Study Plan — CCISO Textbook

All User Stories & Template

A polished, output-driven set of user story cards covering Domains 1–5.

How to Use This Document

Use the blank card to add or adjust stories. Each domain below contains multiple ready-to-execute cards aligned to the lesson plan.

Blank Story Card (Duplicate & Fill)

ID-XXXX — Short, Action-Oriented Title

Epic / Feature	Domain/Chapter or Capability
Business Value	Concise outcome (why this matters)
Priority / Estimate	Priority: Must SP: 3
Persona	primary persona
Dependencies	key upstream/downstream
Assumptions / Risks	assumptions *Risks:* risks

Story *As a **persona**, I want to **Short, Action-Oriented Title** so that **Concise outcome**.*

Non-Functional

Performance

Security

Reliability

Accessibility

Privacy

i18n

Acceptance Criteria (BDD)

Scenario
Happy path
Given ...
When ...
Then ...

Scenario
Negative / edge
Given ...
When ...
Then ...

Tasks

- ❑ First concrete task (commands/paths/files where useful).
- ❑ Second concrete task.
- ❑ Third concrete task.
- ❑ Validation: job summary/dashboard shows metric(s) A/B/C.

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

Domain 1 — Governance & Risk Management

D1-01 — Establish Governance Charter

Epic / Feature	Domain 1 — Governance & Risk Management
Business Value	Board-aligned mandate defining roles, scope, decision rights, and metrics
Priority / Estimate	Priority: Must SP: 5
Persona	CISO
Dependencies	Org strategy; legal/compliance; exec sponsor
Assumptions / Risks	Policies exist in draft; governance board available *Risks:* Delayed approvals; unclear appetite

Story *As a **CISO**, I want to **publish a Governance Charter** so that **security objectives and metrics align to strategy and risk appetite**.* **Non-Functional**

Security

Reliability

Acceptance Criteria (BDD)

Scenario
Charter approved
Given a drafted charter and stakeholder feedback
When the sponsor signs and comms are published
Then the charter is versioned and visible on the intranet

Tasks

- ❑ Draft charter (scope, roles, cadence)
- ❑ Define risk appetite statement and governance metrics (KPI/KRI)
- ❑ Stakeholder review and approval routing
- ❑ Publish to intranet and policy repo

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D1-02 — Policy Manual & Standards Catalog

Epic / Feature	Domain 1 — Governance & Risk Management
Business Value	Single source of truth for policies and technical standards with lifecycle control
Priority / Estimate	Priority: Must SP: 5
Persona	Policy Owner
Dependencies	Charter approved; SMEs available
Assumptions / Risks	Existing scattered documents *Risks:* Inconsistent guidance; audit findings

Story *As a* ***Policy Owner****, I want to* ***publish a policy manual and standards catalog*** *so that* ***teams use consistent, approved guidance.*** **Non-Functional**

Security

Reliability

Accessibility

Acceptance Criteria (BDD)

Scenario
Manual published
Given policy drafts exist
When they are normalized and merged
Then a versioned manual with review dates exists

Scenario
Standards mapped
Given standards per domain are drafted
When they link to policies and controls
Then a catalog exists with owners, review cadence

Tasks

- ❑ Inventory policies/standards; normalize format
- ❑ Define policy lifecycle (draft, approve, communicate, attest, review)
- ❑ Publish catalog with owners and review cadence
- ❑ Set up attestation workflow

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D1-03 — Risk Management Policy & Procedure

Epic / Feature	Domain 1 — Governance & Risk Management
Business Value	Consistent risk assessments and treatments with acceptance criteria
Priority / Estimate	Priority: Must SP: 5
Persona	Risk Manager
Dependencies	Framework chosen (ISO 31000/27005 or NIST); tool available
Assumptions / Risks	Limited risk data *Risks:* Inconsistent scoring; unapproved residual risk

Story *As a* ***Risk Manager****, I want to* ***establish risk policy and procedures*** *so that* ***risks are identified, analyzed, treated and accepted consistently.*** **Non-Functional**

Security

Reliability

Privacy

Acceptance Criteria (BDD)

Scenario
Procedure approved
Given draft policy and workflow
When leadership approves
Then the procedure is published with templates

Tasks

- ❑ Select framework and scales; define acceptance thresholds
- ❑ Create templates (register, assessment, treatment plan)
- ❑ Train stakeholders; pilot on two business processes
- ❑ Publish results and lessons learned

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D1-04 — Baseline Risk Register & Acceptance Rules

Epic / Feature	Domain 1 — Governance & Risk Management
Business Value	Centralized, prioritized view of enterprise risks and decisions
Priority / Estimate	Priority: Must SP: 3
Persona	Risk Analyst
Dependencies	Risk policy in place; SMEs
Assumptions / Risks	Sparse inventory *Risks:* Gaps in coverage; duplicate entries

Story *As a* ***Risk Analyst****, I want to* ***seed a risk register and acceptance criteria*** *so that* ***decision makers see prioritized risks and owners.*** **Non-Functional**

Security

Reliability

Acceptance Criteria (BDD)

Scenario
Register created
Given inputs from audits, incidents, assessments
When entries are normalized and scored
Then the register shows owner, treatment, due dates

Tasks

- ❑ Create repository (/governance/risk/register.csv or tool)
- ❑ Import initial risks (top 20); normalize and score
- ❑ Assign owners and due dates; define acceptance thresholds
- ❑ Publish dashboard/baseline report

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D1-05 — Compliance Obligations Map

Epic / Feature	Domain 1 — Governance & Risk Management
Business Value	Traceability from laws/regs to policies, controls and evidence
Priority / Estimate	Priority: Should SP: 3
Persona	Compliance Lead
Dependencies	List of obligations; control catalog
Assumptions / Risks	Ambiguous mappings *Risks:* Audit gaps

Story *As a* ***Compliance Lead****, I want to* ***map obligations to controls*** *so that* ***evidence and ownership are clear for audits****.* **Non-Functional**

Security

Privacy

Acceptance Criteria (BDD)

Scenario
Mapping complete
Given obligations list exists
When each clause is mapped
Then every clause has a control/evidence/owner

Tasks

- ❑ Collect obligations (SOX, PCI DSS, HIPAA, GLBA, etc.)
- ❑ Map to policies and control IDs
- ❑ Record evidence location and owner per mapping
- ❑ Publish matrix and review quarterly

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D1-06 — Privacy Principles Integration

Epic / Feature	Domain 1 — Governance & Risk Management
Business Value	Policy and control updates reflecting privacy principles and data subject rights
Priority / Estimate	Priority: Could SP: 3
Persona	Privacy Officer
Dependencies	Data classification; legal review
Assumptions / Risks	Legacy data handling *Risks:* Non-compliance risk

Story *As a* ***Privacy Officer****, I want to* ***embed privacy principles in policies/controls*** *so that* ***processing aligns with regulatory expectations****.* **Non-Functional**

Privacy

Security

Acceptance Criteria (BDD)

Scenario
Principles applied
Given policy set exists
When privacy requirements are added
Then policies list lawful basis, minimization, retention

Tasks

- ❑ Review policies for privacy gaps
- ❑ Add consent/lawful basis, retention, DSAR handling
- ❑ Update training and attestation

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D1-07 — Governance Metrics Dashboard

Epic / Feature	Domain 1 — Governance & Risk Management
Business Value	Executive visibility via KPI/KRI set and reporting cadence
Priority / Estimate	Priority: Should SP: 3
Persona	CISO
Dependencies	Data sources; BI tool
Assumptions / Risks	Data quality issues *Risks:* Misinterpretation

Story *As a **CISO**, I want to **publish governance metrics** so that **leadership tracks outcomes and trends.*** **Non-Functional**

Performance

Reliability

Acceptance Criteria (BDD)

Scenario
Dashboard live
Given metric definitions exist
When data is connected
Then dashboards show baseline and targets

Tasks

- ❑ Define metrics and owners
- ❑ Connect data sources; build dashboard
- ❑ Schedule monthly review and QBR snapshot

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D1-08 — Policy Attestation Workflow

Epic / Feature	Domain 1 — Governance & Risk Management
Business Value	Evidence that staff acknowledged policies on cadence
Priority / Estimate	Priority: Could SP: 2
Persona	Compliance Officer
Dependencies	IDP/email system
Assumptions / Risks	Low completion rates *Risks:* Stale attestations

Story *As a* ***Compliance Officer****, I want to* ***automate policy attestation*** *so that* ***evidence exists for audits.*** **Non-Functional**

Security

Accessibility

Acceptance Criteria (BDD)

Scenario
Attestations recorded
Given AD groups exist
When campaign is launched
Then completion is tracked and reminders sent

Tasks

- ❑ Configure campaign; target audiences
- ❑ Send notifications; track completions
- ❑ Export attestation report to evidence store

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

Domain 2 — Security Risk Management, Controls & Audit

D2-01 — Baseline Control Framework

Epic / Feature	Domain 2 — Security Risk Management, Controls & Audit
Business Value	Unified control catalog with test procedures and evidence locations
Priority / Estimate	Priority: Must SP: 5
Persona	Risk Manager
Dependencies	Framework chosen; evidence store
Assumptions / Risks	Over-scoping *Risks:* Duplicate controls

Story *As a **Risk Manager**, I want to **publish a control catalog** so that **audits use a single, testable baseline**.* **Non-Functional**

Security

Reliability

Acceptance Criteria (BDD)

Scenario
Catalog published
Given controls mapped to requirements
When catalog merged to /governance/controls/
Then each control lists owner, frequency, test, evidence link

Scenario
Audit readiness
Given an auditor requests samples
When the control is tested
Then results and CAPA are recorded

Tasks

- ❑ Import framework controls; normalize IDs
- ❑ Add owners, frequencies, test procedures
- ❑ Link policies/standards and dashboards
- ❑ Pilot internal test on 5 controls

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D2-02 — Access Control Policy & SoD

Epic / Feature	Domain 2 — Security Risk Management, Controls & Audit
Business Value	Clear identity lifecycle rules with segregation-of-duties
Priority / Estimate	Priority: Must SP: 3
Persona	IAM Lead
Dependencies	HR feed; ticketing system
Assumptions / Risks	Shadow access *Risks:* Excess privileges

Story *As an **IAM Lead**, I want to **publish access control policy and SoD** so that **joiner/-mover/leaver is enforced and risk reduced**.* **Non-Functional**

Security

Privacy

Acceptance Criteria (BDD)

Scenario
Policy approved
Given draft policy exists
When stakeholders approve
Then policy is published with examples and SoD matrix

Tasks

- ❑ Define roles, SoD matrix, review cadence
- ❑ Document joiner/mover/leaver workflow
- ❑ Automate access review reminders

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D2-03 — Compliance Management SOP

Epic / Feature	Domain 2 — Security Risk Management, Controls & Audit
Business Value	Repeatable compliance calendar and evidence collection
Priority / Estimate	Priority: Should SP: 3
Persona	Compliance Lead
Dependencies	Obligation map; owners
Assumptions / Risks	Missed deadlines *Risks:* Evidence gaps

Story *As a* ***Compliance Lead****, I want to* ***run a compliance calendar with SOP*** *so that* ***evidence is timely and complete.*** **Non-Functional**

Reliability

Security

Acceptance Criteria (BDD)

Scenario
Calendar active
Given obligations are known
When events are scheduled
Then reminders and checklists exist per event

Tasks

- ❑ Create calendar with owners and due dates
- ❑ Standardize evidence naming and storage
- ❑ Run monthly checkpoint meeting

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D2-04 — Annual Audit Plan & CAPA

Epic / Feature	Domain 2 — Security Risk Management, Controls & Audit
Business Value	Planned audits with corrective/preventive actions tracked to closure
Priority / Estimate	Priority: Must SP: 5
Persona	Internal Auditor
Dependencies	Control catalog; risk register
Assumptions / Risks	Scope creep *Risks:* Unowned actions

Story *As an **Internal Auditor**, I want to **publish an audit plan and CAPA process** so that **issues are addressed and verified.*** **Non-Functional**

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Plan approved
Given draft plan exists
When audit committee approves
Then plan is published with timelines

Scenario
CAPA closed
Given findings are logged
When actions are assigned
Then verification evidence is stored

Tasks

- ❑ Prioritize audits by risk
- ❑ Publish plan with sampling approach
- ❑ Create CAPA workflow; dashboards for status
- ❑ Hold monthly follow-ups

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D2-05 — Evidence Repository & Sampling

Epic / Feature	Domain 2 — Security Risk Management, Controls & Audit
Business Value	Central evidence with consistent sampling instructions
Priority / Estimate	Priority: Should SP: 3
Persona	Auditor
Dependencies	Storage system; versioning
Assumptions / Risks	Inconsistent files *Risks:* Missing timestamps

Story *As an* ***Auditor****, I want to* ***standardize evidence storage and sampling*** *so that* ***audits are repeatable and defensible.*** **Non-Functional**

Reliability

Acceptance Criteria (BDD)

Scenario
Evidence standardized
Given templates exist
When teams use them
Then files include timestamps, owner, system, scope

Tasks

- ❑ Create evidence templates and directory structure
- ❑ Document sampling sizes per control/type
- ❑ Train teams; spot-check usage

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D2-06 — Control Effectiveness Metrics

Epic / Feature	Domain 2 — Security Risk Management, Controls & Audit
Business Value	Quantified view of control health and failures
Priority / Estimate	Priority: Should SP: 3
Persona	CISO
Dependencies	BI tool; control catalog
Assumptions / Risks	Gaming metrics *Risks:* Data latency

Story *As a **CISO**, I want to **track control effectiveness** so that **we prioritize improvements by impact.*** **Non-Functional**

Performance

Reliability

Acceptance Criteria (BDD)

Scenario
Dashboard live
Given metrics are defined
When data is connected
Then weekly/quarterly views show trends and failures

Tasks

- ❑ Define metrics per control category
- ❑ Connect data; build dashboards
- ❑ Set review cadence with owners

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D2-07 — SOX/PCI Mapping Exercise

Epic / Feature	Domain 2 — Security Risk Management, Controls & Audit
Business Value	Confidence that critical regulations are fully covered
Priority / Estimate	Priority: Could SP: 2
Persona	Compliance Analyst
Dependencies	Obligation map; control catalog
Assumptions / Risks	Gaps unspotted *Risks:* Audit surprises

Story *As a* ***Compliance Analyst****, I want to* ***map SOX/PCI clauses to controls*** *so that* ***we confirm coverage and evidence.*** **Non-Functional**

Security

Reliability

Acceptance Criteria (BDD)

Scenario
Mapping complete
Given clause list exists
When each clause maps to controls
Then evidence and owners are verified

Tasks

- ❑ Build mapping spreadsheet
- ❑ Review with control owners
- ❑ Publish gap list and remediation items

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D2-08 — Identity Reviews & Recertification

Epic / Feature	Domain 2 — Security Risk Management, Controls & Audit
Business Value	Periodic access reviews with sign-off and exceptions handling
Priority / Estimate	Priority: Could SP: 2
Persona	IAM Lead
Dependencies	Directory; app lists
Assumptions / Risks	Review fatigue *Risks:* Stale entitlements

Story *As an **IAM Lead**, I want to **run periodic access reviews** so that **excessive privileges are removed.*** **Non-Functional**

Security

Privacy

Acceptance Criteria (BDD)

Scenario
Reviews completed
Given review windows are open
When owners certify or revoke
Then exceptions are documented and tracked

Tasks

- ❑ Schedule campaigns per system
- ❑ Generate reviewer lists and instructions
- ❑ Track completion and exceptions; archive results

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

Domain 3 — Security Program Management & Operations

D3-01 — Program Roadmap & Quarterly OKRs

Epic / Feature	Domain 3 — Program Management & Operations
Business Value	Multi-year capability plan and measurable quarterly outcomes
Priority / Estimate	Priority: Must SP: 5
Persona	Program Manager
Dependencies	Strategy; budget guardrails
Assumptions / Risks	Overcommitment *Risks:* Misaligned priorities

Story *As a* ***Program Manager****, I want to* ***publish a roadmap and OKRs*** *so that* ***security investments deliver outcomes.*** **Non-Functional**

Performance

Reliability

Acceptance Criteria (BDD)

Scenario
Roadmap approved
Given draft exists
When governance board approves
Then timeline and dependencies are published

Tasks

- ❑ Define capabilities and milestones (12–24 months)
- ❑ Set quarterly OKRs and metrics
- ❑ Publish roadmap; review each quarter

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D3-02 — Incident Response Plan & Tabletop

Epic / Feature	Domain 3 — Program Management & Operations
Business Value	Rehearsed breach response with roles and SLAs
Priority / Estimate	Priority: Must SP: 5
Persona	IR Lead
Dependencies	SIEM; on-call; comms
Assumptions / Risks	Slow comms *Risks:* Role confusion

Story *As an **IR Lead**, I want to **publish an IR plan and run a tabletop** so that **we validate detection-to-recovery**.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Plan approved
Given runbook drafted
When stakeholders approve
Then versioned plan is in repo

Scenario
Tabletop executed
Given scenario is prepared
When simulation is run end-to-end
Then issues are captured and actions assigned

Tasks

- ❑ Write runbook (triage, containment, eradication, recovery, comms)
- ❑ Define SEV levels and timelines
- ❑ Schedule tabletop; after-action report
- ❑ Update runbook

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D3-03 — BCP/DR Playbooks & RTO/RPO

Epic / Feature	Domain 3 — Program Management & Operations
Business Value	Resilience targets validated for critical services
Priority / Estimate	Priority: Must SP: 5
Persona	Resilience Lead
Dependencies	Asset inventory; owners
Assumptions / Risks	Unrealistic targets *Risks:* Unpracticed steps

Story *As a **Resilience Lead**, I want to **publish BCP/DR playbooks with RTO/RPO** so that **critical services recover predictably**.* **Non-Functional**

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Playbooks approved
Given drafts exist
When owners approve
Then RTO/RPO per service are recorded

Scenario
Test executed
Given a DR test is scheduled
When failover is performed
Then results and gaps are documented

Tasks

- ❑ Identify critical services and dependencies
- ❑ Document playbooks and contacts
- ❑ Schedule DR test; capture results
- ❑ Remediate and retest when needed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D3-04 — Vulnerability Management Process

Epic / Feature	Domain 3 — Program Management & Operations
Business Value	Risk-based patching and remediation workflow with SLAs
Priority / Estimate	Priority: Must SP: 5
Persona	VM Lead
Dependencies	Scanner; ticketing; owners
Assumptions / Risks	Backlogs grow *Risks:* Exceptions untracked

Story *As a* ***VM Lead****, I want to* ***run a risk-based VM process*** *so that* ***critical exposures are remediated on SLA****.* **Non-Functional**

Security

Performance

Acceptance Criteria (BDD)

Scenario
Process running
Given assets are scanned
When findings are triaged by risk
Then tickets are created and tracked to SLA

Tasks

- ❑ Define severity/risk model; set SLAs
- ❑ Integrate scanner with ticketing
- ❑ Weekly triage; monthly metrics
- ❑ Exception management workflow

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D3-05 — Logging/SIEM Use Case Catalog

Epic / Feature	Domain 3 — Program Management & Operations
Business Value	Detectable behaviors prioritized by risk and feasibility
Priority / Estimate	Priority: Should SP: 3
Persona	Detection Engineer
Dependencies	SIEM; data sources
Assumptions / Risks	Noise *Risks:* Alert fatigue

Story *As a* ***Detection Engineer****, I want to* ***publish a use case catalog*** *so that* ***detections are risk-aligned and testable.*** **Non-Functional**

Security

Performance

Acceptance Criteria (BDD)

Scenario
Catalog published
Given threats are prioritized
When detections authored
Then test cases and owners are listed

Tasks

- ❑ Inventory data sources and gaps
- ❑ Define top 15 use cases; add test data
- ❑ Publish detection runbook and owners

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D3-06 — Awareness & Training Program

Epic / Feature	Domain 3 — Program Management & Operations
Business Value	Behavioral change through targeted content and measurement
Priority / Estimate	Priority: Should SP: 3
Persona	Awareness Lead
Dependencies	LMS; comms
Assumptions / Risks	Low engagement *Risks:* No behavior shift

Story *As an* ***Awareness Lead****, I want to* ***run a targeted training program*** *so that* ***measurable behaviors improve.*** **Non-Functional**

Accessibility

Security

Acceptance Criteria (BDD)

Scenario
Program live
Given audiences defined
When content and schedule set
Then metrics show completion and phish-resist scores

Tasks

- ❑ Segment audiences and objectives
- ❑ Build content calendar and campaigns
- ❑ Measure outcomes; iterate quarterly

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D3-07 — Change Management Integration

Epic / Feature	Domain 3 — Program Management & Operations
Business Value	Security reviews embedded in change and release processes
Priority / Estimate	Priority: Could SP: 2
Persona	Change Manager
Dependencies	ITSM; CAB schedule
Assumptions / Risks	Shadow changes *Risks:* Late review

Story *As a **Change Manager**, I want to **embed security checks in change mgmt** so that **risk is assessed before deployment.*** **Non-Functional**

Reliability

Security

Acceptance Criteria (BDD)

Scenario
CAB gates active
Given change types labeled
When risk questions answered
Then security approvals required for high-risk

Tasks

- ❑ Define security questions and thresholds
- ❑ Update change forms and workflows
- ❑ Train CAB; monitor compliance

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

Domain 4 — Information Security Core Concepts

D4-01 — Access Control Standard & UAR

Epic / Feature	Domain 4 — Information Security Core Concepts
Business Value	Approved models and user access reviews for joiner/mover/leaver
Priority / Estimate	Priority: Must SP: 3
Persona	Security Architect
Dependencies	IAM; HR feed
Assumptions / Risks	Legacy model *Risks:* Manual reviews

Story *As a* ***Security Architect****, I want to* ***publish an access control standard and UAR process*** *so that* ***access is appropriate and reviewed.*** **Non-Functional**

Security

Privacy

Acceptance Criteria (BDD)

Scenario
Standard adopted
Given model and rules defined
When teams review and sign off
Then quarterly UAR cadence is live

Tasks

- ❑ Document models (RBAC/ABAC), SoD, review frequency
- ❑ Define UAR workflow and evidence
- ❑ Publish exceptions process

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D4-02 — Cryptography Standard & KMS

Epic / Feature	Domain 4 — Information Security Core Concepts
Business Value	Consistent, secure use of approved algorithms and key lifecycle
Priority / Estimate	Priority: Should SP: 3
Persona	Security Architect
Dependencies	KMS/HSM; app owners
Assumptions / Risks	Legacy ciphers *Risks:* Ad-hoc keys

Story *As a* ***Security Architect****, I want to* ***publish a crypto standard*** *so that* ***systems use approved algorithms with managed keys****.* **Non-Functional**

Security

Privacy

Reliability

Acceptance Criteria (BDD)

Scenario
Standard adopted
Given approved algorithms and lifecycles listed
When teams sign off
Then non-compliant suites are remediated

Tasks

- ❑ Draft algorithms, TLS profiles, sizes
- ❑ Document key lifecycle (gen/rotate/escrow/revoke/destroy)
- ❑ Create exceptions and remediation plan

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D4-03 — Logging & Retention Standard

Epic / Feature	Domain 4 — Information Security Core Concepts
Business Value	Consistent telemetry with retention mapped to legal/privacy requirements
Priority / Estimate	Priority: Should SP: 3
Persona	Security Engineer
Dependencies	SIEM; storage
Assumptions / Risks	Gaps *Risks:* Excess retention

Story *As a* ***Security Engineer****, I want to* ***define logging/retention standards*** *so that* ***evidence and detection are reliable.*** **Non-Functional**

Security

Privacy

Reliability

Acceptance Criteria (BDD)

Scenario
Standard published
Given sources and formats defined
When retention set per class
Then teams configure shipping and verify

Tasks

- ❑ List required logs per system
- ❑ Define schemas and timestamps; time sync policy
- ❑ Map retention to privacy/legal; update SIEM pipelines

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D4-04 — Digital Forensics SOP

Epic / Feature	Domain 4 — Information Security Core Concepts
Business Value	Evidence preservation and chain-of-custody processes
Priority / Estimate	Priority: Should SP: 3
Persona	Forensics Lead
Dependencies	Case management; storage
Assumptions / Risks	Spoiled evidence *Risks:* Unusable findings

Story *As a **Forensics Lead**, I want to **publish a forensics SOP** so that **evidence handling is defensible.*** **Non-Functional**

Security

Reliability

Acceptance Criteria (BDD)

Scenario
SOP approved
Given procedures drafted
When legal signs off
Then forms for custody and reporting exist

Tasks

- ❑ Write acquisition/preservation/analysis/report sections
- ❑ Create chain-of-custody template
- ❑ Train IR team; run a dry run

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D4-05 — Secure SDLC Policy & CI Gates

Epic / Feature	Domain 4 — Information Security Core Concepts
Business Value	Embedded security checks across SDLC with CI pipeline gates
Priority / Estimate	Priority: Must SP: 5
Persona	AppSec Lead
Dependencies	Repo; CI; scanners
Assumptions / Risks	Developer friction *Risks:* False positives

Story *As an **AppSec Lead**, I want to **publish secure SDLC policy and CI gates** so that **defects are prevented earlier**.* **Non-Functional**

Security

Performance

Acceptance Criteria (BDD)

Scenario
Gates active
Given policy defines required checks
When CI runs SAST/SCA/DAST/IaC
Then builds fail on thresholds; exceptions tracked

Tasks

- ❑ Define policy: required checks and thresholds
- ❑ Integrate scanners into CI
- ❑ Create exception workflow and dashboards

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D4-06 — Physical Security Integration

Epic / Feature	Domain 4 — Information Security Core Concepts
Business Value	Alignment between physical access and information security
Priority / Estimate	Priority: Could SP: 2
Persona	Security Architect
Dependencies	Facilities; badge system; CCTV
Assumptions / Risks	Tailgating *Risks:* Unlinked revocations

Story *As a* ***Security Architect****, I want to* ***align physical and logical access*** *so that* ***risk is reduced across domains.*** **Non-Functional**

Security

Reliability

Acceptance Criteria (BDD)

Scenario
Feeds integrated
Given badge data exists
When feeds linked to IAM
Then joiner/mover/leaver applies to badges

Tasks

- ❑ Document integration points
- ❑ Implement feed to IAM or SIEM
- ❑ Create periodic reconciliation report

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

Domain 5 — Strategic Planning, Finance, Procurement & Vendor Management

D5-01 — 3-Year Security Strategy & Investment Thesis

Epic / Feature	Domain 5 — Strategy, Finance, Procurement & Vendor Management
Business Value	Board-ready strategy translating risk to funded capabilities
Priority / Estimate	Priority: Must SP: 5
Persona	CISO
Dependencies	Enterprise strategy; risk register
Assumptions / Risks	Budget limits *Risks:* Shifting priorities

Story *As a **CISO**, I want to **publish a 3-year strategy and investment thesis** so that **funding aligns to risk and outcomes**.* **Non-Functional**

Performance

Reliability

Acceptance Criteria (BDD)

Scenario
Strategy approved
Given draft strategy exists
When executives approve
Then portfolio and milestones are baselined

Tasks

- ❑ Write executive narrative and capability map
- ❑ Prioritize portfolio; define success metrics
- ❑ Publish roadmap and review cadence

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D5-02 — Financial Plan & Budget Model

Epic / Feature	Domain 5 — Strategy, Finance, Procurement & Vendor Management
Business Value	Transparent run/grow/transform budget with ROI/TCO views
Priority / Estimate	Priority: Must SP: 5
Persona	Finance Partner
Dependencies	Tooling; vendor quotes
Assumptions / Risks	Cost overruns *Risks:* Underfunded ops

Story *As a **Finance Partner**, I want to **build a financial plan** so that **spend is justified and tracked.*** **Non-Functional**

Performance

Acceptance Criteria (BDD)

Scenario
Plan approved
Given inputs collected
When scenario model prepared
Then budget submitted and approved

Tasks

- ❑ Collect OPEX/CAPEX inputs; model scenarios
- ❑ Define ROI/TCO and benefits tracking
- ❑ Publish monthly forecast dashboard

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D5-03 — RFI/RFP & SLA Template Pack

Epic / Feature	Domain 5 — Strategy, Finance, Procurement & Vendor Management
Business Value	Consistent sourcing artifacts and enforceable service levels
Priority / Estimate	Priority: Should SP: 3
Persona	Sourcing Lead
Dependencies	Legal; SMEs
Assumptions / Risks	Ambiguous bids *Risks:* Weak SLAs

Story *As a* ***Sourcing Lead****, I want to* ***publish RFI/RFP and SLA templates*** *so that* ***vendors are evaluated consistently.*** **Non-Functional**

Reliability

Acceptance Criteria (BDD)

Scenario
Templates published
Given requirements gathered
When templates finalized
Then evaluation matrix and SLA catalog exist

Tasks

- ❑ Draft templates and scoring matrix
- ❑ Define SLA/KPI catalog and penalties
- ❑ Publish pack; train evaluators

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D5-04 — Vendor Tiering & Due Diligence

Epic / Feature	Domain 5 — Strategy, Finance, Procurement & Vendor Management
Business Value	Risk-based tiers with questionnaires and evidence lists
Priority / Estimate	Priority: Must SP: 4
Persona	TPRM Lead
Dependencies	Vendor list; owners
Assumptions / Risks	Shadow IT *Risks:* Incomplete reviews

Story *As a* ***TPRM Lead****, I want to* ***establish vendor tiering and due diligence*** *so that* ***third-party risk is known and managed****.* **Non-Functional**

Security

Privacy

Reliability

Acceptance Criteria (BDD)

Scenario
Tiering live
Given criteria defined
When vendors tiered
Then required controls/evidence per tier recorded

Tasks

- ❑ Publish tiering rules and required controls
- ❑ Roll out questionnaires and evidence lists
- ❑ Track remediation and exceptions

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D5-05 — QBR & Vendor Performance Monitoring

Epic / Feature	Domain 5 — Strategy, Finance, Procurement & Vendor Management
Business Value	Operational visibility of SLAs and continuous improvement
Priority / Estimate	Priority: Should SP: 3
Persona	Vendor Manager
Dependencies	SLA reports; dashboard
Assumptions / Risks	Data delays *Risks:* Unclear owners

Story *As a* ***Vendor Manager****, I want to* ***run QBRs with SLA dashboards*** *so that* ***service quality improves.*** **Non-Functional**

Performance

Reliability

Acceptance Criteria (BDD)

Scenario
QBR cadence running
Given SLA data collected
When dashboards shared
Then actions and outcomes tracked per vendor

Tasks

- ❑ Ingest SLA data monthly
- ❑ Prepare QBR deck; track actions
- ❑ Publish scorecards per vendor

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

D5-06 — Exit & Termination Plan

Epic / Feature	Domain 5 — Strategy, Finance, Procurement & Vendor Management
Business Value	Controlled offboarding with data return/destruction and continuity
Priority / Estimate	Priority: Could SP: 2
Persona	TPRM Lead
Dependencies	Legal; owners
Assumptions / Risks	Stranded data *Risks:* Service disruption

Story *As a **TPRM Lead**, I want to **publish exit plans** so that **vendor transitions are orderly and compliant.*** **Non-Functional**

Security

Reliability

Privacy

Acceptance Criteria (BDD)

Scenario
Plan adopted
Given requirements drafted
When legal approves clauses
Then runbook exists per critical vendor

Tasks

- ❑ Define data return/destruction clauses
- ❑ Document exit runbook per critical vendor
- ❑ Schedule annual tabletop for one vendor

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. Definition of Done: All ACs pass; Tests green; Security/a11y checks; Docs updated; Deployed/flagged.

Writing Effective User Stories (Quick Guide)

INVEST — Independent, Negotiable, Valuable, Estimable, Small, Testable. **3 Cs** — Card, Conversation, Confirmation. **Skeletons**

- As a [persona], I want to [action] so that [benefit].
- When [situation], as [persona], I want [motivation] so I can [outcome].

Acceptance Criteria Tips

- Prefer observable outcomes; one behavior per scenario.
- Cover happy path, negatives, edges; specify data bounds/messages.
- Tie to dashboards/metrics where useful.