PLATOPS

### Evaluate vendor security risks

PlatOps provides security-first DevOps, cloud, and managed IT services for small and mid-sized businesses. We help organizations achieve compliance certifications, secure their infrastructure, and modernize their operations — without the enterprise price tag.

From SOC 2 and HIPAA compliance to cloud migrations and 24/7 monitoring, our team of engineers delivers measurable results with a 100% audit pass rate across 60+ client engagements.

| 100% | 60+ | 8-12 wk | 24/7 |
|---|---|---|---|
| AUDIT PASS RATE | ORGANIZATIONS | AVG. TO COMPLIANCE | MONITORING |

# Vendor Security Assessment Questionnaire

## Third-Party Risk Evaluation Template

**Prepared by PlatOps Security Version 1.0 | January 2026**

## QUESTIONNAIRE OVERVIEW

| ATTRIBUTE | VALUE |
|---|---|
| Total Questions | 50 |
| Categories | 8 security domains |
| Time to Complete | 30-45 minutes (by vendor) |
| Scoring | Pass/Fail + Risk Rating |
| Output | Vendor risk rating + approval recommendation |

### How to Use This Template

1. Send to vendors before onboarding or during annual review
2. Request evidence for critical controls
3. Score responses and calculate risk rating
4. Make approval/rejection decision based on risk tolerance

© 2026 PlatOps. All rights reserved.

| FIELD | RESPONSE |
|---|---|
| Vendor Name | |
| Primary Contact | |
| Contact Email | |
| Website | |
| Service Description | |
| Data Accessed | [ ] PII [ ] PHI [ ] PCI [ ] Confidential [ ] Public |
| Integration Type | [ ] API [ ] File Transfer [ ] Portal [ ] Direct Access |
| Criticality | [ ] Critical [ ] High [ ] Medium [ ] Low |
| Assessment Date | |
| Assessor | |

## SECTION 1: COMPANY & GOVERNANCE (6 Questions)

| # | QUESTION | RESPONSE | EVIDENCE REQUIRED |
|---|---|---|---|
| 1 | How long has your company been in business? | _____ years | |
| 2 | How many employees does your company have? | _____ | |
| 3 | Do you have a dedicated security team or officer? | [ ] Yes [ ] No | Org chart |
| 4 | Do you have a documented information security policy? | [ ] Yes [ ] No | Policy document |
| 5 | Is your security policy reviewed at least annually? | [ ] Yes [ ] No | Review records |
| 6 | Do you carry cyber liability insurance? | [ ] Yes [ ] No | Certificate |

**Coverage Amount (if yes):** $_______________

| # | QUESTION | RESPONSE | EVIDENCE REQUIRED |
|---|---|---|---|
| 7 | Do you have SOC 2 Type II certification? | [ ] Yes [ ] No [ ] In Progress | SOC 2 Report |
| 8 | Do you have ISO 27001 certification? | [ ] Yes [ ] No [ ] In Progress | Certificate |
| 9 | Are you PCI-DSS compliant (if applicable)? | [ ] Yes [ ] No [ ] N/A | AOC |
| 10 | Are you HIPAA compliant (if applicable)? | [ ] Yes [ ] No [ ] N/A | Attestation |
| 11 | Do you conduct annual penetration testing? | [ ] Yes [ ] No | Executive summary |
| 12 | Do you conduct regular vulnerability assessments? | [ ] Yes [ ] No | Sample report |
| 13 | Have you had any security breaches in the last 3 years? | [ ] Yes [ ] No | Incident details |
| 14 | If yes, please describe the breach and remediation: | | |

**Certifications held (list all):** ___________________________________

## SECTION 3: ACCESS CONTROL (7 Questions)

| # | QUESTION | RESPONSE | EVIDENCE REQUIRED |
|---|---|---|---|
| 15 | Do you enforce unique user accounts (no shared accounts)? | [ ] Yes [ ] No | |
| 16 | Is multi-factor authentication (MFA) required for access? | [ ] Yes [ ] No | |
| 17 | Is role-based access control (RBAC) implemented? | [ ] Yes [ ] No | |
| 18 | How quickly is access revoked upon termination? | [ ] <24 hrs [ ] 24-48 hrs [ ] >48 hrs | |
| 19 | Are access reviews conducted at least quarterly? | [ ] Yes [ ] No | |
| 20 | Is privileged access limited and monitored? | [ ] Yes [ ] No | |
| 21 | Is there a password policy meeting industry standards? | [ ] Yes [ ] No | Policy document |

**Password requirements (if yes):** ___________________________________

| # | QUESTION | RESPONSE | EVIDENCE REQUIRED |
|---|---|---|---|
| 22 | Is customer data encrypted at rest? | [ ] Yes [ ] No | |
| 23 | What encryption algorithm is used at rest? | [ ] AES-256 [ ] Other: _____ | |
| 24 | Is customer data encrypted in transit? | [ ] Yes [ ] No | |
| 25 | What TLS version is supported? | [ ] 1.2 [ ] 1.3 [ ] Both | |
| 26 | Is there a data classification policy? | [ ] Yes [ ] No | |
| 27 | Where is customer data stored (geographic location)? | | |
| 28 | Is data backed up regularly? | [ ] Yes [ ] No | |
| 29 | Can you provide data upon contract termination? | [ ] Yes [ ] No | |

**Data retention period:** _____ days/months/years

## SECTION 5: NETWORK & INFRASTRUCTURE (6 Questions)

| # | QUESTION | RESPONSE | EVIDENCE REQUIRED |
|---|---|---|---|
| 30 | Is your network segmented? | [ ] Yes [ ] No | |
| 31 | Do you use intrusion detection/prevention systems? | [ ] Yes [ ] No | |
| 32 | Are firewalls deployed and managed? | [ ] Yes [ ] No | |
| 33 | Is your infrastructure hosted in a compliant data center? | [ ] Yes [ ] No | |
| 34 | Do you use a reputable cloud provider (AWS, Azure, GCP)? | [ ] Yes [ ] No | |
| 35 | Is there DDoS protection for public-facing services? | [ ] Yes [ ] No | |

**Primary hosting location/provider:** ________________________________

## SECTION 6: INCIDENT RESPONSE (5 Questions)

| # | QUESTION | RESPONSE | EVIDENCE REQUIRED |
|---|---|---|---|
| 36 | Do you have a documented incident response plan? | [ ] Yes [ ] No | IR Plan |
| 37 | Is the incident response plan tested at least annually? | [ ] Yes [ ] No | Test records |
| 38 | What is your SLA for notifying customers of security incidents? | [ ] <24 hrs [ ] 24-72 hrs [ ] >72 hrs | |
| 39 | Do you have an external incident response retainer? | [ ] Yes [ ] No | |
| 40 | Is there 24/7 security monitoring? | [ ] Yes [ ] No | |

| # | QUESTION | RESPONSE | EVIDENCE REQUIRED |
|---|---|---|---|
| 41 | Do you have a business continuity plan? | [ ] Yes [ ] No | BC Plan |
| 42 | Do you have a disaster recovery plan? | [ ] Yes [ ] No | DR Plan |
| 43 | What is your Recovery Time Objective (RTO)? | _____ hours | |
| 44 | What is your Recovery Point Objective (RPO)? | _____ hours | |
| 45 | Is the DR plan tested at least annually? | [ ] Yes [ ] No | Test records |

**Uptime SLA offered:** _____%

## SECTION 8: SUBCONTRACTORS & FOURTH PARTIES (5 Questions)

| # | QUESTION | RESPONSE | EVIDENCE REQUIRED |
|---|---|---|---|
| 46 | Do you use subcontractors to process customer data? | [ ] Yes [ ] No | |
| 47 | If yes, are subcontractors subject to security assessments? | [ ] Yes [ ] No | |
| 48 | Are subcontractors contractually bound to security requirements? | [ ] Yes [ ] No | |
| 49 | Can you provide a list of subcontractors with data access? | [ ] Yes [ ] No | Subcontractor list |
| 50 | Will you notify us if subcontractors change? | [ ] Yes [ ] No | |

**List critical subcontractors:** ___________________________________

## SCORING & RISK ASSESSMENT

### Section Scores

| SECTION | CRITICAL QUESTIONS | PASSED | FAILED | SCORE |
|---|---|---|---|---|
| Governance | 3, 4, 6 | _____ | _____ | ___/3 |
| Compliance | 7 or 8, 11, 13 | _____ | _____ | ___/3 |
| Access Control | 15, 16, 18, 20 | _____ | _____ | ___/4 |
| Data Protection | 22, 24, 28 | _____ | _____ | ___/3 |
| Infrastructure | 30, 32, 34 | _____ | _____ | ___/3 |
| Incident Response | 36, 38, 40 | _____ | _____ | ___/3 |
| Business Continuity | 41, 42, 45 | _____ | _____ | ___/3 |
| Subcontractors | 47, 48 | _____ | _____ | ___/2 |
| **TOTAL** | | **_____** | **_____** | **___/24** |

| SCORE | RISK RATING | RECOMMENDATION |
|---|---|---|
| 22-24 | **Low Risk** | Approve |
| 18-21 | **Medium Risk** | Approve with conditions |
| 14-17 | **High Risk** | Require remediation plan |
| 0-13 | **Critical Risk** | Do not approve |

## REQUIRED EVIDENCE CHECKLIST

### Documents to Request

| DOCUMENT | RECEIVED | REVIEWED | ACCEPTABLE |
|---|---|---|---|
| SOC 2 Type II Report | [ ] | [ ] | [ ] |
| Penetration Test Summary | [ ] | [ ] | [ ] |
| Security Policy | [ ] | [ ] | [ ] |
| Incident Response Plan | [ ] | [ ] | [ ] |
| Business Continuity Plan | [ ] | [ ] | [ ] |
| Cyber Insurance Certificate | [ ] | [ ] | [ ] |
| Subprocessor List | [ ] | [ ] | [ ] |

## ASSESSMENT SUMMARY

### Vendor Risk Profile

| ATTRIBUTE | VALUE |
|---|---|
| **Overall Risk Rating** | [ ] Low [ ] Medium [ ] High [ ] Critical |
| **Data Sensitivity** | [ ] Low [ ] Medium [ ] High |
| **Business Criticality** | [ ] Low [ ] Medium [ ] High |
| **Combined Risk Score** | ______ / 24 |

### Findings Summary

**Strengths:**

1. ______________________________

2. ______________________________

1.

2.

3.

### Conditions for Approval (if applicable)

| CONDITION | DEADLINE | OWNER |
|---|---|---|
| | | |
| | | |
| | | |

## APPROVAL DECISION

| DECISION | DATE | APPROVER |
|---|---|---|
| [ ] Approved | | |
| [ ] Approved with Conditions | | |
| [ ] Requires Remediation | | |
| [ ] Rejected | | |

**Justification:**

**Next Review Date:** ________________

## CONTRACTUAL REQUIREMENTS

### Security Clauses to Include in Contract

- □ Right to audit clause
- □ Security incident notification requirements
- □ Data protection obligations
- □ Subcontractor notification
- □ Insurance requirements
- □ Termination and data return
- □ Compliance with applicable regulations

## ABOUT THIS TEMPLATE

This template is provided by PlatOps Security to help organizations assess vendor security. For assistance with vendor risk management:

## Ready to Get Started?

Let our team of security and infrastructure experts help you achieve your goals faster.

| 100% | 60+ | 8-12 wk | 24/7 |
|---|---|---|---|
| AUDIT PASS RATE | ORGANIZATIONS SERVED | AVG. TIME TO COMPLIANCE | MONITORING & SUPPORT |

Get Free Assessment    Book Strategy Call    Security Services

Email: hello@platops.com    Phone: (202) 864-1197    Web: platops.com

This document is provided for informational purposes only. Requirements may vary based on your organization's specific circumstances. PlatOps is a registered trademark. Redistribution without permission is prohibited.

© 2026 PlatOps. All rights reserved.