AUJAS
CYBERSECURITY
A NuSummit Company

aujas.com

GUIDE

Guide on Vendor Risk Tiering for Continuous Monitoring

Introduction

Effective Third-Party Risk Management (TPRM) requires understanding of the relative risks associated with each vendor. By categorizing or “tiering” vendors based on their risk levels, organizations can allocate resources effectively and implement appropriate monitoring strategies. This guide provides a step-by-step approach to creating a vendor risk tiering system that supports continuous monitoring, helping you focus on high-risk vendors while maintaining oversight of lower-risk partners.

Step 1: Define Vendor Risk Tiers

Before categorizing vendors, it’s essential to establish clear criteria for each tier. Here’s an example of a three-tier system:

Tier 1: High-Risk Vendors

Vendors with direct access to sensitive data, financial records, or critical systems. Breaches involving Tier 1 vendors could severely impact operations, reputation, or compliance standing. These vendors require the most comprehensive monitoring.

Tier 2: Moderate-Risk Vendors

Vendors who have indirect access to important data or systems but whose role or access level limits potential impacts. Tier 2 vendors need regular monitoring but at a lower frequency than Tier 1.

Tier 3: Low-Risk Vendors

Vendors with limited or no access to sensitive information or core systems. These vendors present minimal risk and require only periodic assessments and basic monitoring.

Step 2: Develop Risk Assessment Criteria

Assess each vendor against key risk factors to determine their appropriate tier. Consider criteria such as:

Data Sensitivity

Level of access the vendor has with your organization's data (e.g., customer records, financial data).

System Access

Type and extent of access to critical systems.

Regulatory Impact

Compliance requirements that apply to the vendor's services (e.g., GDPR, HIPAA).

Vendor Size and Complexity

Larger or more complex vendors may present increased operational risk.

Geographical Location

Vendors in certain regions may be subject to different regulations and risks.

Using a scoring system for each criterion can simplify the categorization process. For example, assign a score (e.g., 1-5) for each factor, then sum the scores to determine the vendor's overall risk level and corresponding tier.

Step 3: Implement Tier-Specific Monitoring Strategies

Once the vendors are tiered, design a continuous monitoring strategy for each tier that reflects their risk level:

Tier 1 (High-Risk Vendors)

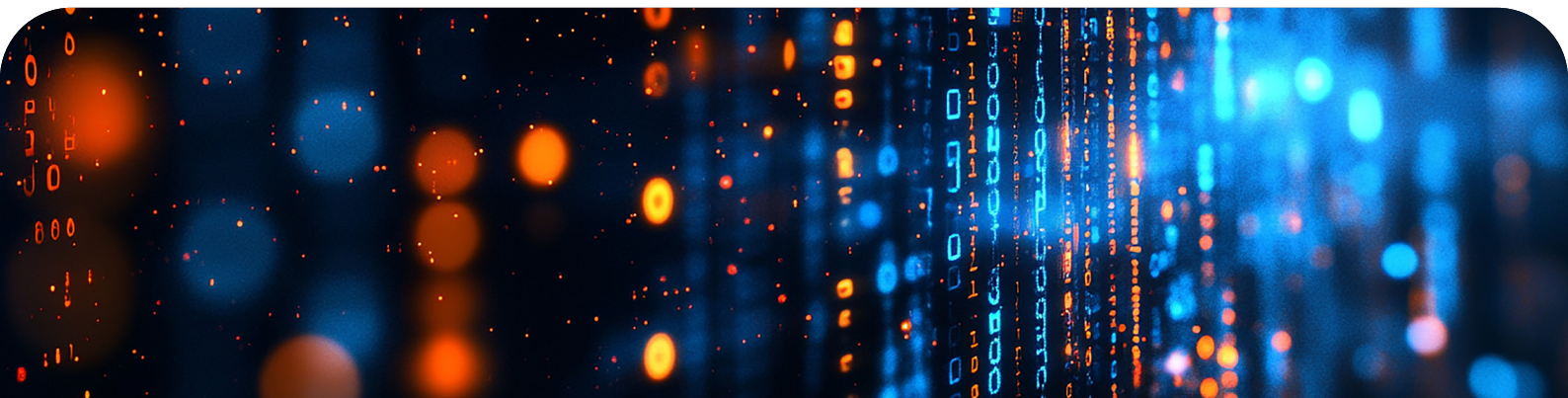
Frequency	Activities	Review Meetings
Continuous or real-time monitoring.	Ongoing vulnerability scanning, security posture assessments, and incident reporting.	Monthly or quarterly check-ins with the vendor's risk management team.

Tier 2 (Moderate-Risk Vendors)

Frequency	Activities	Review Meetings
Quarterly or Bi-annual monitoring.	Regular risk assessments, periodic vulnerability scans, and review of security policies.	Bi-annual discussions to address security posture and any recent incidents.

Tier 3 (Low-Risk Vendors)

Frequency	Activities	Review Meetings
Annual monitoring.	Basic assessments, policy compliance checks, and an annual review.	Annual check-in to confirm any changes to the vendor's access or risk profile.



Step 4: Integrate Automated Monitoring Tools

Automation streamlines continuous monitoring, providing real-time insights without extensive manual effort. Automated tools can:

1. Track security alerts, system changes, and incident reports in real time.
2. Assess vulnerabilities based on key risk indicators specific to each vendor's tier.
3. Generate risk reports and notify your team of critical changes or anomalies.

Integrating these tools can improve both the efficiency and accuracy of monitoring efforts, especially for high-risk vendors.

Step 5: Establish Communication and Response Protocols

Maintaining open communication with vendors is essential to ensure they're prepared to respond to emerging risks. Establish protocols for:

Incident Reporting

Ensure vendors report incidents according to agreed timelines based on their risk tier.

Regular Updates

Require vendors to provide updates on their security measures, especially when they experience security events.

Escalation Procedures

Define escalation paths for each tier, specifying when incidents should be elevated to senior management or regulatory bodies.

Conclusion

Vendor risk tiering is a vital component of a proactive TPRM framework. By categorizing vendors based on risk and implementing tier-specific monitoring, your organization can focus its resources effectively and maintain robust security oversight. Continuous monitoring, particularly when supported by automation, helps you stay ahead of emerging risks and strengthens your vendor management program's resilience.

This guide provides a foundation for risk-based monitoring that you can tailor to fit your organization's specific needs, industry requirements, and regulatory standards.

About Aujas Cybersecurity

Aujas Cybersecurity - A NuSummit Company, helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services. Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information, visit us at **www.aujas.com** or write to us at **contact@aujas.com.**

Cupertino | Dallas | Jersey City | Ottawa | Riyadh | Dubai | Mumbai | New Delhi | Bangalore

Follow us at: