NIST SP 800-171

Compliance Assessment Questionnaire

48 Assessment Questions • 14 Control Domains

ORGANIZATION INFORMATION

Organization Name: _____

Assessment Date: _____

Assessor Name / Title: _____

System / Scope: _____

SCORING METHOD

- ☐ **YES** (2 points) — Fully implemented — control is in place, documented, and operating effectively.
- ☐ **PARTIAL** (1 point) — Partially implemented — some elements are in place but gaps remain.
- ☐ **NO** (0 points) — Not implemented — control is missing or not operating.

Compliance Score = (Total Points ÷ Maximum Points) × 100%

Maximum possible points: 96 (48 questions × 2 points each)

ACCESS CONTROL

Reference: 3.1

Q1 [3.1.1]

Do you limit system access to authorized users, processes acting on behalf of authorized users, and devices?

A 'Yes' response indicates that access controls are in place to ensure only authorized entities can access the system. Evidence includes access control policies, user access lists, and system configuration settings.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q2 [3.1.2]

Do you restrict users to only the transactions and functions they are permitted to execute?

A 'Yes' response signifies that role-based access controls are implemented, limiting users to their authorized activities. Evidence includes role definitions, access control matrices, and audit logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q3 [3.1.12]

Do you monitor and control remote access sessions?

A 'Yes' response means that remote access is actively monitored and controlled. Evidence includes remote access logs, monitoring reports, and remote access policies.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q4 [3.1.20]

Do you use session lock mechanisms to prevent unauthorized access when users are inactive?

A 'Yes' response indicates that session locks are enforced after a period of inactivity. Evidence includes system configuration settings and session lock policies.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q5 [3.1.22]

Do you control information posted or processed on publicly accessible systems?

A 'Yes' response means that measures are in place to prevent unauthorized information disclosure on public systems. Evidence includes content management policies and review procedures.

☐ YES ☐ PARTIAL ☐ NO Explanation:

AWARENESS AND TRAINING

Reference: 3.2

Q6 [3.2.1]

Do you ensure that all users are aware of the security risks associated with their activities?

A 'Yes' response indicates that security awareness training is provided to all users. Evidence includes training materials, attendance records, and training schedules.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q7 [3.2.2]

Do you provide role-based security training to personnel with significant security responsibilities?

A 'Yes' response signifies that specialized training is given to personnel with security roles. Evidence includes training curricula, completion certificates, and role definitions.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q8 [3.2.3]

Do you ensure that personnel are trained to recognize and report potential security incidents?

A 'Yes' response means that incident reporting training is provided. Evidence includes training records, incident reporting procedures, and communication logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

AUDIT AND ACCOUNTABILITY

Reference: 3.3

Q9 [3.3.1]

Do you create and retain system audit logs to monitor user activity?

A 'Yes' response indicates that audit logs are generated and maintained. Evidence includes audit log configurations, retention policies, and sample logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q10 [3.3.2]

Do you ensure that audit logs are protected from unauthorized access, modification, and deletion?

A 'Yes' response signifies that safeguards are in place to protect audit logs. Evidence includes access control settings, integrity checks, and backup procedures.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q11 [3.3.3]

Do you regularly review and analyze audit logs for indications of inappropriate or unusual activity?

A 'Yes' response means that audit logs are periodically reviewed. Evidence includes review schedules, analysis reports, and documented follow-up actions.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q12 [3.3.4]

Do you alert appropriate personnel in the event of audit processing failures?

A 'Yes' response indicates that mechanisms are in place to notify personnel of audit failures. Evidence includes alert configurations, notification logs, and incident response procedures.

☐ YES ☐ PARTIAL ☐ NO Explanation:

CONFIGURATION MANAGEMENT

Reference: 3.4

Q13 [3.4.1]

Do you establish and maintain baseline configurations for your systems?

A 'Yes' response signifies that baseline configurations are defined and maintained. Evidence includes configuration management plans, baseline documents, and change logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q14 [3.4.2]

Do you enforce security configuration settings for information technology products employed in your systems?

A 'Yes' response means that security configurations are applied and enforced. Evidence includes configuration guides, compliance checklists, and audit results.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q15 [3.4.3]

Do you track, review, approve, and log changes to your systems?

A 'Yes' response indicates that a formal change management process is in place. Evidence includes change requests, approval records, and change logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q16 [3.4.4]

Do you analyze the security impact of changes prior to implementation?

A 'Yes' response signifies that security impact analyses are conducted before changes are made. Evidence includes impact analysis reports, risk assessments, and approval records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

IDENTIFICATION AND AUTHENTICATION

Reference: 3.5

Q17 [3.5.1]

Do you identify and authenticate users before granting system access?

A 'Yes' response indicates that user identification and authentication mechanisms are in place. Evidence includes authentication policies, user credentials, and access logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q18 [3.5.2]

Do you use multifactor authentication for network access to privileged accounts?

A 'Yes' response signifies that multifactor authentication is required for privileged access. Evidence includes authentication configurations, policy documents, and access logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q19 [3.5.3]

Do you enforce password complexity and expiration requirements?

A 'Yes' response means that password policies enforce complexity and expiration. Evidence includes password policy documents, system settings, and compliance reports.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q20 [3.5.4]

Do you prohibit the reuse of passwords within a specified number of generations?

A 'Yes' response indicates that password reuse is restricted. Evidence includes password history settings, policy documents, and system configurations.

☐ YES ☐ PARTIAL ☐ NO Explanation:

INCIDENT RESPONSE

Reference: 3.6

Q21 [3.6.1]

Do you establish an incident response capability that includes preparation, detection, analysis, containment, recovery, and user response activities?

A 'Yes' response signifies that a comprehensive incident response plan is in place. Evidence includes the incident response plan, training records, and incident reports.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q22 [3.6.2]

Do you track, document, and report incidents to appropriate officials and/or authorities?

A 'Yes' response means that incidents are formally documented and reported. Evidence includes incident logs, reporting procedures, and communication records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q23 [3.6.3]

Do you test your incident response capability at least annually?

A 'Yes' response indicates that incident response plans are tested regularly. Evidence includes test plans, test results, and lessons learned documentation.

☐ YES ☐ PARTIAL ☐ NO Explanation:

MAINTENANCE

Reference: 3.7

Q24 [3.7.1]

Do you perform regular maintenance on your systems?

A 'Yes' response signifies that systems are maintained according to a schedule. Evidence includes maintenance logs, schedules, and maintenance procedures.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q25 [3.7.2]

Do you control and monitor the use of maintenance tools?

A 'Yes' response means that maintenance tools are managed securely. Evidence includes tool inventories, access logs, and monitoring reports.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q26 [3.7.3]

Do you ensure that maintenance personnel are supervised when performing maintenance activities?

A 'Yes' response indicates that maintenance activities are supervised. Evidence includes supervision logs, visitor access records, and maintenance policies.

☐ YES ☐ PARTIAL ☐ NO Explanation:

MEDIA PROTECTION

Reference: 3.8

Q27 [3.8.1]

Do you protect information on media during transport outside of controlled areas?

A 'Yes' response signifies that media is secured during transport. Evidence includes transport policies, encryption procedures, and transport logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q28 [3.8.2]

Do you sanitize or destroy media containing CUI before disposal or reuse?

A 'Yes' response means that media is properly sanitized or destroyed. Evidence includes sanitization procedures, destruction logs, and policy documents.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q29 [3.8.3]

Do you limit access to CUI on media to authorized users?

A 'Yes' response indicates that media access is restricted. Evidence includes access control lists, authorization records, and access logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

PERSONNEL SECURITY

Reference: 3.9

Q30 [3.9.1]

Do you screen individuals prior to authorizing access to systems containing CUI?

A 'Yes' response signifies that background checks are conducted. Evidence includes screening policies, background check records, and access authorization documents.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q31 [3.9.2]

Do you ensure that CUI is removed from systems before individuals are terminated or transferred?

A 'Yes' response means that CUI is secured during personnel changes. Evidence includes termination procedures, transfer checklists, and access revocation records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

PHYSICAL PROTECTION

Reference: 3.10

Q32 [3.10.1]

Do you limit physical access to systems containing CUI to authorized individuals?

A 'Yes' response indicates that physical access controls are in place. Evidence includes access control policies, access logs, and physical security measures.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q33 [3.10.2]

Do you escort visitors and monitor visitor activity?

A 'Yes' response signifies that visitor access is controlled and monitored. Evidence includes visitor logs, escort procedures, and monitoring records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q34 [3.10.3]

Do you maintain audit logs of physical access?

A 'Yes' response means that physical access is logged. Evidence includes access logs, monitoring reports, and audit procedures.

☐ YES ☐ PARTIAL ☐ NO Explanation:

RISK ASSESSMENT

Reference: 3.11

Q35 [3.11.1]

Do you periodically assess the risk to organizational operations, assets, and individuals?

A 'Yes' response indicates that risk assessments are conducted regularly. Evidence includes risk assessment reports, methodologies, and schedules.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q36 [3.11.2]

Do you scan for vulnerabilities in your systems and applications periodically and when new vulnerabilities are identified?

A 'Yes' response signifies that vulnerability scanning is performed. Evidence includes scan reports, schedules, and remediation records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q37 [3.11.3]

Do you remediate vulnerabilities in accordance with risk assessments?

A 'Yes' response means that identified vulnerabilities are addressed based on risk. Evidence includes remediation plans, risk assessment reports, and change logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

SECURITY ASSESSMENT

Reference: 3.12

Q38 [3.12.1]

Do you periodically assess the security controls in your systems to determine their effectiveness?

A 'Yes' response indicates that security control assessments are conducted. Evidence includes assessment reports, methodologies, and schedules.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q39 [3.12.2]

Do you develop and implement plans of action to correct deficiencies and reduce vulnerabilities?

A 'Yes' response signifies that POA&Ms are used to address security gaps. Evidence includes POA&M documents, remediation plans, and tracking records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q40 [3.12.3]

Do you monitor security controls on an ongoing basis to ensure their effectiveness?

A 'Yes' response means that continuous monitoring is performed. Evidence includes monitoring reports, logs, and review schedules.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q41 [3.12.4]

Do you develop, document, and maintain a system security plan (SSP) that describes system boundaries, operational environment, and security requirements?

A 'Yes' response indicates that an SSP is in place and up to date. Evidence includes the SSP document, update logs, and approval records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

SYSTEM AND COMMUNICATIONS PROTECTION

Reference: 3.13

Q42 [3.13.1]

Do you monitor, control, and protect communications at external boundaries and key internal boundaries of your systems?

A 'Yes' response signifies that boundary protections are implemented. Evidence includes network diagrams, firewall configurations, and monitoring logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q43 [3.13.2]

Do you employ cryptographic methods to protect CUI during transmission?

A 'Yes' response means that encryption is used for transmitting CUI. Evidence includes encryption policies, configurations, and transmission logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q44 [3.13.5]

Do you implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks?

A 'Yes' response indicates that demilitarized zones (DMZs) or similar architectures are used. Evidence includes network architecture diagrams, configurations, and access control policies.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q45 [3.13.11]

Do you employ FIPS-validated cryptography when protecting CUI?

A 'Yes' response signifies that FIPS-validated cryptographic modules are used. Evidence includes cryptographic module certificates, configurations, and policy documents.

☐ YES ☐ PARTIAL ☐ NO Explanation:

SYSTEM AND INFORMATION INTEGRITY

Reference: 3.14

Q46 [3.14.1]

Do you identify, report, and correct system flaws in a timely manner?

A 'Yes' response indicates that a process exists for managing system flaws. Evidence includes flaw remediation procedures, reports, and timelines.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q47 [3.14.2]

Do you provide protection from malicious code at appropriate locations within your systems?

A 'Yes' response signifies that anti-malware measures are in place. Evidence includes anti-malware policies, software configurations, and scan logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q48 [3.14.3]

Do you monitor system security alerts and advisories and take appropriate actions in response?

A 'Yes' response means that security alerts are actively monitored and addressed. Evidence includes monitoring procedures, alert logs, and response records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

COMPLIANCE SCORE SUMMARY

Control Domain	Questions	Points Earned	Max Points	Score %
Access Control	5	___	10	___ %
Awareness and Training	3	___	6	___ %
Audit and Accountability	4	___	8	___ %
Configuration Management	4	___	8	___ %
Identification and Authentication	4	___	8	___ %
Incident Response	3	___	6	___ %
Maintenance	3	___	6	___ %
Media Protection	3	___	6	___ %
Personnel Security	2	___	4	___ %
Physical Protection	3	___	6	___ %
Risk Assessment	3	___	6	___ %
Security Assessment	4	___	8	___ %
System and Communications Protection	4	___	8	___ %
System and Information Integrity	3	___	6	___ %
TOTAL	**48**	___	**96**	___ **%**

SCORE INTERPRETATION

- **90–100% — Strong Compliance**
  Organization demonstrates robust controls across all domains. Minor improvements may be needed.
- **70–89% — Moderate Compliance**
  Most controls are in place but notable gaps exist. Remediation plan recommended within 90 days.
- **50–69% — Partial Compliance**
  Significant gaps in compliance posture. Prioritized remediation required. Consider engaging a consultant.
- **Below 50% — Non-Compliant**
  Organization does not meet minimum compliance requirements. Immediate action required.

ATTESTATION

Assessed by: _____ Signature: _____

Title: _____ Date: _____

Reviewed by: _____ Signature: _____

Title: _____ Date: _____

authorized auditor) for official compliance validation.