Risk Management Guide

Table of Contents

[Welcome to Risk Management 2](#_Toc203402864)

[The Foundation: What is Risk Management? 2](#_Toc203402865)

[The Framework at a Glance 2](#_Toc203402866)

[System Risk vs. Vendor Risk 3](#_Toc203402867)

[Conducting a Risk Assessment 4](#_Toc203402868)

[Step 1: Scoping Your Assessment (Prepare) 4](#_Toc203402869)

[Step 2: Conducting the Assessment 4](#_Toc203402870)

[Step 3: Rate the Risk 6](#_Toc203402871)

[Step 4: Treat the Risk (Communicate & Act) 8](#_Toc203402872)

[Step 5: Maintain a Risk Register 9](#_Toc203402873)

[Extra Tips: What to Look for in a System or Vendor 9](#_Toc203402874)

[Helpful Resources 9](#_Toc203402875)

[Final Note 10](#_Toc203402876)

[APPENDIX A: Example of Cyber Threats and Risk Management 11](#_Toc203402877)

[APPENDIX B: Risk Assessment Scoping (Prepare for Assessment) 12](#_Toc203402878)

[APPENDIX C: Example of a High-Level Risk Assessment 14](#_Toc203402879)

# Welcome to Risk Management

Risk Management doesn’t have to be overwhelming. This guide is designed to help you take the first steps in building a cybersecurity risk assessment program—starting with what you already know, using tools you likely already have. Whether you're managing a school system, city IT environment, or small county network, the principles are the same:  
**Know your risks. Reduce your exposure. Plan for resilience.**

# The Foundation: What is Risk Management?

Risk management is the process of identifying, assessing, and responding to potential threats that could disrupt your organization’s operations, systems, or data.  
It helps you:

* Protect student or citizen data
* Improve decision-making
* Meet regulatory requirements
* Plan proactively, not reactively

# The Framework at a Glance

Diagram, venn diagram

AI-generated content may be incorrect.The framework combines risk assessment, threat-based analysis, and planning. You don’t have to implement it all at once—start where you are and build over time.

# System Risk vs. Vendor Risk

Before diving into the process, it helps to understand the difference between the two primary types of risk you’ll assess. Most organizations deal with both. Use this table to determine where to focus your assessment.

|  |  |  |
| --- | --- | --- |
| Aspect | System Risk | Vendor Risk |
| Definition | Risk associated with internal systems, applications, data, and infrastructure. | Risk associated with third-party vendors and their impact on your organization. |
| Scope | Systems, applications, data, facilities, integrations, or processes within the organization. | Third-party vendors providing services or products to the organization. |
| Stakeholders | Security team, IT/System owners, Business unit leads, Risk/compliance officers. | Security team, IT/System owners, Business unit leads, Risk/compliance officers, Third-party vendors. |
| Assessment Timing | At system implementation or major change, annual compliance, or post-incident. | During vendor onboarding, annual review, post-incident. |
| Assessment Focus | Identify critical assets, threats, vulnerabilities, and controls. | Evaluate vendor's security practices, compliance, and data protection measures. |
| Data Location | On-premises data centers, cloud environments (cloud service provider), and remote work environments. | Vendor's data storage and processing locations, jurisdictional laws. |
| Compliance & Certifications | FISMA, HIPAA, ISO 27001, etc. | GDPR, CCPA, HIPAA, SOC 2, ISO 27001, FedRAMP, etc. |
| Incident Response | Internal incident response plan, Breach notification procedures. | Vendor's incident response plan, Breach notification commitments. |
| Data Access & Control | Internal access controls, Data logs, Audit trails, etc. | Vendor's access controls, customer's ability to export/delete data, etc. |
| Contractual Protections | Internal policies, procedures, standards, and regulatory requirements. | Data Processing Agreement (DPA), Service Level Agreement (SLA), Right to audit, and regulatory requirements. |
| Organizational Indicators | Dedicated security/privacy team, Regular security training, etc. | Vendor's security/privacy team, security awareness training, public security contact, etc. |

# Conducting a Risk Assessment

## Step 1: Scoping Your Assessment (Prepare)

Use the “Who, What, Where, When, Why” method to define your scope:

* **Who**: Security, IT/system owners, business leads, vendors (if applicable)
* **What**: Which systems, data, or services are in scope?
* **Where**: Where is data stored or processed (on-prem, cloud, vendor-hosted)?
* **When**: Is this triggered by a change, requirement, or review cycle?
* **Why**: What’s the purpose—compliance, incident response, general risk posture, supporting business continuity and data protection goals?

## Step 2: Conducting the Assessment

You can assess systems in different ways depending on how deep you want to go. Start with basic information-gathering and review key areas such as:

| Topic | Details to Identify | Web Resource To Locate Items |
| --- | --- | --- |
| Privacy | * What data is collected (PII, cookies, usage data, etc.) * How it’s used (e.g., advertising, analytics, personalization, third-party sharing) * With whom it’s shared (partners, advertisers, vendors) * User rights (access, deletion, correction, opt-out) * Data retention period * Legal basis for processing | * Privacy Policy * Terms of Use * Legal Page * Frequently Asked Questions (FAQs) * Cookie Policy * Community Standards * Resources |
| Security Practices | * Encryption (in transit and at rest) * Access control and authentication mechanisms * Data segregation (especially in multi-tenant cloud environments) * Secure development practices (e.g., regular code reviews, pen testing) * Security certifications (e.g., SOC 2, ISO 27001, FedRAMP, GovRAMP) * Customer access to data logs or audit trails * Ability to export or delete your data * Administrative tools to manage user permissions, data sharing, retention   Check if the vendor has:   * A documented incident response plan * Commitments to notify customers of a breach within a defined time frame * Historical transparency (look up past breaches or incidents) | * Security Page * Trust Center * Security Whitepapers * Documentation * Knowledge Base Articles * Data and Privacy * Safety * Transparency * Version History * End User Level Agreement (EULA) * Resources |
| Compliance and Certifications | Look for alignment with laws or frameworks such as:   * GDPR, CCPA, HIPAA, FERPA, GLBA * SOC 2, ISO/IEC 27001, PCI DSS, FedRAMP, GovRAMP   If compliance is claimed, request supporting documentation:   * Audit reports * Data Processing Agreements (DPAs) * Vendor risk assessment documentation * SOC II Type 2 Report | Ask for:   * A Data Processing Agreement (DPA) * A Service Level Agreement (SLA) with security/privacy terms * Right to audit or request third-party audit reports |
| Third-Party Sharing and Sub processors | * Who is your data shared with? * Where are those third parties located? * Does the vendor publish a list of subprocessors? * How are third parties evaluated? * Can you audit or review third-party practices? | * Privacy Policy * Terms of Service * Trust Center * Subprocessor List |
| Data Location and Residency | Understand where your data is:   * Stored and processed (especially important for cross-border compliance) * Subject to which jurisdiction’s laws * Whether customers can choose or restrict the data residency region (e.g., US-only, EU-only) | * Terms of Service * Privacy Policy |
| AI and Emerging Technology Use | * Is AI used in the service? * What models are used? * Is customer data used for training? * Are decisions automated? | * Privacy Policy * AI Use Disclosures * Terms of Service * Security/Trust Center |
| Incident History and Transparency | * Has the vendor disclosed past breaches? * Do they report incidents publicly or notify customers? * Is there a responsible disclosure process? | * Trust Center * Security Page * News Articles * Vendor Status Page |

## Step 3: Rate the Risk

To determine risk likelihood and impact ratings, you’re essentially assessing how probable a risk is and how severe its consequences might be. It’s like asking, “How likely is this to go wrong—and how bad would it be if it did?” Here's how to break it down:

Risk = **Likelihood x Impact**

|  |  |
| --- | --- |
| **Likelihood Rating** | **Definition** |
| 1 – Rare | May happen only in exceptional cases |
| 2 – Unlikely | Could happen, but probably won’t |
| 3 – Possible | Might happen occasionally |
| 4 – Likely | Will happen in many cases |
| 5 – Almost Certain | Expected to happen frequently |

|  |  |
| --- | --- |
| **Impact Rating** | **Definition** |
| 1 – Insignificant | No real impact; easily managed |
| 2 – Minor | Some disruption; minor cost or delay |
| 3 – Moderate | Noticeable impact needing response |
| 4 – Major | Serious consequences for goals or operations |
| 5 – Critical | Devastating impact; major failure |

Multiply them to get a risk score and use a matrix to categorize:

* 1–5 = Low
* 6–10 = Medium
* 11–15 = High
* 16–25 = Critical

These thresholds are flexible—adjust them to fit your organization or project’s context.

A picture containing website

AI-generated content may be incorrect.

#### Alternative Approach: Threat-Based Risk Assessment

A traditional risk assessment starts with the asset. A threat-based approach starts with the danger. Use this to zero in on high-risk cyber threats.

A **cyber threat–based risk assessment** is a process that:

* **Identifies cybersecurity threats** (like malware, phishing, ransomware, insider threats)
* **Analyzes vulnerabilities** in your systems (e.g., outdated software, weak passwords)
* **Calculates risk levels** by combining the *likelihood* of those threats with the *impact* they’d have
* **Prioritizes actions** to reduce risk through controls or mitigation strategies

It narrows your focus to digital threats that could compromise systems, data, or users.

**Key Components:**

|  |  |
| --- | --- |
| Element | Description |
| Assets | What you’re protecting (data, devices, infrastructure) |
| Threats | Potential sources of harm (cybercriminals, nation-states, human error, etc.) |
| Vulnerabilities | Weaknesses that can be exploited (lack of encryption, open ports, weak passwords, etc.) |
| Likelihood | How probable is it that a threat will exploit a vulnerability? What’s the likelihood rating? |
| Impact | What would happen if the threat succeeds? What’s the impact rating? (financial, loss, downtime, etc.) |
| Controls | Safeguards to reduce risk (firewalls, training, backups, MFA, etc.) |

**Why It Matters?**

* Helps organizations **stay ahead of attackers** by knowing what threats are most relevant
* Guides investment in the **most effective security measures**
* Supports compliance with frameworks like **NIST**, **ISO 27001**, or **HIPAA**
* Builds confidence for customers, executives, and regulators

## Step 4: Treat the Risk (Communicate & Act)

Once you’ve identified and rated your risks, take action. A solid risk treatment plan helps organizations systematically address risks to minimize potential harm. Here’s a structured approach to include:

**Risk Treatment Plan:**

1. Identify Risks: Pinpoint potential threats that could impact operations, finances, or security.
2. Assess Likelihood and Impact: Evaluate the likelihood and impact of each risk to prioritize accordingly.
3. Choose a Treatment Strategy (Mitigate, Transfer, Accept, Avoid)
4. Create an Action Plan: Outline detailed steps to manage each risk, assigning responsibilities and deadlines.
5. Implement Controls: Put measures in place such as policies, technologies, or training to minimize risk exposure.
6. Monitor and Review: Continuously track risk management effectiveness and adjust plans as needed.
7. Communicate Results: Ensure stakeholders stay informed and aligned with risk strategies.

## Step 5: Maintain a Risk Register

A cyber risk register is a centralized document or tool used to identify, assess, and manage cybersecurity risks within an organization. It works much like a traditional risk register but focuses specifically on threats to digital assets, data, systems, and networks.

Here’s what a cyber risk register typically includes:

* Risk Description: A clear explanation of the cyber threat (e.g., phishing attacks, ransomware, insider threats, etc.).
* Likelihood: An estimate of how probable the risk is.
* Potential Impact: What could happen if the risk materializes? (e.g., data loss, financial loss, reputational harm, etc.)
* Risk Rating: Often a combination of likelihood and impact, sometimes visualized with a heat map.
* Mitigation Measures: Controls or actions in place to reduce the risk. (e.g., MFA, firewalls, training, etc.)
* Risk Owner: The person or team responsible for monitoring and managing the risk.
* Status: Current status of the risk (e.g., open, in progress, mitigated, etc.)

🛠️ **Free Tool**: [Infotech Risk Register Template](https://www.infotech.com/research/risk-register-tool#unlock-modal)

## Extra Tips: What to Look for in a System or Vendor

Use this checklist during assessments or procurement reviews:

✅ Privacy policy and data usage terms  
✅ Security documentation (whitepapers, SOC 2 reports, MFA support)  
✅ Data location and sovereignty  
✅ Patch schedules and CVE checks  
✅ Use of AI or emerging tech (check NDIT’s AI Policy)  
✅ Certifications (FedRAMP, HITRUST, etc.)

## Helpful Resources

* **NIST SP 800-30**: [Risk Assessment Guide](https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final)
* **NIST SP 800-53**: Security and Privacy Controls
* **ISACA Journal**: [Risk Assessment and Analysis Methods, Vol. 2 (2021)]
* **NDIT Policy Site**: [www.ndit.nd.gov/governance/policies](https://www.ndit.nd.gov/governance/policies)

# Final Note

This guide isn’t meant to turn you into a risk analyst overnight. It’s here to help you start strong and build confidence. The key to success is consistency—review regularly, involve the right people, and don’t wait until something breaks.

Need help? Reach out to your state or regional IT partners. You don’t have to go it alone.

# APPENDIX A: Example of Cyber Threats and Risk Management

This appendix outlines common cyber threats your organization may face, along with their potential impacts, existing controls, and areas for improvement. Use this table to spark discussion during tabletop exercises or help prioritize where to focus your security efforts.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Threat Type | Description | Potential Impact | Existing Controls | Gaps/Areas for Improvement |
| Phishing | Deceptive emails to trick users | Credential theft, malware spread | Email filtering | Lacking comprehensive user training and reporting procedures |
| Ransomware | Malware that encrypts files for ransom | Data loss, operational downtime | Backup systems | Incident response plan untested |
| Insider Threats | Threats from current or former employees | Data leakage, sabotage | Access controls | No user activity monitoring in place |
| DDoS Attacks | Overwhelming traffic to disrupt services | Service outage, reputational harm | Firewall, rate limiting | No third-party mitigation solution |
| Zero-Day Exploits | Attack on previously unknown vulnerabilities | System compromise, data breach | Patch management | Slow detection and response capabilities |
| Emerging Technology Risks | Risk introduced by AI, IoT, or untested tools | Unknown outcomes, compliance issues | Pilot programs, policy review | No formal evaluation criteria yet |

# APPENDIX B: Risk Assessment Scoping (Prepare for Assessment)

This appendix offers a deeper dive into the “Who, What, Where, When, Why” framework introduced in Step 1. It provides practical examples and web resources to help you gather relevant details about your systems or vendors before you begin your risk assessment.

| Topic | Details to Identify | Web Resource  to Locate Items |
| --- | --- | --- |
| Privacy | * What data is collected (PII, cookies, usage data, etc.) * How it’s used (e.g., marketing, analytics, third-party sharing) * With whom it’s shared (partners, advertisers, vendors) * User rights (access, deletion, correction, opt-out) * Data retention period * Legal basis for processing | * Privacy Policy * Terms of Use * Legal Page * Frequently Asked Questions (FAQs) * Cookie Policy * Community Standards * Resources |
| Security Practices | * Encryption (in transit and at rest) * Access control and authentication mechanisms * Data segregation (especially in multi-tenant cloud environments) * Secure development practices (e.g., regular code reviews, pen testing) * Security certifications (e.g., SOC 2, ISO 27001, FedRAMP, GovRAMP) * Customer access to data logs or audit trails * Ability to export or delete your data * Administrative tools to manage user permissions, data sharing, retention   Check if the vendor has:   * A documented incident response plan * Commitments to notify customers of a breach within a defined time frame * Historical transparency (look up past breaches or incidents) | * Security Page * Trust Center * Security Whitepapers * Documentation * Knowledge Base Articles * Data and Privacy * Safety * Transparency * Version History * End User Level Agreement (EULA) * Resources |
| Compliance and Certifications | Look for alignment with laws or frameworks such as:   * GDPR, CCPA, HIPAA, FERPA, GLBA * SOC 2, ISO/IEC 27001, PCI DSS, FedRAMP, GovRAMP   If compliance is claimed, request supporting documentation (e.g., audit reports, SOC 2 Type 2, DPAs) | Ask for:   * A Data Processing Agreement (DPA) * A Service Level Agreement (SLA) with security/privacy terms * Right to audit or request third-party audit reports |
| Third-Party Sharing and Sub processors | * Who is your data shared with? * Where are those third parties located? * Does the vendor publish a list of subprocessors? * How are third parties evaluated? * Can you audit or review third-party practices? | * Privacy Policy * Terms of Service |
| Data Location and Residency | Understand where your data is:   * Stored and processed (especially important for cross-border compliance) * Subject to which jurisdiction’s laws * Whether you have a choice of data region (e.g., EU, US) | * Terms of Service * Privacy Policy |

# APPENDIX C: Example of a High-Level Risk Assessment

This appendix walks you through a simplified example of a real-world risk assessment. It includes a template to document findings, identify gaps, and begin forming an action plan. Use it as a starting point or hands-on training tool to build comfort with the process.

| Category | Applicable Details/Likelihood and Impact | Actionable Gaps | Notes for Implementation |
| --- | --- | --- | --- |
| Privacy Policy/Terms of Use/Acceptable Use Policy on website |  |  | **Privacy Policy/Terms of Use/Acceptable Use Policy:** Check privacy policy for types of data collected, how it’s shared, locations of concern specifically out of country threats. (if none found, this is actionable gap) |
| Any security solution documentation provided? |  |  | **Security Solution Documentation:** Example could be whitepapers on the solution, any documentation or notes the vendor provides. Check for a SOC2 type 2 security report if available. (if none found, this is actionable gap) |
| What is the type of data protection in place? |  |  | Look at Single Sign on and Multifactor Authentication Options. Encryption being used and data hosting locations |
| Review for any Common Vulnerabilities and Exposures (CVE) exposures |  |  | Check for any active CVE threats. ([NIST](https://nvd.nist.gov/vuln/search)/[MITRE](https://cve.mitre.org/cve/search_cve_list.html) CVE Databases). |
| Review patching schedule |  |  | Check to see how often the system is getting regular and security patches. |
| Check to see if the system has any malicious exes using virus check websites. |  |  | Use [VirusTotal - Home](https://www.virustotal.com/gui/home/upload) and [Trend Micro Site Safety Center](https://global.sitesafety.trendmicro.com/) to verify URL and exe is not malicious. |
| Check News Security/ Risk Releases |  |  | Determine if the application or vendor is in the news or has any known breaches. |
| Check for AI Reference |  |  | What AI is used? What AI models are used? Does the AI system generate content or decisions that affect operations or privacy? Has the vendor disclosed their model training data and safeguards? Is the AI model trained using customer data?  Reference NDIT Policies  *Artificial Intelligence Policy*  (www.ndit.nd.gov/governance/policies) |
| Check to see if the solution is FedRAMP/GovRAMP Certified? |  |  | Check FedRAMP Marketplace ([www.fedramp.gov](http://www.fedramp.gov))  Check GovRAMP authorized product list and progressing product list (govramp.org) |
| Type of Data Involved |  |  | What data is processed and needs security protections? |
| [Data Classification](https://www.ndit.nd.gov/governance/data-classification-policy) |  |  | Reference NDIT Policies  *Data Classification Policy*  (www.ndit.nd.gov/governance/policies) |
| Company’s URL |  |  |  |
| Other External Threats |  |  | What are some other external threats? |
| Risk Rating See Matrix: |  |  | What should the qualitative risk rating be? Low, Moderate, High, Critical based on Likelihood and Impact findings? |