vijilan
IT Security: Enabled

SOC READINESS CHECKLIST

Is Your Organization Ready for Managed SOC?

PURPOSE

This checklist helps you evaluate your organization's readiness for a Managed SOC engagement. Complete each section to identify gaps and prepare for a successful deployment.

Scoring: Check each item that applies. Higher scores indicate better readiness.

SECTION 1: ORGANIZATIONAL READINESS

Leadership & Governance

- ☐ Executive sponsor identified for security initiatives
- ☐ Budget allocated for managed security services
- ☐ Clear decision-making authority for security investments
- ☐ Security is discussed at board/leadership level
- ☐ Containment authorization defined

Internal Team

- ☐ Primary security contact identified
- ☐ Escalation contacts defined (nights/weekends)
- ☐ IT team understands SOC integration requirements
- ☐ Communication preferences established
- ☐ Time allocated for onboarding and ongoing collaboration

Section 1 Score: _/10

SECTION 2: TECHNICAL ENVIRONMENT

Endpoint Coverage

- ☐ Endpoint inventory exists (or willing to create)
- ☐ Endpoint count known (workstations, servers, laptops)
- ☐ Operating system versions documented
- ☐ Existing endpoint security tool identified (AV, EDR)
- ☐ Agent deployment process established

Network & Infrastructure

- ☐ Network topology documented
- ☐ Firewall rules accessible for review
- ☐ Remote access methods documented (VPN, RDP, etc.)
- ☐ Cloud environments identified (AWS, Azure, GCP)
- ☐ Critical servers and applications listed

Identity & Access

- ☐ Directory service identified (AD, Entra ID, Okta)
- ☐ Admin account inventory exists
- ☐ MFA status known across user population
- ☐ Service account inventory exists (or willing to create)
- ☐ Privileged access management approach defined

Section 2 Score: _/10

SECTION 3: CURRENT SECURITY POSTURE

Existing Tools

- ☐ Current security tools inventoried
- ☐ Tool overlap/gaps identified
- ☐ SIEM in place (or log aggregation)
- ☐ EDR/AV solution deployed
- ☐ Email security in place

Logging & Visibility

- ☐ Critical systems logging to central location
- ☐ Log retention policy defined
- ☐ Windows event logging configured
- ☐ Firewall logging enabled
- ☐ Cloud audit logging enabled

Incident Response

- ☐ Incident response plan exists (even if basic)
- ☐ Incident classification defined (what's critical?)
- ☐ Communication plan for security incidents
- ☐ Legal/PR contacts for breach scenarios
- ☐ Cyber insurance policy in place

Section 3 Score: _/10

SECTION 4: COMPLIANCE & DOCUMENTATION

Regulatory Requirements

- ☐ Applicable regulations identified (HIPAA, PCI, CMMC, etc.)
- ☐ Compliance gaps known
- ☐ Audit schedule understood
- ☐ Evidence collection process exists
- ☐ Third-party risk requirements documented

Documentation

- ☐ Network diagrams available
- ☐ Asset inventory accessible
- ☐ Security policies documented
- ☐ User access procedures documented
- ☐ Change management process exists

Section 4 Score: _/10

SECTION 5: DEPLOYMENT READINESS

Technical Prerequisites

- ☐ Internet connectivity from all endpoints
- ☐ Firewall rules can be modified for agent communication
- ☐ Administrative access to deploy agents
- ☐ Group Policy or MDM for mass deployment
- ☐ Test environment available for pilot

Timeline & Resources

- ☐ Deployment timeline defined
- ☐ Internal resources allocated for onboarding
- ☐ Maintenance windows identified (if needed)
- ☐ Success criteria defined
- ☐ Rollback plan considered

Section 5 Score: _/10

vijilan
IT Security: Enabled

AICPA SOC · ISO 27001 · A-LIGN

vijilan.com
info@vijilan.com
+1 (954) 334-9988

SCORING SUMMARY

Section	Your Score	Max Score
Organizational Readiness		10
Technical Environment		15
Current Security Posture		15
Compliance & Documentation		10
Deployment Readiness		10
Total		60

READINESS LEVELS

50–60 Points: Highly Ready ✅
You're well-prepared for Managed SOC. Expect a smooth onboarding with minimal gaps to address.

Next step: Schedule deployment planning call.

35–49 Points: Moderately Ready ⚠️
Good foundation, but some gaps exist. Most can be addressed during onboarding.

Next step: Schedule readiness assessment to identify priorities.

20–34 Points: Preparation Needed 🔶
Significant gaps that should be addressed before or during deployment.

Next step: Schedule discovery call to build remediation roadmap.

Below 20 Points: Foundation Building 🔴
Foundational work needed before managed SOC will be effective.

Next step: Consider security assessment to establish baseline.

COMMON GAPS & SOLUTIONS

Gap	Quick Win	With Vijilan
No endpoint inventory	Export from AD/Intune	Falcon Discover provides automatic inventory
Unclear escalation path	Document 3 contacts	We help define during onboarding
No incident response plan	Use free template	We provide IR playbook
Logging gaps	Enable Windows audit logging	We identify critical log sources
Unknown compliance requirements	Review contracts for requirements	We map to HIPAA, PCI, CMMC

AICPA SOC · ISO 27001 · A-LIGN

PREPARATION RESOURCES

Before Your First Call

- [ ] Complete this checklist
- [ ] Gather endpoint count (estimate okay)
- [ ] List current security tools
- [ ] Identify primary contact and escalation path
- [ ] Note any compliance requirements

Documents to Have Ready

Before Your First Call

- [ ] Network diagram (even if rough)
- [ ] List of critical applications
- [ ] Current security tool inventory
- [ ] Any recent security assessments
- [ ] Compliance audit results (if applicable)

NEXT STEPS

Ready to proceed?

Schedule a Readiness Assessment
Our team will review your checklist answers and provide:

- Gap analysis with prioritized recommendations
- Estimated deployment timeline
- Custom onboarding plan
- Pricing based on your environment

Have questions first?

Schedule a Discovery Call

No preparation needed. We'll walk through your environment and answer questions.

vijilan
IT Security: Enabled
vijilan.com
info@vijilan.com
+1 (954) 334-9988