Understand the system

Compliance means meeting the obligations that apply to your organization: laws and regulations, contracts, adopted standards, and internal policies. Controls are how you meet them; evidence shows they operated.

One model for every control

Layer	Meaning	Example: production access	Evidence it leaves
01 **Policy** What must be true?	The organization's rules and intent.	Access to production must match job responsibilities.	The approved policy, with its owner and review date.
02 **Procedure** Who does what, when, and how?	The repeatable steps people follow.	Request access, get approval, receive a time-limited role, and lose it when no longer needed.	Access request tickets with approvals.
03 **Implementation** What enforces it?	The technical and organizational mechanisms that make the rule real.	Scoped roles, single sign-on with MFA, automated provisioning and expiry, and audit logs.	Configuration exports and provisioning logs.
04 **Management** Who keeps it working?	Ownership, review, exceptions, and correction.	A named owner reviews access quarterly, manages exceptions, and corrects failures.	Review results, exception records, and remediation tickets.

What to keep in mind

Evidence

Dated, attributable, complete for the population, and covering the whole period. Exports and logs beat screenshots.

Scope

Follows the data into logs, error trackers, analytics, backups, warehouses, and vendors. Keeping data out of a system is often the cheapest control.

Ownership

Every control has a named owner who keeps it working, checks its evidence each period, and fixes the cause when it fails.

Risk

How likely something is, and how much harm it would cause. Controls are chosen to treat risk; accepting a risk is a decision for an authorized owner.

The course in nine lines

1. Compliance is meeting applicable obligations; controls meet them; evidence shows they operated.
2. Scope follows the data. Find every copy before deciding which rules apply.
3. Least privilege for people and pipelines; just-in-time for sensitive access; revoke exposed secrets first.
4. Every change explainable: independent review, tests, recorded deployment. Exceptions are approved and time-bound.
5. Collect only what a purpose needs; set retention per store; make deletion reach every copy.
6. Evidence is dated, attributable, complete, and covers the period. Fix causes, not just instances.
7. Escalate possible incidents early; contain without destroying evidence; there is no universal deadline.
8. AI features need intended use, data and vendor review, evaluation, human oversight, monitoring, and change control.
9. Frameworks differ in why they apply and who checks. The engineering practice is the same.

CC BY 4.0 · Made by Workstreet

Developer checklist

Check these at each stage of the work. Each item maps to a lesson in the course.

Design

- [ ] Which data does this touch, and where will copies end up (logs, analytics, backups, vendors)?
- [ ] Is every field needed for a stated purpose? What is the retention for each store?
- [ ] Does a new vendor or integration receive sensitive data? Is it approved for that data?
- [ ] Can deletion and access requests reach every store?

Code review

- [ ] No secrets in code, config, or test fixtures.
- [ ] No credentials, tokens, or personal data in logs or error payloads.
- [ ] Authorization is checked on the server for every object a caller can name.
- [ ] Tests cover the security-relevant behavior, such as cross-account access.

Deployment

- [ ] Changes merge through a reviewed pull request, approved by someone other than the author.
- [ ] Deployments run from the pipeline, with short-lived credentials.
- [ ] Emergency changes get approval and an after-the-fact review.
- [ ] Exceptions are written down, approved by the risk owner, time-bound, and tracked.

Operation

- [ ] Access is granted through roles, reviewed periodically, and removed when people leave or move.
- [ ] Sensitive access is just-in-time and logged.
- [ ] Control owners check their own evidence each period: dated, complete, attributable.
- [ ] Findings are fixed at the cause, and the fix is verified and recorded.

Incident response

- [ ] Escalate through the incident process as soon as something might be wrong.
- [ ] Do not decide alone whether it is a breach, or notify anyone outside the process.
- [ ] Contain without destroying evidence: preserve logs and inventories first.
- [ ] Revoke exposed secrets immediately.

AI changes

- [ ] Intended use and out-of-scope uses are documented.
- [ ] Sensitive data is masked before prompts; vendor terms and agreements are reviewed.
- [ ] Evaluated against agreed acceptance criteria, including adversarial inputs.
- [ ] A human approves outputs that reach customers; quality is monitored in production.
- [ ] Model versions are pinned, and model, prompt, and provider changes go through change control.

CC BY 4.0 · Made by Workstreet

Framework reference

SOC 2 Attestation report	A Type 1 report covers the system description and whether controls are suitably designed as of a specific date. A Type 2 report also covers whether those controls operated effectively throughout a specified period. The criteria state what must be achieved; management decides how, and defines the system boundaries. Example: Ship production changes only through the defined process: a reviewed pull request, passing checks, and a recorded deployment. AICPA Trust Services Criteria
ISO 27001 Certifiable ISMS standard	It is a management system standard. It requires you to understand your risks, choose controls to treat them, measure whether they work, and correct what does not. Annex A controls are selected through risk treatment, not adopted as a fixed checklist. Example: Connect a security risk you own (for example, leaked credentials) to its treatment, an owner, a periodic check, and corrective action when the check fails. ISO/IEC 27001:2022
ISO 42001 Certifiable AI management system standard	It manages AI as an organizational system (intended use, impacts on people, data, life cycle, oversight, and monitoring), not just model accuracy. A model provider's certification covers the provider's own management system, not how your organization uses the model. Example: Document an AI feature's intended use, evaluation results, human oversight, and monitoring, and send model or prompt changes through change control. ISO/IEC 42001:2023
HIPAA U.S. federal law and regulations	Applicability comes first. Within scope, Security Rule implementation specifications are either required or addressable. Addressable does not mean optional: the organization must assess whether the specification is reasonable and appropriate, implement it if so, and otherwise document why and implement an equivalent alternative where reasonable and appropriate. Example: Keep ePHI out of systems that are not approved for it. For example, redact it before logs reach an observability vendor that has not signed a business associate agreement. HHS Security Rule summary
GDPR EU regulation	It concerns personal data and people's rights, not only security. Data protection by design and by default asks you to build minimisation, purpose limits, and retention into systems, and accountability means you must be able to demonstrate that you did. Example: Collect only the fields a stated purpose needs, set retention for each store, and support access and erasure requests across every place the data lives. GDPR
CMMC U.S. DoD contract program	Scope follows the information. Assets that process, store, or transmit CUI, and the assets that provide security protection for them, are in the assessment scope. Keeping CUI inside a defined boundary is therefore an engineering decision with compliance consequences. Example: Keep CUI inside the systems within the assessed boundary. Before adding a tool, service, or integration that would touch CUI, have it assessed and documented in the system security plan. 32 CFR Part 170

Illustrative connections, not claims that one control satisfies a framework. Dated status notes (CMMC rollout, proposed rule changes) are on the course reference page.

Glossary

Control. A safeguard or practice that reduces a risk or keeps it within an accepted level.

Evidence. Records showing that a control exists and operated.

Scope. The people, systems, data, locations, and vendors an obligation or control applies to.

Risk. The combination of how likely an event is and how much harm it would cause.

Operating effectiveness. Whether a control worked as designed, consistently, throughout a period.

Exception. A documented, approved, time-bound departure from a requirement, usually with compensating controls.

Least privilege. Only the access an identity needs, for only as long as it needs it.

Just-in-time access. Access requested for a specific need, approved, time-limited, and logged.

Trust Services Criteria. The AICPA criteria used in SOC 2 examinations, covering security, availability, processing integrity, confidentiality, and privacy.

Type 1 / Type 2. SOC 2 report types. Type 1: design as of a date. Type 2: design and operating effectiveness throughout a period.

ISMS / AIMS. Information security management system (ISO/IEC 27001); AI management system (ISO/IEC 42001).

Statement of Applicability. The ISO/IEC 27001 record of which controls are necessary, why, whether they are implemented, and why any Annex A controls are excluded.

Covered entity. Under HIPAA: a health plan, health care clearinghouse, or health care provider that conducts certain transactions electronically.

Business associate. A person or organization that creates, receives, maintains, or transmits PHI on behalf of a covered entity or another business associate.

PHI / ePHI. Individually identifiable health information transmitted or maintained in any form, with limited exclusions such as employment records. ePHI is PHI transmitted or maintained in electronic media.

Personal data. Under the GDPR: any information relating to an identified or identifiable natural person.

Controller / processor. The controller decides why and how personal data is processed; the processor processes it on the controller's behalf.

DPIA. Data protection impact assessment, required under the GDPR for processing likely to result in a high risk to people.

FCI. Federal Contract Information: information not intended for public release that is provided by or generated for the U.S. government under a contract, excluding public and simple transactional information.

CUI. Controlled Unclassified Information: information that a law, regulation, or government-wide policy requires or permits to be protected with safeguarding or dissemination controls.

System security plan (SSP). The document describing a system's boundary, environment, and how each security requirement is implemented.

POA&M. Plan of action and milestones: a record of unmet requirements and the plan to close them. CMMC allows them only in limited cases.

CC BY 4.0 · Made by Workstreet