COMPTIA SECURITY+ SY0-701 · WEEK 15

Governance, Compliance, and Audits



Objectives 5.1 to 5.6 · 90-minute lesson

Presenter: Trapper Brown

What you will be able to do in 90 minutes

1. Distinguish policies, standards, procedures, and guidelines, and give an example of each.
2. Identify governance structures and the roles of owners, controllers, processors, and custodians.
3. Describe how to select, assess, contract with, and monitor a vendor.
4. Match agreement types such as SLA, MOU, MOA, MSA, SOW, NDA, and BPA to their purpose.
5. Explain compliance reporting, the consequences of non-compliance, and core privacy terms.
6. Compare internal and external audits and the three penetration testing environments.
7. Plan a security awareness program with phishing campaigns and recurring training.

AGENDA

3 min	Governance turns security into a program
10 min	Policies, standards, procedures, guidelines
8 min	Governance structures and data roles
9 min	Selecting and assessing vendors
7 min	Agreement types
10 min	Compliance and privacy
7 min	Audits and assessments
8 min	Penetration testing
10 min	Exercise 1: name the document, agreement, or role
9 min	Security awareness practices
7 min	Exercise 2: awareness scenarios
2 min	Wrap-up

Policies say what, procedures say how

Document	What it is	Clinic example
Policy	Required high-level intent from leadership	Acceptable use policy
Standard	Mandatory, specific rule that supports a policy	Passwords at least 14 characters
Procedure	Step-by-step instructions for one task	Offboarding checklist for leavers
Guideline	Recommended practice; advice, not mandatory	Tips for spotting fake invoices

Who governs, and who answers for the data

Boards and committees

Set direction and oversee risk; committees focus it

Audit committee

Data owner

Senior person accountable for a data set

Practice manager

Controller

Decides why and how personal data is processed

The clinic

Processor

Processes personal data for the controller

Cloud billing company

Custodian/steward

Custodian does daily care; steward guards quality

IT runs backups and access

Manage a vendor from selection to monitoring

1

Select

Due diligence; check for conflicts of interest

2

Assess

Questionnaire, audits, pen tests, supply chain

3

Contract

Right to audit, SLA, NDA, rules of engagement

4

Monitor

Review performance, reports, and new risks

5

Reassess

Repeat yearly or when the vendor changes

Match the agreement to the relationship

Agreement	Purpose
SLA	Measurable service levels, such as 99.9% uptime
MOU / MOA	MOU states shared intent; MOA sets specific duties
MSA	Master terms that govern all future work
WO / SOW	One job's deliverables, schedule, and price
NDA	Keeps shared information confidential
BPA	Partnership duties, shares, and decision rights

What non-compliance costs

Fines

Monetary penalties set by regulators or courts

HIPAA civil money penalties

Sanctions

Restrictions on what the organization may do

Barred from bidding on contracts

Reputational damage

Lost trust, customers, and future business

A breach on the local news

Loss of license

Right to operate or practice is suspended

Operating or professional license

Contractual impacts

Penalties, terminated deals, lost partners

Card processing terminated

Internal audits prepare, external audits prove

Internal

- Compliance checks run by the organization
- Audit committee oversees the audit function
- Self-assessments against a framework
- Finds gaps before an outsider does

External

- Regulatory audits and examinations
- Assessments against a standard such as PCI DSS
- Independent third-party audit, such as SOC 2
- Attestation: a qualified outsider vouches for it

Know the environment and the team's role

Term	Meaning
Known environment	Full details: diagrams, code, and accounts
Partially known	Some details, such as IP ranges or a user account
Unknown environment	No details; testers start like an outsider
Offensive / defensive	Red team attacks; blue team defends
Integrated	Red and blue work together (purple team)
Reconnaissance	Passive: no contact. Active: probes the target

EXERCISE 1 · NAME IT

Name the document, agreement, or role



8

MINUTES · PAIRS

For each item, name the governance document type, agreement type, role, or test environment it describes, with one sentence of reasoning.

1. Laptops must use full disk encryption with AES-256
2. Step-by-step list for disabling a departing employee's access
3. The billing company processes claims for the clinic
4. A contract says the vendor answers outages within one hour
5. Two clinics state their intent to share a backup site someday
6. The practice manager decides who may see patient billing data
7. Tips on writing a strong passphrase, offered as advice
8. Under one master contract, a new document sets one job's price
9. Testers get network diagrams and source code before starting
10. IT backs up the EHR database and applies access rights daily

Build awareness that changes behavior

Phishing campaigns

Simulated phish, then short training on the spot

Monthly test emails

Report, do not delete

One-click reporting and fast feedback to the user

Report Phish button

Anomalous behavior

Spot risky, unexpected, or unintentional acts

3 a.m. login from abroad

User guidance

Handbooks, passwords, media, remote work, OPSEC

No found USB drives

Reporting, monitoring

Initial and recurring training, tracked by metrics

Click rate and report rate

Develop and execute

Build for the audience, deliver, measure, repeat

Clinic-specific examples

Risky, unexpected, or unintentional



6

MINUTES · SMALL GROUPS

Classify each behavior as risky, unexpected, or unintentional, and name the awareness topic or response that fits it.

1. A nurse plugs a USB drive found in the parking lot into a PC
2. The billing clerk's account logs in at 3 a.m. from overseas
3. A receptionist emails a patient list to the wrong Dr. Smith
4. A doctor shares her EHR password with a medical student
5. An admin who never touches payroll downloads the whole file
6. A user reports a phish after entering her password. Next steps?
7. A remote worker discusses patients on a coffee shop patio

REVIEW

Five questions: write your answers first

1. What is the difference between a policy and a standard?
2. A cloud billing company handles patient data on the clinic's instructions. What is its privacy role?
3. Which agreement sets the deliverables and price of one project under an existing master contract?
4. What is the difference between passive and active reconnaissance?
5. Name the three kinds of anomalous behavior in objective 5.6, with an example of each.

TAKEAWAYS

Four things to take with you

01

Know the document hierarchy

Policy is intent, standard is rule, procedure is steps, guideline is advice.

02

Owners decide, custodians do

Controllers set the purpose; processors act on their instructions.

03

Vendors carry your risk

Diligence, questionnaires, audits, contracts, then keep monitoring.

04

Train, test, and track

Phishing campaigns and easy reporting make people a control.

NEXT Lab 15: An acceptable use policy and a vendor risk questionnaire