AWS components supporting CSSP activities

WWT Federal Cloud Services | Capability manifest v1.1 | 17 September 2026

Start with the defensive service, then choose the components

A Cybersecurity Service Provider (CSSP) delivers an agreed defensive service through people, procedures, access and technology. Amazon Web Services (AWS) components can supply visibility, detection, protection and execution. The operating arrangement connects those capabilities to a mission and its designated defenders.

This manifest covers 28 selected AWS components and component groups. It is an architecture and advisory reference, not an inventory of a deployed customer environment or an executable deployment specification. Its main scope is AWS GovCloud (US). Commercial, Secret and Top Secret environments need their own review.

Read each entry in three layers

- **Capability:** What AWS documents the component can contribute, including region and feature limits.
- **Service delivery:** Our proposed setup, operating owner and demonstration. These are design recommendations, not automatically delivered services.
- **Authority:** The actual offering, impact level, authorization boundary, agreement and permitted performer still govern use. Every entry is unassessed for a mission; the Authorizing Official (AO) retains authorization decisions.

A documented GovCloud service is not proof that every feature is available, included in a particular provisional authorization, enabled in an account or accepted by a CSSP. Confirm the exact offering and inherited controls using the applicable authorization material. AWS DoD scope.

Architecture vocabulary

A General Support System (GSS) is the shared managed system. A landing zone implements its cloud foundation. The Virtual Data Center Security Stack (VDSS) describes security functions; Virtual Data Center Managed Services (VDMS) describes shared host and management functions. They overlap the actual architecture rather than defining a mandatory product bundle. The companion learning guide explains the relationships and includes a diagram.

Reference update: 17 September 2026. The selected AWS feature limits were rechecked against primary documentation; each source retains its own checked date. Other entries retain the 16 September baseline. Role assignments, activity mappings and acceptance checks are our advisory synthesis. Recheck feature support before design acceptance and at scheduled source review.

Follow the signal to an accountable outcome

This sequence is an illustrative integration design. Components are selected for a demonstrated need; the list is not a requirement to deploy all 28.

Stage	AWS building blocks and the human handoff
Define scope	Organizations, Control Tower and IAM establish account and access boundaries. Owners confirm which systems are covered.
Collect	CloudTrail, CloudWatch Logs, VPC Flow Logs and selected network/host sensors supply different kinds of visibility. Teams prove delivery and notice gaps.
Detect and prioritize	GuardDuty, Inspector and posture checks produce findings. Security Hub/CSPM provide supported views. Analysts validate relevance and mission impact.
Investigate	Detective, retained logs and optionally Security Lake help assemble context. The CSSP keeps the case record and evidence trail.
Act and report	Approved playbooks use supported event/workflow tools or the receiving team's case system. Named authorities decide containment and government reporting.
Recover and learn	Platform and application teams restore service, validate outcomes and close corrective actions. The mission authorizes return to operation.

A fictional worked example

A fictional application role makes an unexpected administrative change. CloudTrail records the API action. A supported detection or configured analytic raises a finding; the receiving integration opens a case. An analyst checks the application owner and dependency context, preserves the relevant events, and requests an authorized reversible response. The platform team executes it, the mission verifies service, and the case records reporting and closure.

The proof is the traceable sequence: event, finding, receipt, analyst decision, authority, action, result and closure. A green console or an enabled service does not demonstrate that chain.

RMF cross-reference

The Risk Management Framework (RMF) connects this work to Prepare, Categorize, Select, Implement, Assess, Authorize and Monitor. This manifest mainly helps define scope, describe implementation and plan demonstrations; it does not replace assessment or authorization. NIST RMF.

Control IDs in entries are illustrative discussion pointers from NIST SP 800-53: AC = Access Control; AU = Audit and Accountability; CA = Assessment, Authorization, and Monitoring; CM = Configuration Management; CP = Contingency Planning; IA = Identification and Authentication; IR = Incident Response; RA = Risk Assessment; SC = System and Communications Protection; SI = System and Information Integrity. They are not a selected baseline, complete crosswalk or assessment result. NIST control catalog.

Gaps to settle before committing a service

Responsibilities that a service catalog cannot assign

The actual CSSP agreement must establish staffing and coverage, incident categorization/reporting, threat intelligence handling, escalation, response authority, evidence custody and mission acceptance. A product subscription does not establish an organization's provider authorization. Agency connection services, approved endpoint defense, vulnerability-scanning equivalence, case management and packet-retention needs may require existing government or third-party capabilities.

DoD Directive-type Memorandum (DTM) 24-001, Change 2 (7 May 2026), allocates cloud cybersecurity activities by service model and impact level. The activity examples retain the 16 September educational reading; the full memo was not re-verified for this update and has no retained body hash. Confirm the current text, component direction and service authorization before assigning activities. **DTM 26-003 remains an open verification item:** its complete text could not be retrieved. No new provider eligibility rules, performance deadlines or evaluator criteria from that memorandum are prescribed here. See the guide's source register and limitation.

Specific design checks

- **Detection and blocking:** Establish who reviews a finding and who may change a firewall or isolate a workload. Automatic action needs approved scope and safe failure behavior.
- **Endpoints and vulnerabilities:** Inspector and GuardDuty contribute particular capabilities. Do not assume they replace required host protection or an approved vulnerability-scanning solution.
- **Packets and flows:** Flow metadata supports communication analysis. Packet capture requires suitable collection, retention and retrieval, or an explicitly accepted equivalent.
- **Logs and evidence:** Security Lake is an analytics store. Its buckets do not support S3 Object Lock; use a compatible, separately designed evidence archive where required.
- **GovCloud integrations:** Validate the exact source, target, protocol, region and feature. Commercial tutorials can depend on unavailable features.
- **Conditional services:** The checked Macie endpoint list does not establish GovCloud support. AWS Shield response support or AWS Security Incident Response offerings require separate regional, contractual and authorization review; no CSSP designation is implied or assessed here.

Use the manifest in an engagement

Select the required activity, then record the boundary, impact level, region, exact feature, delivery owner, permitted performer, integration path, acceptance test, evidence reference and remaining gap. Keep **proposed, agreed, configured, demonstrated and accepted** separate. Use the existing engagement record for these facts and cite the selected component IDs, manifest revision and file hash. Keep evidence references, decisions and owned gaps together; this reference does not create another questionnaire or a new CSSP package.

Costs depend on account/resource coverage, telemetry volume, retention, scans, mirrored traffic, analyst workload and recovery tests. Obtain a scoped estimate after selecting components; no price or effort commitment is made here.

Maintenance

Codex maintains this hub-owned reference under the existing source-review workflow. Recheck changed vendor features, regional restrictions, governing policy and broken links; record the decision and revision. Engine/Studio adoption follows its own evaluation and release. Public sources and fictional examples only: do not put client evidence into this library.

Terms used in the component register

Term	Plain-English meaning
API	Application programming interface: a defined way for software or an operator's tool to request an action.
VPC	Virtual private cloud: the network space you define inside AWS.
DNS	Domain Name System: translates names into network addresses; DNS activity can also provide defensive clues.
IAM	Identity and Access Management: identities, roles and permissions for AWS resources.
MFA	Multi-factor authentication: requires different kinds of proof to sign in. A particular government credential still needs its own integration.
CSPM	Cloud Security Posture Management: checks cloud configuration and presents findings. It does not make an authorization decision.
SSM	Systems Manager: AWS host-management capabilities. An SSM document defines a command or automation procedure.
S3	Simple Storage Service: AWS object storage, used for many log, data and evidence repositories.
FIPS	Federal Information Processing Standards. A FIPS endpoint and the required validated cryptographic configuration must be checked for the actual use.
ACAS	Assured Compliance Assessment Solution: a DoD vulnerability-assessment capability. A different scanner requires the applicable approval and evidence of equivalence.
SCCA	Secure Cloud Computing Architecture: includes cloud access, security, management and privileged-credential functions.
HTTP / HTTPS	Web communication protocols; HTTPS protects the transport with encryption. Availability of a particular integration still needs checking.

The register's control IDs are explained in the RMF cross-reference. All setup and demonstration steps are recommendations for an authorized delivery team, using safe test data and the mission's approved procedures.

Component register 1-2

AWS-CSSP-01 | Landing Zone Accelerator on AWS

Architecture: Foundation / VDSS / VDMS

Contribution: Foundation pattern

Activity: Establish shared platform

AWS capability: Automates a configurable foundation across accounts; supplies parts of the security and management architecture.

Inputs: Account plan, network design, configuration repository.

Outputs: Deployed baseline and versioned configuration.

Implementation work: Choose scope; review configuration and supplemental services.

Operating owner: Platform team maintains baseline; CSSP agrees visibility.

Limits: A deployed LZA is not a complete CSSP service or proof of compliance. AWS lists partial and uncovered SCCA functions.

Suggested demonstration: Reconcile the actual configuration to requirements and demonstrate each required log path.

RMF examples: CM-2, CM-6, CA-7

GovCloud: Deployment solution, not a regional service. Validate the chosen release and every underlying service in each target region.

Primary sources: Landing Zone Accelerator overview · AWS SCCA / VDSS mapping · AWS SCCA / VDMS mapping

AWS-CSSP-02 | AWS Organizations

Architecture: Foundation / governance

Contribution: Enablement

Activity: Maintain account coverage

AWS capability: Groups accounts and applies organization policies and delegated administration.

Inputs: Account inventory and organizational units.

Outputs: Membership and policy assignments.

Implementation work: Enroll accounts and define administrative boundaries.

Operating owner: Platform governance owns accounts; CSSP checks coverage gaps.

Limits: GovCloud organizations are separate from commercial organizations. Account creation involves linked commercial accounts; policies do not grant permissions.

Suggested demonstration: Detect an unmonitored account and show how it enters the approved monitoring scope.

RMF examples: CM-8, AC-2, AC-6

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: AWS Organizations - GovCloud differences

Component register 3-4

AWS-CSSP-03 | AWS Control Tower

Architecture: Foundation / governance

Contribution: Enablement

Activity: Establish consistent baseline

AWS capability: Coordinates landing-zone setup and controls for governed accounts.

Inputs: Organization, region selection and enrollment plan.

Outputs: Control status and account baseline.

Implementation work: Enroll existing and new accounts; manage drift and exceptions.

Operating owner: Platform team owns enrollment and repair.

Limits: GovCloud has control and account-factory differences. Resource control policy controls are unavailable; a dashboard status is not an assessment.

Suggested demonstration: Check one enrolled and one excluded account; demonstrate exception ownership.

RMF examples: CM-2, CM-6, CA-7

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: AWS Control Tower - GovCloud differences

AWS-CSSP-04 | AWS Identity and Access Management (IAM)

Architecture: VDMS / privileged access

Contribution: Enforcement enabler

Activity: Constrain operator access

AWS capability: Controls access to AWS resources through identities, roles and policies.

Inputs: Approved roles, trust relationships and permissions.

Outputs: Access decisions and attributable API activity.

Implementation work: Define separate read, response and administration roles.

Operating owner: Identity team administers; mission grants response authority.

Limits: GovCloud uses separate credentials and partition identifiers. A technical permission is not mission authority to act.

Suggested demonstration: Prove analyst read access, deny unauthorized changes, and trace an approved responder action.

RMF examples: AC-2, AC-6, IA-2

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: AWS IAM - GovCloud differences

Component register 5-6

AWS-CSSP-05 | AWS IAM Identity Center

Architecture: VDMS / privileged access

Contribution: Identity integration

Activity: Connect workforce access

AWS capability: Connects workforce identities to accounts and supported applications with temporary access.

Inputs: Identity provider, groups and account permission sets.

Outputs: Assignments and workforce sign-in access.

Implementation work: Integrate the approved identity provider; test joiner and leaver handling.

Operating owner: Identity team and account owners maintain access.

Limits: GovCloud multi-region support is unavailable in the checked guide. Common Access Card integration needs its own approved identity design; MFA alone does not prove it. Use FIPS endpoints for the IAM Identity Center administrative console, SDK and CLI in GovCloud.

Suggested demonstration: Revoke a fictional user and verify loss of all assigned access.

RMF examples: AC-2, AC-6, IA-2

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: IAM Identity Center - GovCloud differences

AWS-CSSP-06 | AWS Config

Architecture: VDMS / configuration

Contribution: Posture evidence

Activity: Track configuration and drift

AWS capability: Records resource configuration and evaluates configured rules.

Inputs: Supported resource types, recorders and rule selection.

Outputs: Configuration history and rule findings.

Implementation work: Select resource coverage, delivery and regional rules.

Operating owner: Platform remediates; CSSP or assurance team reviews exceptions.

Limits: GovCloud lacks custom/third-party resource recording and SSM documents for Config remediation. Managed rules vary by region.

Suggested demonstration: Change a fictional resource; verify the change, finding, assigned owner and closure evidence.

RMF examples: CM-6, CM-8, CA-7

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: AWS Config - GovCloud differences

Component register 7-8

AWS-CSSP-07 | AWS CloudTrail

Architecture: VDMS / audit

Contribution: Telemetry

Activity: Trace AWS administrative actions

AWS capability: Records supported AWS API activity with actor, time and source context.

Inputs: Accounts, trails and selected event categories.

Outputs: Audit events for investigation and evidence.

Implementation work: Set organization coverage, destinations, retention and event selectors.

Operating owner: Platform protects delivery; CSSP analyzes agreed events.

Limits: Management API records do not replace application or host logs. GovCloud global service events need US-West coverage; review data-event selection separately. GovCloud lacks Lake integrations, generated queries, results summaries and data stores for Config items, Audit Manager evidence or non-AWS events. Network activity events cover KMS, S3, CloudTrail and Secrets Manager; AWS also documents CloudWatch events through its monitoring VPC interface endpoint. Enriched events are unsupported.

Suggested demonstration: Perform a safe test API change and retrieve the attributed event from the receiving system.

RMF examples: AU-2, AU-6, AU-12

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: AWS CloudTrail - GovCloud differences

AWS-CSSP-08 | Amazon CloudWatch Logs

Architecture: VDMS / logging

Contribution: Telemetry transport

Activity: Collect host and application events

AWS capability: Collects and retains configured log streams for search and delivery.

Inputs: Application, operating-system and service log producers.

Outputs: Timestamped log streams and agreed feeds.

Implementation work: Install/configure collectors, access, subscriptions and retention.

Operating owner: Application/platform teams supply logs; CSSP monitors feed health.

Limits: Logs are only present when producers deliver them. GovCloud Live Tail is unavailable; names and tags have handling restrictions.

Suggested demonstration: Generate a unique fictional event; verify arrival, access and a missing-feed alarm.

RMF examples: AU-2, AU-6, AU-9

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: CloudWatch Logs - GovCloud differences

Component register 9-10

AWS-CSSP-09 | Amazon CloudWatch metrics and alarms

Architecture: VDMS / service health

Contribution: Monitoring enabler

Activity: Detect loss of defensive visibility

AWS capability: Provides metrics and alarms for configured operational signals.

Inputs: Log delivery counts, service metrics and custom health signals.

Outputs: Alarms and health history.

Implementation work: Define meaningful thresholds and route alarms to staffed owners.

Operating owner: Platform handles sensor health; CSSP tracks coverage interruptions.

Limits: GovCloud cross-account observability and dashboard sharing are unavailable. Alarms do not supply incident judgment.

Suggested demonstration: Stop a fictional test feed and demonstrate timely operator acknowledgment and restoration.

RMF examples: SI-4, CA-7, IR-5

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: Amazon CloudWatch - GovCloud differences

AWS-CSSP-10 | Amazon VPC Flow Logs

Architecture: VDSS / network visibility

Contribution: Telemetry

Activity: Observe network communications

AWS capability: Records IP traffic metadata for selected network interfaces and sends it to configured destinations.

Inputs: VPC/subnet/interface scope and log format.

Outputs: Flow metadata: endpoints, ports and traffic attributes.

Implementation work: Choose scope, destinations and correlation to application inventory.

Operating owner: Network team enables; CSSP interprets with mission context.

Limits: Flow records are not packet payloads, application transactions or approved traffic policy. Review documented collection limits.

Suggested demonstration: Generate an allowed and a rejected fictional connection; correlate records to the correct application.

RMF examples: SI-4, AU-12, CM-8

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: VPC Flow Logs · Amazon VPC - GovCloud differences

Component register 11-12

AWS-CSSP-11 | Route 53 Resolver DNS Firewall

Architecture: VDSS / DNS

Contribution: Detection and enforcement

Activity: Control suspicious domain resolution

AWS capability: Filters outbound DNS queries through the VPC Resolver using associated rule groups.

Inputs: Approved domain policy, resolver path and query visibility.

Outputs: DNS decisions, logs and metrics.

Implementation work: Associate rule groups; tune exceptions and fail behavior.

Operating owner: Network/security team owns rules; CSSP reviews detections.

Limits: DNS controls only cover the resolver path they inspect. Other resolvers or encrypted DNS require separate design.

Suggested demonstration: Resolve a safe blocked test domain and prove both enforcement and analyst visibility.

RMF examples: SC-7, SI-4

GovCloud: AWS lists GovCloud (US) availability without distinguishing East/West on this page. Confirm the chosen endpoint and features before design acceptance.

Primary sources: Resolver DNS Firewall · DNS Firewall availability

AWS-CSSP-12 | AWS Network Firewall

Architecture: VDSS / network boundary

Contribution: Detection and enforcement

Activity: Inspect and filter routed traffic

AWS capability: Provides managed stateful network firewall and intrusion detection/prevention capabilities for VPC traffic.

Inputs: Routed traffic, rule groups and inspection policy.

Outputs: Traffic decisions and configured firewall logs.

Implementation work: Engineer routes, resilience, rule lifecycle and log delivery.

Operating owner: Network team operates; CSSP tunes detections under agreed change authority.

Limits: Only traffic traversing the inspection path is covered. Validate encrypted-traffic handling and exceptions; do not infer full packet recording.

Suggested demonstration: Prove inspection in both directions and detect a route that bypasses the firewall.

RMF examples: SC-7, SI-4

GovCloud: Documented in GovCloud US-East and US-West; AWS lists no GovCloud service differences. Validate the proposed configuration.

Primary sources: AWS Network Firewall - GovCloud differences

Component register 13-14

AWS-CSSP-13 | AWS WAF

Architecture: VDSS / web protection

Contribution: Detection and enforcement

Activity: Protect supported web entry points

AWS capability: Inspects supported web requests and applies allow, block or other configured rule actions.

Inputs: Protected endpoints, web access control lists and application context.

Outputs: Web decisions and configured event records.

Implementation work: Attach to supported resources; tune false positives with the application team.

Operating owner: Application security owns policy; CSSP monitors agreed findings.

Limits: GovCloud Marketplace managed rule groups are unavailable. AWS documents export-controlled-data restrictions; resolve those before use. WAF does not inspect every protocol.

Suggested demonstration: Use a benign test request to prove blocking, application continuity and receipt of the event.

RMF examples: SC-7, SI-4

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: AWS WAF - GovCloud differences

AWS-CSSP-14 | AWS Firewall Manager

Architecture: VDSS / policy governance

Contribution: Policy distribution

Activity: Keep network protection consistent

AWS capability: Applies supported firewall and security-group policies across an organization.

Inputs: Organization scope, policy and resource selection.

Outputs: Policy deployment and policy-conformance status; not a control assessment.

Implementation work: Enroll resources; review exclusions and drift.

Operating owner: Security platform team owns policy rollout and exceptions.

Limits: GovCloud does not support Shield Advanced or WAF Classic through Firewall Manager; WAF CloudFront policies and Marketplace rule groups are restricted.

Suggested demonstration: Add a fictional account/resource and show policy application plus a documented exception.

RMF examples: CM-6, SC-7, CA-7

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: AWS Firewall Manager - GovCloud differences

Component register 15-16

AWS-CSSP-15 | Amazon VPC Traffic Mirroring

Architecture: VDSS / packet visibility

Contribution: Telemetry enabler

Activity: Deliver packet copies to a separate inspection or capture stack

AWS capability: Copies eligible interface traffic to separately operated monitoring appliances.

Inputs: Supported sources, filters, mirror targets and network capacity.

Outputs: Mirrored packets delivered to the target.

Implementation work: Provide the collector, storage, decoding and retention design.

Operating owner: Network team delivers traffic; receiving team operates the capture stack.

Limits: Mirroring alone does not retain packets or decrypt them. GovCloud target owners cannot see sessions created by other accounts. Coverage and truncation require testing.

Suggested demonstration: Capture known test packets and verify completeness, loss handling, retention and retrieval.

RMF examples: SI-4, AU-12

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: Traffic Mirroring · Amazon VPC - GovCloud differences

AWS-CSSP-16 | Amazon GuardDuty

Architecture: VDSS / threat detection

Contribution: Detection

Activity: Identify suspicious AWS activity

AWS capability: Analyzes supported activity sources and enabled protection plans to generate threat findings.

Inputs: Account scope and supported foundational/optional telemetry.

Outputs: Security findings and attack context.

Implementation work: Enable region/account coverage; select plans; connect analysts and test notifications.

Operating owner: CSSP analysts triage; platform team sustains coverage.

Limits: GovCloud lacks entity lists, the CompromisedCredentials IAM finding and eight specified EKS anomalous-behavior findings. EC2 malware scans skip Marketplace product-code instances; Backup malware scans exclude EC2/EBS recovery points. Cross-Region data transfer and Investigation preview are unavailable. Runtime Monitoring uses the regional guardduty-data-fips endpoint. A finding is neither automatic containment nor complete endpoint protection.

Suggested demonstration: Generate sample findings; verify routing, triage ownership and coverage of every in-scope account.

RMF examples: SI-4, IR-5

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: Amazon GuardDuty - GovCloud differences · GuardDuty data sources and setup

Component register 17-18

AWS-CSSP-17 | Amazon Inspector

Architecture: VDMS / vulnerability management

Contribution: Assessment input

Activity: Find supported workload vulnerabilities

AWS capability: Assesses supported AWS resources for vulnerabilities and produces prioritized findings.

Inputs: Supported compute, images/packages and scan coverage.

Outputs: Vulnerability findings and coverage status.

Implementation work: Enable supported scans; connect owners and remediation workflow.

Operating owner: Workload owners remediate; vulnerability team validates closure.

Limits: GovCloud lacks Lambda Code Scanning and Managed Code Repository Scanning. Linux deep-inspection plugin is not FIPS compliant. Inspector is not assumed ACAS or endpoint-security equivalence.

Suggested demonstration: Demonstrate a known test vulnerability, remediation, rescan and visibility of unscanned resources.

RMF examples: RA-5, SI-2

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: Amazon Inspector - GovCloud differences

AWS-CSSP-18 | AWS Security Hub CSPM

Architecture: VDMS / security posture

Contribution: Findings and posture

Activity: Collect posture checks and findings

AWS capability: Aggregates supported findings and evaluates enabled cloud security posture checks.

Inputs: Enabled controls, account coverage and supported integrations.

Outputs: Findings, insights and control-check results.

Implementation work: Enable required checks and integrations; assign exceptions and review owners.

Operating owner: Security assurance/CSSP reviews; platform fixes configuration.

Limits: GovCloud controls and integrations differ. Cross-region aggregation is limited to supported findings/updates/insights between the two GovCloud regions.

Suggested demonstration: Trigger a safe failed check, find its source evidence and verify owner disposition.

RMF examples: CA-7, CM-6, RA-5

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: Security Hub CSPM - GovCloud differences

Component register 19-20

AWS-CSSP-19 | AWS Security Hub

Architecture: Security operations

Contribution: Risk prioritization

Activity: Correlate security signals

AWS capability: Combines and contextualizes security signals to help teams prioritize issues.

Inputs: Supported findings and resource context.

Outputs: Prioritized security issues and investigation context.

Implementation work: Validate supported integrations and response paths for the chosen region.

Operating owner: CSSP prioritizes with mission impact; authorized owners act.

Limits: Distinct from Security Hub CSPM. GovCloud lacks third-party integrations and automation rules for integrations; generic feature lists must not be imported unchanged. The Extended plan and Network Scanning are unavailable. The Account coverage page/widget omits GovCloud coverage counts; verify each account.

Suggested demonstration: Follow one fictional issue from source finding to assigned decision and closure.

RMF examples: IR-4, IR-5, CA-7

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: AWS Security Hub - GovCloud differences

AWS-CSSP-20 | Amazon Security Lake

Architecture: VDMS / security data

Contribution: Data integration

Activity: Centralize security telemetry

AWS capability: Normalizes supported security events into a customer-account data lake using Open Cybersecurity Schema Framework records.

Inputs: Enabled native sources, approved custom sources and subscribers.

Outputs: Normalized data and subscriber access.

Implementation work: Configure regions, sources, schema mapping, access and lifecycle.

Operating owner: Data platform maintains lake; CSSP owns analytic use cases.

Limits: GovCloud HTTPS subscriber notifications are unavailable. Security Lake does not support S3 Object Lock on its lake buckets; use a separately designed evidence archive if needed.

Suggested demonstration: Trace a test event through normalization and subscriber retrieval; test missing-source detection.

RMF examples: AU-6, AU-9, SI-4

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: Amazon Security Lake - GovCloud differences · Security Lake introduction · Security Lake considerations

Component register 21-22

AWS-CSSP-21 | Amazon Detective

Architecture: Security operations

Contribution: Investigation

Activity: Reconstruct suspicious activity

AWS capability: Builds behavior graphs from supported activity and findings to support analyst investigation.

Inputs: Enabled member accounts and supported activity sources.

Outputs: Behavior context and investigation views.

Implementation work: Enroll accounts, assign investigator permissions and document export needs.

Operating owner: CSSP investigators interpret results and maintain case evidence.

Limits: GovCloud does not send membership invitation emails or automatically remove terminated accounts from graphs. Graph context does not establish forensic completeness.

Suggested demonstration: Investigate a fictional finding and preserve the analyst conclusion with supporting event references.

RMF examples: IR-4, IR-5, AU-6

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: Amazon Detective - GovCloud differences

AWS-CSSP-22 | AWS Systems Manager

Architecture: VDMS / host administration

Contribution: Operational execution

Activity: Maintain and remediate managed nodes

AWS capability: Provides managed-node inventory, configuration, patching and automation capabilities.

Inputs: Enrolled nodes, agent/connectivity, baselines and runbooks.

Outputs: Inventory, execution results and patch status.

Implementation work: Enroll nodes; test permissions, maintenance windows and rollback.

Operating owner: Platform/workload team operates under approved changes.

Limits: GovCloud lacks Incident Manager and Change Manager; Quick Setup patch policies and some runbooks are unavailable. Patch status is not complete vulnerability or endpoint defense coverage. Incident Manager stopped accepting new customers on 7 November 2025; existing enabled accounts can continue using it where available.

Suggested demonstration: Patch a fictional test node with approval; prove result, reboot handling and exception for an unreachable node.

RMF examples: CM-8, CM-6, SI-2

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: AWS Systems Manager - GovCloud differences · AWS SCCA / VDMS mapping · Incident Manager new-customer availability change

Component register 23-24

AWS-CSSP-23 | Amazon EventBridge

Architecture: Security operations / integration

Contribution: Workflow routing

Activity: Deliver findings to the receiving workflow

AWS capability: Routes selected events to configured targets for operational processing.

Inputs: Finding/event schema, rules and supported targets.

Outputs: Delivered events and delivery failures.

Implementation work: Define filters, retries, failure handling and duplicate protection.

Operating owner: Integration owner maintains routes; CSSP owns receipt and escalation.

Limits: GovCloud lacks API destinations, Pipes and API Gateway as an event-bus target. A delivered event is not a staffed acknowledgment.

Suggested demonstration: Test a finding and failed target; demonstrate recovery without losing or duplicating the case.

RMF examples: IR-5, IR-6, SI-4

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: Amazon EventBridge - GovCloud differences

AWS-CSSP-24 | AWS Lambda and Step Functions

Architecture: Security operations / response

Contribution: Automation enabler

Activity: Execute approved response workflows

AWS capability: Combine event-driven code and workflow orchestration to run defined response steps.

Inputs: Approved playbook, trusted event data and scoped execution roles.

Outputs: Execution history and action results.

Implementation work: Build approval gates, idempotency, error paths, evidence and rollback.

Operating owner: Mission authorizes actions; platform/CSSP executes assigned steps.

Limits: GovCloud Lambda Function URLs and Step Functions HTTPS API calls are unavailable. Automation cannot supply incident authority or government reporting decisions.

Suggested demonstration: Rehearse an approved reversible action; prove denied unauthorized action, failure handling and restoration.

RMF examples: IR-4, AC-6, AU-12

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: AWS Lambda - GovCloud differences · AWS Step Functions - GovCloud differences

Component register 25-26

AWS-CSSP-25 | Amazon S3 evidence archive / Object Lock

Architecture: VDMS / evidence

Contribution: Evidence preservation

Activity: Retain attributable security records

AWS capability: Stores evidence objects; versioning and Object Lock can protect selected versions against alteration or deletion.

Inputs: Approved evidence, retention policy and access model.

Outputs: Retained object versions and retrieval records.

Implementation work: Design a separate archive; approve retention and access before locking.

Operating owner: Evidence custodian governs retention; CSSP supplies case records.

Limits: Object Lock applies to versions, not log completeness or chain of custody. Governance mode can be bypassed by authorized principals. Do not enable it on Security Lake buckets. GovCloud does not support S3 MFA delete.

Suggested demonstration: Retrieve a test record by version; verify integrity, allowed access and deletion denial under the selected mode.

RMF examples: AU-9, AU-11, IR-4

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: Amazon S3 - GovCloud differences · S3 Object Lock · Security Lake considerations

AWS-CSSP-26 | AWS Key Management Service

Architecture: VDMS / cryptographic support

Contribution: Supporting control

Activity: Protect service data and evidence keys

AWS capability: Provides managed cryptographic key services and access policies for integrated workloads.

Inputs: Key policy, service integrations and custody requirements.

Outputs: Key usage and policy-controlled cryptographic operations.

Implementation work: Define custodians, recovery access, rotation and allowed use.

Operating owner: Key custodians/platform own policy; assessors verify actual configuration.

Limits: An available key service does not prove the required cryptographic configuration, module validation or workload authorization. GovCloud external-key-store constraints apply.

Suggested demonstration: Demonstrate permitted decrypt, denied unauthorized use and recovery without exposing key material.

RMF examples: SC-12, SC-13, AC-6

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: AWS KMS - GovCloud differences

Component register 27-28

AWS-CSSP-27 | AWS Backup

Architecture: VDMS / recovery

Contribution: Recovery enabler

Activity: Restore systems after an incident

AWS capability: Centralizes backup policies and execution for supported resources.

Inputs: Resource selections, backup plans and recovery objectives.

Outputs: Recovery points, job results and restore evidence.

Implementation work: Select coverage and retention; design isolated recovery exercises.

Operating owner: Platform restores; mission validates service and authorizes return.

Limits: GovCloud automated Restore testing and multi-account/multi-region Backup Audit Manager reporting are unavailable. Successful backups alone do not prove recoverability.

Suggested demonstration: Manually exercise restoration of a fictional workload and verify integrity, dependencies and required recovery time.

RMF examples: CP-9, CP-10, IR-4

GovCloud: Documented in GovCloud US-East and US-West; feature limits below apply.

Primary sources: AWS Backup - GovCloud differences

AWS-CSSP-28 | Amazon Macie - conditional candidate

Architecture: Data discovery

Contribution: Classification input

Activity: Find sensitive patterns in S3

AWS capability: Discovers supported sensitive-data patterns and reports S3 security posture.

Inputs: Accessible supported S3 objects and discovery configuration.

Outputs: Discovery findings and coverage results.

Implementation work: Only evaluate after confirming regional support, data authority and permissions.

Operating owner: Data owners validate classification; security team handles findings.

Limits: Checked endpoints omit GovCloud. Exclude from a GovCloud baseline pending authoritative confirmation. Generic Security Hub mentions of Macie do not establish regional availability.

Suggested demonstration: If regionally admitted, use fictional test patterns and verify scope, exclusions and owner review.

RMF examples: RA-3, SI-4

GovCloud: Not established for GovCloud in the reviewed endpoint list; held from GovCloud baseline. Commercial-region capability does not imply GovCloud availability.

Primary sources: Amazon Macie introduction · Macie endpoints