Cybersecurity Fundamentals

Module 5: Quiz

Question 1

Which of the following can be used to map data flows through an organization and the relevant security controls used at each point along the way?

A) Encryption

B) Hashing

C) Hard copy

D) Data life cycle

Question 2

Why is an asset inventory so important?

A) It tells you what to encrypt

B) You can't protect what you don't know you have

C) The law requires it

D) It contains a price list

Question 3

Who is responsible for publishing and signing the organization's policies?

Question options:

A) The security office

B) Human Resources

C) Senior management

D) The legal department

Question 4

Which of the following is always true about logging?

Question options:

A) Logs should be very detailed

B) Logs should be in English

C) Logs should be concise

D) Logs should be stored separately from the systems they're logging

Question 5

A mode of encryption for ensuring confidentiality efficiently, with a minimum amount of processing overhead

A) Asymmetric

B) Symmetric

C) Hashing

D) Covert

Question 6

A ready visual cue to let anyone in contact with the data know what the classification is.

A) Encryption

B) Label

C) Graphics

D) Photos

Question 7

A set of security controls or system settings used to ensure uniformity of configuration throughout the IT environment.

A) Patches

B) Inventory

C) Baseline

D) Policy

Question 8

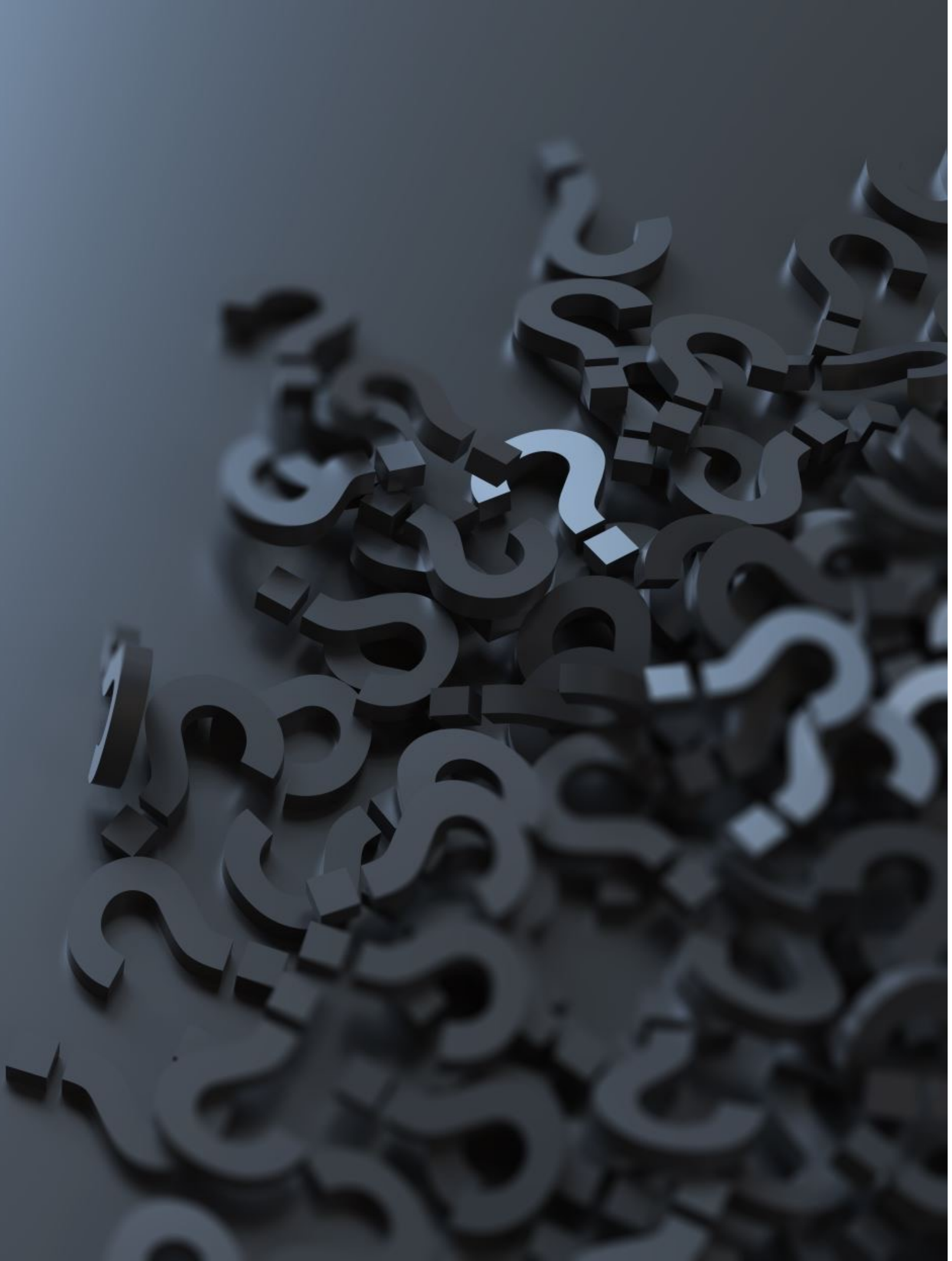
What is the most important aspect of security awareness/training?

A) Protecting assets

B) Maximizing business capabilities

C) Ensuring the confidentiality of data

D) Protecting health and human safety



Question 9

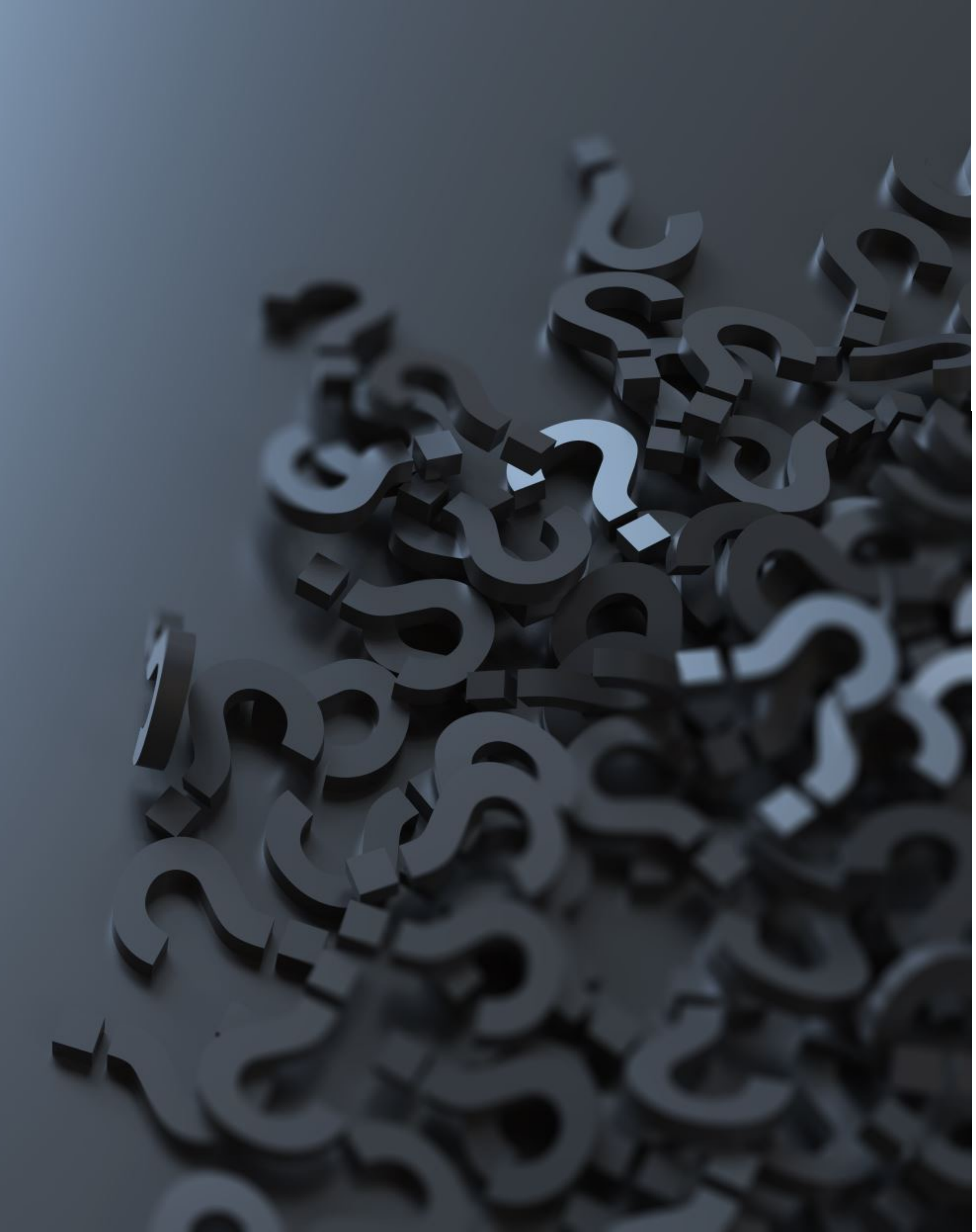
Which entity is most likely to be tasked with monitoring and enforcing security policy?

A) The Human Resources office

B) The legal department

C) Regulators

D) The security office



Question 10

Which organizational policy is most likely to indicate which types of smartphones can be used to connect to the internal IT environment?

A) The CM policy (change management)

B) The password policy

C) The AUP (acceptable use policy)

D) The BYOD policy (bring your own device)