## Task 1: Introduction

Answer the questions below

I am ready to start the room.

No answer needed — ✓ Correct Answer

## Task 2: Why is it important?

Answer the questions below

The term used for legal and regulatory frameworks that govern the use and protection of information assets is called?

Regulation — ✓ Correct Answer

Health Insurance Portability and Accountability Act (HIPAA) targets which domain for data protection?

Healthcare — ✓ Correct Answer

## Task 3: Information Security Frameworks

Answer the questions below

The step that involves periodic evaluation of policies and making changes as per stakeholder's input is called?

Review and update — ✓ Correct Answer

A set of specific steps for undertaking a particular task or process is called?

Procedure — ✓ Correct Answer

## Task 4: Governance, Risk, and Compliance (GRC)

Answer the questions below

What is the component in the GRC framework involved in identifying, assessing, and prioritising risks to the organisation?

Risk Management — ✓ Correct Answer

Is it important to monitor and measure the performance of a developed policy? (yea/nay)

yea — ✓ Correct Answer

## **Task 5**: Privacy and Data Protection

Answer the questions below

What is the maximum fine for Tier 1 users as per GDPR (in terms of percentage)?

4 — ✓ Correct Answer

In terms of PCI DSS, what does CHD stand for?

cardholder data — ✓ Correct Answer — Hint

## **Task 6**: NIST Special Publications

Answer the questions below

Per NIST 800-53, in which control category does the media protection lie?

Physical — ✓ Correct Answer

Per NIST 800-53, in which control category does the incident response lie?

Administrative — ✓ Correct Answer

Which phase (name) of NIST 800-53 compliance best practices results in correlating identified assets and permissions?

Map — ✓ Correct Answer

## **Task 7**: Information Security Management and Compliance

Answer the questions below

Which ISO/IEC 27001 component involves selecting and implementing controls to reduce the identified risks to an acceptable level?

Risk treatment — ✓ Correct Answer

In SOC 2 generic controls, which control shows that the system remains available?

Availability — ✓ Correct Answer

## **Task 8**: Conclusion

Answer the questions below

Click the **View Site** button at the top of the task to launch the static site in split view. What is the flag after completing the exercise?

THM{SECURE_1001} — ✓ Correct Answer