CMMC

Compliance Assessment Questionnaire

63 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: 126 (63 questions × 2 points each)

ACCESS CONTROL

Reference: 3.1

Q1 [3.1.1]

Are access control policies established and documented?

Provide policies and procedures that outline access control measures.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q2 [3.1.2]

Is access to systems and data limited to authorized users?

Evidence of user access lists and authorization procedures.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q3 [3.1.5]

Are access control devices audited regularly?

Records of audits and reviews of access control devices.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q4 [3.1.6]

Are remote access sessions restricted and managed?

Remote access logs and restrictions documentation.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q5 [3.1.8]

Is separation of duties enforced through access restrictions?

Role-based access control lists and separation of duties policies.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q6 [3.1.22]

Is external system access limited to authorized connections?

List of authorized external connections and monitoring reports.

☐ YES ☐ PARTIAL ☐ NO Explanation:

AWARENESS AND TRAINING

Reference: 3.2

Q7 [3.2.1]

Is security awareness training provided regularly to personnel?

Records of training sessions and attendance logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q8 [3.2.2]

Are personnel trained to recognize and report potential insider threats?

Training materials and incident reporting procedures.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q9 [3.2.3]

Is role-based security training provided based on specific responsibilities?

Curriculum outlines and role-specific training documentation.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q10 [3.2.1, 3.2.3]

Is refresher training mandatory following significant updates?

Training schedule and update logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

AUDIT AND ACCOUNTABILITY

Reference: 3.3

Q11 [3.3.1]

Are audit logs maintained for all critical systems?

Audit logs and retention policies.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q12 [3.3.2]

Are audit logs reviewed regularly for anomalous activity?

Review schedules and analysis reports.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q13 [3.3.3]

Are audit logs protected from unauthorized access or modifications?

Access control policies for audit logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q14 [3.3.5]

Are log changes detected and reported?

Log monitoring tools and alteration reports.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q15 [3.3.9]

Are audit logging processes tested and verified?

Testing results and verification documentation.

☐ YES ☐ PARTIAL ☐ NO Explanation:

CONFIGURATION MANAGEMENT

Reference: 3.4

Q16 [3.4.1]

Are configuration settings defined and documented for all systems?

Configuration setting documents and baselines.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q17 [3.4.2]

Are changes to configuration settings tracked and approved?

Change management logs and approval records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q18 [3.4.3]

Are unauthorized changes to configurations detected and corrected?

Monitoring logs and incident reports on unauthorized changes.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q19 [3.4.5]

Is software inventory maintained and regularly updated?

Software inventory records and update schedules.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q20 [3.4.6]

Are system configurations periodically reviewed against the baseline?

Review schedules and baseline comparison reports.

☐ YES ☐ PARTIAL ☐ NO Explanation:

IDENTIFICATION AND AUTHENTICATION

Reference: 3.5

Q21 [3.5.1]

Are unique identifiers assigned to all users and devices?

Identification policies and user/device ID records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q22 [3.5.2]

Is multifactor authentication implemented for access to sensitive systems?

Multifactor authentication setup and logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q23 [3.5.3]

Are password policies enforced and regularly reviewed?

Documentation of password policies and review records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q24 [3.5.5]

Are inactive accounts disabled or removed after a defined period?

Account management procedures and deactivation logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q25 [3.5.10]

Are authentication attempts monitored for unusual activity?

Logs and reports of authentication monitoring.

☐ YES ☐ PARTIAL ☐ NO Explanation:

INCIDENT RESPONSE

Reference: 3.6

Q26 [3.6.1]

Is there an established incident response plan?

Incident response plan documentation and approval records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q27 [3.6.2]

Are incidents reported and documented in accordance with procedures?

Incident reports and documentation procedures.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q28 [3.6.3]

Are incident response activities regularly tested and updated?

Test results and update logs of incident response plans.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q29 [3.6.1, 3.6.3]

Is personnel trained in incident response roles and responsibilities?

Training materials and personnel records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

MAINTENANCE

Reference: 3.7

Q30 [3.7.1]

Are maintenance processes and schedules documented and reviewed?

Maintenance schedule and review records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q31 [3.7.2]

Is maintenance conducted by authorized personnel only?

Authorization records and maintenance logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q32 [3.7.4]

Are maintenance tools inspected and secured?

Tool inspection records and security procedures.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q33 [3.7.6]

Is remote maintenance of systems restricted and monitored?

Remote maintenance access logs and restriction policies.

☐ YES ☐ PARTIAL ☐ NO Explanation:

MEDIA PROTECTION

Reference: 3.8

Q34 [3.8.1]

Are media containing sensitive information identified and protected?

Inventory and labeling records of sensitive media.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q35 [3.8.3]

Is data destructed using approved methods when no longer needed?

Documentation of data destruction procedures and logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q36 [3.8.5]

Is access to media restricted to authorized personnel?

Access control lists for storage areas.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q37 [3.8.6]

Are media sanitization processes audited for effectiveness?

Audit reports and effectiveness evaluations.

☐ YES ☐ PARTIAL ☐ NO Explanation:

PERSONNEL SECURITY

Reference: 3.9

Q38 [3.9.1]

Are personnel security policies defined and reviewed?

Policies and review documentation.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q39 [3.9.2]

Are background checks conducted on personnel prior to granting access?

Records of background checks and access authorizations.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q40 [3.9.1, 3.9.2]

Are security policies communicated to all employees?

Communication records and acknowledgment receipts.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q41 [3.9.1]

Are personnel re-evaluated for security clearance periodically?

Re-evaluation schedules and clearance records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

PHYSICAL PROTECTION

Reference: 3.10

Q42 [3.10.1]

Are physical access controls implemented at all entry points?

Documentation of access controls and security measures.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q43 [3.10.2]

Is physical access to sensitive areas restricted and monitored?

Access logs and monitoring records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q44 [3.10.4]

Are physical security controls reviewed and tested regularly?

Review logs and test documentation.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q45 [3.10.6]

Are visitor access records maintained and reviewed?

Visitor logs and review schedules.

☐ YES ☐ PARTIAL ☐ NO Explanation:

RISK ASSESSMENT

Reference: 3.11

Q46 [3.11.1]

Is a risk assessment process defined and documented?

Risk assessment documents and processes.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q47 [3.11.2]

Are risk assessments performed periodically?

Risk assessment schedules and result reports.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q48 [3.11.3]

Are identified risks prioritized and mitigated effectively?

Risk mitigation plans and prioritization records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q49 [3.11.1, 3.11.2]

Are risk assessments updated following significant changes?

Change logs and updated risk assessments.

☐ YES ☐ PARTIAL ☐ NO Explanation:

SECURITY ASSESSMENT

Reference: 3.12

Q50 [3.12.1]

Is a security assessment policy defined and in practice?

Security assessment policies and implementation records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q51 [3.12.2]

Are system security assessments conducted to verify compliance?

Assessment schedules and compliance reports.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q52 [3.12.3]

Are security control deficiencies documented and remediated promptly?

Deficiency reports and remediation plans.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q53 [3.12.4]

Are periodic security assessments reviewed by management?

Review records and management feedback.

☐ YES ☐ PARTIAL ☐ NO Explanation:

SYSTEM AND COMMUNICATIONS PROTECTION

Reference: 3.13

Q54 [3.13.1]

Are network boundaries controlled and monitored?

Network diagrams and monitoring logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q55 [3.13.2]

Are communication protocols protected from unauthorized access?

Protocol security settings and protection records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q56 [3.13.3]

Are cryptographic mechanisms used to protect data integrity?

Encryption policies and implementation records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q57 [3.13.5]

Is information output from systems checked for accuracy?

Output validation procedures and logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q58 [3.13.16]

Are system communications monitored for security violations?

Communication monitoring logs and violation reports.

☐ YES ☐ PARTIAL ☐ NO Explanation:

SYSTEM AND INFORMATION INTEGRITY

Reference: 3.14

Q59 [3.14.1]

Are systems regularly scanned to identify vulnerabilities?

Scan schedules and vulnerability reports.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q60 [3.14.2]

Are anti-malware measures implemented and updated regularly?

Anti-malware policies and update logs.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q61 [3.14.3]

Is unauthorized software installation prevented?

Software installation policies and enforcement records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q62 [3.14.5]

Are security alerts monitored and addressed promptly?

Alert monitoring systems and response records.

☐ YES ☐ PARTIAL ☐ NO Explanation:

Q63 [3.14.7]

Are integrity verification applications in place to detect unauthorized changes?

Verification application logs and change reports.

☐ YES ☐ PARTIAL ☐ NO Explanation:

COMPLIANCE SCORE SUMMARY

Control Domain	Questions	Points Earned	Max Points	Score %
Access Control	6	___	12	___ %
Awareness and Training	4	___	8	___ %
Audit and Accountability	5	___	10	___ %
Configuration Management	5	___	10	___ %
Identification and Authentication	5	___	10	___ %
Incident Response	4	___	8	___ %
Maintenance	4	___	8	___ %
Media Protection	4	___	8	___ %
Personnel Security	4	___	8	___ %
Physical Protection	4	___	8	___ %
Risk Assessment	4	___	8	___ %
Security Assessment	4	___	8	___ %
System and Communications Protection	5	___	10	___ %
System and Information Integrity	5	___	10	___ %
TOTAL	**63**	___	**126**	___ **%**

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.