Preview: IT3358 : Information Security Concepts for the IT Professional

Syllabus

Course Overview

Learners in this course demonstrate their knowledge of information security fundamentals. Learners apply their understanding of the concepts of confidentiality, integrity, and availability to the basics of access control and network security measures.

Technology Resources

This Capella course offers real-world, hands-on labs provided by Practice-Labs.com. These labs offer guided practice in performing tasks related to achieving course competencies and completing assessments. If you require the use of assistive technology or alternative communication methods to participate in these activities, please contact DisabilityServices@Capella.edu to request accommodations.

Course Competencies

(Read Only)

To successfully complete this course, you will be expected to:

1. Define business problems that can be solved using security concepts, technologies, and standards.
2. Describe fundamental principles of IT security.
3. Describe common vulnerabilities and threats found in IT infrastructures.
4. Apply fundamental security strategies for securing IT infrastructures.
5. Explain ethical, legal and policy security issues related to information security.
6. Communicate effectively.

Syllabus >> Course Materials

Required

The materials listed below are required to complete the learning activities in this course.

Library

The following required readings are provided in the Capella University Library or linked directly in this course. To find specific readings by journal or book title, use Journal and Book Locator. Refer to the Journal and Book Locator library guide to learn how to use this tool.

- Andress, J. (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice* (2nd ed.). St. Louis, MO: Elsevier Science.

Suggested

The following materials are recommended to provide you with a better understanding of the topics in this course. These materials are not required to complete the course, but they are aligned to course activities and assessments and are highly recommended for your use.

Optional

The following optional materials are offered to provide you with a better understanding of the topics in this course. These materials are not required to complete the course.

Projects

Project >> Enterprise Security

Project Overview

Throughout this course, you will learn about best network security practices and strategies for building an effective, efficient Enterprise Security for your organization. These include methods for analyzing critical components and integrating these components with one another to ensure that they are interoperable and configured for optimum security. You will use these strategies to create a plan and strategic decision supporting documentation for an effective Enterprise Network Security course project.

The project includes the following:

- Executive summary and cover sheet.
- Scope and requirements rationale.
- Role of availability, confidentiality, authentication, and integrity in identifying a security solution.
- Global challenges to security.
- Types of cryptography.
- Strategies for supporting the AAA framework.
- Physical security strategies for protecting the networks and data.
- Intrusion detection system strategy.
- Basic strategies for hardening an operating system.
- Ethical standards and implications of sharing network resources externally.
- Screen shots of your diagram supporting the project components. See the study in Unit 1 for instructions on downloading Microsoft Visio, a helpful diagramming tool.
- A list of references.

You are to choose an organization that you have worked in, have interest in or know someone who works for an organization and is willing to share their thoughts, and then integrate the project required components. Specific detailed instructions for each project component are located in the assignment activity in the unit in which the component is due.

To achieve a successful project experience and outcome, you are expected to meet the following requirements:

- Written communication: Written communication is free of errors that detract from the overall message.
- Paper components:
    - Title page or cover sheet.
    - Executive summary.
    - Body of paper.
    - Diagram or diagrams created in a network simulation tool (where applicable).
    - Reference page.
- You are encouraged to provide resources and citations. Any references should be formatted according to APA (6th Edition) Style and Formatting.
- Length of paper: There are no page length requirements. The architecture will dictate the number of pages required to convey your design.
- Font and font size: Arial, 10 point.

Unit 1 >> Introduction to Security

Introduction

Welcome to the first week of the course. In this unit, you will cover some of the most basic concepts of information security. Information Security is a concept that becomes ever more enmeshed in many aspects of our society, largely as a result of our nearly ubiquitous adoption of computing technology. More importantly, you will get to know more about the different types security attacks, models for analyzing security issues, and how to protect organizations' assets from such attacks.

Learning Activities

u01s1 - Study

Readings

In your *The Basics of Information Security* text, complete the following readings:

- Chapter 1, "What is Information Security?"
- Chapter 2, "Identification and Authentication."

u01s2 - Software Preparation and Technology Access

In this course, you will be using software and technology that is needed to complete designated activities and assignments. There is no additional cost for this software and technology. Some software packages will be made available to you at no additional cost through Capella's subscription with Microsoft, while other software packages are available for free download through open-source licensing.

Capella University requires learners to meet certain minimum computer requirements. Please note that some software required for a course may exceed these minimum requirements. Check the requirements for the software you may need to download and install to make sure it will work on your device. Most software will require a Windows PC. If you use a Mac, refer to Installing a Virtual Windows Environment.

The software and technologies below are strongly recommended to support you in completing the course objectives. If you have access to other tools that you believe may still meet course requirements or if you have any difficulties accessing this resource or completing the related assignments, please contact your course faculty member to discuss potential alternatives.

If you use assistive technology or any alternative communication methods to access course content, please contact DisabilityServices@Capella.edu with any access-related questions or to request accommodations.

For this course, follow the instructions provided through the links below to download and install software or register for an account, as required.

Microsoft Software

1. Visit Capella’s Microsoft Software page for instructions on obtaining free Microsoft software.
2. Identify the version of MS Visio that is compatible with your operating system.
3. Download and install.

Practice Labs

This Capella course offers real-world, hands-on labs provided by Practice Labs in many of the units of this course. Click the Practice Labs Orientation link in this unit to access an introductory lab.

Note: As a Capella learner, you have access to IT online resources through Capella's Skillsoft subscription, where you can find helpful materials.

u01v1 - Practice Labs Orientation: Module Zero – Basics

This lab is designed to familiarize you with the Practice Labs platform. This is a great time to ensure that you can access the labs without any technical difficulty.

Click the linked title heading above to access the hands-on lab.

u01a1 - Project Scope

For this assignment, you will develop an initial scope document and proposal for deploying an Enterprise Security Infrastructure Project. This is done by gathering facts about the selected organization and identifying project needs.

First, select a global IT organization with which you are currently affiliated, have worked for in the past, or one you would like to learn more about. This organization should be relevant to your professional goals and sufficient information about this organization should be available through experience or research. You will use this same organization as a foundation for all of your project assignments in this course.

Once you have selected your organization, you will evaluate the existing security infrastructure and suggest improvements appropriate to improving the cost and efficiency of managing the security. If assumptions need to be made as part of your project, please list those assumptions so that your instructor is aware.

For this assignment, use the suggested resources, the Capella library, and the Internet to research the subject matter.

Instructions

Now that you have an understanding of the project and the company's needs, include the following in the initial scope document and proposal:

- Describe the scope of your project by providing an overview to the selected organization: the reasons for your choice, its size, and the location of the organization.
- Describe the main business problems and goals as they relate to information technology. Include information relative to organizational user, organizational systems, and the security requirements.
- Describe decision makers and stakeholders on whom you would rely to develop a requirements analysis and traverse through the information gathering phases of a security infrastructure deployment project.
- Define a project timeline and outline that coincides with the system and/or infrastructure component life cycle stages. Additionally, identify the security components, requirements, and concerns that will need to be addressed.
- Explain the role of Availability, Confidentiality, Authentication, and Integrity in identifying the project scope for the organization.
- Given the global nature of the organization, identify any unique challenges that you anticipate facing from a regulatory, human resources, and cultural standpoint.

- You are encouraged to provide resources and citations. Any references should be formatted according to APA (6th Edition) style and formatting.

Refer to the Project Scope Scoring Guide to ensure that you meet the grading criteria for this assignment. Submit your document in the assignment area.

Course Resources

APA Style and Format

u01d1 - Security Vulnerabilities: Policies and Controls

When developing a network security strategy, you need to make decisions on what security vulnerabilities need to be controlled in that environment. In your own words, describe how you believe vulnerabilities for global organizations differ from those that are non-local or domestic? Provide at least one (1) example supporting your stance.

Response Guidelines

Respond to at least two (2) other learners' posts. Do you agree with their points or have anything to add?

Course Resources

Undergraduate Discussion Participation Scoring Guide

Unit 2 » AAA Framework and Cryptography

Introduction

In this unit, you will learn in-depth details about the AAA Framework, various types and tools of Cryptography, and how to protect your organizations' stored data, data in transit, and users.

Learning Activities

u02s1 - Study

Readings

In your *The Basics of Information Security* text, complete the following reading:

- Chapter 3, "Authorization and Access Control."
- Chapter 4, "Auditing and Accountability."
- Chapter 5, "Cryptography."

u02v1 - Hands-On Lab: Cryptography – PKI Concepts

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u02v2 - Hands-On Lab: Access Control – RADIUS

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u02v3 - Hands-On Lab: Compliance – User Rights and Permissions

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u02v4 - Hands-On Lab: Application Data – Data Encryption

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u02v5 - Hands-On Lab: Cryptography – Transport Encryption

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u02a1 - AAA Framework and Cryptography Strategy

For this assignment, you will complete a data security strategy. This is done by gathering facts about the selected organization and identifying project needs. For this assignment, use the suggested resources, the Capella library, and the Internet to research the subject matter.

Instructions

For this assignment, complete the following components for your Perimeter Security Strategy:

- Describe vulnerabilities and threats associated with data being stored, in transit and in use.
- Compare two cryptography tools and strategies for the project that would be beneficial for protecting data being stored, in transit and in use.
- Describe at least three (3), non-cryptography strategies for protecting stored data, data in transit and/or data in use for the company.
- Describe strategies and identify at least two (2) tools for supporting the AAA framework in your company's security solution.
- Determine how you would consider applying access control and identify management to protect stored data, data in transit and/or data in use in the company.
- Define at least two (2) policies or guidelines that you would include your organization's data security manual. You are encouraged to provide resources and citations. Any references should be formatted according to APA (6th Edition) Style and Formatting.

Note: Make sure that you follow the scoring guide prior to submitting. Submit your document to the assignment area once completed.

u02d1 - AAA Framework and Cryptography

The concepts of auditing, authorization, and accountability within the area of information security have helped to ease some burdens of IT security professionals relating to the control of data flow and how data and network security policies are managed. Describe the relationship between auditing, authorization, and accountability within data and network security. Additionally, describe at least one (1) tool that you believe can assist IT professionals with the security of data and networks and explain how this tool can be functional in organizations.

Response Guidelines

Respond to at least one two (2) other learners' posts. Do you agree with their points or have anything to add?

Course Resources

Undergraduate Discussion Participation Scoring Guide

Unit 3 >> Physical and Network Security

Introduction

In this unit, you will learn a number of the main categories of physical security controls. These controls include deterrent, detective, and preventive measures; you will also learn how these controls might be implemented to mitigate physical security risks and threats. Three of the main concerns of physical security in relation to protecting an organization's assets are the protection of people, equipment, and data. This unit will address protecting the components of each of these three asset categories. In addition, as a result of the numerous potential threats from attackers, this unit covers network security and best practices, including misconfigurations of infrastructure or network-enabled device or even simple outages.

Learning Activities

u03s1 - Study

Readings

In your *The Basics of Information Security* text, complete the following readings:

- Chapter 9, "Physical Security."
- Chapter 10, "Network Security."

u03v1 - Hands-On Lab: Network Security Routers, Firewall Rule-Based Management, and Firewalls

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u03v2 - Hands-On Lab: Protocols and Services – IPSec

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u03v3 - Hands-On Lab: Threats – Mitigation and Deterrent Techniques

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u03v4 - Hands-On Lab: Understanding IDS Firewall Evasion and Honeypots

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u03a1 - Physical Network Security Strategy

For this assignment, you will complete your Physical and Network Security strategy. Each organization/company would need to show how their data, assets, and networks are protected. In this assignment, you will outline, address, and discuss your overall physical and network security strategy where you plan, design, and implement your security strategy around the organization's global network infrastructure. For this assignment, use the suggested resources, the Capella library, and the Internet to research the subject matter.

Instructions

For this week, you are to complete the following components:

- Describe at least three (3) threats and vulnerabilities associated to physical security.
- Define at least two (2) physical security strategies for protecting each of the following categories in the company: (a) data, (b) human resources and (c) hardware.
- Describe strategies for protecting the company's network perimeter from external threats.
- Describe strategies for protecting the company's internal and external network traffic and identify at least two (2) network security tools you would consider utilizing.
- Define at least two (2) policies or guidelines that you would include in the organization's physical security manual.
- You are encouraged to provide resources and citations. Any references should be formatted according to APA (6th Edition) style and formatting.

Ensure to follow the scoring guide prior to submitting and submit your document to the assignment area.

u03d1 - Physical Security Controls

The assignment and readings for this week have included various physical network security controls, practices, and policies. Discuss why you believe systems and people can be (a) countermeasures, (b) vulnerabilities, and (c) threats to your physical network assets? Provide at least one (1) example on how this can be the case for each of these categories.

Response Guidelines

Respond to two (2) other learners' posts. Do you agree with their points or have anything to add?

Course Resources

Undergraduate Discussion Participation Scoring Guide

Unit 4 >> Operating System (OS) and Application Security

Introduction

In this unit, you will learn hardening as one of the primary tools for securing the operating system and the steps needed to do so. In protecting data, processes, and applications against concerted attacks, one of the largest areas in which we might find weaknesses is on the operating system that hosts these components. It is a critical endeavor to ensure that operating systems are hardened and protecting to ensure a reasonably strong security footing is established. Additionally, the hardening of application components, such as Web-based and database systems will be explored.

Learning Activities

u04s1 - Study

Readings

In your *The Basics of Information Security* text, complete the following readings:

- Chapter 11, "Operating System Security."
- Chapter 12, "Application Security."

u04v1 - Hands-On Lab: Threats – Trojans and Malware Protection

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u04v2 - Hands-On Lab: Application Data – Establish Host Security

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u04v3 - Hands-On Lab: Threats – Network Vulnerabilities

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u04v4 - Hands-On Lab: Application Data – Application Security

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u04v5 - Hands-On Lab: Compliance – Patching

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

Course Resources

Compliance – Patching

u04v6 - Hands-On Lab: Remote Server Administration Tools

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u04a1 - OS and Application Security Strategy

For this assignment, you will explain how to secure your applications and operating systems through the use of various security tools. For this assignment, use the suggested resources, the Capella library, and the Internet to research the subject matter.

Instructions

For this assignment, complete the following components to secure your applications and operating systems:

- Describe threats and vulnerabilities associated with at least two (2) operating systems.
- Describe an anti-malware solution for the organization and indicate on which operating systems it supports.

- Select a suitable intrusion detection system (IDS) solution for the organization and explain the reasoning for your suggestion.
- Describe at least two (2) control strategies you would consider implementing for securing the company's web-based infrastructure.
- Describe at least two (2) control strategies you would consider implementing for securing the company's database infrastructure.
- Define two (2) items that you would include in the organization's operating system security hardening procedures.
- You are encouraged to provide resources and citations. Any references should be formatted according to APA (6th Edition) Style and Formatting.

Follow the scoring guide and submit to the assignment section once completed.

u04d1 - OS and Application Vulnerability

One of the primary goals when selecting a particular technology to implement and secure an IT infrastructure is to ensure that data, operating systems, and applications are secured with competent security tools. Based on your practical experience and research on this topic, identify a vulnerability to a specific application and describe at least two (2) countermeasures or tools you would consider recommending to an organization to mitigate that vulnerability. In addition, explicate why you believe it is important for organizations to protect against this vulnerability while including the potential outcomes if this vulnerability were accepted or ignored.

Response Guidelines

Respond to at least two (2) other learners' posts. Do you agree with their points or have anything to add?

Course Resources

Undergraduate Discussion Participation Scoring Guide

Unit 5 >> Security Policy

Introduction

In this unit, you will learn more about security standards; security, legal, and ethical issues; and how security ethical standards can be addressed when designing a security project.

Learning Activities

u05s1 - Study

Reading

In your *The Basics of Information Security* text, complete the following reading:

- Chapter 7, "Operations Security."

u05v1 - Hands-On Lab: Cryptography – Certificate Management

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u05v2 - Hands-On Lab: Network Security – Spam Filter

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u05v3 - Hands-On Lab: Compliance – Backup Execution and Frequency

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u05v4 - Hands-On Lab: Network Security – Cloud Computing

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u05v5 - Hands-On Lab: Compliance – RAID

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u05v6 - Hands-On Lab: Compliance – Clustering

Read the requirements for all related course activities in this unit before completing this lab. Follow the lab instructions carefully, as you may be required to take screen captures or produce lab related documents as part of graded activities. Take notes as needed as you complete the lab to help you meet all requirements.

Click the linked title heading above to access the hands-on lab.

u05a1 - Security Policy

As part of your course project, you are to develop, and design your overall security policy strategy.

Instructions

- Identify a complete list of security standards that must be addressed in a comprehensive solution for the organization.
- Discuss legal and regulatory issues that must be considered in relation to the management of information assets.
- Identify the steps that you took throughout the quarter to ensure that your security solution will succeed internationally and describe how you addressed globalization in your security design.
- For your final submission, include all your previous work for weeks 1–4 as part of this submission. Review the feedback that your instructor provided throughout the quarter and use that to finalize the security solution for your organization.
- You are encouraged to provide resources and citations. Any references should be formatted according to APA (6th Edition) style and formatting.

Note: Make sure that your paper is professionally written and free of errors, and that APA formatting is applied throughout. Once complete, submit your document in the assignment area.

u05d1 - Course Reflections

Reflecting on what you have learned in this course, explain what you believe to be the most concerning security threat to organizations today and why you believe that to be the case. Additionally, assume you were implementing a security strategy for an organization that had no previous security operations; determine the first three (3) security controls you would consider implementing and explain why you believe these are the most important to commence these efforts.