Lab: Conduct a compliance review for a mock project and document findings

In this lab, you'll practice **conducting a compliance review** for a **fictional or mock project**. You'll be guided through:

1. **Defining a Mock Scenario** (e.g., a healthcare web application).
2. **Identifying Relevant Regulations** (e.g., GDPR, HIPAA).
3. **Completing a Compliance Checklist** to see where gaps might be.
4. **Creating a Risk Register** to prioritize issues.
5. **Summarizing Your Findings** in a short Compliance Review Report.

---

1. Define a Mock Project Scenario

- **Describe** a hypothetical app that handles sensitive data.
  - **Example**: A small web app called *HealthTrack* for storing basic patient info (name, age, diagnosis).
- **Mention Stakeholders**: (Product Owner, Developer, Compliance Officer).

Your Task:

- Write 1 paragraph about the app's purpose, data collected, and key stakeholders.

---

2. Pick Relevant Regulations

- **List** which regulations apply (e.g., GDPR, HIPAA).
- **Briefly state why** (e.g., EU personal data → GDPR; health info in the US → HIPAA).

Example Table:

Regulation	Reason
GDPR	EU data
HIPAA	US health data

---

3. Complete a Simple Checklist

Create a **short table** with 3–5 key items from each regulation.

GDPR Example:

Requirement	Status	Notes
Consent	No	No consent checkbox on form
Right to Erasure	Partial	Have deletion function, but not exposed

HIPAA Example:

Standard	Status	Notes
Security Rule	Partial	Basic encryption, but no unique logins
Breach Notification	No	No formal procedure if data is compromised

---

4. Create a Small Risk Register

Use a **table** to rank the risks from your checklist.

Risk/Issue	Reg.	Likely	Impact	Risk	Mitigation	Owner	Timeline
Missing Consent Checkbox	GDPR	M	M	M	Add checkbox & privacy notice	Dev Team	2 Weeks
No Breach Process	HIPAA	L	H	M	Create breach response plan & train staff	Security	1 Month

---

5. Write a Short Review Report

Outline (1–2 pages max):

1. **Introduction** (Brief overview of your app & data).
2. **Regulations in Scope** (List GDPR/HIPAA and why).
3. **Key Findings** (Summarize checklist gaps).
4. **Risk Register Highlights** (Top 2–3 high risks).
5. **Recommendations** (Short steps to fix issues).
6. **Conclusion** (Emphasize importance of closing gaps).

Final Submission

- **Checklists** (GDPR/HIPAA)
- **Risk Register** with at least 3–5 items
- **Short Report** (1–2 pages) summarizing findings

Summary

By following these steps and referencing the **examples**, you'll conduct a **full compliance review** of a mock project. You've:

- Created a **project scenario** with potentially sensitive data.
- Checked **GDPR/HIPAA** compliance against **real or simulated** checklists.
- Documented **risks** in a structured **risk register**.
- Summarized everything in a **short compliance review report** that highlights necessary fixes.

This process mirrors **real-world** compliance practices, ensuring you understand how to systematically identify, document, and prioritize compliance gaps in a project.