# Study Plan — The Official $(ISC)^2$ CISSP CBK Reference (6th Ed.)

User Story Card Template (Runaway-proof, portable checkboxes)

October 27, 2025

## Contents

# 1 Story Card Definition (Required Fields)

| | |
|---|---|
| **Epic / Feature** | The capability or chapter grouping this story advances (e.g., "Domain 1: Security & Risk Management"). |
| **Business Value** | The outcome the story enables (e.g., "risk-based decision-making" or "$\geq$ 80% on domain practice set"). |
| **Priority / Estimate** | Priority (Must/Should/Could) and rough size (story points or hours). |
| **Persona** | Who benefits or performs the work ("CISSP candidate"). |
| **Dependencies** | Prereqs (prior chapters, tools, accounts, baseline knowledge). |
| **Assumptions** | What you believe to be true going in (CBK access, practice bank). |
| **Risks** | What could block success (limited time, weak crypto background). |
| **Story** | **As a** *[persona]*, **I want** *[capability]* **so that** *[business value]*. |
| **Non-Functional** | Tags such as Security, Reliability, Privacy, Accessibility. |
| **Acceptance Criteria (BDD)** | Use Given/When/Then. Aim for 3–6 criteria that are objectively verifiable. |
| **Definition of Ready** | Persona clear; AC drafted; dependencies known; estimate set; scope $\leq$ 1 week. |
| **Definition of Done** | All AC pass; notes updated; flashcards created; practice set completed; retrospective logged. |

# 2 Blank Story Card (Copy Me)

| | |
|---|---|
| **Epic / Feature** | <Domain or chapter grouping> |
| **Business Value** | <Outcome this story enables> |
| **Priority / Estimate** | Priority: <Must/Should/Could> SP: <1–5> (or hours) |
| **Persona** | <Who benefits / executes> |
| **Dependencies** | <Prereqs> |
| **Assumptions** | <Starting assumptions> |
| **Risks** | <Potential blockers> |
| **Story** | *As a <persona>, I want <capability> so that <business value>.* |
| **Non-Functional** | Security Reliability Privacy Accessibility |

**Acceptance Criteria (BDD)**

| | |
|---|---|
| **Scenario** | Happy path |
| **Given** | <preconditions> |
| **When** | <action or study work is completed> |
| **Then** | <observable outcome / evidence> |

**Definition of Ready:** persona clear; AC drafted; dependencies known; estimate set.
**Definition of Done:** all AC pass; notes/flashcards updated; practice set completed;

retrospective logged.

**Tasks**

- ☐ <Task 1 (concrete, 15–60 minutes)>
- ☐ <Task 2>
- ☐ <Task 3>
- ☐ <Create 10–20 flashcards; complete 30–50 domain questions>
- ☐ <Summarize key confusions for review>

# 3 CISSP CBK Domain User Stories

| | |
|---|---|
| **Epic / Feature** | Domain 1: Security & Risk Management |
| **Business Value** | Establish a risk-based, policy-driven foundation that improves decision-making across all domains. |
| **Priority / Estimate** | Priority: Must SP: 3 |
| **Persona** | CISSP candidate |
| **Dependencies** | Access to CBK ch. 1 materials; practice Q bank; note/flashcard system |
| **Assumptions** | 4-hour timebox; basic familiarity with risk terms |
| **Risks** | Over-scoping legal topics; skipping retrospective |
| **Story** | *As a CISSP candidate, I want to master ethics, governance, and risk analysis so that I can justify control selection and compliance tradeoffs.* |
| **Non-Functional** | Security Reliability Privacy |

**Acceptance Criteria (BDD)**

| | |
|---|---|
| **Scenario** | Governance & risk application |
| **Given** | a domain objective list and a risk register template |
| **When** | I complete a 1-page summary and compute SLE/ALE for 3 assets |
| **Then** | I can map administrative/technical/physical controls to risks and score $\geq 80\%$ on 40 Domain 1 questions |

**Definition of Ready:** objectives known; templates ready; time-box defined.
**Definition of Done:** summary saved; 40Q $\geq 80\%$; flashcards synced; retrospective logged.

**Tasks**

- ☐ Capture ethics, due care/diligence, and policy hierarchy on 1 page.
- ☐ Build a mini risk register with 3 assets, threats, impacts, and controls.
- ☐ Draft 15 flashcards (CIANA, risk appetite, residual risk, e-Discovery, BCP/DR).
- ☐ Do 40 mixed Domain 1 questions; tag misses by subtopic.
- ☐ Write a 5-sentence takeaway on governance vs management and supply-chain risk.

| | |
|---|---|
| **Epic / Feature** | Domain 2: Asset Security |
| **Business Value** | Correctly classify and handle data/assets through their lifecycle to meet legal and business needs. |
| **Priority / Estimate** | Priority: Must SP: 2 |
| **Persona** | CISSP candidate |
| **Dependencies** | D1 foundations |
| **Assumptions** | Access to sample classification policy |
| **Risks** | Unclear ownership roles; mishandling retention |
| **Story** | *As a CISSP candidate, I want to design a classification and handling scheme so that data is protected appropriately at each lifecycle stage.* |
| **Non-Functional** | Security Privacy Compliance |

**Acceptance Criteria (BDD)**

| | |
|---|---|
| **Scenario** | Classification and handling |
| **Given** | a 4-level classification model and role definitions |
| **When** | I label owners/custodians and define handling/storage/destruction |
| **Then** | I can choose masking/tokenization/DLP strategies and pass 30 Domain 2 questions at $\geq 80\%$ |

**Tasks**

- ☐ Draft a 4-level classification schema with owners/custodians.
- ☐ Map lifecycle stages to controls (create, store, use, share, archive, destroy).
- ☐ Create 10 flashcards (tokenization vs encryption, media sanitization levels).
- ☐ Complete 30 Domain 2 questions; review missed explanations.
- ☐ Write retention and disposal rules for each class.

| | |
|---|---|
| **Epic / Feature** | Domain 3: Security Architecture & Engineering |
| **Business Value** | Engineer resilient systems by applying secure design principles, models, and cryptography. |
| **Priority / Estimate** | Priority: Must SP: 3 |
| **Persona** | CISSP candidate |
| **Dependencies** | D1 concepts |
| **Assumptions** | Time to sketch architecture diagrams |
| **Risks** | Confusing model goals (Bell-LaPadula vs Biba); crypto misuse |
| **Story** | *As a CISSP candidate, I want to apply secure design and crypto choices so that architectures resist common failure and attack modes.* |
| **Non-Functional** | Security Reliability |

**Acceptance Criteria (BDD)**

| | |
|---|---|
| **Scenario** | Architecture decision |
| **Given** | an app with data flows across trust boundaries |
| **When** | I annotate controls (TCB, hardware roots, virtualization, key mgmt) |
| **Then** | I explain which model enforces confidentiality/integrity and select safe crypto modes for the use case |

**Tasks**

- ☐ List 10 secure design principles; give an example for each.
- ☐ Summarize Bell-LaPadula, Biba, Clark-Wilson, Brewer-Nash in 6 lines each.
- ☐ Create 12 flashcards (block modes, AEAD, key lifecycles, HSM/TPM).
- ☐ Draw a simple architecture and mark control points and trust boundaries.
- ☐ Do 35 Domain 3 questions; target weak subtopics.

| | |
|---|---|
| **Epic / Feature** | Domain 4: Communication & Network Security |
| **Business Value** | Design and defend segmented networks and secure communications. |
| **Priority / Estimate** | Priority: Must SP: 2 |
| **Persona** | CISSP candidate |
| **Dependencies** | D3 overview |
| **Assumptions** | Diagram tool available |
| **Risks** | Layer confusion; misplacing controls |
| **Story** | *As a CISSP candidate, I want to map threats to layered network controls so that I can justify TLS vs IPsec and wireless protections.* |
| **Non-Functional** | Security Reliability |

**Acceptance Criteria (BDD)**

| | |
|---|---|
| **Scenario** | Segmentation and secure comms |
| **Given** | a 3-tier app topology |
| **When** | I produce a segmented diagram with FW/IDS/IPS/WAF/NAC annotations |
| **Then** | I explain TLS vs IPsec tradeoffs and pass 30 Domain 4 questions at $\geq$ 80% |

**Tasks**

- ☐ Draw a 3-zone network; mark control points.
- ☐ Write 1 paragraph: TLS vs IPsec use cases.
- ☐ Create 10 flashcards on Wi-Fi protections and common network attacks.
- ☐ Complete 30 Domain 4 questions; review misses.
- ☐ Note 5 troubleshooting cues per control (e.g., SSL/TLS versions, cipher suites).

| | |
|---|---|
| **Epic / Feature** | Domain 5: Identity & Access Management |
| **Business Value** | Govern identities and enforce strong authentication and authorization. |
| **Priority / Estimate** | Priority: Should SP: 2 |
| **Persona** | CISSP candidate |
| **Dependencies** | D1 policy concepts |
| **Assumptions** | Example IdP diagrams |
| **Risks** | Confusing federation flows; weak lifecycle governance |
| **Story** | *As a CISSP candidate, I want to compare authN/authZ patterns and lifecycle governance so that I can choose RBAC/ABAC and federation appropriately.* |
| **Non-Functional** | Security Privacy |

**Acceptance Criteria (BDD)**

| | |
|---|---|
| **Scenario** | IAM selection |
| **Given** | human, device, and service identities |
| **When** | I diagram joiner/mover/leaver and federation (SAML/OIDC) flows |
| **Then** | I justify MFA/SSO/PAM choices and pass 30 Domain 5 questions at $\geq 80\%$ |

**Tasks**

- ☐ Sketch IdP/SP trust and token flows (SAML/OIDC).
- ☐ Define RBAC vs ABAC and give 2 examples each.
- ☐ Create 12 flashcards (MFA factors, OAuth scopes, session mgmt).
- ☐ Complete 30 Domain 5 questions.
- ☐ Write lifecycle governance checklist (JML, reviews, recertification).

| | |
|---|---|
| **Epic / Feature** | Domain 6: Security Assessment & Testing |
| **Business Value** | Verify control effectiveness and communicate prioritized remediation. |
| **Priority / Estimate** | Priority: Should SP: 2 |
| **Persona** | CISSP candidate |
| **Dependencies** | D1 risk context |
| **Assumptions** | Access to sample reports |
| **Risks** | Confusing audit independence vs testing |
| **Story** | *As a CISSP candidate, I want to plan and execute assessments so that I can select tests, analyze results, and support audits.* |
| **Non-Functional** | Security Reliability |

**Acceptance Criteria (BDD)**

| | |
|---|---|
| **Scenario** | Assessment planning |
| **Given** | a scoped system and control list |
| **When** | I choose technical/administrative/physical tests and sampling |
| **Then** | I produce a short report with prioritized fixes and pass 25 Domain 6 questions at $\geq 80\%$ |

**Tasks**

- ☐ Map control types to test techniques; build a tiny test matrix.
- ☐ Draft 8 report bullets: findings, risk, recommendation, owner.
- ☐ Create 8 flashcards (sampling, coverage, MTTD/MTTR proxies).
- ☐ Complete 25 Domain 6 questions.
- ☐ Compare audit vs assessment in 5 bullets.

| | |
|---|---|
| **Epic / Feature** | Domain 7: Security Operations |
| **Business Value** | Run daily security: monitoring, IR, change/config mgmt, continuity, and safety. |
| **Priority / Estimate** | Priority: Must SP: 3 |
| **Persona** | CISSP candidate |
| **Dependencies** | D1/D6 |
| **Assumptions** | Access to IR checklist template |
| **Risks** | Skipping BCP/DR testing steps |
| **Story** | *As a CISSP candidate, I want to coordinate incident response and operational controls so that I can minimize impact and recover effectively.* |
| **Non-Functional** | Security Reliability |

**Acceptance Criteria (BDD)**

| | |
|---|---|
| **Scenario** | Incident drill |
| **Given** | an IR playbook and logs |
| **When** | I walk through prepare/detect/contain/eradicate/recover |
| **Then** | I define evidence handling basics and pass 35 Domain 7 questions at $\geq 80\%$ |

**Tasks**

- ☐ Outline IR lifecycle with roles and SLAs.
- ☐ List 10 monitoring use cases and associated signals.
- ☐ Create 12 flashcards (EDR, NAC, WAF, backups, RTO/RPO).
- ☐ Complete 35 Domain 7 questions.
- ☐ Draft a DR test plan (tabletop + restore verification).

| | |
|---|---|
| **Epic / Feature** | Domain 8: Software Development Security |
| **Business Value** | Integrate security into SDLC and supply chain; enforce secure coding. |
| **Priority / Estimate** | Priority: Should SP: 2 |
| **Persona** | CISSP candidate |
| **Dependencies** | D3 architecture basics |
| **Assumptions** | Access to a CI/CD checklist |
| **Risks** | Overemphasis on tools vs controls |
| **Story** | *As a CISSP candidate, I want to embed security in the SDLC so that I can assess software and manage supply-chain risk.* |
| **Non-Functional** | Security Reliability |

**Acceptance Criteria (BDD)**

| | |
|---|---|
| **Scenario** | Secure SDLC checklist |
| **Given** | an SDLC stage map (req → design → build → test → deploy) |
| **When** | I place security activities and artifacts per stage |
| **Then** | I review SAST/DAST/IAST/SCA basics and pass 30 Domain 8 questions at $\geq 80\%$ |

**Tasks**

- ☐ Build a secure-SDLC checklist across stages and environments.
- ☐ Draft 8 code review checks tied to common CWE classes.
- ☐ Create 10 flashcards (SAST vs DAST vs IAST vs SCA; SBOM; secrets mgmt).
- ☐ Complete 30 Domain 8 questions.
- ☐ Evaluate an acquisition scenario for license & supply-chain risk.