BAKER COLLEGE
STUDENT LEARNING OUTCOMES

ITS3050

Security Policies and Auditing

3 Semester Hours

Student Learning Outcomes and Enabling Objectives

1. Exercise skills necessary to perform regular risk assessments for their organizations as risk management should be the foundational tool used to facilitate thoughtful and purposeful defense strategies

    a. Explain the basic concepts of and need for risk management.
    b. Explain methods of mitigating risk by managing threats vulnerabilities, and exploits.
    c. Identify compliancy laws, standards, best practices, and policies of risk management.
    d. Describe the components of an effective organizational risk management program.
    e. Describe techniques for identifying and analyzing relevant threats, vulnerabilities, and exploits.
    f. Describe the process of performing risk assessments.
    g. Identify assets and activities to protect within an organization.
    h. Identify threats, vulnerabilities, and exploits.
    i. Identify risk mitigation security controls.
    j. Describe concepts for planning risk mitigation throughout an organization.
    k. Describe concepts for implementing a risk mitigation plan.
    l. Perform a business impact analysis.
    m. Construct a business continuity plan (BCP) based on the findings of a given risk assessment for an organization.
    n. Construct a disaster recovery plan (DRP) based on the findings of a given risk assessment for an organization.
    o. Construct a computer incident response team (CIRT) plan for an organization.

2. Formulate well-written security policies (which can be identified and measured or evaluated) that establishes what must be done to protect information stored on computers.

    a. Identify the role of an information systems security (ISS) policy framework in overcoming business challenges.
    b. Recognize the relationship between business drivers and information systems security policies.

c. Analyze how security policies help mitigate risks and support business processes in various domains of a typical IT infrastructure.
d. Analyze issues related to security policy implementations and the keys to success.
e. Describe the components and basic requirements for creating a security policy framework.
f. Describe how to design, organize, implement, and maintain IT security policies.
g. Describe the different methods, roles, responsibilities, and accountabilities of personnel, along with the governance and compliance of a security policy framework.
h. Describe the different ISS policies associated with the User Domain.
i. Describe the different ISS policies associated with the IT infrastructure.
j. Describe the different ISS policies associated with risk management.
k. Describe the different ISS policies associated with incident response teams (IRTs).
l. Describe issues related to implementing ISS policies.
m. Describe issues related to enforcing ISS policies.
n. Describe the different issues related to defining, tracking, monitoring, reporting, automating, and organizing compliance systems and compliance technologies.

These SLOs are not approved for experiential credit.

Effective: Fall 2017