Third-Party Risk Management

Third-Party Risk Management

Prepared for:

ComplianceAutomator.com

Contact: Tori R. Patterson

SaaS / Technology Industry

Generated: March 30, 2026

ComplianceAutomator.com

Third-Party Risk Management

Prepared for: ComplianceAutomator.com **Primary contact:** Tori R. Patterson **Date:** 2026-03-30 **Version:** 1.0 **Last Updated:** 2026-03-30 **Generated by:** ComplianceAutomator

---

0.1 Intake Summary

- Industry: SaaS / Technology

Assumptions Used

- Operating model not provided; assume lean startup processes.
- Company size not provided; assume startup/SMB scale.
- Regions not provided; assume US-focused operations.
- Data types not provided; assume standard customer and operational data.
- Hosting not provided; assume cloud-hosted (AWS/GCP/Azure).
- Security maturity not provided; assume early-stage controls with room to mature.

0.2 How to Use This Compliance Toolkit

1. Replace any remaining placeholders (if any).
2. Assign document owners and reviewers.
3. Review recommended status tables and adjust targets.
4. Schedule an internal review meeting.
5. Store finalized documents in your compliance repository.

---

1. Vendor Risk Management Framework

1.1 ComplianceAutomator.com

1.2 Executive Summary

This Vendor Risk Management (VRM) framework provides ComplianceAutomator.com with a comprehensive approach to identifying, assessing, and mitigating risks associated with third-party vendors. As a SaaS provider handling sensitive compliance data, our vendor relationships directly impact our security posture, regulatory compliance, and service delivery capabilities.

1.3 1. Framework Overview

1.1 Objectives

- Ensure vendor relationships align with business objectives and risk tolerance
- Maintain regulatory compliance across all vendor engagements
- Protect customer data and intellectual property
- Minimize operational disruptions from vendor-related incidents
- Optimize vendor performance and cost-effectiveness

1.2 Scope

This framework applies to all vendors providing:

- Cloud infrastructure services (AWS, Azure, GCP)
- Software development tools and platforms
- Data processing and analytics services
- Security and monitoring solutions
- Professional services (legal, consulting, audit)
- Business operations support (HR, finance, marketing tools)