Prepare the mission. Build the authorization case.

WWT Federal Cloud Services | Cloud Waypoint reference library

Research edition: 19 September 2026. Public sources and fictional examples. This is an educational preparation map, not a complete component-specific authorization checklist.

PREPARE > **IMPLEMENT** > **ASSESS** > **AUTHORIZE** > **MONITOR**

Preparation contributes inputs. Each later stage has its own work, evidence and authority.

One operating model, several decisions

Cloud modernization and authorization preparation share much of the same groundwork: understand the mission, define the system, identify its dependencies, assign responsibilities and collect evidence. Cloud Waypoint can organize that groundwork into reviewable work products while the receiving platform and operating teams prepare their parts.

The practical outcome is a foundation design and draft documentation that the next team can develop further. Actual implementation, control assessment, network connection and authorization remain separate work and decisions.

Decision	What it addresses	Who holds the decision
Provider Provisional Authorization (PA)	The cloud service offering and its conditions	DISA authorizing official in the described DoD cloud process
Interim Authorization to Test (IATT)	Bounded testing in a specified environment and time	The applicable authorizing official
Mission Authorization to Operate (ATO)	Acceptability of risk for the mission system	The mission's applicable authorizing official
Connection approval	Permission for the specified network connection	The responsible connection authority

These are different scopes, not four mandatory steps in one queue. A provider PA is not an early mission ATO. Testing permission is constrained by the written decision. [Sources 1, 2, 3]

Start with five concrete questions

- Which mission system and information are in scope?
- Which services and controls can it actually inherit, with evidence?
- What does the cloud foundation team operate?
- What does the cyber team provide, and who can direct a response?
- What remains with the mission, and who will close each gap?

Follow the work through its lifecycle

The Risk Management Framework (RMF) connects preparation to ongoing operation. NIST SP 800-37 describes the process; SP 800-53 supplies controls, 800-53B supplies baseline guidance and 800-53A supplies assessment procedures. Applicable DoD/component rules determine how these are used for the mission. [Sources 4, 5, 6, 7]

Stage	Preparation work product	What must happen beyond the draft
Prepare	Mission context, boundary proposal, roles and provider map	Confirm decision authority, agreements and actual scope
Categorize	Information types and impact rationale	Responsible authorities validate categorization
Select	Control set, tailoring rationale and inheritance map	Confirm applicable baseline, parameters and provider evidence
Implement	Implementation plan and draft security narratives	Build/configure controls and document actual behavior
Assess	Evidence index, gaps and assessment coordination	Assessors execute the agreed plan and record findings
Authorize	Organized package inputs and unresolved decisions	AO evaluates risk and grants, constrains or denies authorization
Monitor	Cadence, handoffs and change/reassessment triggers	Operating teams perform monitoring and keep evidence current

What an authorization package needs

NIST's authorization-package task identifies security/privacy plans, assessment reports, a plan of action and milestones (POA&M), and an executive summary, with additional information required by the AO. Draft plans are a useful start; they do not substitute for assessed results. [Source 4, task R-1, printed pages 69-70]

Cloud Waypoint's draft System Security Plan (SSP), POA&M, concept of operations (CONOPS), boundary and inheritance work contribute to this preparation. A formal Security Assessment Plan (SAP), Security Assessment Report (SAR), completed remediation and authorization decision remain distinct from our advisory maturity assessment.

Baseline selection is a mission decision

Do not convert IL5 or IL6 directly into a generic control count. National security system categorization uses CNSSI 1253; other systems use the applicable FIPS 199 methodology. Confirm the governing version, overlays and component direction. NIST's 5.2.0 catalog update does not automatically establish the baseline required for an engagement. [Sources 6, 8]

The handshake makes the boundary real

A boundary includes technology, people and process. This proposed scenario follows an application identity making an unexpected database connection. An anomaly prompts investigation; it does not prove compromise.

Event step	Teams involved	The handoff record
1. Detect and receive	Foundation monitoring to cyber intake	Timestamp, resource, alert source, evidence pointer and acknowledgment
2. Understand and validate	Cyber with mission application owner	Expected dependencies, planned changes, mission impact and triage result
3. Notify and decide	Cyber, mission duty lead and foundation lead	Severity, named recipients, requested action and escalation
4. Contain within authority	Authorized incident lead to operators	Approved action, scope, impact, duration and recovery route
5. Recover and accept	Operators to mission service owner, consulting cyber	Service/health checks, residual concerns and recovery acceptance
6. Close and improve	Incident lead, problem owner, ISSM and change authority	Findings, root cause, corrective actions, evidence and reassessment needs

What Foundations and ADM contribute

Foundations documents the operating model, ownership, boundary and required handoffs. Application Dependency Mapping (ADM) adds observed communication context that owners review. Together they help prepare the scenario, expected behavior and documentation to carry into a tabletop exercise.

Runtime monitoring detects the event. The agreed cyber service investigates. Authorized operators act. Those operational services are not delivered merely by drawing the flow or exporting the preparation package.

Four different kinds of evidence

- **Documented design:** the team has described what should happen.
- **Completed tabletop:** participants rehearsed the scenario and recorded actual responses and gaps.
- **Technical test:** evidence shows how configured controls behaved under a test plan.
- **Assessment and decision:** assessors report results; the AO makes the applicable authorization decision.

The diagram is a proposed consulting model. Assignments, notification times and containment authority must be reconciled with actual agreements; none are universal allocations. [Source 3 supports agreement/connection distinctions]

Name the teams. Keep the authorities visible.

Three operating teams

Mission team: business purpose, application behavior, mission impact and retained workload responsibilities.

Cloud foundation team: agreed shared infrastructure and platform services. A commercial Cloud Service Provider (CSP) and the organization operating the landing zone may be different parties. Separate them wherever their commitments differ.

Cyber team / Cybersecurity Service Provider (CSSP): agreed defensive services, such as monitoring, triage and reporting. Identify the delivering organization, covered services and response permissions. A security product or cloud hosting contract alone does not establish CSSP coverage.

Authorities alongside the teams

- **ISSM / ISSO:** information system security manager/officer; coordinates assigned security management and evidence work.
- **SCA / assessor:** security control assessor; evaluates controls and records findings.
- **AO:** authorizing official; retains the authorization and associated risk-acceptance decision.
- **Incident and change authorities:** approve the actions delegated to them; these roles are not automatically the AO or CSSP.
- **Connection authority:** approves the covered network connection separately.

Make responsibility measurable

For each activity name who performs it, who owns completion, who is consulted and who is informed. This is a RACI matrix: Responsible, Accountable, Consulted, Informed. Its accountable role does not acquire the AO's risk-acceptance power.

Record a sender, receiver, acceptance condition, escalation path, evidence location and source agreement for every handoff. Unassigned work stays a named gap.

Where GSS and SCCA fit

A General Support System (GSS) is the shared-system design/management context; its actual boundary must be established. Secure Cloud Computing Architecture (SCCA) describes cloud security functions. Our event walkthrough names the Boundary Cloud Access Point (BCAP). AWS's IL4/IL5 guidance uses the broader name Cloud Access Point (CAP), alongside Virtual Data Center Security Stack (VDSS), Virtual Data Center Managed Services (VDMS), and Trusted Cloud Credential Manager (TCCM). These functions can support a foundation, but a reference architecture is not an authorization. Do not extrapolate this IL4/IL5 description into a complete IL6 design. [Source 9]

A useful package with an honest completion boundary

Our review of the accepted reusable Cloud Waypoint SOW template found a bounded Foundations plus ADM engagement. It includes authorization-preparation drafts and explicitly excludes the complete authorization package and the authorization decision. An executed customer agreement, not this guide, determines contractual scope.

Existing preparation output	Useful contribution	Work still required
Application/dependency register	Current-state context and connection hypotheses	Validate coverage and unresolved observations
GSS exit receipt	Foundation decisions and monitoring ownership	Implement services and execute provider agreements
SSP draft and inheritance map	Boundary, roles and control narratives	Validate actual controls and inherited evidence
POA&M	Owned findings, actions and dates	Perform remediation and verify closure
CONOPS and RACI	Operating responsibilities and handoffs	Agree authority, rehearse and test
Transformation and closeout packages	Sequenced work and explicit handover	Receiving team acceptance and continued delivery

Use the existing tools

Package visibility: Studio's export manifest maps available, partial and unavailable outputs to the navigator. Its Package summary index shows engagement-specific documents, holders, status and next steps. Reuse both; an available export does not establish a complete authorization package. The ISSM and assessor confirm the required artifact list.

Cyber handoffs: use the event walkthrough and its existing incident-step model, alongside Studio's event-handshake instructions and RACI. Confirm the actual CSSP agreement and action authority; the fictional model does not establish either.

Tabletop findings: reuse Studio's Annex G projection of planned or run scenarios and linked corrective actions. A planned walkthrough is not evidence that an exercise occurred.

These existing tools support preparation; they add no contracted deliverable. Receiving-provider onboarding and evidence acceptance still need confirmation. No partner integration or authorization outcome is implied.

What remains unresolved

This research has not verified the full current component-specific IATT checklist, current CNSSI 1253 control tables, all DoD cybersecurity-activity directives, or the operational transition rules accompanying the 2025 Cybersecurity Risk Management Construct announcement. Those holds prevent a claim of complete mission-authorization coverage. They do not prevent using this guide to structure the next conversation with the ISSM, assessor, AO and providers.

Start with the right data call

Use the existing engagement record, decisions, gaps and RACI to capture these answers. Request pointers and authorized access through the client's approved environment; never upload client information to this public library.

Ask for	Confirm with	What it enables
Mission purpose, applications and information types	Mission owner and information owner	A defensible scope and a categorization discussion
Named ISSM, assessor and authorization route	Mission security lead	The right reviewers, required artifacts and decision path
Applicable instructions and versions	ISSM and receiving authority	Requirements grounded in this component's actual process
Proposed boundary and inherited services	Foundation provider, mission and cyber leads	Control ownership, provider evidence and explicit gaps
Monitoring coverage and response agreement	Cyber provider and authorized mission lead	Who receives events, investigates and can authorize action
Observation permissions, coverage and window	Application owners, network team and data custodian	Usable dependency evidence with known limits
Existing plans, diagrams, assessments and open findings	Document owners	Reuse of current work rather than a second document set

Record applicability before asserting coverage

For each governing instruction, record its publisher, version/date, source location, applicability rationale, confirming role and unresolved questions. Keep a working Impact Level hypothesis distinct from the responsible authority's determination. Confirm the specific cloud offering and its conditions; a provider brand alone does not establish inheritance.

Capture restrictions on collection, transfer, storage and disconnected operation. These are delivery constraints to resolve within the executed agreement; they do not create a new disconnected-environment service or authorize handling sensitive data.

Begin the baseline when evidence supports it

Establish the current-state baseline as early as sufficient, representative evidence is available. Record its date, observation period, scope and unknowns. Do not manufacture a complete day-one score to satisfy a calendar. Make later comparisons on compatible scope and positions.

Coordinate the two paths

The accepted executive preview describes an **18-week total engagement**, with the **two-week data call inside the eight-week Foundations period**. These are overlapping activities, not eight weeks plus eighteen more. The existing reusable 20-week SOW variant is separate and unchanged; the executed customer agreement governs delivery dates and scope.

The table below explains dependencies. It adds no contractual milestones or automatic extensions.

When the input is available	Modernization work	Authorization-preparation work
Mission context and existing records	Frame application scope, outcomes and candidate pathways	Identify authority, boundary hypothesis and applicable instructions
Provider and operating-team commitments	Reconcile target services and operating responsibilities	Map inherited controls, retained duties and cyber handoffs
Authorized, representative observations	Review dependency patterns and sequence transition options	Add observed communication context to boundary and control narratives
Owners validate findings and assumptions	Refine transformation priorities and the transition plan	Reconcile draft SSP, CONOPS, RACI, gaps and proposed tabletop
Receiving teams review the package	Agree the next bounded delivery step	Record accepted inputs, remaining assessment work and decisions

If access or an agreement is late

Name the blocked activity, missing input, accountable owner and expected resolution. Record the effect on coverage, confidence and dates. Continue independent work using clearly labeled drafts or declared information. Replan dependent work with the client through the existing change process; do not invent observations or silently move delivery dates.

A missing authority, unresolved handling rule or unavailable observation window stays an explicit gap. Escalate before proceeding with dependent work. Cancellation, paid extensions and new scope require the applicable commercial decision; this guide establishes none of them.

A useful tabletop starts before the meeting

Agree a scenario, the expected flow, participating mission/foundation/cyber roles, action authority and the records each handoff needs. The meeting then tests those expectations. Record what participants actually did and the corrective actions; retain the distinction between a planned scenario, a completed rehearsal and a technical control test.

Read CSRMC alongside RMF

The official September 2025 Cybersecurity Risk Management Construct (CSRMC) publication links its five phases to RMF steps. The mapping below follows the published diagram; it is not a newly invented Cloud Waypoint crosswalk. [Sources 10, 11]

Published CSRMC phase	RMF steps shown in the diagram	Preparation question for the consultant
Design	Prepare, Categorize, Select	Are mission, requirements, teams and inherited services understood?
Build	Implement	Who implements each requirement and supplies monitoring data?
Test	Assess	Who assesses actual behavior, records results and owns remediation?
Onboard	Authorize	Which applicable authorities and providers review admission and conditions?
Operations	Monitor	Who operates monitoring, responds and keeps risk information current?

The third column is our explanatory preparation aid. The diagram also describes NextGen CSSP risk review, onboarding and operational monitoring. It does not establish those permissions for a particular engagement or provider. Confirm the applicable component direction and actual agreements before assigning authority. The AO's authorization decision remains distinct from provider onboarding and incident action permissions.

What this adds to the conversation

The companion tenets emphasize automation, critical controls, continuous monitoring, DevSecOps, survivability, training, inheritance, operationalization, reciprocity and assessment. For our preparation work, the practical questions remain concrete: whose service, whose evidence, whose action and whose decision? [Source 12]

What remains to be verified

We have read the official construct and tenets. We have not verified the complete implementation instructions in force for each component, the applicable current CSP/Mission Owner Security Requirements Guide package, or a component-specific IATT artifact checklist. Do not infer a new authorization route, mandatory control allocation or continuous ATO entitlement from this explanatory map.

Use the client's security lead to confirm the governing process and record the answer with its source. Preserve familiar RMF work products where required; rename or reorganize them only against the receiving authority's instructions.

Make the handover usable

Treat package generation, factual completeness and receiving-team acceptance as three separate checks. Use Studio's existing export manifest, Package summary index, decisions and gaps rather than maintaining a second report register.

Check the actual package with its receiver

- Agree the required artifact list with the ISSM, assessor and receiving delivery team. Available exports are not the contracted deliverable list.

- Identify the record version, selected environment, boundary and evidence period represented by the package. Preserve file versions or digests where the existing exporter supplies them.

- Open the actual files in the agreed receiving tools. Check legibility, field meanings, scope, links, ownership and unresolved blanks. Record the tool/version, result and any transformation still needed.

- Reconcile draft narratives with actual implementation and inherited evidence. An exported SSP draft is not an assessed SSP; an export labeled available may contain incomplete engagement data.

- Record who accepted each handoff, what remains open and who owns the next action. Keep authorization decisions with the designated authority.

At this review, the source registry has **71 entries**. The navigator's **31 mapped rows** comprise **15 exported, 9 partial and 7 not exported**. These describe different inventories, not competing counts or a service promise. Consult the current manifest when assembling a package.

Microsoft Project XML has passed schema checks; a receiving-tool open/save round trip remains unverified. No eMASS or ServiceNow import compatibility is established by these exports. Confirm the receiver's required format and procedure before promising automated loading.

Score what the evidence supports

Progression in the existing maturity model	Required support
0 to 1	Evidence-supported intent, draft or occasional practice
1 to 2	A named client owner confirms the practice is defined and operating
2 to 3	Current operational evidence supports consistent execution
3 to 4	Governed, monitored automation with exception handling

Producing a template does not automatically raise a score. Levels 3 and 4 are not prohibited during an engagement; they require the model's evidence. An agreed target is a client decision, distinct from the measured result.

Sources and use notes

Sources 1-9 reviewed 18 September 2026; CSRMC sources 10-12 retrieved and reviewed 19 September 2026. Publisher documents govern; this guide is an explanatory synthesis. Version-specific and inaccessible material is identified below.

1. DISA - DoD Cloud Authorization Process, June 2024. Pages 4-7 separate cloud PA and mission authorization; page 13 describes cloud offering artifacts.

2. NIST glossary - Interim Authorization to Test. Definition attributed to CNSSI 4009-2022; conditions and time are established by the written authorization.

3. DISA - DISN Connection Process Guide. Retrieved edition 6.1, March 2023; sections 2.7.4, 2.8.3, C.3.4 and C.4. Current component implementation must be confirmed.

4. NIST SP 800-37 Revision 2. December 2018; chapter 3 and task R-1, printed pages 69-70. PDF readable through research browser; direct local download unavailable in this review.

5. NIST SP 800-53 Revision 5. Control catalog; publication page identifies release 5.2.0 updates dated August 2025.

6. NIST SP 800-53B. Baselines and tailoring; release 5.2.0 notice reports no baseline changes in that release.

7. NIST SP 800-53A Revision 5. Assessment procedures; January 2022 publication with release 5.2.0 update notice.

8. NIST glossary - Categorization. Distinguishes CNSSI 1253 and FIPS 199 methodologies. Does not replace the governing control-selection instruction.

9. AWS Prescriptive Guidance - SCCA components. Vendor architectural guidance for IL4/IL5; not a mission authorization or government validation of a deployment.

10. CIO - CSRMC announcement, September 24, 2025. Announces the construct; linked diagrams below were retrieved directly.

11. CIO - Cyber Security Risk Management Construct diagram. One-page diagram, cleared September 23, 2025; explicitly maps five phases to RMF steps. This is not a complete component implementation instruction.

12. CIO - CSRMC strategic tenets. One-page companion, cleared September 23, 2025.

Source holds

The official DoDI 8510.01 PDF, Army PPM CIO-026 PDF and Navy transition memorandum could not be fully retrieved. DTM 24-001 / 26-003 and related CSSP activity allocations retain the earlier verification holds. Search snippets and older local notes were not promoted into current mandatory requirements. The CSRMC announcement and both linked diagrams are verified; governing component implementation details and the applicable current CSP/Mission Owner SRG package remain to be confirmed. An HTTP 200 response from the DISA portal was an application shell, not verification of an SRG revision.

Handling and ownership

Public references and fictional examples only. This material accepts no evidence, credentials, Controlled Unclassified Information (CUI) or client material. AO decisions and provider authorizations remain with their designated authorities. WWT Federal Cloud Services identifies this team learning material; no government endorsement is implied.