Risk Management Policy

Introduction
Risk management is a critical aspect of ComplianceAide's cybersecurity strategy and organizational governance. This policy establishes actionable protocols, frameworks, and controls to identify, evaluate, and mitigate risks to the organization's assets and operations effectively.

Purpose
The Risk Management Policy is designed to protect ComplianceAide’s infrastructure, data, and operations against risks. It provides a framework for proactive threat identification, assessment, mitigation, and continuous improvement to maintain security and compliance.

Scope
This policy applies to all ComplianceAide personnel, organizational processes, technologies, and third-party vendors involved in operational activities. It encompasses data security, infrastructure security, incident response, vendor risk management, employee awareness, endpoint protection, and network security.

Policy Statement
ComplianceAide commits to implementing robust risk management measures, integrating advanced technologies and methodologies, and adopting industry standards to safeguard against cyber threats and vulnerabilities.

Roles and Responsibilities
- ComplianceAide Leadership: Ensure sufficient budget, resources, and oversight for the implementation and enforcement of this policy.
- Risk Management Team: Conduct risk assessments, monitor vulnerabilities, develop mitigation strategies, and oversee compliance.
- Employees: Comply with security protocols and participate in training programs to mitigate organizational risks.
- Third-Party Vendors: Adhere to ComplianceAide’s security and compliance requirements through contractual agreements and performance evaluations.

Policy Details

Security Frameworks
ComplianceAide aligns its risk management practices with the following industry frameworks:
- \*\*Cyber Essentials\*\*: A foundational guide to combating common cyber threats.
- \*\*NIST Cybersecurity Framework (NIST CF)\*\*: A comprehensive framework for securing critical infrastructure.

Risk Assessment Procedures
- \*\*Frequency\*\*: Risk assessments are conducted quarterly and after major organizational changes.
- \*\*Process\*\*:
 - Identify assets and their vulnerabilities.
 - Catalog risks based on severity using frameworks such as FAIR or CVSS.
 - Conduct threat modeling (e.g., STRIDE or PASTA) to simulate attack outcomes.
 - Prioritize risks by impact and likelihood.
 - Define mitigation plans for high-priority risks.

Vendor Risk Management
- \*\*Pre-Contract Assessments\*\*: Evaluate vendor compliance with standards such as SOC 2, GDPR, or CCPA.
- \*\*Ongoing Audits\*\*: Schedule annual audits to validate adherence to security protocols.
- \*\*SLAs\*\*: Ensure the vendor’s service-level agreements (SLAs) specify cybersecurity and incident response timeframes.

Incident Response Plan
- \*\*Phases\*\*:
 - \*\*Preparation\*\*: Assign roles (incident manager, forensic analyst, etc.) and maintain playbooks for common scenarios.
 - \*\*Detection and Analysis\*\*: Enable real-time threat detection via SIEM platforms.
 - \*\*Containment\*\*: Isolate affected systems to prevent widespread damage.
 - \*\*Eradication and Recovery\*\*: Remove malicious actors or components, revalidate systems, and restore operations.
 - \*\*Post-Incident Review\*\*: Conduct root cause analyses and lessons learned sessions to prevent recurrence.
- \*\*Escalation Paths\*\*: Define communication protocols for notifying stakeholders, clients, and regulatory bodies.

Data Security

Encryption-in-Transit
ComplianceAide encrypts data in transit using TLS 1.3 to maintain secure communication channels.

Data Retention and Deletion
Data processed by ComplianceAide is deleted immediately upon completion to mitigate exposure risks and uphold privacy standards.

Backups
Daily backups are enabled across all critical systems, stored in encrypted formats, and tested bi-weekly for recovery reliability.

Infrastructure Security

Infrastructure-as-Code (IaC)
IaC methodologies are applied to automate secure deployment of resources while maintaining consistency. Platforms such as Terraform and Ansible are employed for real-time monitoring and drift detection.

Environment Segregation
Production, development, and testing environments are segregated to ensure customer data remains isolated. Direct data access within non-production environments is strictly prohibited.

Status Monitoring
Continuous uptime monitoring is facilitated using Azure Monitor tools integrated across all hosted environments in North America.

Access Control
- \*\*Dynamic RBAC\*\*: Implementation of role-based access controls adapting to geo-location, behavior, and temporal factors. Teams use IAM tools such as Okta or AWS IAM.
- \*\*Audit Procedures\*\*: Annual audits ensure compliance with mandatory access permissions.
- \*\*Credential Storage\*\*: Secure vaults, such as HashiCorp Vault, are employed for password management alongside enforcement of MFA protocols.

Endpoint Security

- \*\*Patch Management\*\*: Automated patching systems are configured for software updates. Vulnerability scanning tools such as Nessus are used quarterly.
- \*\*EDR Integration\*\*: Sophos Intercept X monitors endpoint activity with actionable insights.
- \*\*Mobile Device Policy\*\*: All employee mobile devices are registered under an MDM system. Device hardening baselines follow CIS Benchmarks for endpoint protection.

Network Security

Firewall
Traditional firewalls and Kubernetes-native Cilium Network Policies safeguard incoming and outgoing traffic through granular control.

Intrusion Detection Systems (IDS)
ComplianceAide integrates IDS solutions that log network activity and benchmark behavior to identify anomalies. Actionable alerts are escalated to the Incident Response Team.

Continuous Monitoring
SIEM platforms such as Splunk aggregate logs, threat intelligence feeds, and data across systems for centralized security analysis. The implementations are supplemented by artificial intelligence to preemptively identify threats.

Employee Awareness and Training
- \*\*Frequency\*\*: Training programs occur quarterly with additional phishing simulations monthly.
- \*\*Focus Areas\*\*:
 - Role-specific cybersecurity practices (e.g., secure coding for developers).
 - Breach simulation exercises to test incident response readiness.
- \*\*Accountability\*\*: Human Resources, in collaboration with Risk Management, track compliance and effectiveness.

Policy Review and Updates
- \*\*Periodic Review\*\*: The Risk Management Policy is reviewed semi-annually to ensure relevance given emerging threats and regulatory changes. Revisions are approved by the Policy Review Board.
- \*\*Update Log\*\*: All modifications are cataloged for transparency and historical comparisons.

References and Appendices
The updated references include:
- Cyber Essentials Framework Overview
- NIST Cybersecurity Framework Documentation
- Azure Security and Compliance Guide

Conclusion
ComplianceAide’s revised Risk Management Policy represents a robust approach to identifying, assessing, and mitigating risks, ensuring the organization remains a secure and trusted entity within its operational landscape.

This comprehensive overhaul reflects heightened attention to detail and precedent-driven standards, while remaining actionable for implementation.