CSSP and cloud preparation

WWT Federal Cloud Services | Reference learning guide v1.2 | 17 September 2026

CSSP means Cybersecurity Service Provider. ATO means Authorization to Operate.

Establish who defends the cloud environment

Cloud preparation connects a defined system, shared platform protections, and the people who operate its defenses. This guide explains those relationships and gives teams a practical way to discuss scope, evidence, and handoff.

Read it with the AWS capability manifest, which separates available tools from the service responsibilities around them.

Four connected responsibilities

Layer	The question it answers
Cloud offering authorization	Which provider services and controls can this mission inherit?
Mission system ATO	Does the mission's Authorizing Official (AO) accept the risk of operating this defined system?
CSSP service authorization	Is this organization authorized to deliver the stated cybersecurity services?
Mission-to-provider alignment	Who covers this mission, with what access, procedures, and evidence?

The DISA connection guide separates cloud offering approval, CSSP alignment, and mission authorization. The provider assessment described in the DoD cybersecurity procedures manual can itself produce an ATO for cybersecurity services. Always name the scope when someone says "ATO." [Sources 1, 3]

Two perspectives, one shared approach

Mission enablement: Establish coverage for a mission: inventory, boundaries, responsibilities, telemetry, incident procedures, and accepted service handoff. The method applies to on-premises, cloud, and hybrid environments.

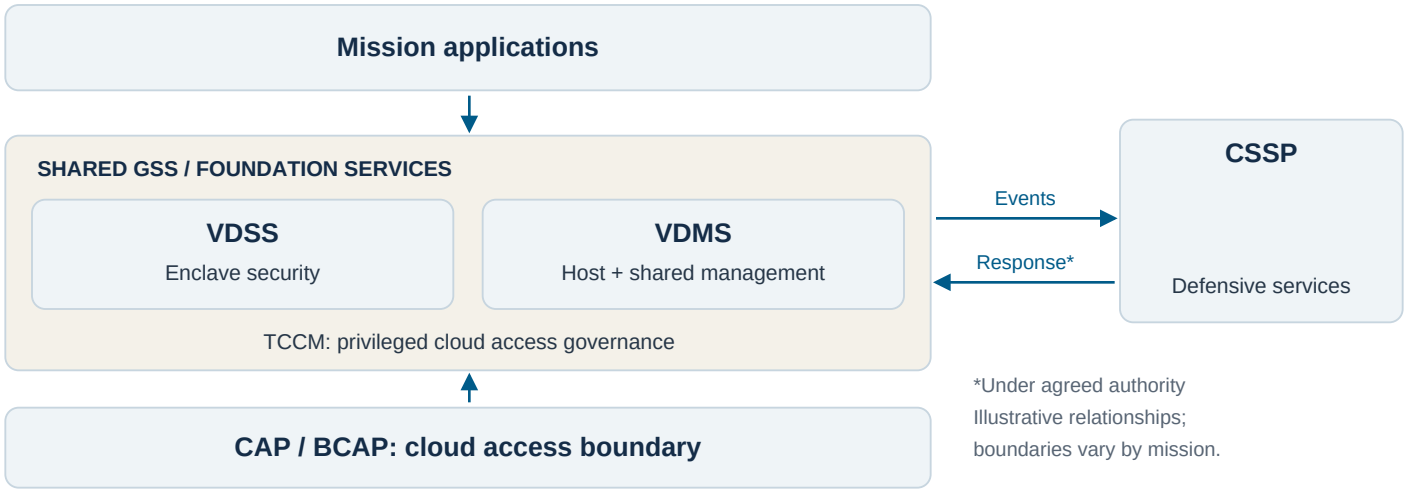
Provider enablement: Help the delivering organization establish or improve the people, procedures, technical integrations, and evidence for its agreed services. Identify whether it supports an existing CSSP, expands an authorized service, or seeks a new provider authorization.

Name the delivering organization and its authorized service scope. A commercial contract or a product name does not by itself establish who holds the provider authorization.

Unpack the cloud foundation

GSS means General Support System. Think of the shared environment, people, and procedures that support applications under common management.

VDMS is the acronym: Virtual Data Center Managed Services. Some DISA material uses "Management Services." VDSS means Virtual Data Center Security Stack. Both appear in the Secure Cloud Computing Architecture (SCCA). [Sources 3, 8]



What each part contributes

VDSS - protect the enclave and its applications. Traffic separation, inspection and filtering, firewall and web application protection, detection, and security-event feeds. [Source 9]

VDMS - administer and sustain shared services. Host protection, vulnerability assessment, configuration and patching, directory and identity services, a separated management network, and centralized logs. [Source 10]

Cloud Access Point (CAP) / Boundary Cloud Access Point (BCAP). Provides the applicable Defense Information Systems Network (DISN) connection to cloud and boundary protection. **TCCM - Trusted Cloud Credential Manager:** governs privileged cloud credentials and access. These are the other SCCA components. [Source 8]

How this fits a GSS

A general support system groups shared resources under common management. VDSS and VDMS capabilities can support that foundation, but their placement, inheritance, and authorization boundaries must be documented for the actual implementation. The diagram shows service relationships, not an approved system boundary. [Source 12; advisory interpretation]

The CSSP uses the visibility and agreed access to deliver defensive services. Establish separately who operates the platform, who analyzes and reports events, and who may direct or execute response. The AO retains authorization decisions.

AWS starting point: Landing Zone Accelerator (LZA) supplies foundation components with documented gaps. Check configuration, approved equivalents, and operating proof. Flow records alone do not establish full packet capture. [Sources 9-11; advisory checks]

Translate cloud into RMF language

The Risk Management Framework (RMF) organizes how we define a system, establish protections, evaluate them, authorize operation, and keep checking. Its seven steps are Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor. [Source 15]

A practical picture of the GSS

A landing zone provides a starting cloud environment: account organization, network layout, identity, logging, and governance. Security and management services can already be part of that design. Adding the names VDSS and VDMS does not necessarily add two new products or two separate builds. [Sources 8-11, 16]

Useful mental model: The landing zone is how the cloud foundation is arranged. VDSS and VDMS describe security and management functions. The GSS describes the shared system, its management, and the services it provides. Document its actual authorization boundary and any separately provided services. [Sources 8, 12, 14; advisory synthesis]

Familiar RMF idea	Cloud example and what to record
System / authorization boundary	Which platform resources belong to this system? Which mission applications and external services have separate boundaries?
Common control	A shared protection, such as centralized audit-log storage, that several applications can use. Name its provider and evidence.
Control inheritance	The application relies on assessed shared protection. Record the protection supplied, its conditions, and the work still owed by the application team.
Control implementation	Document how the selected security or management service is configured, who runs it, and how it meets the requirement.
Assessment	Examine configuration and records, interview responsible people, and test the agreed outcome. An installed tool alone is insufficient evidence.
Authorization	The AO decides whether the defined system may operate with the documented risks.
Continuous monitoring	Keep checking protections, changes, vulnerabilities, and service performance after handoff. CSSP operations contribute to this work.

The examples translate the concepts; they are not a control-by-control assessment or a claim of automatic inheritance. [Sources 13-15]

A fictional example: shared logging

The GSS team runs a protected log collection service. A mission application sends its required events to that service. The CSSP receives agreed visibility and handles assigned defensive activities. The application team still selects the right events and fixes application problems. The record identifies who supplies each part, demonstrates delivery, and documents what the mission can inherit.

How the work proceeds

Two paths share the same scope, responsibility, and evidence record.

Mission path: establish usable coverage

1. **Define the mission.** Identify systems, applications, data sensitivity, deployment locations, connections, mission owner, and AO. Record cloud service model and impact level where applicable.
2. **Confirm the receiving provider.** Establish the designated CSSP and the services its authorization and agreement actually cover. Identify the platform or GSS operator and application owners.
3. **Agree the operating arrangement.** Assign every activity; identify required access, logs, escalation, response authority, service expectations, and evidence delivery.
4. **Connect and demonstrate.** Have the delivery teams configure the agreed integrations. Exercise a safe test event from source through detection, acknowledgment, escalation, action, and closure.
5. **Close gaps and hand over.** Record unresolved items, owners, and decisions. Give the AO the relevant authorization inputs and the operating teams a maintainable service record.

This is our proposed consulting sequence. DISA's guide establishes the alignment and mission-authorization relationship; DoD's Cloud Security Playbook emphasizes early CSSP integration, monitoring access, and incident responsibilities. [Sources 3, 4]

Provider path: prepare the service for evaluation

The 2023 manual describes application and assessment work covering service scope, a concept of operations, architecture, subscribers, self-assessment, evaluation, corrective actions, authorization, and continuing assurance. An existing provider's scope change needs to be evaluated against its current authorization. [Source 1]

Our advisory work would organize:

1. **Service definition:** named authority, customer population, environments, activities, exclusions, and subcontractor roles.
2. **Capability baseline:** staffing, access, tooling, procedures, training, and coverage against the applicable criteria.
3. **Demonstrated performance:** traceable evidence from actual service execution and approved exercises.
4. **Evaluation preparation:** evidence index, rehearsal, findings, remediation ownership, and government evaluation support.
5. **Sustainment handoff:** recurring evidence collection, change review, corrective-action tracking, and reassessment triggers.

Current-policy checkpoint: The official issuances site lists Directive-type Memorandum (DTM) 26-003, *Cybersecurity Service Provider Definition Clarification*. Its text was not retrievable in this research session. Confirm its effect and obtain the applicable evaluator criteria before committing to a provider qualification plan. [Source 7]

Where cloud changes the conversation

Cloud adds a provider relationship and a shared platform boundary to the mission's operating model.

Allocate activities before selecting tools

DTM 24-001, Change 2 dated 7 May 2026, allocates cybersecurity activities among CSSPs, government and commercial entities by service model and impact level. [Source 2]

Verification limit, 17 September 2026: These examples retain the 16 September reading. The full memo was not re-verified; no body hash was retained. Confirm current text before assigning activities.

Illustrative activity in the memo	Stated performer category
External vulnerability scanning; enclave monitoring	Government or commercial entity
Incident categorization and reporting	CSSP
Warning intelligence	Government entity

Confirm allocations against DTM 26-003, component direction and authorization scope. The cloud memo calls for an activity checklist coordinated with the CSSP and AO. Commercial delivery requires agreements, evaluation access and evidence; the mission owner retains responsibility and the AO addresses risk. [Source 2]

Five roles to make explicit

Role	What the advisory should establish
AWS / cloud service provider	Exact offering, region, inherited controls, service limits, and contracted operational activities
Landing-zone or GSS operator	Shared identity, network, configuration, logging, and platform responsibilities
Designated CSSP	Agreed defensive services, required access, reporting paths, and evidence acceptance
Mission / application owner	Application context, remaining controls, change and recovery procedures, and operational contacts
Authorizing Official	Authorization boundary, inherited risk, outstanding gaps, and authorization decision

Confirm these proposed roles with the customer. AWS responsibilities vary by service; its provisional authorization supports control inheritance, not the mission's authorization. [Sources 5, 6]

Practical AWS question: What would AWS deliver, within which boundary and authority? What stays with the mission and CSSP?

A bounded advisory engagement

Proposed work products for discussion. Timing and effort follow scope discovery.

One record, five useful outputs

Work	Reusable input	Proposed handoff output
Scope	Foundations: inventory, ownership, boundaries	Service coverage map and gaps
Allocate	GSS and control-responsibility work	Activity-by-activity owner and authority matrix
Connect	Application dependency mapping: applications and flows	Telemetry and integration requirements with acceptance checks
Demonstrate	Operating procedures and delivery-team evidence	Exercise results, evidence index, and remediation register
Transfer	AO preparation and closeout	Authorization inputs, agreed handoff state and owned gaps

Reuse existing reports. Demonstrations and acceptance follow the commissioned scope. GSS: general support system. ADM: application dependency mapping.

ADM's specific contribution

Application flows identify visibility needs, dependencies, investigation owners and containment risks. They can also inform a later micro-segmentation handoff.

Discovery records establish observed behavior. Receiving teams validate permitted behavior, demonstrate detection and response, and provide enduring coverage after ADM ends.

Reuse the existing engagement record

Reuse roles/RACI, interconnects and monitoring notes, evidence, exercises and decisions. These feed CONOPS, the GSS exit receipt and closeout; unresolved gaps retain owners and next actions.

For each cybersecurity activity, check:

- **Scope:** boundary, service model, impact level, accounts and locations.
- **Basis:** source version, permitted performer, authorization or agreement.
- **Delivery:** accountable organization, team, contact and service expectations.
- **Integration:** data, access, sensor/log path, dependencies and implementation owner.
- **Proof:** acceptance check, dated evidence, reviewer and observed result.
- **Decision:** status, gap, action owner, due date and risk-decision reference.

Describe progress as proposed, agreed, configured, demonstrated or accepted; no new system fields. Record authorized acceptance by person, scope and date. Demonstration does not confer authorization.

Start with a service-scope workshop

A proposed 60-minute discovery meeting with the mission or service owner, CSSP lead, cloud operator, AO representative, and WWT delivery lead.

Start from disciplines you already know

Established enterprise-management and compliance disciplines offer useful starting points. These are teaching analogies, not a claim that different regulatory regimes are equivalent.

Familiar discipline	Connection to this work
Asset inventory and configuration baselines	Define the supported system and the shared management capabilities.
Controlled changes and evidence of execution	Record intended configuration, authorized changes, test results, and drift.
Audit trails and attributable actions	Show what happened, when, who acted, and whether the record can be trusted.
Approval authority and separation of duties	Name the operator, defender, assessor, and risk decision-maker. Change approval and system authorization answer different questions.

What the advisory needs to establish

First, clarify and map: inventory capabilities, owners, evidence, and gaps. **Scope implementation where a gap requires it.** Instrumenting means configuring sensors, logs, and connections so an operating team can see what is happening. Specify who installs, tunes, and operates them; additional delivery scope needs an explicit agreement.

Questions that settle the engagement

1. Are we enabling a subscriber mission, improving an existing CSSP service, or preparing a prospective provider for evaluation?
2. What organization holds the relevant authorization today, and what activities, environments, and subscribers does it cover?
3. For a provider engagement, is the deliverable staff augmentation, an operated service, an integration, or provider evaluation support?
4. Which service models, impact levels, regions, applications, and boundaries are in scope? What is government-retained?
5. Which current policy, component direction, evaluator criteria, and contractual service expectations govern acceptance?
6. Who receives the work, and what demonstration will make that team comfortable accepting it?

Leave with: a one-page scope statement, named receiving owners, a first responsibility matrix, an evidence request list, and the next bounded work package. The advisory team prepares recommendations and evidence; the authorized officials make authorization and risk decisions.

Examples of DoD cybersecurity service providers

Historical inventory: December 2024. GAO published this inventory on 17 September 2025. Reference review: 17 September 2026. These dates do not establish a current authorized-provider roster. [Provider source S1]

Service / context	Example and dated context
Air Force	**16th Air Force.** A separate January 2024 account describes the 688th Cyberspace Wing and its 33rd Cyberspace Operations Squadron; these are operational-unit context, not additional provider listings. [S1, S2]
Army	**U.S. Army Cyber Command** and **DEVCOM C5ISR Center** are two separate providers in the inventory. DEVCOM's center page supports the organizational name. [S1, S6]
Navy	**Navy Cyber Defense Operations Command (NCDOC)**. A May 2025 article describes its CSSP mission and training. [S1, S3]
Navy / supported DoD organizations	**Naval Information Warfare Center Atlantic (NIWC Atlantic)** is a separate entry, with a June 2023 CSSP capability description. Neither Navy entry is presented as the sole provider. [S1, S4]
Marine Corps	**Marine Corps Forces Cyberspace Command (MARFORCYBER)**. Provider-level example; no subordinate-unit assignment is inferred. [S1]
Space Force	**U.S. Space Force.** Retain the provider-level inventory name. The January 2024 Delta 6 account is historical; a current subordinate CSSP designation has not been established here. [S1, S2, S5]
Cross-component services	**Defense Information Systems Agency (DISA)**. GAO recorded external service provision at the inventory date. This does not establish universal eligibility or coverage. [S1]

Illustrative examples only. The applicable CSSP and agreed service coverage are confirmed for each mission environment during discovery and GSS planning. Listing does not imply affiliation, endorsement, or a prescribed provider.

Agency examples and mission scope

GAO's December 2024 inventory also lists CSSPs associated with the following agencies. [Provider source S1]

Acronym	Agency
DIA	Defense Intelligence Agency
DLA	Defense Logistics Agency
MDA	Missile Defense Agency
DTRA	Defense Threat Reduction Agency
DFAS	Defense Finance and Accounting Service
DARPA	Defense Advanced Research Projects Agency
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
NSA	National Security Agency

Listing an agency CSSP does not establish coverage for every agency system. This is an illustrative historical reference, not a referral or assignment directory.

Keep three decisions separate

CSSP coverage: name the provider relationship, agreement status, included assets and services, exclusions, and required feeds and access.

GSS operating ownership: name the shared-service operators and the tasks retained by mission and application teams.

Authorization boundary and controls: document the proposed system, control responsibilities and evidence for the responsible owners and AO to consider. Service coverage may cross boundaries; no universal hierarchy is implied.

Carry discovery into the known record

Record a proposed alignment as proposed. Confirm scope with the designated organizations, identify onboarding dependencies, and assign incident notification, response authority and remediation handoffs. Carry unresolved items with an owner and next action. Reference examples never prepopulate a customer's selected provider or agreement.

Provider sources and naming decisions

Last reference verification: 17 September 2026. S1 was retrieved directly. S2-S4 were checked through indexed official-page text; direct automated retrieval returned HTTP 403 and no full-body hash was retained. This is a source review, not verification of a provider's current authorization or mission coverage.

Dated source register

S1. GAO-25-107121: DOD Cyberspace Operations: About 500 Organizations Have Roles, with Some Potential Overlap. Published **17 September 2025**; Appendix VIII, Table 5. **Inventory effective: December 2024.** Last verified: **17 September 2026**.

S2. Integrating space into Information Warfare. 16th Air Force Public Affairs / U.S. Cyber Command. Published **16 January 2024**. Inventory effective: not applicable; dated operational account. Last verified: **17 September 2026**, indexed official text.

S3. TRIDENT Training Center Opens - NCDOC Hosts Ribbon Cutting Ceremony. U.S. Fleet Forces Command. Published **27 May 2025**. Inventory effective: not applicable. Last verified: **17 September 2026**, indexed official text. Its broad sole-provider wording is not adopted: S1 separately lists NIWC Atlantic.

S4. NIWC Atlantic Cyber Security Service Provider (CSSP). NIWC Atlantic. Published **22 June 2023**. Inventory effective: not applicable. Last verified: **17 September 2026**, indexed official capability description. Use the publisher's "Naval Information Warfare Center Atlantic" name; GAO labels it "Navy Information Warfare Center Atlantic."

S5. USSF Space Systems Command Announces Formation of Defensive Cyber Squadrons. Published **23 March 2026**. Inventory effective: not applicable. Last verified: **17 September 2026**, official printable article. It reports organizational changes; it does not establish Delta 6's current CSSP designation. Current subordinate-unit wording is therefore omitted.

S6. DEVCOM C5ISR Center. DEVCOM. Publication date: **not stated**. Inventory effective: not applicable. Last verified: **17 September 2026**, indexed official page. Used for the organizational name; S1 supplies the historical CSSP entry.

Sources and verification limits

Source register and limits

The educational source baseline was reviewed on 16 September 2026. This 17 September update clarifies record reuse and verification limits and adds the separately dated provider examples above. Sources 1 and 2 were not re-verified and no retained full-text hash is available; Source 7 remains a full-text hold. Government documents retain their published edition names.

1. DoDM 8530.01, Cybersecurity Activities Support Procedures, 31 May 2023. Appendix 4A: provider assessment, authorization, application and maintenance. Baseline process; reconcile newer direction.

2. DTM 24-001, Cloud Cybersecurity Activities, Change 2, 7 May 2026. Attachment 3, sections 1-2 and Table 1: activity allocation and commercial delivery. Retrieved version extends expiry to 27 February 2028.

3. DISN Connection Process Guide, version 6.1, March 2023. Appendix C.3.4 and C.4: CSSP alignment and mission authorization. A process guide, not new policy.

4. DoD CIO Cloud Security Playbook, Volume 1, Play 12, p.56. CSSP integration, shared incident responsibilities, and early log access. Relevant section retrieved through official indexed text.

5. AWS DoD SRG compliance. Provider explanation of provisional authorization and customer obligations; no specific customer's service scope was verified.

6. AWS shared-responsibility model. Infrastructure and customer responsibilities depend on the selected services.

7. Official issuances announcements. Lists DTM 26-003. Full text could not be retrieved; its detailed requirements, effective status, and effect on earlier guidance remain a verification item.

8. AWS: SCCA components. Component names and relationships.

9. AWS: Virtual Data Center Security Stack. Security capabilities and LZA coverage mapping.

10. AWS: Virtual Data Center Managed Services. Shared host and management services; supplemental configuration required.

11. AWS: Landing Zone Accelerator overview. Foundation deployment guidance; LZA alone does not establish compliance.

12. NIST glossary: General support system. Definition sourced to CNSSI 4009-2022 and NIST publications.

13. NIST: Common control and control inheritance. Shared protection and the responsibilities behind reuse.

14. NIST: Authorization boundary. Components included in an authorization; separately authorized connected systems remain distinct.

15. NIST: Risk Management Framework. Seven-step lifecycle.

16. AWS: Landing-zone and account strategy. Starting environment, account organization, networking, and security.

Research boundary: Public sources only; examples are fictional. No contract, customer evidence, system configuration, provider authorization letter, or current evaluator scoring package was inspected. Recommendations here are advisory design, not a finding of compliance or an approved offering. This public learning edition is maintained in the WWT team Reference Studio. Its advisory outputs are proposals for evaluation, not newly committed services.