CIS 060: INFORMATION SYSTEMS SECURITY

Originator

fmarhuenda

Co-Contributor(s)

Name(s)
Flores, Martin

Justification / Rationale

Regularly scheduled update

Effective Term

Fall 2023

Credit Status

Credit - Degree Applicable

Subject

CIS - Computer Information Systems

Course Number

060

Full Course Title

Information Systems Security

Short Title

SYSTEMS SECURITY

Discipline

Disciplines List
Computer Information Systems (Computer network installation, microcomputer technology, computer applications)

Modality

Face-to-Face
100% Online
Hybrid

Catalog Description

This course ensures that students gain hands-on practical skills, ensuring they are better prepared to problem solve a wider variety of today's complex issues. The baseline cybersecurity skills are applicable across more of today's job roles to secure systems, software, and hardware. This course covers the most core technical skills in risk assessment and management, incident response, forensics, enterprise networks, hybrid/cloud operations, and security controls, ensuring high-performance on the job.

Schedule Description

An introduction to the fundamental principles and topics of Information Technology Security and Risk Management at the organizational level. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Information and System Security incorporates best practices in hands-on troubleshooting, ensuring candidates have practical security problem-solving skills required to assess the security posture of an enterprise environment and recommend and implement appropriate security solutions. Monitor and secure hybrid environments, including cloud, mobile, and IoT. Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance Identify, analyze, and respond to security events and incidents. Note: This course requires a strong background in networking fundamentals.

Lecture Units

2

Lecture Semester Hours

36

Lab Units
1
Lab Semester Hours
54

In-class Hours
90

Out-of-class Hours
72

Total Course Units
3
Total Semester Hours
162

Class Size Maximum
35

Required Text and Other Instructional Materials

Resource Type
Web/Other

Year
2021

Description
TestOut Security Pro

https://w3.testout.com/courses/security-pro

Course Content
1.0 Introduction
· Security Overview
· Defense Planning
· Using the simulator
2.0 Threats, Attacks, and Vulnerabilities
· Understanding Attacks
· Malware
· Social Engineering
· Vulnerability Concerns
3.0 Physical Threats
· Physical Threats
· Device and Network Protection
· Environmental Controls
4.0 Networks and Host Design and Diagnosis
· Manageable Network Plan
· Windows System Hardening
· File Server Security
· Linux Host Security
5.0 Devices and Infrastructure
· Security Appliances
· Demilitarized Zones

- Firewalls
- Network Address Translation (NAT)
- Virtual Private Network (VPN)
- Web Threat Protection
- Network Access Control (NAC)
- Network Threats
- Network Device Vulnerabilities
- Network Appliances
- Switch Security and Attacks
- Using Virtual Local Area Networks (VLANs)
- Router Security

6.0 Identity, Access, and Account Management

- Access Control Models
- Authentication
- Authorization
- Windows User Management
- Active Directory
- Hardening Authentication
- Linux Users
- Linux Groups
- Remote Access
- Network Authentication

7.0 Cryptography and Public Key Infrastructure (PKI)

- Cryptography
- Cryptography Implementations
- Hashing
- File Encryption
- Public Key Infrastructure (PKI)

8.0 Wireless Threat

- Wireless Overview
- Wireless Attacks
- Wireless Defense

9.0 Virtualization, Cloud Security and Securing Mobile Devices

- Host Virtualization
- Virtual Networking
- Software-Defined Networking
- Cloud Service
- Cloud Security
- Mobile Devices
- Mobile Device Management
- Bring Your Own Device (BYOD) Security
- Embedded and Specialized Systems

10.0 Securing Data and Applications

- Data Transmission Security
- Data Loss Prevention
- Web Application Attacks
- Application Development and Security

11.0 Security Assessments

- Penetration Testing
- Monitoring and Reconnaissance
- Intrusion Detection

- Security Assessment Techniques
- Protocol Analyzers
- Analyzing Network Attacks
- Password Attacks

12.0 Incident Response, Forensics, and Recovery

- Incident Response
- Mitigation of an Incident
- Log Management
- Windows Logging
- Digital Forensics
- File and Packet Manipulation
- Redundancy
- Backup and Restore

13.0 Risk Management

- Organizational Security Policies
- Risk Management
- Email

14.0 Governance and Compliance

- Audits
- Controls and Frameworks
- Sensitive Data and Privacy

Lab Content

Lab content will be covered through individual and/or group activities. These activities will be centered on the following content:

1. Identifying Attacks and Malicious Code
2. Applying E-Mail Security
3. Identifying and Mitigating Web Security Vulnerabilities
4. Domain Name System (DNS) Compromises and Mitigation
5. File Transfer Compromises and Mitigation
6. Configuring and Operating an Intrusion Detection System
7. Basic Computer Forensics

Course Objectives

	Objectives
Objective 1	Describe the fundamental principles of information systems security.
Objective 2	Define the concepts of threat, evaluation of assets, information assets, physical, operational, and information security and how they are related.
Objective 3	Evaluate the need for the careful design of a secure organizational information infrastructure.
Objective 4	Perform risk analysis and risk management.
Objective 5	Determine both technical and administrative mitigation approaches.
Objective 6	Create and maintain a comprehensive security model.
Objective 7	Define basic cryptography, its implementation considerations, and key management.
Objective 8	Design and guide the development of an organization's security policy.
Objective 9	Determine appropriate strategies to assure confidentiality, integrity, and availability of information.
Objective 10	Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/controls.
Objective 11	Explain the need for a comprehensive security model and its implications for the security manager or Chief Security Officer (CSO).

Student Learning Outcomes

	Upon satisfactory completion of this course, students will be able to:
Outcome 1	Inspect data inventory and network vulnerabilities.
Outcome 2	Determine security protocols that companies need to have in place for proper business data security.
Outcome 3	Describe the fundamental principles of information systems security.

Methods of Instruction

Method	Please provide a description or examples of how each instructional method will be used in this course.
Demonstration, Repetition/Practice	Demonstrate proper procedures to develop a professional computer network vulnerability report. Students will create several of these reports throughout the semester.
Technology-based instruction	Use of NetLab to create real-world scenarios in which students have to diagnose the cause of an outage.
Role Playing	Develop and assign tasks/activities such as web quests and online paper submissions to design an efficient network security policy.
Participation	Students will participate in class discussion regarding best practices in internet security.
Lecture	Present lectures and text descriptions to define the functions of a Certified Information Systems Security Professional.
Collaborative/Team	Create and have students take part in cooperative learning tasks such as a small group or paired role play to name and apply effective communication tools and techniques.
Activity	Develop and assign activities such as web quests, router setups, and presentations to assess the categories of skills and work habits.Develop and assign lab activities that are directed toward professional certification, that need mastery of Access Controls, Cryptography, Risk, and Security operations.
Discussion	Students will participate in classroom and online discussion forums centered around best practices for network security and administration.

Methods of Evaluation

Method	Please provide a description or examples of how each evaluation method will be used in this course.	Type of Assignment
Written homework	Written reports designed to assess the categories of skills and filtering technology needed for a secure environment. Written reports to show the ability to design an efficient information security policy.	Out of Class Only
Mid-term and final evaluations	Students will complete midterm and final exams for this course.	In and Out of Class
Tests/Quizzes/Examinations	Develop and assign class exercises such as drills and practice quizzes to define terms that relate to information security.	In and Out of Class
Product/project development evaluation	Evaluation will include hands-on projects and a combination of examinations, presentations, discussions, or problem-solving assignments.	In and Out of Class
Group activity participation/observation	Individual, small group, or paired presentations designed to find and apply effective communication tools and techniques.	In and Out of Class
Presentations/student demonstration observations	Individual or class projects designed to test security technology and software security needed for network control.	In and Out of Class
Computational/problem-solving evaluations	Individual security projects designed to find types of network security that lend themselves to application protocol verification and relate them to their areas of interest.	In and Out of Class

Self-paced testing	Develop and assign lab activities that are directed toward professional certification, that need mastery of Access Controls, Cryptography, Risk, and Security operations. Develop labs that deliver fundamental information security principles packed with real-world applications. Develop lab assignments and tasks/activities to test security needed for a virtual Private Networks.	In and Out of Class
Guided/unguided journals	Written/online journal or written online summaries designed to describe the functions and purposes of network security.	Out of Class Only

Assignments

Other In-class Assignments

1. Implement security configuration parameters on network devices and other technologies
2. Given a scenario, user secure network administration policies
3. Explain network design elements and components
4. Given a scenario, implement common protocols and services
5. Given a scenario troubleshoot security issues related to wireless networking
6. Explain the importance of risk related concepts
7. Summarize the security implications of integrating systems and data with third parties
8. Given a scenario, execute appropriate risk mitigation strategies
9. Given a scenario, implement basic forensic procedures
10. Summarize common incident response procedures
11. Explain the importance of security related awareness and training
12. Compare and contrast physical security and environmental controls
13. Summarize risk management best practices
14. Given a scenario, select the appropriate control to meet the goals of security
15. Explain types of malware
16. Summarize various types of attacks
17. Summarize social engineering attacks and the associate effectiveness with each attack
18. Explain types of wireless attacks
19. Explain types of application attacks
20. Analyze a scenario and select the appropriate type of mitigation and deterrent techniques
21. Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities
22. Explain the proper use of penetration testing versus vulnerability scanning
23. Explain the importance of application security controls and techniques
24. Summarize mobile security concepts and technologies
25. Given a scenario, select the appropriate solution to establish host security
26. Implement the appropriate controls to ensure data security
27. Compare and contrast alternative methods to mitigate security risks in static environments
28. Compare and contrast the function and purpose of authentication services
29. Given a scenario, select the appropriate authentication, authorization and access control
30. Install and configure security controls when performing account management based on best practices

Other Out-of-class Assignments

1. Textbook reading and/or other resource reading that cover the functions and purposes of information security and telecommuting or virtual environments, and describe an ergonomic and efficient network security.
2. Develop online/distance learning tasks/activities such as web quests, router setups, and online presentations to assess the categories of skills and work habits of a secure work environment. Develop online/distance learning tasks/activities such as web quests, website reviews, and discussion posting to show types of employment that lend themselves to security work and relate them to their areas of information security. Develop and assign online/distance learning tasks/activities such as web quests and online paper submissions to design an ergonomic and efficient network security.
3. Online activities such as web quests in order to identify and list 5 strategies to organize and manage home/security and office/security duties.
4. Given a scenario, utilize general cryptography concepts

5. Given a scenario, use appropriate cryptographic methods
6. Given a scenario, use appropriate PKI, certificate management and associated components

Grade Methods

Letter Grade Only

Distance Education Checklist

Include the percentage of online and on-campus instruction you anticipate.

Instructional Materials and Resources

If you use any other technologies in addition to the college LMS, what other technologies will you use and how are you ensuring student data security?

We will be using TestOut to conduct lab simulations of computer networks.

If used, explain how specific materials and resources outside the LMS will be used to enhance student learning.

TestOut contains simulations of computer networks and configurations. These simulations will give students the "hands-on" experience they need to be successful in the class and in finding a career.

Effective Student/Faculty Contact

Which of the following methods of regular, timely, and effective student/faculty contact will be used in this course?

Within Course Management System:

Discussion forums with substantive instructor participation
Online quizzes and examinations
Private messages
Regular virtual office hours
Timely feedback and return of student work as specified in the syllabus
Video or audio feedback
Weekly announcements

External to Course Management System:

Direct e-mail
Posted audio/video (including YouTube, 3cmediasolutions, etc.)
Telephone contact/voicemail

Briefly discuss how the selected strategies above will be used to maintain Regular Effective Contact in the course.

There will be weekly discussions regarding topics related to the course with appropriate instructor participation.
Students will create logs describing the process to diagnose an issue. These logs are uploaded to the LMS and receive appropriate instructor feedback.

If interacting with students outside the LMS, explain how additional interactions with students outside the LMS will enhance student learning.

As described above, TestOut provides a substitute for the hands-on with hardware that f2f courses have when dealing with servers and appliances.

Other Information

Comparable Transfer Course Information

University System

CSU

Campus

CSU San Bernardino

Course Number

IST 2610

Course Title

Cybersecurity

Catalog Year
2018

MIS Course Data

CIP Code
11.1003 - Computer and Information Systems Security/Auditing/Information Assurance.

TOP Code
070810 - Computer Networking

SAM Code
C - Clearly Occupational

Basic Skills Status
Not Basic Skills

Prior College Level
Not applicable

Cooperative Work Experience
Not a Coop Course

Course Classification Status
Credit Course

Approved Special Class
Not special class

Noncredit Category
Not Applicable, Credit Course

Funding Agency Category
Not Applicable

Program Status
Program Applicable

Transfer Status
Transferable to CSU only

General Education Status
Y = Not applicable

Support Course Status
N = Course is not a support course

C-ID
ITIS 160

Allow Audit
Yes

Repeatability
No

Materials Fee
No

Additional Fees?
No

Approvals

Curriculum Committee Approval Date
03/01/2022

Academic Senate Approval Date
03/10/2022

Board of Trustees Approval Date
06/16/2022

Chancellor's Office Approval Date
12/04/2022

Course Control Number
CCC000634488

Programs referencing this course
Computer Information Systems Associate of Science and Transfer Preparation (http://catalog.collegeofthedesert.eduundefined/?key=221)
Liberal Arts: Business and Technology AA Degree (http://catalog.collegeofthedesert.eduundefined/?key=27)
Network Specialist Certificate of Achievement (http://catalog.collegeofthedesert.eduundefined/?key=312)
Computer Information Systems Associate of Science (http://catalog.collegeofthedesert.eduundefined/?key=323)
Computer Information Systems AS Degree for Employment Preparation (http://catalog.collegeofthedesert.eduundefined/?key=61)