Study Plan — Cloud Computing Security (User Story Cards)

Aligned to “Cloud Computing Security: Foundations and Challenges (2nd ed.)”

One story card per chapter with example tasks and BDD acceptance criteria.

Contents

1 Section I — Introduction

CCS-1 — Foundations & Essentials

Epic / Feature	Cloud Foundations
Business Value	Establish shared vocabulary and ownership to reduce onboarding confusion and security drift.
Priority / Estimate	Priority: Must SP: 3
Persona	Developer starting on a cloud project
Dependencies	Sandbox account, org security policy, provider docs
Assumptions / Risks	Teams may interpret shared responsibility differently; risk of inconsistent defaults
Cloud (AWS) Mapping	AWS Organizations & Control Tower (Landing Zone), IAM Identity Center (AWS SSO), Well-Architected Framework

Story

As a developer, I want to document cloud foundations and shared responsibility so that I make secure choices and keep main green. **Non-Functional**

Security Reliability Accessibility **Acceptance Criteria (BDD)**

Scenario	Shared understanding is captured
Given	A sandbox and policy references
When	I create a one-page shared responsibility matrix and a glossary of essential characteristics
Then	The documents are linked in onboarding and referenced by future stories

Definition of Ready: Persona clear; AC drafted; Dependencies identified. • *Definition of Done:* Matrix and glossary committed; reviewed by AppSec; referenced in README. **Tasks**

- □ Write `docs/shared-responsibility-matrix.md`.
- □ Capture five essential characteristics of cloud with examples.
- □ Add link in `README.md` and onboarding checklist.
- □ Open issues for disagreements or unclear ownership.

AWS Tailoring

- □ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- □ Deploy AWS Config conformance packs; record all resources.
- □ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-2 — Overview of Cloud Computing

Epic / Feature	Cloud Foundations
Business Value	Reduce design churn by listing provider primitives and portability considerations.
Priority / Estimate	Priority: Must SP: 3
Persona	Solution architect
Dependencies	Access to AWS, Azure, and GCP docs
Assumptions / Risks	Feature parity differs; lock-in may be acceptable for value
Cloud (AWS) Mapping	AWS Organizations & Control Tower (Landing Zone), IAM Identity Center (AWS SSO), Well-Architected Framework

Story

As a solution architect, I want a lift-and-shift bill of materials so that teams can compare provider primitives and portability risks. **Non-Functional**

Performance Security Reliability **Acceptance Criteria (BDD)**

Scenario	Cross-provider comparison documented
Given	A reference three-tier app
When	I create a bill of materials for AWS, Azure, and GCP with security notes
Then	Tradeoffs and lock-in vectors are captured with mitigation ideas

Definition of Ready: Reference app defined; providers chosen. • *Definition of Done:* BOM spreadsheet checked in; reviewed by platform and security. **Tasks**

- □ Produce `bom/cloud-bom.xlsx` with compute, storage, network, IAM.
- □ Annotate security defaults and required hardening per service.
- □ Note portability blockers and alternatives.
- □ File follow-up ADR if a single provider is selected.

AWS Tailoring

- □ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- □ Deploy AWS Config conformance packs; record all resources.
- □ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-14 — Security Essentials & Reference Architectures

Epic / Feature	Reference Architecture
Business Value	Provide a secure, repeatable pattern for web workloads.
Priority / Estimate	Priority: Must SP: 5
Persona	Solutions architect
Dependencies	Diagramming tool, baseline modules
Assumptions / Risks	Pattern must be simple yet adaptable
Cloud (AWS) Mapping	AWS Organizations & Control Tower (Landing Zone), IAM Identity Center (AWS SSO), Well-Architected Framework, Amazon VPC (Subnets, Route Tables, NACLs, SGs), AWS Transit Gateway, AWS Network Firewall, AWS WAF & AWS Shield, PrivateLink & VPC Endpoints

Story

As a solutions architect, I want a secure reference architecture so that teams can adopt consistent controls quickly.

Non-Functional

Security Reliability

Acceptance Criteria (BDD)

Scenario	Reference published
Given	Common requirements for a web app
When	I include logging, monitoring, KMS, WAF, and CIEM
Then	The diagram and bill of materials are reviewed and adopted

Definition of Ready: Scope finalized. • *Definition of Done:* Drawio file and BOM committed; approval recorded.

Tasks

- ☐ Draw diagram with shared services.
- ☐ List components and controls.
- ☐ Map to controls framework.
- ☐ Create adoption checklist.

AWS Tailoring

- ☐ Hub-and-spoke VPCs via TGW; centralized egress with Network Firewall.
- ☐ Disable public access for S3/EBS/RDS; require VPC endpoints for AWS APIs.
- ☐ Protect internet edges with WAF and (optionally) Shield Advanced.

CCS-15 — Architecture & Security Concepts

Epic / Feature	Zero Trust & Immutable Infra
Business Value	Reduce lateral movement and configuration drift.
Priority / Estimate	Priority: Should SP: 3
Persona	Platform architect
Dependencies	Image builder, autoscaling, CI/CD
Assumptions / Risks	Rebuild cadence must align with release cycles
Cloud (AWS) Mapping	Amazon VPC (Subnets, Route Tables, NACLs, SGs), AWS Transit Gateway, AWS Network Firewall, AWS WAF & AWS Shield, PrivateLink & VPC Endpoints

Story

As a platform architect, I want immutable images with micro-segmentation so that drift and attack paths are minimized. **Non-Functional**

Security Reliability **Acceptance Criteria (BDD)**

Scenario	Mutable to immutable migration
Given	A mutable VM pattern
When	I move to image-based deployments with autoscaling
Then	Patching occurs via rebuild and health checks stay green

Definition of Ready: Current pattern documented. • *Definition of Done:* New pattern deployed in staging; runbook updated. **Tasks**

- □ Create hardened base image.
- □ Update pipeline for image promotion.
- □ Add health checks and rollbacks.
- □ Retire in-place patching runbooks.

AWS Tailoring

- □ Hub-and-spoke VPCs via TGW; centralized egress with Network Firewall.
- □ Disable public access for S3/EBS/RDS; require VPC endpoints for AWS APIs.
- □ Protect internet edges with WAF and (optionally) Shield Advanced.

CCS-16 — Secure Cloud Architecture

Epic / Feature	Threat-Driven Design
Business Value	Align controls with threats and evidence.
Priority / Estimate	Priority: Must SP: 5
Persona	Security architect
Dependencies	Threat modeling tool, control catalog
Assumptions / Risks	Over-design if threats not prioritized
Cloud (AWS) Mapping	Amazon VPC (Subnets, Route Tables, NACLs, SGs), AWS Transit Gateway, AWS Network Firewall, AWS WAF & AWS Shield, PrivateLink & VPC Endpoints

Story

As a security architect, I want a threat model linked to controls so that architectural choices are justified. **Non-Functional**

Security Reliability **Acceptance Criteria (BDD)**

Scenario	STRIDE model created
Given	The reference architecture
When	I document threats and mitigations
Then	Missing controls generate backlog items with owners

Definition of Ready: Architecture stable. • *Definition of Done:* Threat model published; issues created and prioritized. **Tasks**

- ☐ Run a STRIDE session.
- ☐ Map threats to controls.
- ☐ Create tickets for gaps.
- ☐ Review annually or after changes.

AWS Tailoring

- ☐ Hub-and-spoke VPCs via TGW; centralized egress with Network Firewall.
- ☐ Disable public access for S3/EBS/RDS; require VPC endpoints for AWS APIs.
- ☐ Protect internet edges with WAF and (optionally) Shield Advanced.

CCS-29 — Regions, Zones, & Trust Boundaries

Epic / Feature	Multi-Region Planning
Business Value	Improve resilience and clarify trust boundaries.
Priority / Estimate	Priority: Should SP: 3
Persona	Site reliability engineer
Dependencies	Provider region matrix, latency data
Assumptions / Risks	Cost vs availability tradeoffs
Cloud (AWS) Mapping	AWS Regions & AZs, Amazon VPC, Private Hosted Zones (Route 53), AWS Transit Gateway, AWS PrivateLink, AWS KMS (CMKs), S3 Server-Side Encryption (SSE-KMS), Amazon Macie, AWS Lake Formation

Story

As an SRE, I want a region selection ADR so that latency, compliance, and trust boundaries are explicit. **Non-Functional**

Reliability Security **Acceptance Criteria (BDD)**

Scenario	Regions selected
Given	Latency and compliance constraints
When	I pick primary and failover regions
Then	ADR documents tradeoffs and dependencies

Definition of Ready: Constraints collected. • *Definition of Done:* ADR merged; DNS and data plans documented. **Tasks**

- □ Measure latency from users.
- □ Check data residency needs.
- □ Choose primary and secondary.
- □ Document dependencies and costs.

AWS Tailoring

- □ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- □ Deploy AWS Config conformance packs; record all resources.
- □ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-3 — Security Baselines

Epic / Feature	Baseline Security
Business Value	Create fast feedback on misconfigurations and reduce time to first fix.
Priority / Estimate	Priority: Must SP: 5
Persona	Cloud security engineer
Dependencies	Sandbox account/project, Prowler or ScoutSuite, read-only creds
Assumptions / Risks	Findings volume may be high; prioritize by risk
Cloud (AWS) Mapping	AWS Security Hub (CIS/AWS Foundational), AWS Config & Conformance Packs, Systems Manager Patch Manager, IAM Access Analyzer

Story

As a cloud security engineer, I want to run a baseline scan so that we triage top risks and create a remediation backlog. **Non-Functional**

Security Reliability Privacy **Acceptance Criteria (BDD)**

Scenario	Baseline executed and triaged
Given	Read-only scanner access
When	I run Prowler or ScoutSuite and export results
Then	Top ten findings have owners, due dates, and tickets

Definition of Ready: Scanner configured; scope agreed. • *Definition of Done:* Report stored; backlog created; first PR opened for a fix. **Tasks**

- ☐ Execute scan and export JSON plus HTML.
- ☐ Create `baseline-findings.md` with risk ranking.
- ☐ Open issues for top findings; tag teams.
- ☐ Document suppressions and rationale.

AWS Tailoring

- ☐ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- ☐ Deploy AWS Config conformance packs; record all resources.
- ☐ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-4 — Privacy & Trust Baselines

Epic / Feature	Data Protection
Business Value	Reduce regulatory risk through inventory, tagging, and residency controls.
Priority / Estimate	Priority: Must SP: 5
Persona	Data protection officer / privacy engineer
Dependencies	Data catalog access, tagging standard
Assumptions / Risks	Unknown data flows; legacy datasets may be unlabeled
Cloud (AWS) Mapping	AWS Security Hub (CIS/AWS Foundational), AWS Config & Conformance Packs, Systems Manager Patch Manager, IAM Access Analyzer, AWS KMS (CMKs), S3 Server-Side Encryption (SSE-KMS), Amazon Macie, AWS Lake Formation

Story

As a privacy engineer, I want to inventory and tag datasets so that location, residency, and access are controlled. **Non-Functional**

Privacy Security Reliability **Acceptance Criteria (BDD)**

Scenario	Inventory completed for one workload
Given	Access to data catalog and cloud storage
When	I tag datasets by sensitivity and residency
Then	Policies and controls reference the tags for enforcement

Definition of Ready: Scope selected; tagging keys agreed. • *Definition of Done:* Inventory CSV committed; policies updated; gaps tracked. **Tasks**

- ☐ Export dataset list and classify sensitivity.
- ☐ Tag objects and databases by owner and residency.
- ☐ Map to retention and legal requirements.
- ☐ Open tasks to fix unlabeled datasets.

AWS Tailoring

- ☐ Use KMS CMKs with rotation and least-privilege key policies.
- ☐ Encrypt S3, EBS, RDS by default; enforce via SCP/Config rules.
- ☐ Scan and classify sensitive data with Macie for key buckets.

CCS-6 — Risk & Trust Assessment Schemes

Epic / Feature	Risk Management
Business Value	Make risk-driven decisions using a consistent scheme.
Priority / Estimate	Priority: Must SP: 3
Persona	Risk analyst
Dependencies	Risk register template, stakeholder access
Assumptions / Risks	Disagreement on scoring methods
Cloud (AWS) Mapping	AWS KMS (CMKs), S3 Server-Side Encryption (SSE-KMS), Amazon Macie, AWS Lake Formation, AWS Audit Manager, AWS Artifact (Reports), AWS Security Hub

Story

As a risk analyst, I want a risk register using a simple method so that leaders can compare and prioritize risks. **Non-Functional**

Security Reliability **Acceptance Criteria (BDD)**

Scenario	Register populated for one project
Given	A template and stakeholder interviews
When	I capture top risks with likelihood and impact
Then	Owners and treatments are assigned and accepted

Definition of Ready: Template chosen; scope set. • *Definition of Done:* Register committed; review notes added; next review scheduled. **Tasks**

- ☐ Create `risk-register.xlsx`.
- ☐ Schedule 30-minute interviews with owners.
- ☐ Draft KRIs for top items.
- ☐ Publish review cadence.

AWS Tailoring

- ☐ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- ☐ Deploy AWS Config conformance packs; record all resources.
- ☐ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-7 — Managing Risk in the Cloud

Epic / Feature	Risk Treatment
Business Value	Reduce probability or impact through concrete control choices.
Priority / Estimate	Priority: Must SP: 5
Persona	Security program manager
Dependencies	Control catalog, platform team availability
Assumptions / Risks	Limited capacity; tradeoffs required
Cloud (AWS) Mapping	AWS Audit Manager, AWS Artifact (Reports), AWS Security Hub

Story

As a security program manager, I want risk treatments tied to controls so that we see measurable reduction in risk. **Non-Functional**

Security Reliability **Acceptance Criteria (BDD)**

Scenario	Treatments committed
Given	A prioritized risk list
When	I link risks to controls and create implementation tickets
Then	KRIs and due dates are visible on the roadmap

Definition of Ready: Owners identified; catalog agreed. • *Definition of Done:* Tickets created; dashboard shows KRIs; exec summary published. **Tasks**

- □ Map each top risk to controls and team.
- □ Create epics with AC and success criteria.
- □ Add KRI queries to dashboard.
- □ Send monthly status note.

AWS Tailoring

- □ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- □ Deploy AWS Config conformance packs; record all resources.
- □ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-8 — Cloud Security Risk Management

Epic / Feature	Policy as Code
Business Value	Prevent misconfigurations from merging to main.
Priority / Estimate	Priority: Must SP: 5
Persona	DevOps engineer
Dependencies	CI pipeline, IaC repo, OPA or Checkov
Assumptions / Risks	False positives can slow teams
Cloud (AWS) Mapping	AWS Audit Manager, AWS Artifact (Reports), AWS Security Hub

Story

As a DevOps engineer, I want policy-as-code in CI so that insecure IaC cannot be merged.

Non-Functional

Security Reliability

Acceptance Criteria (BDD)

Scenario	CI blocks insecure patterns
Given	A repo with Terraform modules
When	I add checks for public buckets and wildcard IAM
Then	Failing PRs show clear messages and remediation links

Definition of Ready: Rules selected; threshold agreed. • *Definition of Done:* Checks enforced; docs added; exceptions process documented.

Tasks

- ☐ Add OPA or Checkov job to CI.
- ☐ Write two guardrails: storage public access and IAM wildcards.
- ☐ Add test fixtures that fail until fixed.
- ☐ Document remediation steps.

AWS Tailoring

- ☐ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- ☐ Deploy AWS Config conformance packs; record all resources.
- ☐ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-9 — Risk Mitigation Methods

Epic / Feature	Mitigation Patterns
Business Value	Choose effective mitigations for data and perimeter.
Priority / Estimate	Priority: Should SP: 3
Persona	Security architect
Dependencies	KMS, WAF, segmentation capability
Assumptions / Risks	Cost and latency tradeoffs
Cloud (AWS) Mapping	AWS Audit Manager, AWS Artifact (Reports), AWS Security Hub

Story

As a security architect, I want to compare mitigation options so that we pick the best fit per risk. **Non-Functional**

Performance Security **Acceptance Criteria (BDD)**

Scenario	Decision record created
Given	Candidate mitigations and constraints
When	I evaluate tokenization, KMS, WAF, and micro-segmentation
Then	An ADR records the chosen approach and rationale

Definition of Ready: Alternatives listed; constraints known. • *Definition of Done:* ADR merged; next steps filed as tickets. **Tasks**

- ☐ Draft ADR comparing options.
- ☐ Measure expected latency impact.
- ☐ Validate cost estimates.
- ☐ Get sign-off from stakeholders.

AWS Tailoring

- ☐ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- ☐ Deploy AWS Config conformance packs; record all resources.
- ☐ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-10 — Access Policy Specification & Enforcement

Epic / Feature	Identity and Access Management
Business Value	Reduce privilege and prevent policy sprawl.
Priority / Estimate	Priority: Must SP: 5
Persona	IAM engineer
Dependencies	Policy engine, repo access
Assumptions / Risks	Legacy policies contain wildcards
Cloud (AWS) Mapping	AWS IAM (Policies, Roles, Permission Boundaries), Service Control Policies (SCPs), Attribute-based access control (ABAC), Verified Permissions (Cedar)

Story

As an IAM engineer, I want least-privilege policies with automated checks so that access stays minimal and auditable.

Non-Functional

Security Reliability

Acceptance Criteria (BDD)

Scenario	Wildcards prevented
Given	Policy files in version control
When	I add a rule that fails `"Action: *"` or `"Resource: *"`
Then	PRs fail with a clear message and link to examples

Definition of Ready: Policy style guide drafted. • *Definition of Done:* Rules enabled; examples published; old policies queued for refactor.

Tasks

- ☐ Create policy lints for wildcards and unused permissions.
- ☐ Build reusable role templates.
- ☐ Add presubmit unit tests.
- ☐ Document escalation and exceptions.

AWS Tailoring

- ☐ Use IAM Identity Center for workforce; enforce MFA and SCIM sync.
- ☐ Create least-privilege IAM roles with permission boundaries and Access Analyzer scan.
- ☐ Apply SCP guardrails to deny wildcards and restrict regions where required.
- ☐ Rotate keys; prohibit long-lived access keys.

CCS-12 — Distributed Access Control

Epic / Feature	Service Authorization
Business Value	Enforce consistent policies across microservices.
Priority / Estimate	Priority: Should SP: 3
Persona	Platform engineer
Dependencies	OPA sidecar or service mesh, K8s cluster
Assumptions / Risks	Policy changes must be versioned and tested
Cloud (AWS) Mapping	AWS IAM (Policies, Roles, Permission Boundaries), Service Control Policies (SCPs), Attribute-based access control (ABAC), Verified Permissions (Cedar)

Story

As a platform engineer, I want sidecar policy enforcement so that services follow the same authorization rules. **Non-Functional**

Security Reliability **Acceptance Criteria (BDD)**

Scenario	Policy enforced at runtime
Given	A sample API deployed on Kubernetes
When	I deny requests lacking a required claim
Then	Access logs and metrics confirm policy decisions

Definition of Ready: Sidecar pattern approved. • *Definition of Done:* Policy repo created; sample deployed; dashboards live. **Tasks**

- ☐ Deploy OPA sidecar with Rego bundle.
- ☐ Write allow/deny rule based on JWT claim.
- ☐ Emit decision logs to SIEM.
- ☐ Add rollout and rollback steps.

AWS Tailoring

- ☐ Use IAM Identity Center for workforce; enforce MFA and SCIM sync.
- ☐ Create least-privilege IAM roles with permission boundaries and Access Analyzer scan.
- ☐ Apply SCP guardrails to deny wildcards and restrict regions where required.
- ☐ Rotate keys; prohibit long-lived access keys.

CCS-11 — Cryptographic Key Management

Epic / Feature	Data Encryption
Business Value	Protect sensitive data at rest and in transit with managed lifecycle.
Priority / Estimate	Priority: Must SP: 5
Persona	Security engineer
Dependencies	KMS, secrets store, CI access
Assumptions / Risks	Rotation can disrupt apps if not coordinated
Cloud (AWS) Mapping	AWS KMS, AWS CloudHSM, External Key Store (XKS), Envelope Encryption Patterns

Story

As a security engineer, I want envelope encryption with automated rotation so that key compromise risk is minimized. **Non-Functional**

Security Reliability Privacy **Acceptance Criteria (BDD)**

Scenario	Rotation executed without downtime
Given	Apps using KMS for envelope encryption
When	I rotate keys and re-encrypt materials in staging
Then	Metrics show no errors and runbooks are updated

Definition of Ready: Apps instrumented; staging ready. • *Definition of Done:* Rotation proved in staging; prod schedule approved; runbook linked. **Tasks**

- □ Implement envelope encryption example.
- □ Add rotation job and alarms.
- □ Create decrypt fallback and test.
- □ Publish runbook with rollback plan.

AWS Tailoring

- □ Use KMS CMKs with rotation and least-privilege key policies.
- □ Encrypt S3, EBS, RDS by default; enforce via SCP/Config rules.
- □ Scan and classify sensitive data with Macie for key buckets.

CCS-13 — User-Side Key Controls

Epic / Feature	Client-Side Encryption
Business Value	Reduce provider breach blast radius.
Priority / Estimate	Priority: Should SP: 3
Persona	Client app developer
Dependencies	Crypto library, performance test tool
Assumptions / Risks	UX latency and key handling complexity
Cloud (AWS) Mapping	AWS KMS, AWS CloudHSM, External Key Store (XKS), Envelope Encryption Patterns

Story

As a client developer, I want to encrypt data before upload so that exposure risk is reduced.

Non-Functional

Performance Security Privacy

Acceptance Criteria (BDD)

Scenario	Client-side encryption prototype
Given	A demo dataset and upload path
When	I enable client encryption and measure overhead
Then	Latency impact and throughput are documented with limits

Definition of Ready: Test dataset ready. • *Definition of Done:* Prototype merged; thresholds set; backlog items filed.

Tasks

- ☐ Build client encryption function.
- ☐ Add perf test for 1 MB and 10 MB files.
- ☐ Document key custody options.
- ☐ Decide thresholds and guardrails.

AWS Tailoring

- ☐ Use KMS CMKs with rotation and least-privilege key policies.
- ☐ Encrypt S3, EBS, RDS by default; enforce via SCP/Config rules.
- ☐ Scan and classify sensitive data with Macie for key buckets.

CCS-5 — IaaS Focus

Epic / Feature	Compute, Storage, Network Hardening
Business Value	Prevent common misconfigurations at the IaaS layer.
Priority / Estimate	Priority: Must SP: 5
Persona	Platform engineer
Dependencies	Terraform repo, VPC/VNet, KMS, IAM
Assumptions / Risks	Breaking changes if defaults tighten without comms
Cloud (AWS) Mapping	AWS Organizations & Control Tower, AWS Config & Security Hub, CloudTrail, CloudWatch, GuardDuty, AWS KMS

Story

As a platform engineer, I want least-privilege IAM and default-deny networking so that IaaS resources are secure by default. **Non-Functional**

Security Reliability **Acceptance Criteria (BDD)**

Scenario	Secure defaults enforced
Given	A Terraform baseline module
When	I add network policies and least-privilege roles
Then	New resources inherit secure defaults and tests verify enforcement

Definition of Ready: Module owners onboard; tests planned. • *Definition of Done:* Module released; pipelines pass; docs updated. **Tasks**

- □ Harden security groups and route tables to default deny.
- □ Create least-privilege role for compute and storage access.
- □ Add unit tests for denial of wildcard permissions.
- □ Publish module usage guide.

AWS Tailoring

- □ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- □ Deploy AWS Config conformance packs; record all resources.
- □ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-17 — Locking Down Cloud Servers

Epic / Feature	Host Hardening
Business Value	Reduce attack surface of compute instances.
Priority / Estimate	Priority: Must SP: 5
Persona	Systems engineer
Dependencies	CIS benchmark, Ansible, osquery
Assumptions / Risks	Compatibility issues with legacy apps
Cloud (AWS) Mapping	AWS Organizations & Control Tower, AWS Config & Security Hub, CloudTrail, CloudWatch, GuardDuty, AWS KMS

Story

As a systems engineer, I want hardened server images validated by scans so that host-level risk is reduced. **Non-Functional**

Security Reliability **Acceptance Criteria (BDD)**

Scenario	Hardened image baseline
Given	A base operating system image
When	I apply Ansible hardening and validate with osquery
Then	Compliance score meets target and drift alerts are enabled

Definition of Ready: Baseline chosen. • *Definition of Done:* Image published; score documented; rollout plan approved. **Tasks**

- ☐ Build Ansible role for hardening.
- ☐ Add osquery pack for controls.
- ☐ Measure compliance score.
- ☐ Define rollout and fallback.

AWS Tailoring

- ☐ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- ☐ Deploy AWS Config conformance packs; record all resources.
- ☐ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-30 — Availability, Recovery, & Auditing

Epic / Feature	DR Runbook and Evidence
Business Value	Prove recoverability and auditing across sites.
Priority / Estimate	Priority: Must SP: 5
Persona	SRE lead
Dependencies	Backup system, failover tooling, logging
Assumptions / Risks	Testing may cause temporary disruption
Cloud (AWS) Mapping	AWS Backup (Vault Lock), Multi-AZ / Multi-Region patterns, S3 Cross-Region Replication, CloudTrail Lake & Athena

Story

As an SRE lead, I want a game day failover with evidence so that RPO and RTO are validated.

Non-Functional

Reliability Security **Acceptance Criteria (BDD)**

Scenario	Game day executed
Given	A DR runbook and staging environment
When	I fail over traffic and restore data
Then	RPO/RTO targets are met and audit artifacts stored

Definition of Ready: Runbook drafted; window approved. • *Definition of Done:* Postmortem completed; evidence archived; action items filed.

Tasks

- ☐ Dry-run backup restore.
- ☐ Switch traffic in staging.
- ☐ Collect logs and screenshots.
- ☐ Write postmortem with follow-ups.

AWS Tailoring

- ☐ Configure AWS Backup with Vault Lock and cross-account copies.
- ☐ Design Multi-AZ for stateful services and test DR runbooks quarterly.
- ☐ Query CloudTrail Lake for change/audit analytics.

CCS-18 — Third-Party Provider Integrity

Epic / Feature	Vendor Security
Business Value	Reduce supply-chain risk by verifying provider controls.
Priority / Estimate	Priority: Should SP: 3
Persona	TPRM analyst
Dependencies	Vendor portal, questionnaire, evidence store
Assumptions / Risks	Evidence may be incomplete or outdated
Cloud (AWS) Mapping	AWS Marketplace Vendor Controls, IAM cross-account roles & STS, AWS Artifact (BAA, SOC, ISO), AWS Audit Manager (control mapping)

Story

As a TPRM analyst, I want to evaluate a SaaS vendor so that integrity and compliance claims are validated. **Non-Functional**

Security Privacy **Acceptance Criteria (BDD)**

Scenario	Vendor assessed
Given	A completed questionnaire and shared evidence
When	I review SOC 2, ISO certs, pen test summaries
Then	Gaps and compensating controls are recorded with owners

Definition of Ready: Vendor identified. • *Definition of Done:* Assessment logged; renewal date tracked; follow-ups filed. **Tasks**

- □ Collect attestations and reports.
- □ Map to our control set.
- □ Record gaps and compensations.
- □ Schedule next review.

AWS Tailoring

- □ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- □ Deploy AWS Config conformance packs; record all resources.
- □ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-19 — Negotiating Security Requirements

Epic / Feature	Security Addendum
Business Value	Contractualize minimum controls and reporting duties.
Priority / Estimate	Priority: Must SP: 3
Persona	Security lead / legal partner
Dependencies	Contract template, DPA, counsel review
Assumptions / Risks	Negotiations may extend timelines
Cloud (AWS) Mapping	AWS Marketplace Vendor Controls, IAM cross-account roles & STS, AWS Artifact (BAA, SOC, ISO), AWS Audit Manager (control mapping)

Story

As a security lead, I want measurable security clauses so that vendor obligations are enforceable.

Non-Functional

Security Privacy **Acceptance Criteria (BDD)**

Scenario	Addendum executed
Given	A vendor contract in negotiation
When	I add breach notice timing, logging, crypto, and SRT clauses
Then	The executed contract contains measurable commitments

Definition of Ready: Template aligned with legal. • *Definition of Done:* Signed addendum archived; obligations tracked. **Tasks**

- □ Draft 10 key clauses.
- □ Align with DPA terms.
- □ Review with counsel.
- □ Track obligations in register.

AWS Tailoring

- □ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- □ Deploy AWS Config conformance packs; record all resources.
- □ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-20 — Legal Compliance for Personal Data

Epic / Feature	Privacy Compliance
Business Value	Demonstrate lawful processing and accountability.
Priority / Estimate	Priority: Must SP: 5
Persona	Privacy engineer
Dependencies	ROPA template, data map, DPO review
Assumptions / Risks	Data lineage unknown for some fields
Cloud (AWS) Mapping	AWS Marketplace Vendor Controls, IAM cross-account roles & STS, AWS Artifact (BAA, SOC, ISO), AWS Audit Manager (control mapping)

Story

As a privacy engineer, I want a record of processing and DFD so that obligations and flows are clear.

Non-Functional

Privacy Security

Acceptance Criteria (BDD)

Scenario	ROPA completed
Given	Access to systems and owners
When	I capture purposes, lawful basis, retention, and transfers
Then	Data flows and controls are documented and approved

Definition of Ready: Scope bounded; owners engaged. • *Definition of Done:* ROPA and DFD in repo; review sign-off captured.

Tasks

- ☐ Build `privacy/ropa.xlsx`.
- ☐ Draw data flow diagram.
- ☐ Validate retention policies.
- ☐ Add cross-border transfer notes.

AWS Tailoring

- ☐ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- ☐ Deploy AWS Config conformance packs; record all resources.
- ☐ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-27 — Government Certification & Accreditation

Epic / Feature	FedRAMP Readiness (example)
Business Value	Understand inheritance and required artifacts.
Priority / Estimate	Priority: Should SP: 3
Persona	Compliance lead
Dependencies	Control catalog, SSP template
Assumptions / Risks	Scope must be tightly defined
Cloud (AWS) Mapping	AWS GovCloud (US), FedRAMP / DoD SRG mappings, AWS Artifact (ATO packages)

Story

As a compliance lead, I want a control inheritance map so that authorization scope and responsibilities are clear. **Non-Functional**

Security Reliability **Acceptance Criteria (BDD)**

Scenario	Inheritance mapped
Given	A SaaS in scope
When	I mark provider vs customer controls
Then	The SSP references the map and gaps are tracked

Definition of Ready: Boundary defined. • *Definition of Done:* Matrix committed; SSP section drafted; gaps logged. **Tasks**

- □ Build inheritance matrix.
- □ Tag inherited controls.
- □ Draft SSP outline.
- □ Create gap tickets.

AWS Tailoring

- □ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- □ Deploy AWS Config conformance packs; record all resources.
- □ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-28 — Government Regulations & Compliance Risks

Epic / Feature	Regulatory Risk Log
Business Value	Avoid surprise obligations and penalties.
Priority / Estimate	Priority: Should SP: 3
Persona	Compliance analyst
Dependencies	Legal counsel, records policy
Assumptions / Risks	Regulations evolve; periodic review needed
Cloud (AWS) Mapping	AWS Audit Manager, AWS Artifact (Reports), AWS Security Hub, AWS Marketplace Vendor Controls, IAM cross-account roles & STS, AWS Artifact (BAA, SOC, ISO), AWS Audit Manager (control mapping), AWS GovCloud (US), FedRAMP / DoD SRG mappings, AWS Artifact (ATO packages)

Story

As a compliance analyst, I want a regulatory risk log so that export, retention, and sector rules are addressed. **Non-Functional**

Privacy Security **Acceptance Criteria (BDD)**

Scenario	Risks recorded with treatments
Given	A list of applicable regulations
When	I log risks and proposed mitigations
Then	Owners and deadlines are tracked

Definition of Ready: Sources identified. • *Definition of Done:* Log published; review cadence set; items assigned. **Tasks**

- □ List applicable regs per region.
- □ Identify records and retention needs.
- □ Document export-control flags.
- □ Assign owners and dates.

AWS Tailoring

- □ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- □ Deploy AWS Config conformance packs; record all resources.
- □ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-21 — Integrity Assurance for Data Outsourcing

Epic / Feature	Data Integrity
Business Value	Detect tampering and ensure recoverability.
Priority / Estimate	Priority: Should SP: 3
Persona	Storage engineer
Dependencies	Object lock, versioning, checksum pipeline
Assumptions / Risks	Immutability might affect lifecycle costs
Cloud (AWS) Mapping	AWS Nitro System & Nitro Enclaves, AWS Clean Rooms (privacy-enhancing analytics), AWS KMS / CloudHSM

Story

As a storage engineer, I want object immutability and verification so that outsourced data integrity is assured. **Non-Functional**

Reliability Security **Acceptance Criteria (BDD)**

Scenario	Immutability and verification enabled
Given	A critical bucket
When	I enable object lock and periodic checksum verification
Then	Evidence of integrity is logged and alerts fire on mismatch

Definition of Ready: Bucket identified. • *Definition of Done:* Policies active; verification job scheduled; alerts tested. **Tasks**

- ☐ Turn on versioning and object lock.
- ☐ Create checksum job.
- ☐ Store proofs and logs.
- ☐ Test corruption scenario.

AWS Tailoring

- ☐ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- ☐ Deploy AWS Config conformance packs; record all resources.
- ☐ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-22 — Secure Computation Outsourcing

Epic / Feature	Confidential Computing
Business Value	Protect workloads from host compromise.
Priority / Estimate	Priority: Should SP: 3
Persona	Platform engineer
Dependencies	Confidential VM or enclave offering
Assumptions / Risks	Limited tooling; higher cost
Cloud (AWS) Mapping	AWS Nitro System & Nitro Enclaves, AWS Clean Rooms (privacy-enhancing analytics), AWS KMS / CloudHSM

Story

As a platform engineer, I want to deploy a confidential VM demo so that sensitive code and data run in a protected environment. **Non-Functional**

Security Performance **Acceptance Criteria (BDD)**

Scenario	Demo deployed
Given	Access to confidential VM/Enclave service
When	I run a sample workload with attestation
Then	Attestation evidence is captured and documented

Definition of Ready: Service quota available. • *Definition of Done:* Demo works; evidence stored; decision matrix written. **Tasks**

- □ Launch confidential instance.
- □ Run attestation example.
- □ Capture measurements and logs.
- □ Write decision matrix.

AWS Tailoring

- □ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- □ Deploy AWS Config conformance packs; record all resources.
- □ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-23 — Computation Over Encrypted Data

Epic / Feature	Searchable Encryption / FHE Survey
Business Value	Enable limited queries without decrypting data.
Priority / Estimate	Priority: Could SP: 2
Persona	Research engineer
Dependencies	Sample dataset, library support
Assumptions / Risks	Performance and complexity constraints
Cloud (AWS) Mapping	AWS Nitro System & Nitro Enclaves, AWS Clean Rooms (privacy-enhancing analytics), AWS KMS / CloudHSM

Story

As a research engineer, I want to prototype encrypted search so that feasibility and limits are documented. **Non-Functional**

Security Performance **Acceptance Criteria (BDD)**

Scenario	Prototype results recorded
Given	A text dataset
When	I run encrypted keyword search
Then	Latency, correctness, and limits are summarized

Definition of Ready: Dataset ready. • *Definition of Done:* PoC code and report committed; go/no-go noted.

Tasks

- □ Choose library and scheme.
- □ Index and query dataset.
- □ Measure latency and size.
- □ Summarize findings.

AWS Tailoring

- □ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- □ Deploy AWS Config conformance packs; record all resources.
- □ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-24 — Trusted Computing Technology

Epic / Feature	Platform Trust
Business Value	Validate boot and workload integrity.
Priority / Estimate	Priority: Should SP: 3
Persona	Platform engineer
Dependencies	vTPM, secure boot, measurement service
Assumptions / Risks	Hardware support varies by provider
Cloud (AWS) Mapping	AWS KMS (CMKs), S3 Server-Side Encryption (SSE-KMS), Amazon Macie, AWS Lake Formation, AWS Nitro System & Nitro Enclaves, AWS Clean Rooms (privacy-enhancing analytics), AWS KMS / CloudHSM

Story

As a platform engineer, I want to verify secure boot and vTPM so that platform trust is established. **Non-Functional**

Security Reliability **Acceptance Criteria (BDD)**

Scenario	Attestation enabled
Given	A VM image and policy
When	I enable secure boot and verify measurements
Then	Evidence is stored and non-compliant boots alert

Definition of Ready: Image pipeline documented. • *Definition of Done:* Attestation evidence archived; alert tested. **Tasks**

- ☐ Enable secure boot and vTPM.
- ☐ Capture PCR measurements.
- ☐ Store evidence in repo.
- ☐ Add alert for failures.

AWS Tailoring

- ☐ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- ☐ Deploy AWS Config conformance packs; record all resources.
- ☐ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-25 — Trusted Security Tech: Survey & Gaps

Epic / Feature	Capability Heatmap
Business Value	Identify maturity and gaps for trusted tech.
Priority / Estimate	Priority: Could SP: 2
Persona	Security architect
Dependencies	Stakeholder input
Assumptions / Risks	Divergent views on maturity
Cloud (AWS) Mapping	AWS KMS (CMKs), S3 Server-Side Encryption (SSE-KMS), Amazon Macie, AWS Lake Formation

Story

As a security architect, I want a capability heatmap so that prioritization of trust tech investments is clear. **Non-Functional**

Security Reliability **Acceptance Criteria (BDD)**

Scenario	Heatmap published
Given	A list of capabilities
When	I score maturity and document gaps
Then	Roadmap items and owners are assigned

Definition of Ready: Capabilities enumerated. • *Definition of Done:* Heatmap slide shared; roadmap updated. **Tasks**

- □ Define scoring rubric.
- □ Collect scores from owners.
- □ Aggregate and visualize.
- □ File roadmap items.

AWS Tailoring

- □ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- □ Deploy AWS Config conformance packs; record all resources.
- □ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-26 — Trusted Computing Proposals

Epic / Feature	End-to-End Trust Chain
Business Value	Prove device to workload trust with attestations.
Priority / Estimate	Priority: Could SP: 2
Persona	Security engineer
Dependencies	Attestation service, identity provider
Assumptions / Risks	Complexity of chain-of-trust proofs
Cloud (AWS) Mapping	AWS KMS (CMKs), S3 Server-Side Encryption (SSE-KMS), Amazon Macie, AWS Lake Formation, AWS Nitro System & Nitro Enclaves, AWS Clean Rooms (privacy-enhancing analytics), AWS KMS / CloudHSM

Story

As a security engineer, I want an attestation flow design so that trust decisions can be automated. **Non-Functional**

Security Reliability **Acceptance Criteria (BDD)**

Scenario	Flow documented
Given	Components for device, boot, and workload
When	I design sequence of attestations
Then	Verification steps and failure modes are defined

Definition of Ready: Components inventoried. • *Definition of Done:* Sequence diagram and notes committed. **Tasks**

- ☐ Draft sequence diagram.
- ☐ List verification artifacts.
- ☐ Define failure responses.
- ☐ Review with platform team.

AWS Tailoring

- ☐ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- ☐ Deploy AWS Config conformance packs; record all resources.
- ☐ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-31 — Advanced Security Architecture

Epic / Feature	Service Mesh and Zero Trust
Business Value	Strong identity boundaries between services.
Priority / Estimate	Priority: Should SP: 3
Persona	Platform engineer
Dependencies	Istio or Linkerd, PKI
Assumptions / Risks	mTLS introduces complexity
Cloud (AWS) Mapping	Amazon VPC (Subnets, Route Tables, NACLs, SGs), AWS Transit Gateway, AWS Network Firewall, AWS WAF & AWS Shield, PrivateLink & VPC Endpoints, Verified Access, Verified Permissions (Cedar), Zero Trust with PrivateLink/TGW Segmentation

Story

As a platform engineer, I want mTLS via a service mesh so that service-to-service trust is explicit and auditable. **Non-Functional**

Security Reliability Performance **Acceptance Criteria (BDD)**

Scenario	Mesh policy enforced
Given	A cluster and sample services
When	I require authenticated identities for calls
Then	Unauthorized calls fail and metrics show encrypted traffic

Definition of Ready: PKI ready; cluster available. • *Definition of Done:* Policies applied; dashboards in place; rollback steps documented. **Tasks**

- ☐ Install mesh and issue certificates.
- ☐ Enforce mTLS and authZ policy.
- ☐ Expose metrics and logs.
- ☐ Document rollout plan.

AWS Tailoring

- ☐ Hub-and-spoke VPCs via TGW; centralized egress with Network Firewall.
- ☐ Disable public access for S3/EBS/RDS; require VPC endpoints for AWS APIs.
- ☐ Protect internet edges with WAF and (optionally) Shield Advanced.

CCS-32 — Side-Channel Attacks & Defenses

Epic / Feature	Side-Channel Awareness
Business Value	Reduce risk from timing and cache leakage.
Priority / Estimate	Priority: Could SP: 2
Persona	Security researcher
Dependencies	Benchmark harness, controlled environment
Assumptions / Risks	Synthetic tests may not reflect production
Cloud (AWS) Mapping	AWS Nitro System & Nitro Enclaves, AWS Clean Rooms (privacy-enhancing analytics), AWS KMS / CloudHSM
Story	

As a security researcher, I want to measure a simple timing side-channel and mitigation so that risk is understood. **Non-Functional**

Security Performance **Acceptance Criteria (BDD)**

Scenario	Signal measured and reduced
Given	A controlled test harness
When	I demonstrate a cache-timing signal and apply a mitigation
Then	The signal-to-noise ratio decreases per target threshold

Definition of Ready: Harness prepared. • *Definition of Done:* Notebook and results committed; mitigation guidance added. **Tasks**

- ☐ Implement timing measurement.
- ☐ Capture baseline signal.
- ☐ Apply mitigation and remeasure.
- ☐ Document recommendations.

AWS Tailoring

- ☐ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- ☐ Deploy AWS Config conformance packs; record all resources.
- ☐ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-33 — Critical Analysis of Threat Models

Epic / Feature	Meta Threat Modeling
Business Value	Expose assumptions about control planes and multi-tenancy.
Priority / Estimate	Priority: Should SP: 3
Persona	Red team lead
Dependencies	Access to assumptions and architecture docs
Assumptions / Risks	Sensitive topics require careful handling
Cloud (AWS) Mapping	Verified Access, Verified Permissions (Cedar), Zero Trust with PrivateLink/TGW Segmentation

Story

As a red team lead, I want to challenge threat model assumptions so that blind spots in cloud control planes are addressed. **Non-Functional**

Security Reliability **Acceptance Criteria (BDD)**

Scenario	Assumptions documented and tested
Given	An existing threat model
When	I write a red-team hypothesis targeting meta-control plane risks
Then	Detection ideas and mitigations are proposed and tracked

Definition of Ready: Model available. • *Definition of Done:* Hypothesis published; action items filed; follow-up scheduled. **Tasks**

- ☐ List explicit assumptions.
- ☐ Draft hypothesis and tests.
- ☐ Propose mitigations and detections.
- ☐ Track actions to closure.

AWS Tailoring

- ☐ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- ☐ Deploy AWS Config conformance packs; record all resources.
- ☐ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.

CCS-34 — Future Directions, Risks & Challenges

Epic / Feature	Forward-Looking Roadmap
Business Value	Prepare for PQ crypto, confidential ML, and SBOM/SLSA.
Priority / Estimate	Priority: Could SP: 2
Persona	Security strategist
Dependencies	Crypto inventory, CI pipeline, artifact signing
Assumptions / Risks	Changing standards and vendor support
Cloud (AWS) Mapping	AWS Audit Manager, AWS Artifact (Reports), AWS Security Hub, Verified Access, Verified Permissions (Cedar), Zero Trust with PrivateLink/TGW Segmentation

Story

As a security strategist, I want a forward-looking roadmap so that the program is ready for emerging risks and controls. **Non-Functional**

Security Reliability **Acceptance Criteria (BDD)**

Scenario	Roadmap published
Given	Current state inventory
When	I add PQ readiness, confidential ML, and SLSA milestones
Then	Owners and dates are assigned with review cadence

Definition of Ready: Inventory complete. • *Definition of Done:* Roadmap committed; review dates on calendar; scorecard added. **Tasks**

- □ Build crypto inventory and PQ plan.
- □ Define model confidentiality needs.
- □ Add SBOM and SLSA targets.
- □ Create quarterly scorecard.

AWS Tailoring

- □ Enable AWS Security Hub with CIS/AWS Foundational standards in the home region.
- □ Deploy AWS Config conformance packs; record all resources.
- □ Enable org-level CloudTrail with encryption (KMS) and S3 Object Lock.