Third-Party Risk Assessment Report Template
Report Date: [Date Assessment Completed, e.g., 2025-04-23] **Assessment Conducted By:** [Name(s)/Department of Assessor(s)] **Version:** [e.g., 1.0]

1. Assessment Overview

- **Vendor Name:** [Full Legal Name of Vendor]
- **Service(s) Provided:** [Brief description of the product/service being assessed]
- **Assessment Trigger:** [e.g., New Vendor Onboarding, Annual Review, Contract Renewal, Significant Change]
- **Business Owner/Requestor:** [Name/Department requesting/managing the vendor relationship]
- **Assessment Scope:** [Specify what aspects were assessed - e.g., Security Controls for SaaS Platform X, Data Privacy Practices for handling Customer PII, Overall Vendor Operational Resilience]
- **Information Sources Used:** [e.g., Vendor Security Questionnaire (Date), SOC 2 Type II Report (Period), Penetration Test Summary (Date), Vendor Website, Interviews (Date), Public Breach Data]

2. Vendor & Service Profile

- **Vendor Contact:** [Name, Title, Email of primary vendor contact for security]
- **Brief Vendor Description:** [Vendor's primary business, size, industry, location]
- **Detailed Service Description:** [Elaborate on the service, how it integrates with [Your Company Name]'s systems/processes]
- **Data Involved:**
    - **Type(s) of Data Accessed/Processed/Stored:** [List specific data types, e.g., Customer PII (Names, Emails), Financial Transactions, Confidential Business Plans, Usage Analytics (Anonymized), PHI, Public Data]
    - **Data Classification:** [Your Company's classification level, e.g., Confidential, Restricted, Public]
    - **Data Location(s):** [Geographic location(s) where data is stored/processed]
- **System Access:** [Describe level of access to [Your Company Name]'s network/systems, e.g., API integration, VPN access, Cloud console access, No direct access]

3. Inherent Risk Analysis *(Assess risk before considering the vendor's specific controls. Use your org's methodology - scale Low/Med/High or 1-5)*

Factor	Assessment Rationale	Inherent Risk Rating
Data Sensitivity	[e.g., Handles Confidential PII, subject to GDPR]	[High]
Data Volume	[e.g., Processes data for 10,000+ customers]	[Medium]
Service Criticality	[e.g., Essential for core business function X, no immediate alternative]	[High]
System Access Level	[e.g., Direct API access to production database]	[High]
Regulatory Impact	[e.g., Falls under PCI-DSS, potential for large fines]	[Medium]

Factor	Assessment Rationale	Inherent Risk Rating
Vendor Location Risk	[e.g., Operates in high-risk jurisdiction]	[Low]
Subcontractor Reliance	[e.g., Relies heavily on 4th parties for key functions]	[Medium]
... [Other factors] ...		[...]
Overall Inherent Risk	**[Calculate or determine overall level, e.g., High]**	

4. Control Assessment Summary *(Summarize findings based on questionnaire, documentation review, etc. Rate each domain based on adequacy of controls)*

Control Domain	Assessment Summary & Key Findings	Domain Rating
Governance & Compliance	[e.g., Mature policies aligned with ISO 27001, recent SOC 2 Type II with minor exceptions, clear CISO role.]	[Satisfactory]
Data Security & Privacy	[e.g., Strong encryption at rest/transit (TLS 1.2+). Data segregation good. Retention policy exists but disposal process needs clarification. GDPR processes documented.]	[Satisfactory]
Access Control	[e.g., Uses RBAC, MFA enforced for remote/admin access. Access reviews quarterly. Offboarding process timely. Password policy meets standards.]	[Satisfactory]
Infrastructure & Network Security	[e.g., Regular vulnerability scanning (monthly). Patching cadence good for critical (7 days), slower for Highs (45 days). Uses IDS/IPS. Firewall rules reviewed annually.]	[Needs Improvement]
Application Security (if appl.)	[e.g., Claims SSDLC but lacks detail. DAST performed pre-release. Last external pentest 18 months ago; critical finding outstanding. OWASP Top 10 awareness cited.]	[Unsatisfactory]
Incident Response	[e.g., Documented IRP, tested via tabletop 6 months ago. Notification SLA clear (24h for breach affecting our data). 24/7 contact available.]	[Satisfactory]
Business Continuity/DR	[e.g., Documented BCP/DRP.	[Satisfactory]

Control Domain	Assessment Summary & Key Findings	Domain Rating
	Stated RTO/RPO meet requirements. Last DR test successful (full failover). Regular backups, stored offsite.]	
Personnel Security	[e.g., Background checks for sensitive roles. Annual awareness training confirmed.]	[Satisfactory]
Physical Security	[e.g., Uses Tier III data centers with standard controls (audited via SOC 2).]	[Satisfactory]
Subcontractor Management	[e.g., Acknowledges use of key subcontractors (AWS). Claims review process but lacks formal evidence.]	[Needs Improvement]

5. Identified Findings & Gaps *(List specific issues needing attention)*

Finding ID	Control Domain	Description of Finding/Gap	Associated Risk
F-001	Infrastructure & Network Security	Patching timeframe for High vulnerabilities (45 days) exceeds internal policy (30 days).	[Medium]
F-002	Application Security	Last penetration test was 18 months ago; standard requires annual testing.	[High]
F-003	Application Security	Critical vulnerability identified in last pentest remains outstanding beyond remediation SLA.	[High]
F-004	Subcontractor Management	Lack of documented evidence regarding the security assessment process for critical subcontractors (e.g., AWS - reliance on AWS certs okay, but needs stating).	[Medium]
F-005	Data Security & Privacy	Data disposal process lacks specific procedural details.	[Low]

6. Risk Rating & Analysis *(Based on Inherent Risk and the effectiveness of Controls/Findings)*

- **Likelihood:** [Assess likelihood of a risk event occurring given the findings - e.g., Medium]
- **Impact:** [Assess potential impact if a risk event occurs, often linked to Inherent Risk - e.g., High]
- **Residual Risk Rating: [Determine overall risk level using your org's matrix/methodology based on Likelihood/Impact - e.g., High]**
- **Rationale/Justification:** [Explain the rating. e.g., While many controls are satisfactory, the outstanding critical application vulnerability (F-003) and outdated pentest (F-002) significantly increase the likelihood of compromise impacting sensitive data, leading to a High residual risk rating until remediated.]

7. Recommendations & Mitigation Plan *(Actions to address findings and reduce risk)*

Finding ID	Recommendation	Responsibility	Due Date	Status
F-001	Vendor to align patching timeframe for High vulnerabilities with [Your Company Name]'s 30-day requirement, or provide compensating controls.	[Vendor]	[YYYY-MM-DD]	[Open]
F-002	Vendor to conduct an external penetration test and provide summary report.	[Vendor]	[YYYY-MM-DD]	[Open]
F-003	Vendor to remediate outstanding critical vulnerability (Ref: Pentest report [Date/ID]) and provide evidence of remediation.	[Vendor]	[YYYY-MM-DD]	[Open]
F-004	Vendor to provide documentation outlining their subcontractor security assessment process or confirm reliance on AWS compliance documents.	[Vendor]	[YYYY-MM-DD]	[Open]
F-005	Vendor to provide detailed procedure	[Vendor]	[YYYY-MM-DD]	[Open]

Finding ID	Recommendation	Responsibility	Due Date	Status
	for secure data disposal upon contract termination.			
	[Add any internal compensating controls if needed]	[Internal Team]	[YYYY-MM-DD]	[Open]

8. Overall Assessment Decision & Sign-off

- **Decision:** [Choose one]
  - [ ] **Approve:** Residual risk is acceptable.
  - [ ] **Approve with Conditions:** Approval contingent on successful completion of specified recommendations by due dates. Failure to meet conditions may trigger reassessment or termination. (Requires tracking of mitigation plan).
  - [ ] **Reject:** Residual risk is unacceptable. Do not proceed/initiate offboarding.
- **Decision Rationale:** [Briefly explain the final decision based on residual risk and mitigation plan feasibility]
- **Assessor Signature:** _____ Date: _____
- **Business Owner Acceptance/Acknowledgement:** _____ Date: _____
- **Information Security/Risk Lead Approval:** _____ Date: _____ *(Add other required approvers as per your process)*

9. Review Schedule

- **Next Scheduled Assessment Date:** [e.g., YYYY-MM-DD (Based on risk level - High=Annual, Med=Biennial, Low=Triennial, or event-driven)]
- **Review Trigger Notes:** [Any specific events that should trigger an earlier review, e.g., Change in service scope, Security incident at vendor, Change in data processed]