McKonly & Asbury
Tax | Assurance | Consulting | Accounting

Camp Hill | Lancaster | Bloomsburg | Philadelphia
macpas.com | 800-569-5199

CMMC Key Document Checklist

As part of our commitment to your success, we provide the checklist below as a resource to support your journey to CMMC Level 2 compliance. The checklist outlines key requirement areas and their corresponding descriptions, giving your team clear visibility into what is expected across each domain. By organizing complex cybersecurity standards into a structured, easy-to-reference format, this guide helps clarify scope, highlight critical components, and make the overall certification process more transparent and manageable.

System Security Plan (SSP) must address/includ the following:

- CMMC L2 Implementation at the objective level (320 objectives)
  - All 110 security controls and their associated 320 objectives described in detail
  - Reference supporting documents where applicable
- An over/description of the CMMC L2 environment
- All applicable roles and responsibilities
- Version/revision history
- Network diagram
- CUI (Controlled Unclassified Information) diagram

Network Diagrams

- All assets in the categorized asset list should be present on this diagram
- Overall network architecture should be present and apparent
- Should accurately describe the scope of the assessment

CUI (Controlled Unclassified Information) Flow Diagrams:

- Should answer the following questions:
  - Where does CUI enter the environment?
  - Where does the CUI traverse the environment? (in transit)
  - Where is CUI stored in the environment? (at rest)
  - Where does CUI exit the environment?

Categorized Asset List:

- Assets should be categorized IAW the CMMC L2 scoping guide

Shared Responsibility Matrix:

- A good SRM should avoid vague language such as ‘may or may not,’ ‘might,’ ‘possibly,’ when describing the assignment of responsibility.
- The assignment of responsibility should mirror what is in the SSP
- The SRM should specify responsibility down to the objective level
- For objectives marked as shared, what part is OSC’s responsibility, and what part belongs to SRM owner?

CYBER AB CMMC CERTIFICATION
AUTHORIZED C3PAO