Aona

CUI AI service-scope decision tree

Defence contractors, CMMC programme owners and security architects

Read the complete guide on aona.ai

Determine the contract and data scope before sending CUI to an AI service. DFARS cloud requirements and CMMC assessment boundaries concern the actual provider, service and information handled. A commercial privacy promise, zero-retention setting or security-tool installation does not establish permission or provider suitability.

A fictional contractor considers AI drafting and a security intermediary. The tree identifies the evidence required before any actual controlled-data use.

Synthetic contract and data scenario. The fixture contains no CUI or export-controlled technical information. No provider approval or CMMC assessment result is represented.

Your review

Reviewer: _____ Date: _____

Organisation or team: _____

☐ **Establish the contractual data scope**

Record the originator, applicable clauses, information category and permitted recipients.

☐ **Review each provider boundary**

Distinguish cloud/non-cloud, CUI/security protection data and the actual service evidence.

☐ **Keep the assessment handoff**

Connect the data-flow map, system security plan and customer responsibility matrix to the accountable decision.

Checked items record your review, not a compliance approval or an installed-product test result.

Notes and next actions

Decision and scope: _____

Evidence to collect: _____

Owner and next review date: _____

Review matrix

Question	Finding	Next outcome
Applicable contract and data category established?	No or unknown	Resolve with the contract/data owner before transmitting the proposed controlled information.

Question	Finding	Next outcome
Information is CUI or covered defense information in scope?	Yes in the fictional scenario	Identify every storing, processing and transmitting service.
Information falls outside that category?	Yes, established outside for the assessed material	Review other confidentiality/export obligations; no blanket tool approval follows.
External provider is a cloud service handling covered information?	Yes	Obtain evidence for the applicable DFARS cloud requirements and incident obligations.
Level 2 ESP processes CUI or security protection data?	Yes	Apply the relevant 170.19(c) provider category and document SSP/service/CRM responsibilities.
A security intermediary handles only selected event data?	Data category not established	Assess whether it includes security protection data; do not assume automatic exclusion.
Required service evidence is missing?	Yes	Keep the proposed controlled-data path unapproved until the accountable review resolves it.
Unrestricted synthetic fixture only?	Yes	Use it for a scoped test without presenting the result as CUI authorisation.

The boundary includes intermediaries

- **Origin:** Contract and information category
- **AI service:** Processing, storage and provider evidence
- **Security service:** Content or security protection data handled
- **Decision:** SSP/CRM responsibilities and accountable review

Unrestricted synthetic fixture

This is a teaching note about an invented office bracket. It contains no controlled design, dimensions, materials or defence use. Rewrite a generic maintenance reminder without adding technical information.

Fictional review record

Contract reference: CONTRACT-EX-28.
Controlled-data assumption: a separate proposed record is assumed CUI for the exercise; it is not included in this pack.
Recipients: proposed AI service and proposed security intermediary.
Provider evidence: to be obtained for the actual services before real-data use.
Control test: not run.
Authorisation to use CUI: none represented.

Record actual evidence rather than replacing missing provider requirements with a test result.

Practice files

The complete download pack includes these original working files. Keep their original formats when running or inspecting the examples.

- Unrestricted CUI review fixture (unrestricted-cui-review-fixture.txt)

UNRESTRICTED SYNTHETIC TEACHING INPUT, NOT CUI
Rewrite a generic office-maintenance reminder. No controlled design, dimensions, materials, customer information or defence application is supplied. Do not invent technical detail.

Sources and scope

CUI means controlled unclassified information. ESP means external service provider. SSP means system security plan. CRM means customer responsibility matrix in this service-scope review.

Sources checked 2026-09-21. Review the current requirements and your actual agreement before using this workbook for a real decision. General information, not professional approval or a completed control test. No Aona CMMC certification, FedRAMP status or suitability to receive CUI is asserted. Review its own handling and contractual role before controlled-data use.

DFARS 252.204-7012: Safeguarding covered defense information. Covered-defense-information scope, applicable NIST requirements and external cloud-service FedRAMP Moderate-equivalent and incident obligations.

32 CFR 170.19: CMMC scoping. Assessment boundaries and the distinct treatment of cloud/non-cloud external providers processing CUI, security protection data or neither.