CMMC 2.0 Level 2 Pre-Assessment Scoping Exercise

Pre-Engagement Data Flow Diagram Questions

Purpose: The CMMC Data Flow Diagram clearly documents how Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) are received, processed, stored, transmitted, and disposed of within the organization. This diagram:

- Defines the in-scope system boundary for CMMC assessment.
- Identifies people, processes, systems, and third parties that touch FCI/CUI.
- Justifies inclusions and exclusions for scoping.
- Supports risk analysis, control mapping, and assessor validation.
- Communicates a shared understanding of the data environment across executives, IT/security, and compliance staff.

Core Scoping Questions

Contractual & Data Scope

1. Which contracts obligate you to protect FCI and/or CUI?
2. What specific types of information do you consider CUI in your operations?
3. How is this information initially received (email, portal upload, DoD system, subcontractor, physical media)?

System Inventory

1. What systems, applications, or services process or store this data?
2. Which are on-premises, which are cloud/SaaS?
3. Are there any systems that share infrastructure with CUI systems but don’t handle CUI themselves?

Data Flow & Boundaries

1. How does the data move internally (between apps, file shares, databases, user devices)?
2. Where does it leave your organization (deliverables, suppliers, DoD portals)?
3. Are there network zones or enclaves (segregated environments) for CUI?

Users & Access

1. Which internal roles/users have access to FCI/CUI?
2. Do contractors or third parties access it?

3. What authentication methods are used (MFA, CAC, SSO)?
4. Are personal/BYOD devices allowed?

Storage & Retention

1. Where is the data stored at rest (servers, SharePoint, CAD vaults, backups)?
2. How long is it retained?
3. How is it disposed of at end of life?

External & Third-Party Dependencies

1. Which vendors, MSPs, or subcontractors handle FCI/CUI on your behalf?
2. Are you relying on inherited controls (e.g., GCC High, AWS GovCloud)?

Physical & Environmental Controls

1. Where is the data physically located (data centers, offices, manufacturing floor)?
2. Who has physical access to those systems or facilities?

Security Controls Context

1. What security controls already protect these flows (encryption, access control, logging, backups)?
2. Are there any gaps or exceptions already identified?

General Contract Questions (applies to both Prime & Sub)

Contract Details

1. Contract number(s), task orders, delivery orders.
2. Period of performance (start/end dates).
3. Prime vs. Subcontractor role.

Clauses & Requirements

1. Which DFARS clauses are present? (7012, 7019, 7020, 7021)
2. Any export control requirements (ITAR/EAR)?
3. Does the contract specify CMMC level (1 vs 2)?

Data Scope

1. Does the contract require handling FCI only, or CUI?
2. What specific types of FCI/CUI are expected
   (e.g., technical drawings, specifications, personnel info, financial records)?
3. How will the data be delivered
   (DoD portals, encrypted email, physical media, subcontractor hand-off)?

Retention & Destruction

1. Are there minimum or maximum retention requirements?
2. Are destruction or sanitization procedures specified?

Incident Reporting & Cloud Use

1. Is there a timeline for incident reporting (usually 72 hours under DFARS 7012)?
2. Are you allowed to use cloud services, and if so, must they be FedRAMP Moderate/High?

Points of Contact

1. Who is the internal contract manager?
2. Who is the external KO (contracting officer) or COR?

If You Are the Prime Contractor

Subcontractor Identification

1. Which subcontractors are receiving FCI/CUI under this contract?
2. What type of data will each subcontractor receive?

Flow-Down Obligations

1. What clauses and obligations are you required to flow down (DFARS, ITAR/EAR, CMMC)?
2. Do subcontractors have to achieve a certain CMMC level?

Data Transmission

1. How will FCI/CUI be shared with subcontractors (portal, DoD SAFE, secure FTP, encrypted email)?

Oversight & Assurance

1. Are you required to validate subcontractors' compliance (SPRS scores, POA&Ms, certifications)?
2. Do you have the right or obligation to audit subcontractors' cybersecurity posture?

Foreign/Export Issues

1. Are any subcontractors foreign-owned or operating outside the U.S.?
2. Do ITAR/EAR restrictions apply to subcontractor data flows?

Incident Handling

1. If a subcontractor is breached, who reports the incident (the sub or you as the prime)?
2. What contractual reporting chain applies?

If You Are the Subcontractor

Prime Contractor Relationship

1. Who is the prime contractor?
2. What CMMC/DFARS clauses have they flowed down to you?

Data Scope

1. What specific FCI/CUI will the prime provide?
2. Will you need to handle only internal data, or also re-share with lower-tier subs?

Data Transmission

1. How will you receive the data (DoD SAFE, prime's secure portal, encrypted email)?
2. Are there restrictions on how you can transmit or store the data?

Compliance & Evidence

1. Does the prime require proof of your NIST 800-171 self-assessment or SPRS score?
2. Do you need to provide a CMMC certification, or is self-attestation acceptable?
3. Are POA&Ms required to be shared with the prime?

Audit & Oversight

1. Does the prime have contractual rights to audit your environment?
2. Will the prime monitor your compliance posture directly?

Incident Reporting

1. Are you required to report incidents directly to DoD, or only to the prime?
2. What is the reporting chain and timeline?

Points of Contact

1. Who is your POC at the prime for security/compliance issues?