BAKER COLLEGE
STUDENT LEARNING OUTCOMES

ITS4910A Senior Project
3 Semester Credit Hours

Student Learning Outcomes and Enabling Objectives

1. Design an IT network infrastructure that meets the C.I.A Triad (Confidentiality, Integrity and Availability) security requirements for a global manufacturing company
    a. Design an IT network infrastructure and schematic for a global manufacturing company with data centers in multiple countries
    b. Identify network security tools to secure the network connectivity between the global manufacturing company's data centers
    c. Explain the choice of security tools selected and their placement and functionality for securing the connectivity of the global data center networks to meet the C.I.A. Triad security requirements
    d. Incorporate cloud technology and platforms into the infrastructure design
    e. Identify scripting and programming tools that will be needed to deploy, secure, and maintain the designed infrastructure

2. Create IT network infrastructure administrative security policies and programs to support the C.I.A. Triad (Confidentiality, Integrity and Availability) security requirements
    a. Create a Corporate Security Policy for the global manufacturing company
    b. Develop Security Education Training and Awareness (SETA) programs
    c. Create a Final Company Security Policy document integrating the company's Security Policy; Security Education Training and Awareness (SETA) programs; Security Policies/Procedures for the network security tools and equipment; Risk Assessment and Business Impact Analysis, Incident Response Plan and Disaster Recovery Plan into one document
    d. Incorporate cloud technology and platforms into the policies and programs

3. Create network security procedures for each of the IT equipment and security tools identified in the IT network infrastructure schematic
    a. Create security policies/procedures for each of the network security tools and equipment in the schematic design

    b. Create security policies/procedures for the application servers in the schematic design
    c. Create access control security policies/procedures for each of the network security tools, equipment, application servers and end-users
    d. Incorporate cloud technology and platforms into the procedures

4. Identify security risks and the potential impact of each risk to the IT network infrastructure design and security tools in the schematic
    a. Develop a Risk Assessment of IT equipment and security tools used in the design of the IT infrastructure based on the C.I.A. Triad security requirements
    b. Develop a Business Impact Assessment of the controls and/or lack of controls to mitigate security risks
    c. Incorporate cloud technology and platforms into the assessments

5. Develop an Incident Response Plan (IRP) to address responses to catastrophic events and malicious attacks that would impact the IT network infrastructure connectivity and C.I.A. Triad (Confidentiality, Integrity and Availability) security requirements for data between the global manufacturing company's data centers
    a. Develop an Incident Response Plan to response to address catastrophic events and malicious attacks that would impact the IT network infrastructure connectivity between the data centers
    b. Identify incident response notification and escalation procedures
    c. Identify Incident Response Teams (IRT) and team members
    d. Create an Incident Response Plan review and revision procedure
    e. Create Post Incident Activity procedures
    f. Create Incident Response forms
    g. Incorporate cloud technology and platforms into the plan

6. Develop a Disaster Recovery Plan to address response to catastrophic events and malicious attacks that would impact the IT network infrastructure connectivity and C.I.A Triad (Confidentiality, Integrity and Availability) security requirements for data between the global manufacturing company's data centers
    a. Create a Disaster Recovery Plan for catastrophic network outages
    b. Identify notification, escalation and activation procedures
    c. Identify disaster recovery teams
    d. Perform Threat Analysis
    e. Create Post Incident Activity procedures
    f. Create Disaster Recovery Plan forms
    g. Incorporate cloud technology and platforms into the plan

7. Analyze personal insights and reflections on the ITS4910 Information Security Research and Design Project
    a. Discuss the security design securing the IT network infrastructure
    b. Discuss the IT network infrastructure administrative security policies and programs to support the C.I.A. Triad (Confidentiality, Integrity and Availability) security requirements
    c. Discuss the IT equipment and tools used to secure the network connectivity between the global manufacturing company's data centers
    d. Discuss the development and importance of performing a security risks and the potential impact of each risk to the IT network infrastructure connectivity between datacenters
    e. Discuss the development and importance of an Incident Response Plan (IRP) to address catastrophic events and malicious attacks that would impact the IT network infrastructure connectivity between the data centers
    f. Discuss the development and importance of a Disaster Recovery Plan to address catastrophic events and malicious attacks that would impact the IT network infrastructure connectivity between the data centers
    g. Discuss the benefits of the ITS4910 course to current and future career opportunities
    h. Discuss the benefits of IT and information security professional certifications

Big Ideas and Essential Questions

Big Ideas

- Designing IT Infrastructure
- Securing IT Infrastructure
- Maintaining IT Infrastructure
- Integrating Cloud Concepts

Essential Questions

1. How are key IT concepts integrated into infrastructure design?
2. How is IT infrastructure secured?
3. How is IT infrastructure maintained?
4. What are key considerations when IT infrastructure is deployed in the cloud?

These SLOs are not approved for experiential credit.

Effective: Fall 2023