



Cybersecurity Infrastructure Implementation Project Checklist Template 2026

Project Initiation & Risk Assessment

Defining project scope, identifying critical assets, and performing initial vulnerability and threat landscape assessments.

Project Name

Write something...

Project Start Date

Enter date...

Project Scope Statement

Write something...

Identified Critical Assets

- ☐ Customer Databases
- ☐ Proprietary Intellectual Property
- ☐ Financial Records
- ☐ Employee PII (Personally Identifiable Information)
- ☐ Cloud Infrastructure

Initial Risk Level

- ☐ Low
- ☐ Medium
- ☐ High
- ☐ Critical

Initial Risk Assessment Report

 **Upload File**

Project Sponsor Approval

Compliance & Regulatory Requirements

Identifying necessary legal frameworks (GDPR, HIPAA, SOC2, etc.) and establishing security governance standards.

Applicable Regulatory Frameworks

- ☐ GDPR
- ☐ HIPAA
- ☐ PCI DSS
- ☐ SOC2
- ☐ ISO/IEC 27001
- ☐ NIST Cybersecurity Framework
- ☐ SOX

Compliance Gap Analysis Summary

Write something...

Regulatory Compliance Documentation

 Upload File

Audit Deadline Date

Enter date...

Compliance Officer Approval

Network Architecture & Perimeter Defense Design

Planning firewall configurations, VPN deployment, intrusion detection/prevention systems (IDS/IPS), and network segmentation.

Primary Firewall Configuration ID

Write something...

Network Segmentation Zones

☐ DMZ (Demilitarized Zone)

☐ Internal Corporate Network

☐ Guest/IoT Network

☐ Database/Secure Tier

☐ Management Plane

VPN Protocol Standard

☐ IPsec

☐ SSL/TLS

☐ WireGuard

☐ OpenVPN

Network Architecture Review Completion Date

Enter date...

Network Topology Diagram

 Upload File

Access Control List (ACL) Summary

Write something...

Network Security Lead Approval

Identity and Access Management (IAM) Setup

Defining user roles, implementing Multi-Factor Authentication (MFA), Single Sign-On (SSO), and Principle of Least Privilege (PoLP) protocols.

IAM Policy Reference ID

Write something...

Authentication Methods to Implement

- ☐ Multi-Factor Authentication (MFA)
- ☐ Single Sign-On (SSO)
- ☐ Biometric Authentication
- ☐ Hardware Security Keys
- ☐ Certificate-Based Authentication

Access Review Frequency

- ☐ Monthly
- ☐ Quarterly
- ☐ Bi-Annually
- ☐ Annually

User Role Definition Details

Write something...

IAM Deployment Completion Date

Enter date...

Access Control Matrix Document

 Upload File

Security Architect Approval

Endpoint & Server Security Deployment

Installing EDR (Endpoint Detection and Response), managing patch management workflows, and securing server hardening configurations.

Endpoint Detection & Response (EDR) Agent Version

Deployment Completion Deadline

Server Hardening Configuration Logs

 Upload File

Total Number of Endpoints Scanned

Security Lead Approval

Data Protection & Encryption Implementation

Establishing protocols for data-at-rest and data-in-transit encryption, as well as backup and disaster recovery validation.

Encryption Standard Used

Data States Covered

- ☐ Data at Rest
- ☐ Data in Transit
- ☐ Data in Use

Encryption Key Rotation Schedule

Enter date...

Encryption Policy Documentation

 Upload File

Backup Verification Status

- ☐ Verified
- ☐ Pending Testing
- ☐ Failed

Data Classification Summary

Write something...

Security Monitoring & Incident Response Integration

Configuring SIEM (Security Information and Event Management) tools, logging orchestration, and establishing incident response playbooks.

SIEM Configuration Completion Date

Enter date...

Monitoring Tool Integration Status

- ☐ Not Started
- ☐ In Progress
- ☐ Testing Phase
- ☐ Fully Integrated

Alerting Channels Configured

- ☐ Email Notifications
- ☐ SMS/PagerDuty
- ☐ Slack/Microsoft Teams
- ☐ Dashboard/SOC Console

Incident Response Playbook Summary

Write something...

Incident Response Plan Documentation

 Upload File

Security Lead Approval

Security Awareness & Employee Training

Developing phishing simulation programs and security hygiene training for all organizational stakeholders.

Training Modules Completed

- ☐ Phishing Awareness
- ☐ Password Management & MFA
- ☐ Data Privacy & GDPR Compliance
- ☐ Social Engineering Defense
- ☐ Secure Remote Work Protocols

Last Training Completion Date

Enter date...

Number of Employees Trained

Enter a number...

Training Attendance Logs

 Upload File

Post-Training Evaluation Summary

Write something...

Security Officer Acknowledgment

Vulnerability Scanning & Penetration Testing

Conducting rigorous testing of the new infrastructure to identify and remediate security gaps before full production launch.

Scheduled Scan Date

Enter date...

Testing Environment

- ☐ Production
- ☐ Staging/UAT
- ☐ Sandbox/Development

Testing Scope Areas

- ☐ External Network Perimeter
- ☐ Internal Network Infrastructure
- ☐ Web Application Layer
- ☐ Cloud Configuration/API
- ☐ Wireless Network

Identified Vulnerabilities & Findings Summary

Write something...

Upload Penetration Test Report

 Upload File

Security Lead Approval

Project Closure & Continuous Monitoring Plan

Finalizing documentation, transitioning to operational maintenance, and establishing a long-term security audit schedule.

Project Completion Date

Enter date...

Final Security Audit Status

- ☐ Passed
- ☐ Passed with Minor Remediations
- ☐ Failed - Re-testing Required

Final Security Handover Documentation

 Upload File

Post-Implementation Monitoring Tasks

- ☐ Daily Log Review Setup
- ☐ Weekly Vulnerability Scanning Scheduled
- ☐ Quarterly Access Audit Configured
- ☐ Incident Response Drill Scheduled

Chief Information Security Officer (CISO) Approval

Post-Implementation Review & Lessons Learned

Write something...

< Previous

> Next

✓ Finish

 Generate Sample Report