Computer and Information Security Handbook (4e)

Full Study Plan as User Story Cards

Each chapter is represented as a story card with BDD acceptance criteria, DoR/DoD, and a concrete task list.

This text should be removed before printing. Is included because I need empty space.

CISH-001 — Information Security in the Modern Enterprise — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of information security in the modern enterprise and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Information Security in the Modern Enterprise' so that I can apply its concepts to reduce risk and improve outcomes.*

Non-Functional

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Information Security in the Modern Enterprise

Given
the lab environment and topic-specific tools for 'Information Security in the Modern Enterprise' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Information Security in the Modern Enterprise'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Information Security in the Modern Enterprise': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Information Security in the Modern Enterprise'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-002 — Building a Secure Organization — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of building a secure organization and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Program Manager
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Program Manager, I want to study and practice 'Building a Secure Organization' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Building a Secure Organization

Given
the lab environment and topic-specific tools for 'Building a Secure Organization' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Building a Secure Organization'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Building a Secure Organization': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Building a Secure Organization'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-003 — A Cryptography Primer — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of a cryptography primer and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Platform Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, OpenSSL/mkcert, TLS scanner
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Platform Engineer, I want to study and practice 'A Cryptography Primer' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for A Cryptography Primer

Given
the lab environment and topic-specific tools for 'A Cryptography Primer' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'A Cryptography Primer'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'A Cryptography Primer': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'A Cryptography Primer'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-004 — Verifying User and Host Identity — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of verifying user and host identity and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, IDP / MFA-capable test app
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Verifying User and Host Identity' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Privacy

Acceptance Criteria (BDD)

Scenario
Apply key controls for Verifying User and Host Identity

Given
the lab environment and topic-specific tools for 'Verifying User and Host Identity' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Verifying User and Host Identity'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Verifying User and Host Identity': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Verifying User and Host Identity'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-005 — Detecting System Intrusions — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of detecting system intrusions and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Detecting System Intrusions' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Observability

Acceptance Criteria (BDD)

Scenario
Apply key controls for Detecting System Intrusions

Given
the lab environment and topic-specific tools for 'Detecting System Intrusions' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Detecting System Intrusions'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Detecting System Intrusions': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Detecting System Intrusions'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-006 — Intrusion Detection in Contemporary Environments — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of intrusion detection in contemporary environments and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Intrusion Detection in Contemporary Environments' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Observability

Acceptance Criteria (BDD)

Scenario
Apply key controls for Intrusion Detection in Contemporary Environments

Given
the lab environment and topic-specific tools for 'Intrusion Detection in Contemporary Environments' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Intrusion Detection in Contemporary Environments'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Intrusion Detection in Contemporary Environments': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Intrusion Detection in Contemporary Environments'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-007 — Preventing System Intrusions — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of preventing system intrusions and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Preventing System Intrusions' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Preventing System Intrusions

Given
the lab environment and topic-specific tools for 'Preventing System Intrusions' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Preventing System Intrusions'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Preventing System Intrusions': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Preventing System Intrusions'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-008 — Guarding Against Network Intrusions — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of guarding against network intrusions and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Guarding Against Network Intrusions' so that I can apply its concepts to reduce risk and improve outcomes.*

Non-Functional

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Guarding Against Network Intrusions

Given
the lab environment and topic-specific tools for 'Guarding Against Network Intrusions' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Guarding Against Network Intrusions'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Guarding Against Network Intrusions': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Guarding Against Network Intrusions'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-009 — Fault Tolerance and Resilience in Cloud Computing Environments — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of fault tolerance and resilience in cloud computing environments and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Cloud Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Cloud sandbox account, Terraform, Benchmark tool (e.g., CIS)
Assumptions / Risks	Sandbox-only changes; no production accounts; Time-box chapter to one iteration; open issues captured for later

Story *As a Cloud Security Engineer, I want to study and practice 'Fault Tolerance and Resilience in Cloud Computing Environments' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Compliance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Fault Tolerance and Resilience in Cloud Computing Environments

Given
the lab environment and topic-specific tools for 'Fault Tolerance and Resilience in Cloud Computing Environments' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Fault Tolerance and Resilience in Cloud Computing Environments'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Fault Tolerance and Resilience in Cloud Computing Environments': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Fault Tolerance and Resilience in Cloud Computing Environments'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-010 — Securing Web Applications, Services and Servers — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of securing web applications, services and servers and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Application Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Sample web app, SAST/DAST scanner
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Application Security Engineer, I want to study and practice 'Securing Web Applications, Services and Servers' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Securing Web Applications, Services and Servers

Given
the lab environment and topic-specific tools for 'Securing Web Applications, Services and Servers' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Securing Web Applications, Services and Servers'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Securing Web Applications, Services and Servers': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Securing Web Applications, Services and Servers'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-011 — UNIX and Linux Security — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of unix and linux security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Systems Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Scope excludes legacy, unsupported OS versions where impractical; Time-box chapter to one iteration; open issues captured for later

Story *As a Systems Engineer, I want to study and practice 'UNIX and Linux Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for UNIX and Linux Security

Given
the lab environment and topic-specific tools for 'UNIX and Linux Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'UNIX and Linux Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'UNIX and Linux Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'UNIX and Linux Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-012 — Eliminating the Security Weakness of Linux and UNIX Operating Systems — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of eliminating the security weakness of linux and unix operating systems and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Systems Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Scope excludes legacy, unsupported OS versions where impractical; Time-box chapter to one iteration; open issues captured for later

Story *As a Systems Engineer, I want to study and practice 'Eliminating the Security Weakness of Linux and UNIX Operating Systems' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Eliminating the Security Weakness of Linux and UNIX Operating Systems

Given
the lab environment and topic-specific tools for 'Eliminating the Security Weakness of Linux and UNIX Operating Systems' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Eliminating the Security Weakness of Linux and UNIX Operating Systems'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Eliminating the Security Weakness of Linux and UNIX Operating Systems': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Eliminating the Security Weakness of Linux and UNIX Operating Systems'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-013 — Internet Security — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of internet security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Internet Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Internet Security

Given
the lab environment and topic-specific tools for 'Internet Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Internet Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Internet Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Internet Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-014 — The Botnet Problem — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of the botnet problem and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'The Botnet Problem' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for The Botnet Problem

Given
the lab environment and topic-specific tools for 'The Botnet Problem' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'The Botnet Problem'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'The Botnet Problem': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'The Botnet Problem'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-015 — Intranet Security — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of intranet security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Intranet Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Intranet Security

Given
the lab environment and topic-specific tools for 'Intranet Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Intranet Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Intranet Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Intranet Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-016 — Local Area Network Security — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of local area network security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Local Area Network Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Local Area Network Security

Given
the lab environment and topic-specific tools for 'Local Area Network Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Local Area Network Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Local Area Network Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Local Area Network Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-017 — Wireless Network Security — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of wireless network security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Wireless Network Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Wireless Network Security

Given
the lab environment and topic-specific tools for 'Wireless Network Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Wireless Network Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Wireless Network Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Wireless Network Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-018 — Wireless Sensor Network Security: The Internet of Things — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of wireless sensor network security: the internet of things and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Wireless Sensor Network Security: The Internet of Things' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Wireless Sensor Network Security: The Internet of Things

Given
the lab environment and topic-specific tools for 'Wireless Sensor Network Security: The Internet of Things' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Wireless Sensor Network Security: The Internet of Things'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Wireless Sensor Network Security: The Internet of Things': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Wireless Sensor Network Security: The Internet of Things'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-019 — Security for the Internet of Things — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of security for the internet of things and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Security for the Internet of Things' so that I can apply its concepts to reduce risk and improve outcomes.*

Non-Functional

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Security for the Internet of Things

Given
the lab environment and topic-specific tools for 'Security for the Internet of Things' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Security for the Internet of Things'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Security for the Internet of Things': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Security for the Internet of Things'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-020 — Cellular Network Security — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of cellular network security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Cellular Network Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Cellular Network Security

Given
the lab environment and topic-specific tools for 'Cellular Network Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Cellular Network Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Cellular Network Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Cellular Network Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-021 — Radio Frequency Identification Security — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of radio frequency identification security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Radio Frequency Identification Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Radio Frequency Identification Security

Given
the lab environment and topic-specific tools for 'Radio Frequency Identification Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Radio Frequency Identification Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Radio Frequency Identification Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Radio Frequency Identification Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-022 — Optical Network Security — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of optical network security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Optical Network Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Optical Network Security

Given
the lab environment and topic-specific tools for 'Optical Network Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Optical Network Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Optical Network Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Optical Network Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-023 — Optical Wireless Security — Learn & Lab

Epic / Feature	Part 1: Overview of System and Network Security
Business Value	Build a working understanding of optical wireless security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Optical Wireless Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Optical Wireless Security

Given
the lab environment and topic-specific tools for 'Optical Wireless Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Optical Wireless Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Optical Wireless Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Optical Wireless Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-024 — Information Security Essentials for Information Technology Managers: Protecting Mission-Critical Systems — Learn & Lab

Epic / Feature	Part 2: Managing Information Security
Business Value	Build a working understanding of information security essentials for information technology managers: protecting mission-critical systems and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Information Security Essentials for Information Technology Managers: Protecting Mission-Critical Systems' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Information Security Essentials for Information Technology Managers: Protecting Mission-Critical Systems

Given
the lab environment and topic-specific tools for 'Information Security Essentials for Information Technology Managers: Protecting Mission-Critical Systems' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Information Security Essentials for Information Technology Managers: Protecting Mission-Critical Systems'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Information Security Essentials for Information Technology Managers: Protecting Mission-Critical Systems': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Information Security Essentials for Information Technology Managers: Protecting Mission-Critical Systems'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-025 — Security Management Systems — Learn & Lab

Epic / Feature	Part 2: Managing Information Security
Business Value	Build a working understanding of security management systems and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Program Manager
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Program Manager, I want to study and practice 'Security Management Systems' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Security Management Systems

Given
the lab environment and topic-specific tools for 'Security Management Systems' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Security Management Systems'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Security Management Systems': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Security Management Systems'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-026 — Policy-Driven System Management — Learn & Lab

Epic / Feature	Part 2: Managing Information Security
Business Value	Build a working understanding of policy-driven system management and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Program Manager
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Program Manager, I want to study and practice 'Policy-Driven System Management' so that I can apply its concepts to reduce risk and improve outcomes.*

Non-Functional

Security

Reliability

Performance

Compliance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Policy-Driven System Management

Given
the lab environment and topic-specific tools for 'Policy-Driven System Management' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Policy-Driven System Management'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Policy-Driven System Management': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Policy-Driven System Management'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-027 — Information Technology Security Management — Learn & Lab

Epic / Feature	Part 2: Managing Information Security
Business Value	Build a working understanding of information technology security management and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Program Manager
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Program Manager, I want to study and practice 'Information Technology Security Management' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Information Technology Security Management

Given
the lab environment and topic-specific tools for 'Information Technology Security Management' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Information Technology Security Management'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Information Technology Security Management': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Information Technology Security Management'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-028 — The Enemy (The Intruder's Genesis) — Learn & Lab

Epic / Feature	Part 2: Managing Information Security
Business Value	Build a working understanding of the enemy (the intruder's genesis) and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'The Enemy (The Intruder's Genesis)' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for The Enemy (The Intruder's Genesis)

Given
the lab environment and topic-specific tools for 'The Enemy (The Intruder's Genesis)' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'The Enemy (The Intruder's Genesis)'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'The Enemy (The Intruder's Genesis)': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'The Enemy (The Intruder's Genesis)'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-029 — Social Engineering Deceptions and Defenses — Learn & Lab

Epic / Feature	Part 2: Managing Information Security
Business Value	Build a working understanding of social engineering deceptions and defenses and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'Social Engineering Deceptions and Defenses' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Social Engineering Deceptions and Defenses

Given
the lab environment and topic-specific tools for 'Social Engineering Deceptions and Defenses' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Social Engineering Deceptions and Defenses'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Social Engineering Deceptions and Defenses': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Social Engineering Deceptions and Defenses'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-030 — Ethical Hacking — Learn & Lab

Epic / Feature	Part 2: Managing Information Security
Business Value	Build a working understanding of ethical hacking and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Ethical Hacking' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Ethical Hacking

Given
the lab environment and topic-specific tools for 'Ethical Hacking' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Ethical Hacking'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Ethical Hacking': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Ethical Hacking'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-031 — What Is Vulnerability Assessment? — Learn & Lab

Epic / Feature	Part 2: Managing Information Security
Business Value	Build a working understanding of what is vulnerability assessment? and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'What Is Vulnerability Assessment?' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for What Is Vulnerability Assessment?

Given
the lab environment and topic-specific tools for 'What Is Vulnerability Assessment?' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'What Is Vulnerability Assessment?'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'What Is Vulnerability Assessment?': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'What Is Vulnerability Assessment?'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-032 — Security Metrics — Learn & Lab

Epic / Feature	Part 2: Managing Information Security
Business Value	Build a working understanding of security metrics and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Program Manager
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Program Manager, I want to study and practice 'Security Metrics' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Security Metrics

Given
the lab environment and topic-specific tools for 'Security Metrics' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Security Metrics'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Security Metrics': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Security Metrics'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-033 — Security Education, Training, and Awareness — Learn & Lab

Epic / Feature	Part 2: Managing Information Security
Business Value	Build a working understanding of security education, training, and awareness and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Program Manager
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Program Manager, I want to study and practice 'Security Education, Training, and Awareness' so that I can apply its concepts to reduce risk and improve outcomes.*

Non-Functional

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Security Education, Training, and Awareness

Given
the lab environment and topic-specific tools for 'Security Education, Training, and Awareness' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Security Education, Training, and Awareness'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Security Education, Training, and Awareness': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Security Education, Training, and Awareness'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-034 — Risk Management — Learn & Lab

Epic / Feature	Part 2: Managing Information Security
Business Value	Build a working understanding of risk management and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Program Manager
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Program Manager, I want to study and practice 'Risk Management' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Risk Management

Given
the lab environment and topic-specific tools for 'Risk Management' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Risk Management'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Risk Management': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Risk Management'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-035 — Insider Threats — Learn & Lab

Epic / Feature	Part 2: Managing Information Security
Business Value	Build a working understanding of insider threats and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Program Manager
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Program Manager, I want to study and practice 'Insider Threats' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Insider Threats

Given
the lab environment and topic-specific tools for 'Insider Threats' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Insider Threats'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Insider Threats': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Insider Threats'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-036 — Disaster Recovery — Learn & Lab

Epic / Feature	Part 3: Disaster Recovery Security
Business Value	Build a working understanding of disaster recovery and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Disaster Recovery' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Disaster Recovery

Given
the lab environment and topic-specific tools for 'Disaster Recovery' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Disaster Recovery'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Disaster Recovery': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Disaster Recovery'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-037 — Disaster Recovery Plans for Small and Medium Business (SMB) — Learn & Lab

Epic / Feature	Part 3: Disaster Recovery Security
Business Value	Build a working understanding of disaster recovery plans for small and medium business (smb) and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Disaster Recovery Plans for Small and Medium Business (SMB)' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Disaster Recovery Plans for Small and Medium Business (SMB)

Given
the lab environment and topic-specific tools for 'Disaster Recovery Plans for Small and Medium Business (SMB)' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Disaster Recovery Plans for Small and Medium Business (SMB)'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Disaster Recovery Plans for Small and Medium Business (SMB)': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Disaster Recovery Plans for Small and Medium Business (SMB)'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-038 — Security Certification And Standards Implementation — Learn & Lab

Epic / Feature	Part 4: Security Standards And Policies
Business Value	Build a working understanding of security certification and standards implementation and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Program Manager
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Program Manager, I want to study and practice 'Security Certification And Standards Implementation' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Compliance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Security Certification And Standards Implementation

Given
the lab environment and topic-specific tools for 'Security Certification And Standards Implementation' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Security Certification And Standards Implementation'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Security Certification And Standards Implementation': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Security Certification And Standards Implementation'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-039 — Security Policies And Plans Development — Learn & Lab

Epic / Feature	Part 4: Security Standards And Policies
Business Value	Build a working understanding of security policies and plans development and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Security Policies And Plans Development' so that I can apply its concepts to reduce risk and improve outcomes.*

Non-Functional

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Security Policies And Plans Development

Given
the lab environment and topic-specific tools for 'Security Policies And Plans Development' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Security Policies And Plans Development'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Security Policies And Plans Development': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Security Policies And Plans Development'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-040 — Cyber Forensics — Learn & Lab

Epic / Feature	Part 5: Cyber, Network, and Systems Forensics Security and Assurance
Business Value	Build a working understanding of cyber forensics and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Analyst
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Imaging tool (dd/FTK), Hash tool (sha256sum), Write-blocker (emulated ok)
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Analyst, I want to study and practice 'Cyber Forensics' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Compliance

Observability

Acceptance Criteria (BDD)

Scenario
Apply key controls for Cyber Forensics

Given
the lab environment and topic-specific tools for 'Cyber Forensics' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Cyber Forensics'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Cyber Forensics': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Cyber Forensics'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-041 — Cyber Forensics And Incidence Response — Learn & Lab

Epic / Feature	Part 5: Cyber, Network, and Systems Forensics Security and Assurance
Business Value	Build a working understanding of cyber forensics and incidence response and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Analyst
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Imaging tool (dd/FTK), Hash tool (sha256sum), Write-blocker (emulated ok)
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Analyst, I want to study and practice 'Cyber Forensics And Incidence Response' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Compliance

Observability

Acceptance Criteria (BDD)

Scenario
Apply key controls for Cyber Forensics And Incidence Response

Given
the lab environment and topic-specific tools for 'Cyber Forensics And Incidence Response' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Cyber Forensics And Incidence Response'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Cyber Forensics And Incidence Response': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Cyber Forensics And Incidence Response'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-042 — Securing e-Discovery — Learn & Lab

Epic / Feature	Part 5: Cyber, Network, and Systems Forensics Security and Assurance
Business Value	Build a working understanding of securing e-discovery and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Analyst
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Imaging tool (dd/FTK), Hash tool (sha256sum), Write-blocker (emulated ok)
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Analyst, I want to study and practice 'Securing e-Discovery' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Securing e-Discovery

Given
the lab environment and topic-specific tools for 'Securing e-Discovery' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Securing e-Discovery'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Securing e-Discovery': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Securing e-Discovery'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-043 — Network Forensics — Learn & Lab

Epic / Feature	Part 5: Cyber, Network, and Systems Forensics Security and Assurance
Business Value	Build a working understanding of network forensics and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Analyst
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Imaging tool (dd/FTK), Hash tool (sha256sum), Write-blocker (emulated ok), Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Analyst, I want to study and practice 'Network Forensics' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Compliance

Observability

Acceptance Criteria (BDD)

Scenario
Apply key controls for Network Forensics

Given
the lab environment and topic-specific tools for 'Network Forensics' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Network Forensics'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Network Forensics': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Network Forensics'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-044 — Microsoft Office and Metadata Forensics: A Deeper Dive — Learn & Lab

Epic / Feature	Part 5: Cyber, Network, and Systems Forensics Security and Assurance
Business Value	Build a working understanding of microsoft office and metadata forensics: a deeper dive and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Analyst
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Imaging tool (dd/FTK), Hash tool (sha256sum), Write-blocker (emulated ok)
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Analyst, I want to study and practice 'Microsoft Office and Metadata Forensics: A Deeper Dive' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Compliance

Observability

Acceptance Criteria (BDD)

Scenario
Apply key controls for Microsoft Office and Metadata Forensics: A Deeper Dive

Given
the lab environment and topic-specific tools for 'Microsoft Office and Metadata Forensics: A Deeper Dive' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Microsoft Office and Metadata Forensics: A Deeper Dive'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Microsoft Office and Metadata Forensics: A Deeper Dive': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Microsoft Office and Metadata Forensics: A Deeper Dive'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-045 — Hard Drive Imaging — Learn & Lab

Epic / Feature	Part 5: Cyber, Network, and Systems Forensics Security and Assurance
Business Value	Build a working understanding of hard drive imaging and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Analyst
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Imaging tool (dd/FTK), Hash tool (sha256sum), Write-blocker (emulated ok)
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Analyst, I want to study and practice 'Hard Drive Imaging' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Hard Drive Imaging

Given
the lab environment and topic-specific tools for 'Hard Drive Imaging' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Hard Drive Imaging'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Hard Drive Imaging': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Hard Drive Imaging'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-046 — Data Encryption — Learn & Lab

Epic / Feature	Part 6: Encryption Technology
Business Value	Build a working understanding of data encryption and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Platform Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, OpenSSL/mkcert, TLS scanner
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Platform Engineer, I want to study and practice 'Data Encryption' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Data Encryption

Given
the lab environment and topic-specific tools for 'Data Encryption' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Data Encryption'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Data Encryption': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Data Encryption'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-047 — Satellite Encryption — Learn & Lab

Epic / Feature	Part 6: Encryption Technology
Business Value	Build a working understanding of satellite encryption and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Platform Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, OpenSSL/mkcert, TLS scanner
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Platform Engineer, I want to study and practice 'Satellite Encryption' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Satellite Encryption

Given
the lab environment and topic-specific tools for 'Satellite Encryption' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Satellite Encryption'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Satellite Encryption': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Satellite Encryption'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-048 — Public Key Infrastructure — Learn & Lab

Epic / Feature	Part 6: Encryption Technology
Business Value	Build a working understanding of public key infrastructure and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Platform Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, OpenSSL/mkcert, TLS scanner
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Platform Engineer, I want to study and practice 'Public Key Infrastructure' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Public Key Infrastructure

Given
the lab environment and topic-specific tools for 'Public Key Infrastructure' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Public Key Infrastructure'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Public Key Infrastructure': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Public Key Infrastructure'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-049 — Password-based Authenticated Key Establishment Protocols — Learn & Lab

Epic / Feature	Part 6: Encryption Technology
Business Value	Build a working understanding of password-based authenticated key establishment protocols and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Platform Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, OpenSSL/mkcert, TLS scanner
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Platform Engineer, I want to study and practice 'Password-based Authenticated Key Establishment Protocols' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Password-based Authenticated Key Establishment Protocols

Given
the lab environment and topic-specific tools for 'Password-based Authenticated Key Establishment Protocols' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Password-based Authenticated Key Establishment Protocols'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Password-based Authenticated Key Establishment Protocols': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Password-based Authenticated Key Establishment Protocols'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-050 — Context-Aware Multifactor Authentication Survey — Learn & Lab

Epic / Feature	Part 6: Encryption Technology
Business Value	Build a working understanding of context-aware multifactor authentication survey and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Platform Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, IDP / MFA-capable test app
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Platform Engineer, I want to study and practice 'Context-Aware Multifactor Authentication Survey' so that I can apply its concepts to reduce risk and improve outcomes.*

Non-Functional

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Context-Aware Multifactor Authentication Survey

Given
the lab environment and topic-specific tools for 'Context-Aware Multifactor Authentication Survey' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Context-Aware Multifactor Authentication Survey'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Context-Aware Multifactor Authentication Survey': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Context-Aware Multifactor Authentication Survey'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-051 — Instant-Messaging Security — Learn & Lab

Epic / Feature	Part 6: Encryption Technology
Business Value	Build a working understanding of instant-messaging security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Instant-Messaging Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Instant-Messaging Security

Given
the lab environment and topic-specific tools for 'Instant-Messaging Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Instant-Messaging Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Instant-Messaging Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Instant-Messaging Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-052 — Online Privacy — Learn & Lab

Epic / Feature	Part 7: Privacy and Access Management
Business Value	Build a working understanding of online privacy and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Privacy Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Privacy Engineer, I want to study and practice 'Online Privacy' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Privacy

Acceptance Criteria (BDD)

Scenario
Apply key controls for Online Privacy

Given
the lab environment and topic-specific tools for 'Online Privacy' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Online Privacy'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Online Privacy': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Online Privacy'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-053 — Privacy-enhancing Technologies — Learn & Lab

Epic / Feature	Part 7: Privacy and Access Management
Business Value	Build a working understanding of privacy-enhancing technologies and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Privacy Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Privacy Engineer, I want to study and practice 'Privacy-enhancing Technologies' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Privacy

Acceptance Criteria (BDD)

Scenario
Apply key controls for Privacy-enhancing Technologies

Given
the lab environment and topic-specific tools for 'Privacy-enhancing Technologies' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Privacy-enhancing Technologies'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Privacy-enhancing Technologies': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Privacy-enhancing Technologies'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-054 — Personal Privacy Policies — Learn & Lab

Epic / Feature	Part 7: Privacy and Access Management
Business Value	Build a working understanding of personal privacy policies and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Privacy Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Privacy Engineer, I want to study and practice 'Personal Privacy Policies' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Privacy

Acceptance Criteria (BDD)

Scenario
Apply key controls for Personal Privacy Policies

Given
the lab environment and topic-specific tools for 'Personal Privacy Policies' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Personal Privacy Policies'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Personal Privacy Policies': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Personal Privacy Policies'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-055 — Detection Of Conflicts In Security Policies — Learn & Lab

Epic / Feature	Part 7: Privacy and Access Management
Business Value	Build a working understanding of detection of conflicts in security policies and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Detection Of Conflicts In Security Policies' so that I can apply its concepts to reduce risk and improve outcomes.*

Non-Functional

Security

Reliability

Performance

Observability

Acceptance Criteria (BDD)

Scenario
Apply key controls for Detection Of Conflicts In Security Policies

Given
the lab environment and topic-specific tools for 'Detection Of Conflicts In Security Policies' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Detection Of Conflicts In Security Policies'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Detection Of Conflicts In Security Policies': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Detection Of Conflicts In Security Policies'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-056 — Supporting User Privacy Preferences in Digital Interactions — Learn & Lab

Epic / Feature	Part 7: Privacy and Access Management
Business Value	Build a working understanding of supporting user privacy preferences in digital interactions and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Privacy Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Privacy Engineer, I want to study and practice 'Supporting User Privacy Preferences in Digital Interactions' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Privacy

Acceptance Criteria (BDD)

Scenario
Apply key controls for Supporting User Privacy Preferences in Digital Interactions

Given
the lab environment and topic-specific tools for 'Supporting User Privacy Preferences in Digital Interactions' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Supporting User Privacy Preferences in Digital Interactions'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Supporting User Privacy Preferences in Digital Interactions': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Supporting User Privacy Preferences in Digital Interactions'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-057 — Privacy and Security in Environmental Monitoring Systems: Issues and Solutions — Learn & Lab

Epic / Feature	Part 7: Privacy and Access Management
Business Value	Build a working understanding of privacy and security in environmental monitoring systems: issues and solutions and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Privacy Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Privacy Engineer, I want to study and practice 'Privacy and Security in Environmental Monitoring Systems: Issues and Solutions' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Privacy

Observability

Acceptance Criteria (BDD)

Scenario
Apply key controls for Privacy and Security in Environmental Monitoring Systems: Issues and Solutions

Given
the lab environment and topic-specific tools for 'Privacy and Security in Environmental Monitoring Systems: Issues and Solutions' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Privacy and Security in Environmental Monitoring Systems: Issues and Solutions'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Privacy and Security in Environmental Monitoring Systems: Issues and Solutions': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Privacy and Security in Environmental Monitoring Systems: Issues and Solutions'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-058 — Virtual Private Networks — Learn & Lab

Epic / Feature	Part 7: Privacy and Access Management
Business Value	Build a working understanding of virtual private networks and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Virtual Private Networks' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Virtual Private Networks

Given
the lab environment and topic-specific tools for 'Virtual Private Networks' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Virtual Private Networks'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Virtual Private Networks': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Virtual Private Networks'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-059 — Identity Theft — Learn & Lab

Epic / Feature	Part 7: Privacy and Access Management
Business Value	Build a working understanding of identity theft and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Privacy Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, IDP / MFA-capable test app
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Privacy Engineer, I want to study and practice 'Identity Theft' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Privacy

Acceptance Criteria (BDD)

Scenario
Apply key controls for Identity Theft

Given
the lab environment and topic-specific tools for 'Identity Theft' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Identity Theft'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Identity Theft': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Identity Theft'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-060 — VoIP Security — Learn & Lab

Epic / Feature	Part 7: Privacy and Access Management
Business Value	Build a working understanding of voip security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'VoIP Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for VoIP Security

Given
the lab environment and topic-specific tools for 'VoIP Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'VoIP Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'VoIP Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'VoIP Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-061 — SAN Security — Learn & Lab

Epic / Feature	Part 8: Storage Security
Business Value	Build a working understanding of san security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'SAN Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for SAN Security

Given
the lab environment and topic-specific tools for 'SAN Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'SAN Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'SAN Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'SAN Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-062 — Storage Area Networking Devices Security — Learn & Lab

Epic / Feature	Part 8: Storage Security
Business Value	Build a working understanding of storage area networking devices security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Storage Area Networking Devices Security' so that I can apply its concepts to reduce risk and improve outcomes.*

Non-Functional

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Storage Area Networking Devices Security

Given
the lab environment and topic-specific tools for 'Storage Area Networking Devices Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Storage Area Networking Devices Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Storage Area Networking Devices Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Storage Area Networking Devices Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-063 — Securing Cloud Computing Systems — Learn & Lab

Epic / Feature	Part 9: Cloud Security
Business Value	Build a working understanding of securing cloud computing systems and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Cloud Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Cloud sandbox account, Terraform, Benchmark tool (e.g., CIS)
Assumptions / Risks	Sandbox-only changes; no production accounts; Time-box chapter to one iteration; open issues captured for later

Story *As a Cloud Security Engineer, I want to study and practice 'Securing Cloud Computing Systems' so that I can apply its concepts to reduce risk and improve outcomes.*

Non-Functional

Security

Reliability

Performance

Compliance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Securing Cloud Computing Systems

Given
the lab environment and topic-specific tools for 'Securing Cloud Computing Systems' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Securing Cloud Computing Systems'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Securing Cloud Computing Systems': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Securing Cloud Computing Systems'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-064 — Cloud Security — Learn & Lab

Epic / Feature	Part 9: Cloud Security
Business Value	Build a working understanding of cloud security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Cloud Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Cloud sandbox account, Terraform, Benchmark tool (e.g., CIS)
Assumptions / Risks	Sandbox-only changes; no production accounts; Time-box chapter to one iteration; open issues captured for later

Story *As a Cloud Security Engineer, I want to study and practice 'Cloud Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Compliance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Cloud Security

Given
the lab environment and topic-specific tools for 'Cloud Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Cloud Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Cloud Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Cloud Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-065 — Private Cloud Security — Learn & Lab

Epic / Feature	Part 9: Cloud Security
Business Value	Build a working understanding of private cloud security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Cloud Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Cloud sandbox account, Terraform, Benchmark tool (e.g., CIS)
Assumptions / Risks	Sandbox-only changes; no production accounts; Time-box chapter to one iteration; open issues captured for later

Story *As a Cloud Security Engineer, I want to study and practice 'Private Cloud Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Compliance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Private Cloud Security

Given
the lab environment and topic-specific tools for 'Private Cloud Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Private Cloud Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Private Cloud Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Private Cloud Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-066 — Virtual Private Cloud Security — Learn & Lab

Epic / Feature	Part 9: Cloud Security
Business Value	Build a working understanding of virtual private cloud security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Cloud Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Cloud sandbox account, Terraform, Benchmark tool (e.g., CIS)
Assumptions / Risks	Sandbox-only changes; no production accounts; Time-box chapter to one iteration; open issues captured for later

Story *As a Cloud Security Engineer, I want to study and practice 'Virtual Private Cloud Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Compliance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Virtual Private Cloud Security

Given
the lab environment and topic-specific tools for 'Virtual Private Cloud Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Virtual Private Cloud Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Virtual Private Cloud Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Virtual Private Cloud Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-067 — Protecting Virtual Infrastructure — Learn & Lab

Epic / Feature	Part 10: Virtual Security
Business Value	Build a working understanding of protecting virtual infrastructure and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'Protecting Virtual Infrastructure' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Protecting Virtual Infrastructure

Given
the lab environment and topic-specific tools for 'Protecting Virtual Infrastructure' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Protecting Virtual Infrastructure'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Protecting Virtual Infrastructure': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Protecting Virtual Infrastructure'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-068 — SDN and NFV Security — Learn & Lab

Epic / Feature	Part 10: Virtual Security
Business Value	Build a working understanding of sdn and nfv security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Cloud Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Cloud Security Engineer, I want to study and practice 'SDN and NFV Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for SDN and NFV Security

Given
the lab environment and topic-specific tools for 'SDN and NFV Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'SDN and NFV Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'SDN and NFV Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'SDN and NFV Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-069 — Physical Security Essentials — Learn & Lab

Epic / Feature	Part 11: Cyber Physical Security
Business Value	Build a working understanding of physical security essentials and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Physical Security Specialist
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Physical Security Specialist, I want to study and practice 'Physical Security Essentials' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Physical Security Essentials

Given
the lab environment and topic-specific tools for 'Physical Security Essentials' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Physical Security Essentials'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Physical Security Essentials': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Physical Security Essentials'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-070 — Biometrics — Learn & Lab

Epic / Feature	Part 11: Cyber Physical Security
Business Value	Build a working understanding of biometrics and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Privacy Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, IDP / MFA-capable test app
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Privacy Engineer, I want to study and practice 'Biometrics' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Biometrics

Given
the lab environment and topic-specific tools for 'Biometrics' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Biometrics'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Biometrics': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Biometrics'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-071 — Online Identity and User Management Services — Learn & Lab

Epic / Feature	Part 12: Practical Security
Business Value	Build a working understanding of online identity and user management services and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Application Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, IDP / MFA-capable test app
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Application Security Engineer, I want to study and practice 'Online Identity and User Management Services' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Privacy

Acceptance Criteria (BDD)

Scenario
Apply key controls for Online Identity and User Management Services

Given
the lab environment and topic-specific tools for 'Online Identity and User Management Services' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Online Identity and User Management Services'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Online Identity and User Management Services': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Online Identity and User Management Services'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-072 — Intrusion Detection and Prevention Systems — Learn & Lab

Epic / Feature	Part 12: Practical Security
Business Value	Build a working understanding of intrusion detection and prevention systems and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Intrusion Detection and Prevention Systems' so that I can apply its concepts to reduce risk and improve outcomes.*

Non-Functional

Security

Reliability

Performance

Observability

Acceptance Criteria (BDD)

Scenario
Apply key controls for Intrusion Detection and Prevention Systems

Given
the lab environment and topic-specific tools for 'Intrusion Detection and Prevention Systems' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Intrusion Detection and Prevention Systems'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Intrusion Detection and Prevention Systems': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Intrusion Detection and Prevention Systems'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-073 — Transmission Control Protocol/Internet Protocol Packet Analysis — Learn & Lab

Epic / Feature	Part 12: Practical Security
Business Value	Build a working understanding of transmission control protocol/internet protocol packet analysis and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Transmission Control Protocol/Internet Protocol Packet Analysis' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Transmission Control Protocol/Internet Protocol Packet Analysis

Given
the lab environment and topic-specific tools for 'Transmission Control Protocol/Internet Protocol Packet Analysis' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Transmission Control Protocol/Internet Protocol Packet Analysis'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Transmission Control Protocol/Internet Protocol Packet Analysis': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Transmission Control Protocol/Internet Protocol Packet Analysis'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-074 — Firewalls — Learn & Lab

Epic / Feature	Part 12: Practical Security
Business Value	Build a working understanding of firewalls and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Firewalls' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Firewalls

Given
the lab environment and topic-specific tools for 'Firewalls' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Firewalls'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Firewalls': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Firewalls'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-075 — Penetration Testing — Learn & Lab

Epic / Feature	Part 12: Practical Security
Business Value	Build a working understanding of penetration testing and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Application Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Application Security Engineer, I want to study and practice 'Penetration Testing' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Penetration Testing

Given
the lab environment and topic-specific tools for 'Penetration Testing' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Penetration Testing'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Penetration Testing': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Penetration Testing'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-076 — System Security — Learn & Lab

Epic / Feature	Part 12: Practical Security
Business Value	Build a working understanding of system security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Systems Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Systems Engineer, I want to study and practice 'System Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for System Security

Given
the lab environment and topic-specific tools for 'System Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'System Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'System Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'System Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-077 — Access Controls — Learn & Lab

Epic / Feature	Part 12: Practical Security
Business Value	Build a working understanding of access controls and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Privacy Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, IDP / MFA-capable test app
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Privacy Engineer, I want to study and practice 'Access Controls' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Access Controls

Given
the lab environment and topic-specific tools for 'Access Controls' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Access Controls'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Access Controls': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Access Controls'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-078 — Endpoint Security — Learn & Lab

Epic / Feature	Part 12: Practical Security
Business Value	Build a working understanding of endpoint security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Systems Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Systems Engineer, I want to study and practice 'Endpoint Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Endpoint Security

Given
the lab environment and topic-specific tools for 'Endpoint Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Endpoint Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Endpoint Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Endpoint Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-079 — Assessments and Audits — Learn & Lab

Epic / Feature	Part 12: Practical Security
Business Value	Build a working understanding of assessments and audits and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Application Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Application Security Engineer, I want to study and practice 'Assessments and Audits' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Observability

Acceptance Criteria (BDD)

Scenario
Apply key controls for Assessments and Audits

Given
the lab environment and topic-specific tools for 'Assessments and Audits' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Assessments and Audits'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Assessments and Audits': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Assessments and Audits'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-080 — Fundamentals of Cryptography — Learn & Lab

Epic / Feature	Part 12: Practical Security
Business Value	Build a working understanding of fundamentals of cryptography and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Platform Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, OpenSSL/mkcert, TLS scanner
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Platform Engineer, I want to study and practice 'Fundamentals of Cryptography' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Fundamentals of Cryptography

Given
the lab environment and topic-specific tools for 'Fundamentals of Cryptography' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Fundamentals of Cryptography'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Fundamentals of Cryptography': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Fundamentals of Cryptography'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-081 — Securing the Infrastructure — Learn & Lab

Epic / Feature	Part 13: Critical Infrastructure Security
Business Value	Build a working understanding of securing the infrastructure and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'Securing the Infrastructure' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Securing the Infrastructure

Given
the lab environment and topic-specific tools for 'Securing the Infrastructure' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Securing the Infrastructure'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Securing the Infrastructure': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Securing the Infrastructure'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-082 — Threat Landscape and Good Practices for the Internet Infrastructure — Learn & Lab

Epic / Feature	Part 13: Critical Infrastructure Security
Business Value	Build a working understanding of threat landscape and good practices for the internet infrastructure and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Threat Landscape and Good Practices for the Internet Infrastructure' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Threat Landscape and Good Practices for the Internet Infrastructure

Given
the lab environment and topic-specific tools for 'Threat Landscape and Good Practices for the Internet Infrastructure' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Threat Landscape and Good Practices for the Internet Infrastructure'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Threat Landscape and Good Practices for the Internet Infrastructure': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Threat Landscape and Good Practices for the Internet Infrastructure'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-083 — Cyber Attacks Against the Grid Infrastructure — Learn & Lab

Epic / Feature	Part 13: Critical Infrastructure Security
Business Value	Build a working understanding of cyber attacks against the grid infrastructure and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'Cyber Attacks Against the Grid Infrastructure' so that I can apply its concepts to reduce risk and improve outcomes.*

Non-Functional

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Cyber Attacks Against the Grid Infrastructure

Given
the lab environment and topic-specific tools for 'Cyber Attacks Against the Grid Infrastructure' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Cyber Attacks Against the Grid Infrastructure'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Cyber Attacks Against the Grid Infrastructure': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Cyber Attacks Against the Grid Infrastructure'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-084 — Threat Landscape and Good Practices For The Smart Grid Infrastructure — Learn & Lab

Epic / Feature	Part 13: Critical Infrastructure Security
Business Value	Build a working understanding of threat landscape and good practices for the smart grid infrastructure and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Threat Landscape and Good Practices For The Smart Grid Infrastructure' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Threat Landscape and Good Practices For The Smart Grid Infrastructure

Given
the lab environment and topic-specific tools for 'Threat Landscape and Good Practices For The Smart Grid Infrastructure' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Threat Landscape and Good Practices For The Smart Grid Infrastructure'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Threat Landscape and Good Practices For The Smart Grid Infrastructure': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Threat Landscape and Good Practices For The Smart Grid Infrastructure'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-085 — Energy Infrastructure Cyber Security — Learn & Lab

Epic / Feature	Part 13: Critical Infrastructure Security
Business Value	Build a working understanding of energy infrastructure cyber security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'Energy Infrastructure Cyber Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Energy Infrastructure Cyber Security

Given
the lab environment and topic-specific tools for 'Energy Infrastructure Cyber Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Energy Infrastructure Cyber Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Energy Infrastructure Cyber Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Energy Infrastructure Cyber Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-086 — Homeland Security — Learn & Lab

Epic / Feature	Part 13: Critical Infrastructure Security
Business Value	Build a working understanding of homeland security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Homeland Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Compliance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Homeland Security

Given
the lab environment and topic-specific tools for 'Homeland Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Homeland Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Homeland Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Homeland Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-087 — Cyber Warfare — Learn & Lab

Epic / Feature	Part 13: Critical Infrastructure Security
Business Value	Build a working understanding of cyber warfare and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Cyber Warfare' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Cyber Warfare

Given
the lab environment and topic-specific tools for 'Cyber Warfare' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Cyber Warfare'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Cyber Warfare': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Cyber Warfare'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-088 — Cyber Attack Process — Learn & Lab

Epic / Feature	Part 13: Critical Infrastructure Security
Business Value	Build a working understanding of cyber attack process and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Cyber Attack Process' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Cyber Attack Process

Given
the lab environment and topic-specific tools for 'Cyber Attack Process' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Cyber Attack Process'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Cyber Attack Process': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Cyber Attack Process'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-089 — Smart Cities: Cyber Security Concerns — Learn & Lab

Epic / Feature	Part 14: Cyber Security for the Smart City And Smart Homes
Business Value	Build a working understanding of smart cities: cyber security concerns and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'Smart Cities: Cyber Security Concerns' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Smart Cities: Cyber Security Concerns

Given
the lab environment and topic-specific tools for 'Smart Cities: Cyber Security Concerns' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Smart Cities: Cyber Security Concerns'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Smart Cities: Cyber Security Concerns': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Smart Cities: Cyber Security Concerns'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-090 — Community Preparedness Action Groups for Smart City Cyber Security — Learn & Lab

Epic / Feature	Part 14: Cyber Security for the Smart City And Smart Homes
Business Value	Build a working understanding of community preparedness action groups for smart city cyber security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'Community Preparedness Action Groups for Smart City Cyber Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Community Preparedness Action Groups for Smart City Cyber Security

Given
the lab environment and topic-specific tools for 'Community Preparedness Action Groups for Smart City Cyber Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Community Preparedness Action Groups for Smart City Cyber Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Community Preparedness Action Groups for Smart City Cyber Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Community Preparedness Action Groups for Smart City Cyber Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-091 — Smart City Disaster Preparedness and Resilience — Learn & Lab

Epic / Feature	Part 14: Cyber Security for the Smart City And Smart Homes
Business Value	Build a working understanding of smart city disaster preparedness and resilience and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'Smart City Disaster Preparedness and Resilience' so that I can apply its concepts to reduce risk and improve outcomes.*

Non-Functional

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Smart City Disaster Preparedness and Resilience

Given
the lab environment and topic-specific tools for 'Smart City Disaster Preparedness and Resilience' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Smart City Disaster Preparedness and Resilience'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Smart City Disaster Preparedness and Resilience': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Smart City Disaster Preparedness and Resilience'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-092 — Disaster Preparedness and Resiliency Policy Considerations for the Smart City — Learn & Lab

Epic / Feature	Part 14: Cyber Security for the Smart City And Smart Homes
Business Value	Build a working understanding of disaster preparedness and resiliency policy considerations for the smart city and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Program Manager
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Program Manager, I want to study and practice 'Disaster Preparedness and Resiliency Policy Considerations for the Smart City' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Compliance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Disaster Preparedness and Resiliency Policy Considerations for the Smart City

Given
the lab environment and topic-specific tools for 'Disaster Preparedness and Resiliency Policy Considerations for the Smart City' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Disaster Preparedness and Resiliency Policy Considerations for the Smart City'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Disaster Preparedness and Resiliency Policy Considerations for the Smart City': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Disaster Preparedness and Resiliency Policy Considerations for the Smart City'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-093 — Cyber Security in Smart Homes — Learn & Lab

Epic / Feature	Part 14: Cyber Security for the Smart City And Smart Homes
Business Value	Build a working understanding of cyber security in smart homes and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'Cyber Security in Smart Homes' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Cyber Security in Smart Homes

Given
the lab environment and topic-specific tools for 'Cyber Security in Smart Homes' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Cyber Security in Smart Homes'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Cyber Security in Smart Homes': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Cyber Security in Smart Homes'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-094 — Threat Landscape and Good Practices for Smart Homes and Converged Media — Learn & Lab

Epic / Feature	Part 14: Cyber Security for the Smart City And Smart Homes
Business Value	Build a working understanding of threat landscape and good practices for smart homes and converged media and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Threat Landscape and Good Practices for Smart Homes and Converged Media' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Threat Landscape and Good Practices for Smart Homes and Converged Media

Given
the lab environment and topic-specific tools for 'Threat Landscape and Good Practices for Smart Homes and Converged Media' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Threat Landscape and Good Practices for Smart Homes and Converged Media'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Threat Landscape and Good Practices for Smart Homes and Converged Media': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Threat Landscape and Good Practices for Smart Homes and Converged Media'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-095 — Future Trends For Cyber Security for Smart- Cities And Homes — Learn & Lab

Epic / Feature	Part 14: Cyber Security for the Smart City And Smart Homes
Business Value	Build a working understanding of future trends for cyber security for smart- cities and homes and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'Future Trends For Cyber Security for Smart- Cities And Homes' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Future Trends For Cyber Security for Smart- Cities And Homes

Given
the lab environment and topic-specific tools for 'Future Trends For Cyber Security for Smart- Cities And Homes' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Future Trends For Cyber Security for Smart- Cities And Homes'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Future Trends For Cyber Security for Smart- Cities And Homes': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Future Trends For Cyber Security for Smart- Cities And Homes'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-096 — An Overview of Cyber Attacks and Defenses on Intelligent Connected Vehicles — Learn & Lab

Epic / Feature	Part 15: Cyber Security Of Connected And Automated Vehicles
Business Value	Build a working understanding of an overview of cyber attacks and defenses on intelligent connected vehicles and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'An Overview of Cyber Attacks and Defenses on Intelligent Connected Vehicles' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for An Overview of Cyber Attacks and Defenses on Intelligent Connected Vehicles

Given
the lab environment and topic-specific tools for 'An Overview of Cyber Attacks and Defenses on Intelligent Connected Vehicles' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'An Overview of Cyber Attacks and Defenses on Intelligent Connected Vehicles'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'An Overview of Cyber Attacks and Defenses on Intelligent Connected Vehicles': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'An Overview of Cyber Attacks and Defenses on Intelligent Connected Vehicles'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-097 — An Overview Of Cyber Security Issues In Vehicular Ad-hoc Networks (VANETs) — Learn & Lab

Epic / Feature	Part 15: Cyber Security Of Connected And Automated Vehicles
Business Value	Build a working understanding of an overview of cyber security issues in vehicular ad-hoc networks (vanets) and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'An Overview Of Cyber Security Issues In Vehicular Ad-hoc Networks (VANETs)' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for An Overview Of Cyber Security Issues In Vehicular Ad-hoc Networks (VANETs)

Given
the lab environment and topic-specific tools for 'An Overview Of Cyber Security Issues In Vehicular Ad-hoc Networks (VANETs)' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'An Overview Of Cyber Security Issues In Vehicular Ad-hoc Networks (VANETs)'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'An Overview Of Cyber Security Issues In Vehicular Ad-hoc Networks (VANETs)': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'An Overview Of Cyber Security Issues In Vehicular Ad-hoc Networks (VANETs)'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-098 — An Overview: Various Cyber Attacks in VANET — Learn & Lab

Epic / Feature	Part 15: Cyber Security Of Connected And Automated Vehicles
Business Value	Build a working understanding of an overview: various cyber attacks in vanet and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'An Overview: Various Cyber Attacks in VANET' so that I can apply its concepts to reduce risk and improve outcomes.*

Non-Functional

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for An Overview: Various Cyber Attacks in VANET

Given
the lab environment and topic-specific tools for 'An Overview: Various Cyber Attacks in VANET' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'An Overview: Various Cyber Attacks in VANET'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'An Overview: Various Cyber Attacks in VANET': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'An Overview: Various Cyber Attacks in VANET'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-099 — Security Through Diversity — Learn & Lab

Epic / Feature	Part 16: Advanced Security
Business Value	Build a working understanding of security through diversity and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Security Through Diversity' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Security Through Diversity

Given
the lab environment and topic-specific tools for 'Security Through Diversity' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Security Through Diversity'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Security Through Diversity': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Security Through Diversity'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-100 — Online e-Reputation Management Services — Learn & Lab

Epic / Feature	Part 16: Advanced Security
Business Value	Build a working understanding of online e-reputation management services and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Application Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Application Security Engineer, I want to study and practice 'Online e-Reputation Management Services' so that I can apply its concepts to reduce risk and improve outcomes.*

Non-Functional

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Online e-Reputation Management Services

Given
the lab environment and topic-specific tools for 'Online e-Reputation Management Services' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Online e-Reputation Management Services'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Online e-Reputation Management Services': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Online e-Reputation Management Services'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-101 — Content Filtering — Learn & Lab

Epic / Feature	Part 16: Advanced Security
Business Value	Build a working understanding of content filtering and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Application Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Application Security Engineer, I want to study and practice 'Content Filtering' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Content Filtering

Given
the lab environment and topic-specific tools for 'Content Filtering' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Content Filtering'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Content Filtering': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Content Filtering'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-102 — Data Loss Protection — Learn & Lab

Epic / Feature	Part 16: Advanced Security
Business Value	Build a working understanding of data loss protection and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Data Loss Protection' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Data Loss Protection

Given
the lab environment and topic-specific tools for 'Data Loss Protection' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Data Loss Protection'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Data Loss Protection': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Data Loss Protection'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-103 — Satellite Cyber Attack Search and Destroy — Learn & Lab

Epic / Feature	Part 16: Advanced Security
Business Value	Build a working understanding of satellite cyber attack search and destroy and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Satellite Cyber Attack Search and Destroy' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Satellite Cyber Attack Search and Destroy

Given
the lab environment and topic-specific tools for 'Satellite Cyber Attack Search and Destroy' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Satellite Cyber Attack Search and Destroy'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Satellite Cyber Attack Search and Destroy': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Satellite Cyber Attack Search and Destroy'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-104 — Verifiable Voting Systems — Learn & Lab

Epic / Feature	Part 16: Advanced Security
Business Value	Build a working understanding of verifiable voting systems and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Engineer, I want to study and practice 'Verifiable Voting Systems' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Verifiable Voting Systems

Given
the lab environment and topic-specific tools for 'Verifiable Voting Systems' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Verifiable Voting Systems'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Verifiable Voting Systems': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Verifiable Voting Systems'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-105 — Advanced Data Encryption — Learn & Lab

Epic / Feature	Part 16: Advanced Security
Business Value	Build a working understanding of advanced data encryption and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Platform Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, OpenSSL/mkcert, TLS scanner
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Platform Engineer, I want to study and practice 'Advanced Data Encryption' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Advanced Data Encryption

Given
the lab environment and topic-specific tools for 'Advanced Data Encryption' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Advanced Data Encryption'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Advanced Data Encryption': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Advanced Data Encryption'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-106 — Use Of Artificial Intelligence (AI) In Cyber Security — Learn & Lab

Epic / Feature	Part 16: Advanced Security
Business Value	Build a working understanding of use of artificial intelligence (ai) in cyber security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	ML Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a ML Security Engineer, I want to study and practice 'Use Of Artificial Intelligence (AI) In Cyber Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Use Of Artificial Intelligence (AI) In Cyber Security

Given
the lab environment and topic-specific tools for 'Use Of Artificial Intelligence (AI) In Cyber Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Use Of Artificial Intelligence (AI) In Cyber Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Use Of Artificial Intelligence (AI) In Cyber Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Use Of Artificial Intelligence (AI) In Cyber Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-107 — New Cyber Security Vulnerabilities And Trends Facing Aerospace And Defense Systems — Learn & Lab

Epic / Feature	Part 17: Future Cyber Security Trends And Directions
Business Value	Build a working understanding of new cyber security vulnerabilities and trends facing aerospace and defense systems and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'New Cyber Security Vulnerabilities And Trends Facing Aerospace And Defense Systems' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for New Cyber Security Vulnerabilities And Trends Facing Aerospace And Defense Systems

Given
the lab environment and topic-specific tools for 'New Cyber Security Vulnerabilities And Trends Facing Aerospace And Defense Systems' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'New Cyber Security Vulnerabilities And Trends Facing Aerospace And Defense Systems'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'New Cyber Security Vulnerabilities And Trends Facing Aerospace And Defense Systems': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'New Cyber Security Vulnerabilities And Trends Facing Aerospace And Defense Systems'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-108 — How Aerospace And Defense Companies Will Respond To Future Cyber Security Threats — Learn & Lab

Epic / Feature	Part 17: Future Cyber Security Trends And Directions
Business Value	Build a working understanding of how aerospace and defense companies will respond to future cyber security threats and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'How Aerospace And Defense Companies Will Respond To Future Cyber Security Threats' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for How Aerospace And Defense Companies Will Respond To Future Cyber Security Threats

Given
the lab environment and topic-specific tools for 'How Aerospace And Defense Companies Will Respond To Future Cyber Security Threats' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'How Aerospace And Defense Companies Will Respond To Future Cyber Security Threats'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'How Aerospace And Defense Companies Will Respond To Future Cyber Security Threats': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'How Aerospace And Defense Companies Will Respond To Future Cyber Security Threats'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-109 — Understanding the Future Trends of the Aviation Cyber Security Threat Landscape — Learn & Lab

Epic / Feature	Part 17: Future Cyber Security Trends And Directions
Business Value	Build a working understanding of understanding the future trends of the aviation cyber security threat landscape and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Network Security Engineer
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool, Packet capture tool (tcpdump/Wireshark), Firewall/router lab
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Network Security Engineer, I want to study and practice 'Understanding the Future Trends of the Aviation Cyber Security Threat Landscape' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Understanding the Future Trends of the Aviation Cyber Security Threat Landscape

Given
the lab environment and topic-specific tools for 'Understanding the Future Trends of the Aviation Cyber Security Threat Landscape' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Understanding the Future Trends of the Aviation Cyber Security Threat Landscape'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Understanding the Future Trends of the Aviation Cyber Security Threat Landscape': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Understanding the Future Trends of the Aviation Cyber Security Threat Landscape'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-110 — Fighting the Rising Trends Of Cyber Attacks on Aviation — Learn & Lab

Epic / Feature	Part 17: Future Cyber Security Trends And Directions
Business Value	Build a working understanding of fighting the rising trends of cyber attacks on aviation and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'Fighting the Rising Trends Of Cyber Attacks on Aviation' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Fighting the Rising Trends Of Cyber Attacks on Aviation

Given
the lab environment and topic-specific tools for 'Fighting the Rising Trends Of Cyber Attacks on Aviation' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Fighting the Rising Trends Of Cyber Attacks on Aviation'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Fighting the Rising Trends Of Cyber Attacks on Aviation': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Fighting the Rising Trends Of Cyber Attacks on Aviation'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-111 — Future Trends For Cyber Security Hardening of Aviation Systems — Learn & Lab

Epic / Feature	Part 17: Future Cyber Security Trends And Directions
Business Value	Build a working understanding of future trends for cyber security hardening of aviation systems and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'Future Trends For Cyber Security Hardening of Aviation Systems' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Future Trends For Cyber Security Hardening of Aviation Systems

Given
the lab environment and topic-specific tools for 'Future Trends For Cyber Security Hardening of Aviation Systems' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Future Trends For Cyber Security Hardening of Aviation Systems'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Future Trends For Cyber Security Hardening of Aviation Systems': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Future Trends For Cyber Security Hardening of Aviation Systems'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-112 — Future Trends For Cyber Security in the Gaming Industry — Learn & Lab

Epic / Feature	Part 17: Future Cyber Security Trends And Directions
Business Value	Build a working understanding of future trends for cyber security in the gaming industry and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'Future Trends For Cyber Security in the Gaming Industry' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Future Trends For Cyber Security in the Gaming Industry

Given
the lab environment and topic-specific tools for 'Future Trends For Cyber Security in the Gaming Industry' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Future Trends For Cyber Security in the Gaming Industry'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Future Trends For Cyber Security in the Gaming Industry': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Future Trends For Cyber Security in the Gaming Industry'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-113 — Future Trends For Cyber Attacks in the Health Care Industry — Learn & Lab

Epic / Feature	Part 17: Future Cyber Security Trends And Directions
Business Value	Build a working understanding of future trends for cyber attacks in the health care industry and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'Future Trends For Cyber Attacks in the Health Care Industry' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Future Trends For Cyber Attacks in the Health Care Industry

Given
the lab environment and topic-specific tools for 'Future Trends For Cyber Attacks in the Health Care Industry' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Future Trends For Cyber Attacks in the Health Care Industry'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Future Trends For Cyber Attacks in the Health Care Industry': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Future Trends For Cyber Attacks in the Health Care Industry'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-114 — Future Trends For Cyber Defense Of Offshore Drilling Rigs — Learn & Lab

Epic / Feature	Part 17: Future Cyber Security Trends And Directions
Business Value	Build a working understanding of future trends for cyber defense of offshore drilling rigs and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'Future Trends For Cyber Defense Of Offshore Drilling Rigs' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Future Trends For Cyber Defense Of Offshore Drilling Rigs

Given
the lab environment and topic-specific tools for 'Future Trends For Cyber Defense Of Offshore Drilling Rigs' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Future Trends For Cyber Defense Of Offshore Drilling Rigs'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Future Trends For Cyber Defense Of Offshore Drilling Rigs': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Future Trends For Cyber Defense Of Offshore Drilling Rigs'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

CISH-115 — Future Trends In Maritime Cyber Security — Learn & Lab

Epic / Feature	Part 17: Future Cyber Security Trends And Directions
Business Value	Build a working understanding of future trends in maritime cyber security and its place in a modern security program; be able to explain core concepts, map them to the CIA triad, and identify common threats and controls.
Priority / Estimate	**Priority:** Must **SP:** 3
Persona	Security Architect
Dependencies	Lab VM or container runtime, Git repo for notes, Markdown/PDF export tool
Assumptions / Risks	Time-box chapter to one iteration; open issues captured for later

Story *As a Security Architect, I want to study and practice 'Future Trends In Maritime Cyber Security' so that I can apply its concepts to reduce risk and improve outcomes.* **Non-Functional**

Security

Reliability

Performance

Acceptance Criteria (BDD)

Scenario
Apply key controls for Future Trends In Maritime Cyber Security

Given
the lab environment and topic-specific tools for 'Future Trends In Maritime Cyber Security' are available

When
I execute the hands-on objectives and lab: Hands-on: Build a small lab demonstrating key concepts in 'Future Trends In Maritime Cyber Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Then
the deliverables are produced (2–3 page brief on 'Future Trends In Maritime Cyber Security': risks, architecture, controls, and a checklist; plus a one-slide executive summary.); evidence (screenshots/logs/configs) is attached and reviewed

Definition of Ready: Persona clear; AC drafted; Dependencies known; Estimate set. • *Definition of Done:* All ACs pass; Tests green; Security checks; Docs updated; Evidence attached.

Tasks

- ☐ Draft a one-page chapter plan: scope, objectives, interfaces, success metrics.
- ☐ Set up tools, datasets, and accounts; document versions and configuration.
- ☐ Complete objective: Define key terms and articulate why this topic matters to security outcomes.
- ☐ Complete objective: Diagram the architecture/data flows and identify threat surfaces.
- ☐ Execute lab: Hands-on: Build a small lab demonstrating key concepts in 'Future Trends In Maritime Cyber Security'. Capture screenshots/notes and one measurable result (e.g., a passing test, alert fired, or control verified).

Appendix: Attached Definitions/Templates (optional)

StoryCardDefinition.tex not found
UserStoryTemplate.tex not found