BAKER COLLEGE
STUDENT LEARNING OUTCOMES

ITS 3050 Security Policies and Auditing
3 Semester Credit Hours

Student Learning Outcomes and Enabling Objectives

1. Discuss commonly followed processes in Risk Analysis and Risk Management.

2. Discuss the elements of an Information Security Policy set, defining them in the context of common names for each element.

3. Create each of the elements in a Security Policy set for organizations of various sizes and types.
    a. Describe the types of risks that each element should reduce.
    b. Propose a policy that should be enabled when a network feature becomes a security risk.
    c. Propose a policy that should be enabled when a risk becomes a security event.
    d. Propose a guideline about when to create standards and procedures for policies.

4. Understand commonly used frameworks for Information Security Policy sets.
    a. Explain how you would choose a proper framework for an organization of a specific type.
    b. Identify frameworks given examples of policy sets

5. Conduct a review of an organization’s Information Security Policy set.
    a. Analyze the effectiveness of that set for the organization in question.
    b. Analyze how security policies help mitigate risks and support business processes in various domains of a typical IT infrastructure.
    c. Prepare a proposal for improvements in that policy set, including triggers that would call for a repeat audit and revision of said policy set.

Big Ideas and Essential Questions

Big Ideas

- Risk Analysis
- Risk Management
- Information Policies

Essential Questions

1. Why is an information policy set referred to as a control? What does it control?
2. What are some common events that start a development cycle for policies? What are some uncommon events?

These SLOs are not approved for experiential credit.

Effective: Spring 2023