but may not have insight into IT purchases made by decentralized units
- No continuous reviews or monitoring of vendors outside of the procurement process
- The vendor risk assessment process can be repeated with similar, if not the same, outcomes, however this process may not be documented
- Results are reported in a consistent but informal manner to stakeholders
- No metrics on the vendor risk assessment process are gathered

5.3 Defined

Institutions in this tier may exhibit the following practices related to vendor risk assessments:

- Vendor cybersecurity review is a defined step in the procurement process to evaluate new vendors or renewal of contracts
- Ad hoc reviews or monitoring of vendors outside of the procurement process
- The vendor risk assessment process follows a defined and documented process that results in similar and expected results. Extent of assessments align closely with the inherent risk of the vendor being reviewed
- Results are reported in a formal manner, such as using a defined report, that provides consistent and expected results. Identified risks are documented within the institution's risk register
- No metrics on the vendor risk assessment process are gathered

5.4 Managed

Institutions in this tier may exhibit the following practices related to vendor risk assessments:

- Vendor cybersecurity review is a defined step in the procurement process to evaluate new vendors or renewal of contracts
- Continuous monitoring of select high-risk vendors
- The vendor risk assessment process follows a defined and documented process that results in similar and expected results. Extent of assessments align closely with the inherent risk of the vendor being reviewed. A tiered catalog of vendors is maintained and some automation may be used in the assessment process
- Results are reported in a formal, auditable, and structured manner. Risks are documented within the institution's risk register
- Metrics used to monitor the risk assessment process and understand the institution's third-party risk universe

5.5 Optimizing

Institutions in this tier may exhibit the following practices related to vendor risk assessments:

- Vendor cybersecurity review is a defined step in the procurement process to evaluate new vendors or renewal of contracts. This awareness is automated and not reliant on human communication
- Continuous monitoring of all high-risk vendors based on a defined frequency
- The vendor risk assessment process follows a defined and documented process that results in similar and expected results. Extent of assessments align closely with the inherent risk of the vendor being reviewed. A tiered catalog of vendors is maintained and automation is used in the assessment process

- Results are reported in a formal, auditable, and structured manner. Risks are documented within the institution’s risk register and stakeholders are engaged on occasion to follow up on progress made towards identified risks
- Metrics used to monitor the risk assessment process, understand the institution’s third-party risk universe, and improve the risk assessment process

APPENDIX A Definitions

To be added in subsequent version

APPENDIX B Standards and Regulations

Standards

NIST Cybersecurity Framework

- Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
- ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

GLBA Safeguards Rule

Develop a written risk assessment regarding the security of student information. The written assessment will have to cover the following elements:

- The criteria used to evaluate and classify the relevant security risks that the institution has identified
- The criteria used to assess the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face
- The ways in which identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks
- Periodically update risk assessments

2022-007 LAB Audit Recommendation

- Develop a policy to require periodic review of the adequacy of certain cloud-based third-party vendors' internal controls, such as by assigning the responsibility to obtain a service organization audit report and ensuring such reports are reviewed; and
- Annually obtaining and reviewing relevant service organization audit reports.

APPENDIX C Security Rider Example

To be added in subsequent version

APPENDIX D Additional Resources

- Vendor Risk Assessment Report Templates and Reference Sheet
- OneTrust IT Risk Management Software – Available for all institutions to use
- SYS 1039 *Information Security: Risk Management*
- NIST 800-53r5 Security and Privacy Controls for Information Systems and Organizations
- NIST 800-161r1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations