GRC Mastery Case Study: Security Education and Awareness

Scenario

Attached is the publicly available Security Awareness Program Plan for Kentucky Wesleyan College.

Instructions

As a Cyber Security Consultant, you are tasked with assessing the effectiveness of this plan.

Your first task is to read and understand the plan attached.

The following questions can be answered with information provided in the attached plan.

Download

PLAN01-Awareness-Program-Plan.pdf

Quiz

1 / 10

What is the foundation of the Kentucky Wesleyan College Security Awareness Program?

ISO 27001 guidelines

COBIT framework

NIST SP800-16 and SP800-50 standards- Correct

PCI DSS guidelines

Who is responsible for the implementation and maintenance of the Awareness Program?

Director of Information Technology- Correct

Chief Financial Officer

Human Resources Director

Compliance Officer

How long do new hires have to complete their security awareness training?

60 days

90 days

correct30 days- Correct

45 days

What is NOT listed as a component of the Security Awareness and Training Strategy?

Mobile Devices

Social Engineering

Wireless Networks

Robotics Security- Correct

What metric is used to assess the effectiveness of phishing awareness?

Number of successful password updates

Number of users reporting phishing- Correct

Average quiz scores in training modules

Number of users attending face-to-face training

What happens if an employee fails to complete training within the extended two-week deadline?

They will be offered another extension

They will be fined

They will be transferred to another department

Their manager will be notified, and access may be restricted- Correct

How frequently are phishing social engineering tests conducted?

Monthly

Bi-weekly- Correct

Annually

Quarterly

What format is NOT mentioned as part of the training delivery methods?

Instructor-led training

On-site table events

Podcasts- Correct

Computer-based training with quizzes

Which group is required to complete role-based security training in addition to general training?

New hires only

Only faculty

Vendors and third-parties- Correct

Retired employees

How does the plan ensure ongoing effectiveness of the program?

By issuing annual reminders via email

By incorporating results from phishing tests into the program and adjusting training- Correct

By reducing the number of training sessions annually

By eliminating quizzes and tests after initial training

Recommendations:

GRC Mastery by Abed Hamdan