CMMC 2.0 Level 1 Compliance Checklist

The security requirements in CMMC Level 1 are based on FAR 52.204-21. Assessment objectives are provided for each requirement and are based on existing criteria in NIST SP 800-171A that has been modified for FCI rather than CUI.

Access control

- [ ] **AC.L1-B.1.I: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).**

ASSESSMENT OBJECTIVES:

Determine if:
[a] authorized users are identified;
[b] processes acting on behalf of authorized users are identified;
[c] devices (and other systems) authorized to connect to the system are identified;
[d] system access is limited to authorized users;
[e] system access is limited to processes acting on behalf of authorized users; and
[f] system access is limited to authorized devices (including other systems).

- [ ] **AC.L1-B.1.II: Limit information system access to the types of transactions and functions that authorized users are permitted to execute.**

ASSESSMENT OBJECTIVES:

Determine if:
[a] the types of transactions and functions that authorized users are permitted to execute are defined; and
[b] system access is limited to the defined types of transactions and functions for authorized users.

- [ ] **AC.L1-B.1.III: Verify and control/limit connections to and use of external information systems.**

ASSESSMENT OBJECTIVES:

Determine if:
[a] connections to external systems are identified;
[b] the use of external systems is identified;
[c] connections to external systems are verified;
[d] the use of external systems is verified;
[e] connections to external systems are controlled/limited; and
[f] the use of external systems is controlled/limited.

- [ ] **AC.L1-B.1.IV: Control information posted or processed on publicly accessible information systems.**

ASSESSMENT OBJECTIVES:

Determine if:
[a] individuals authorized to post or process information on publicly accessible systems are identified;
[b] procedures to ensure [FCI] is not posted or processed on publicly accessible systems are identified;
[c] a review process is in place prior to posting of any content to publicly accessible systems;
[d] content on publicly accessible systems is reviewed to ensure that it does not include [FCI]; and
[e] mechanisms are in place to remove and address improper posting of [FCI].

Information and authentication

- [ ] **IA.L1-B.1.V: Identify information system users, processes acting on behalf of users, or devices.**

ASSESSMENT OBJECTIVES:

Determine if:
[a] system users are identified;
[b] processes acting on behalf of users are identified; and
[c] devices accessing the system are identified.

- [ ] **IA.L1-B.1.VI: Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.**

ASSESSMENT OBJECTIVES:

Determine if:
[a] the identity of each user is authenticated or verified as a prerequisite to system access;
[b] the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access; and
[c] the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.

Media protection

- [ ] **MP.L1-B.1.VII: Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.**

ASSESSMENT OBJECTIVES:

Determine if:
[a] system media containing [FCI] is sanitized or destroyed before disposal; and
[b] system media containing [FCI] is sanitized before it is released for reuse.

Physical protection

- [ ] **PE.L1-B.1.VIII: Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.**

ASSESSMENT OBJECTIVES:

Determine if:
[a] authorized individuals allowed physical access are identified;
[b] physical access to organizational systems is limited to authorized individuals;
[c] physical access to equipment is limited to authorized individuals; and
[d] physical access to operating environments is limited to authorized individuals.

Physical protection (cont'd)

- [ ] **PE.L1-B.1.IX: Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.**

ASSESSMENT OBJECTIVES:

Determine if:
[a] visitors are escorted;
[b] visitor activity is monitored;
[c] audit logs of physical access are maintained;
[d] physical access devices are identified;
[e] physical access devices are controlled; and

System and communications protection

- [ ] **SC.L1-B.1.X: Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.**

ASSESSMENT OBJECTIVES:

Determine if:
[a] the external system boundary is defined;
[b] key internal system boundaries are defined;
[c] communications are monitored at the external system boundary;
[d] communications are monitored at key internal boundaries;
[e] communications are controlled at the external system boundary;
[f] communications are controlled at key internal boundaries;
[g] communications are protected at the external system boundary; and
[h] communications are protected at key internal boundaries.

- [ ] **SC.L1-B.1.XI: Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.**

ASSESSMENT OBJECTIVES:

Determine if:
[a] publicly accessible system components are identified; and
[b] subnetworks for publicly accessible system components are physically or logically separated from internal networks.

System and information integrity

- [ ] **SI.L1-B.1.XII: Identify, report, and correct information and information system flaws in a timely manner.**

ASSESSMENT OBJECTIVES:

Determine if:
[a] the time within which to identify system flaws is specified;
[b] system flaws are identified within the specified time frame;
[c] the time within which to report system flaws is specified;
[d] system flaws are reported within the specified time frame;
[e] the time within which to correct system flaws is specified; and
[f] system flaws are corrected within the specified time frame.

- [ ] **SI.L1-B.1.XIII: Provide protection from malicious code at appropriate locations within organizational information systems.**

ASSESSMENT OBJECTIVES:

Determine if:
[a] designated locations for malicious code protection are identified; and
[b] protection from malicious code at designated locations is provided.