PLATOPS

Understand your security posture

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

Security Posture Assessment Questionnaire

Comprehensive Self-Assessment for Organizations

Prepared by PlatOps Security Version 1.0 | January 2026

TEMPLATE OVERVIEW

ATTRIBUTE	VALUE
Total Questions	75
Categories	10
Time to Complete	45-60 minutes
Scoring	0-3 per question (0=None, 1=Partial, 2=Mostly, 3=Full)
Max Score	225 points
Output	Security maturity score + priority recommendations

Scoring Guide (For Each Question)

- **0** = Not implemented / Don't know
- **1** = Partially implemented / In progress
- **2** = Mostly implemented / Minor gaps
- **3** = Fully implemented / Documented

 | 4701 Sangamore Road, Suite 100N #2000, Bethesda, MD 20816
hello@platops.com | (202) 864-1197 | platops.com

1.1 Security Leadership

#	QUESTION	SCORE (0-3)	NOTES
1	Do you have a designated security leader (CISO, Security Manager, or equivalent)?	_____	
2	Does security leadership report to executive management or the board?	_____	
3	Is there a documented security budget with annual allocation?	_____	

1.2 Security Policies

#	QUESTION	SCORE (0-3)	NOTES
4	Do you have a written information security policy?	_____	
5	Is the security policy reviewed and updated at least annually?	_____	
6	Are security policies communicated to all employees?	_____	

1.3 Risk Management

#	QUESTION	SCORE (0-3)	NOTES
7	Do you conduct regular security risk assessments?	_____	
8	Is there a risk register that tracks identified risks and remediation?	_____	

Section 1 Score: _____ / 24

SECTION 2: ACCESS CONTROL (10 Questions)

2.1 Identity Management

#	QUESTION	SCORE (0-3)	NOTES
9	Does every user have a unique account (no shared accounts)?	_____	
10	Is multi-factor authentication (MFA) required for all users?	_____	
11	Is MFA required for all administrative/privileged access?	_____	
12	Do you use single sign-on (SSO) for applications?	_____	

#	QUESTION	SCORE (0-3)	NOTES
13	Is role-based access control (RBAC) implemented?	_____	
14	Is the principle of least privilege enforced?	_____	
15	Are user access rights reviewed at least quarterly?	_____	
16	Is access revoked within 24 hours of employee termination?	_____	

2.3 Password Security

#	QUESTION	SCORE (0-3)	NOTES
17	Do you enforce strong password requirements (12+ characters)?	_____	
18	Is a password manager provided to employees?	_____	

Section 2 Score: _____ / 30

SECTION 3: DATA PROTECTION (8 Questions)

3.1 Data Classification

#	QUESTION	SCORE (0-3)	NOTES
19	Do you have a data classification policy (public, internal, confidential, restricted)?	_____	
20	Is sensitive data identified and labeled?	_____	
21	Are data retention and disposal policies documented?	_____	

3.2 Encryption

#	QUESTION	SCORE (0-3)	NOTES
22	Is sensitive data encrypted at rest (AES-256 or equivalent)?	_____	
23	Is data encrypted in transit (TLS 1.2+ enforced)?	_____	
24	Is full-disk encryption enabled on all laptops/workstations?	_____	
25	Are encryption keys properly managed (key rotation, secure storage)?	_____	

3.3 Data Loss Prevention

#	QUESTION	SCORE (0-3)	NOTES
26	Do you have data loss prevention (DLP) controls in place?	_____	

Section 3 Score: _____ / 24

4.1 Perimeter Security

#	QUESTION	SCORE (0-3)	NOTES
27	Are firewalls deployed and properly configured?	_____	
28	Is intrusion detection/prevention (IDS/IPS) implemented?	_____	
29	Is the network segmented (production, development, DMZ)?	_____	

4.2 Remote Access

#	QUESTION	SCORE (0-3)	NOTES
30	Is VPN or zero trust network access required for remote work?	_____	
31	Are remote access sessions logged and monitored?	_____	

4.3 Wireless Security

#	QUESTION	SCORE (0-3)	NOTES
32	Is wireless network security properly configured (WPA3/WPA2-Enterprise)?	_____	
33	Are guest networks separated from corporate networks?	_____	
34	Do you monitor for rogue access points?	_____	

Section 4 Score: _____ / 24

SECTION 5: ENDPOINT SECURITY (7 Questions)

5.1 Endpoint Protection

#	QUESTION	SCORE (0-3)	NOTES
35	Is endpoint detection and response (EDR) deployed on all devices?	_____	
36	Is mobile device management (MDM) implemented?	_____	
37	Are USB and removable media controls in place?	_____	

5.2 Patch Management

#	QUESTION	SCORE (0-3)	NOTES
38	Are operating systems patched within 30 days of release?	_____	
39	Are critical/high vulnerabilities patched within 14 days?	_____	
40	Is third-party software patched regularly?	_____	

 | 4701 Sangamore Road, Suite 100N #2000, Bethesda, MD 20816
hello@platops.com | (202) 864-1197 | platops.com

#	QUESTION	SCORE (0-3)	NOTES
41	Are endpoint security configurations standardized and documented?	_____	

Section 5 Score: _____ / 21

SECTION 6: APPLICATION SECURITY (7 Questions)

6.1 Secure Development

#	QUESTION	SCORE (0-3)	NOTES
42	Is secure coding training provided to developers?	_____	
43	Are code reviews required before deployment?	_____	
44	Is static application security testing (SAST) part of CI/CD?	_____	

6.2 Application Testing

#	QUESTION	SCORE (0-3)	NOTES
45	Is dynamic application security testing (DAST) performed?	_____	
46	Is penetration testing conducted at least annually?	_____	
47	Are third-party dependencies scanned for vulnerabilities?	_____	

6.3 Web Application Security

#	QUESTION	SCORE (0-3)	NOTES
48	Is a web application firewall (WAF) deployed?	_____	

Section 6 Score: _____ / 21

SECTION 7: SECURITY MONITORING & LOGGING (8 Questions)

7.1 Logging

#	QUESTION	SCORE (0-3)	NOTES
49	Are security events logged across all critical systems?	_____	
50	Are logs centralized (SIEM or log management)?	_____	
51	Are logs retained for at least 1 year?	_____	
52	Are logs protected from tampering?	_____	

#	QUESTION	SCORE (0-3)	NOTES
53	Is 24/7 security monitoring in place?	_____	
54	Are security alerts reviewed and triaged promptly?	_____	
55	Is user and entity behavior analytics (UEBA) implemented?	_____	

7.3 Vulnerability Management

#	QUESTION	SCORE (0-3)	NOTES
56	Are vulnerability scans conducted at least monthly?	_____	

Section 7 Score: _____ / 24

SECTION 8: INCIDENT RESPONSE (7 Questions)

8.1 Incident Response Plan

#	QUESTION	SCORE (0-3)	NOTES
57	Is there a documented incident response plan?	_____	
58	Are incident response roles and responsibilities defined?	_____	
59	Is the incident response plan tested at least annually?	_____	

8.2 Incident Handling

#	QUESTION	SCORE (0-3)	NOTES
60	Is there a process for employees to report security incidents?	_____	
61	Are all security incidents documented and tracked?	_____	
62	Is there an external incident response retainer?	_____	

8.3 Communication

#	QUESTION	SCORE (0-3)	NOTES
63	Are notification procedures documented (customers, regulators, law enforcement)?	_____	

Section 8 Score: _____ / 21

9.1 Backup

#	QUESTION	SCORE (0-3)	NOTES
64	Are critical systems and data backed up regularly?	_____	
65	Are backups stored offsite or in a separate cloud region?	_____	
66	Are backups encrypted?	_____	
67	Are backup restoration procedures tested at least quarterly?	_____	

9.2 Disaster Recovery

#	QUESTION	SCORE (0-3)	NOTES
68	Is there a documented disaster recovery plan?	_____	
69	Are RTO (Recovery Time Objective) and RPO (Recovery Point Objective) defined?	_____	

Section 9 Score: _____ / 18

SECTION 10: THIRD-PARTY & VENDOR MANAGEMENT (6 Questions)

10.1 Vendor Assessment

#	QUESTION	SCORE (0-3)	NOTES
70	Is there a vendor security assessment process?	_____	
71	Are vendors with access to sensitive data assessed before onboarding?	_____	
72	Do contracts include security requirements?	_____	

10.2 Ongoing Management

#	QUESTION	SCORE (0-3)	NOTES
73	Are critical vendors reviewed at least annually?	_____	
74	Is there a process for vendor security incident notification?	_____	
75	Are SOC 2 or equivalent reports obtained from critical vendors?	_____	

Section 10 Score: _____ / 18

Calculate Your Scores

SECTION	YOUR SCORE	MAX SCORE	%
1. Governance	_____	24	___%
2. Access Control	_____	30	___%
3. Data Protection	_____	24	___%
4. Network Security	_____	24	___%
5. Endpoint Security	_____	21	___%
6. Application Security	_____	21	___%
7. Monitoring & Logging	_____	24	___%
8. Incident Response	_____	21	___%
9. Business Continuity	_____	18	___%
10. Vendor Management	_____	18	___%
TOTAL	**_____**	**225**	**___%**

MATURITY LEVEL INTERPRETATION

Overall Score Ranges

SCORE RANGE	MATURITY LEVEL	DESCRIPTION
0-56 (0-25%)	**Critical**	Significant security gaps. High risk of breach. Immediate action required.
57-112 (26-50%)	**Developing**	Basic controls in place but major gaps exist. Prioritize remediation.
113-168 (51-75%)	**Defined**	Core security program exists. Focus on consistency and documentation.
169-202 (76-90%)	**Managed**	Strong security posture. Optimize and mature existing controls.
203-225 (91-100%)	**Optimized**	Industry-leading security. Continuous improvement focus.

Section Score Interpretation

SECTION %	PRIORITY	ACTION
0-25%	**Critical**	Address immediately
26-50%	**High**	Address within 30 days
51-75%	**Medium**	Address within 90 days
76-100%	**Low**	Maintain and optimize

 | 4701 Sangamore Road, Suite 100N #2000, Bethesda, MD 20816
hello@platops.com | (202) 864-1197 | platops.com

Based on your scores, prioritize improvements in these order:

Tier 1 - Immediate (Sections scoring <50%)

1.
2.
3.

Tier 2 - Short-term (Sections scoring 50-75%)

1.
2.
3.

Tier 3 - Medium-term (Sections scoring 75-90%)

1.
2.

NEXT STEPS

Want Help Improving Your Security Posture?

Step 1: Schedule a free consultation to review your results → platops.com/book-call

Step 2: Get a detailed remediation roadmap → platops.com/assessment

Step 3: Implement improvements with expert guidance

PlatOps Security Services

- **Security Assessment** - Professional evaluation
- **Gap Remediation** - Implementation support
- **Managed Security** - Ongoing protection
- **Compliance Programs** - SOC 2, HIPAA, PCI-DSS

Contact Us

Email: hello@platops.com **Phone:** (301) 555-0123 **Web:** platops.com

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 Assessment Services

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