Cerro Coso College
Course Outline of Record Report
10/12/2021

CSCIC146 : Introduction to Information Systems Security

General Information

Author:	• Vivian Baker • Karnes, Valerie
Course Code (CB01) :	CSCIC146
Course Title (CB02) :	Introduction to Information Systems Security
Department:	Business Information Technolog
Proposal Start:	Summer 2018
TOP Code (CB03) :	(0702.00) Computer Information Systems
SAM Code (CB09) :	Clearly Occupational
Distance Education Approved:	Yes
Course Control Number (CB00) :	CCC000501567
Curriculum Committee Approval Date:	12/01/2017
Board of Trustees Approval Date:	11/03/2015
External Review Approval Date:	09/27/2010
Course Description:	This course provides an introduction to the fundamental principles and topics of Information Technology Security and Risk Management at the organizational level. It addresses hardware, software, processes, communications, applications, and policies and procedures with respect to organizational Cyber Security and Risk Management.
Submission Type:	Change to Content
	Lab hours added back into course. Added Cyber Security AS and COA to listing
Author:	No value

Faculty Minimum Qualifications

Master Discipline Preferred:	• Computer Science
Alternate Master Discipline Preferred:	No value
Bachelors or Associates Discipline Preferred:	• Computer Information Systems (Computer network installation, microcomputer technology, computer applications)
Additional Bachelors or Associates Discipline Preferred:	No value

Course Development Options

Basic Skills Status (CB08)

Course is not a basic skills course.

Course Special Class Status (CB13)

Course is not a special class.

Grade Options

• Letter Grade Methods
• Pass/No Pass

Allow Students to Gain Credit by Exam/Challenge

Allowed Number of Retakes

0

Course Prior To College Level (CB21)

Not applicable.

Rationale For Credit By Exam/Challenge

No value

Retake Policy Description

Type:|Non-Repeatable Credit

Allow Students To Audit Course

Course Support Course Status (CB26)

No value

Associated Programs

☑ Course is part of a program (CB24)

Associated Program	Award Type	Active
Cyber Security Technology	A.S. Degree Major	Spring 2018
Cyber Security Technician	Certificate of Achievement	Spring 2018
Information Technology Plus	Certificate of Achievement	Spring 2018 to Summer 2019
CC Computer Information Systems-	Certificate of Achievement	Spring 2018 to Summer 2019
CC Computer Information Systems	A.S. Degree Major	Spring 2018 to Summer 2019
CC Information Technology	Certificate of Achievement	Summer 2019
CC Information Technology	A.S. Degree Major	Summer 2019

Transferability & Gen. Ed. Options

Course General Education Status (CB25)

No value

Transferability

Not transferable

Transferability Status

Not transferable

Units and Hours

Summary

Minimum Credit Units (CB07)	3
Maximum Credit Units (CB06)	3
Total Course In-Class (Contact) Hours	90
Total Course Out-of-Class Hours	72
Total Student Learning Hours	162
Faculty Load	0

Credit / Non-Credit Options

Course Credit Status (CB04)

Credit - Degree Applicable

Course Non Credit Category (CB22)

Credit Course.

Non-Credit Characteristic

No Value

Course Classification Status (CB11)

Credit Course.

☐ Variable Credit Course

Funding Agency Category (CB23)

Not Applicable.

☐ Cooperative Work Experience Education Status (CB10)

Weekly Student Hours

	In Class	Out of Classs
Lecture Hours	2	4
Laboratory Hours	3	0
Activity Hours	0	0

Course Student Hours

Course Duration (Weeks)	18
Hours per unit divisor	54
Course In-Class (Contact) Hours	
Lecture	36
Laboratory	54
Activity	0
Total	90
Course Out-of-Class Hours	
Lecture	72
Laboratory	0
Activity	0
Total	72

Time Commitment Notes for Students

No value

Faculty Load

Extra Duties: 0		**Faculty Load:** 0	

Units and Hours - Weekly Specialty Hours

Activity Name	Type	In Class	Out of Class
No Value	No Value	No Value	No Value

Pre-requisites, Co-requisites, Anti-requisites and Advisories

Advisory

CSCIC101 - Introduction to Computer Information Systems

Students need to be able to identify hardware components of a computer system, understand the basics of operating systems and application software, install software, understand what memory is, how to zip and unzip files, how to save and find files and understand the basics of network topology. This material is covered in the CSCI C101 course.

AND

Advisory

CSCIC142 - Information & Communication Technology Essentials

Students need to know the essential skills for individual computer repair to assist them as they complete the skills for an Information Technology Technician. These skills include computer hardware identification and basics of building a computer to include installation of components (power supplies, motherboards, processor, memory, and expansion card). In addition, students need to have experience and knowledge of installing and configuring operating systems, application software and updates. This material is covered in the CSCI C142 course.

Entrance Skills

Entrance Skills	Description
No value	No value

Limitations on Enrollment

Limitations on Enrollment	Description
2 years equivalent experience in the Information Technology field	Advisory ONLY CSCI C101 and CSCI C142 OR 2 years equivalent experience in the Information Technology field

Specifications

Methods of Instruction

Methods of Instruction	Demonstration
Rationale	Textbook and Electronic Readings

Methods of Instruction	Discussion
Rationale	Pre-recorded Training Videos

Methods of Instruction	Lecture
Rationale	No value

Methods of Instruction	Skills Development and Performance
Rationale	No value

Methods of Instruction	Other
Rationale	A. Textbook and Electronic Readings B. Pre-recorded Training Videos C. Real-time Lectures D. Discussions E. Simulation Scenarios

Assignments

A. Chapter reading (Example: Reading the assigned chapters from the textbook based on the topics for the week).
B. Weekly step-by-step security tool assignments (Example – Follow instructions to evaluate computer system vulnerabilities using a vulnerability scanner and document findings).
C. Weekly application simulations assignments (Example: Use Microsoft utilities in a virtual computing environment to identify security threats. Demonstrate ability to detect security threats and appropriate actions to protect computer systems.).

Methods of Evaluation	Rationale
Final Exam	Comprehensive Exam: A comprehensive exam in a proctored environment will evaluate a student's preparedness for the Security+ exam.
Tests	Objective exams will evaluate the student's comprehension of text material and prepare them for the Security+ certification exam environment.
Participation	Discussions: Students will participate in discussions to critically explore concepts and compare elements of the text. For example: Discuss the repercussions of offering unsecured public wi-fi.
Homework	Hands on simulations: Activities will reinforce the practical application of theories presented in the text. Simulations will also provide insight and training into real world tasks for Security Professionals. For example, install the GFI Languard vulnerability scanner and conduct a vulnerability assessment on the local PC. The simulation requires students to complete a series of tasks and submit their results which are scored on a rubric.

Equipment

No Value

Textbooks

Author	Title	Publisher	Date	ISBN
Conklin, Wm. Arthur, White, Greg, Williams, Dwayne, Cothren, Arthur, Chuck and Davis, Roger L.,	CompTIA Security+ Exam SYO-401, 4th	McGraw Hill	2015	

Other Instructional Materials

Description	Cengage. LabSim Security Pro, English 5.1 ed., Security+ lab simulation software
Author	No value
Citation	No value

Materials Fee

No

Learning Outcomes and Objectives

Course Objectives

No value

CSLOs

Apply digital security concepts and best practices to design a secure organizational information infrastructure.	Expected SLO Performance: 70.0

Differentiate among the fundamental principles of information technology security including the concepts of threats, evaluation of assets, and information assets.	Expected SLO Performance: 70.0

Business Information Technolog Computer Information Systems A.A. Degree for Transfer	5. Demonstrate competency in working with servers, storage, and virtualization including implementing and evaluating network security solutions.

Use proper computer and network security counter-measures, protect basic and advanced communications, and use cryptography and Public Key Infrastructure (PKI) to thwart attackers.	Expected SLO Performance: 70.0

Business Information Technolog Computer Information Systems A.A. Degree for Transfer	5. Demonstrate competency in working with servers, storage, and virtualization including implementing and evaluating network security solutions.

Evaluate challenging technical concepts to determine effective and appropriate strategies and security technologies required to maintain security in a corporate environment.

Expected SLO Performance: 70.0

ISLOs Core ISLOs	Students who are completing a program will be able to think critically and creatively and apply reasoning.

Apply security best practices including risk analysis, as they would be applied in a corporate setting.

Expected SLO Performance: 70.0

Business Information Technolog Computer Information Systems A.A. Degree for Transfer	5. Demonstrate competency in working with servers, storage, and virtualization including implementing and evaluating network security solutions.

Outline

Course Outline

I. Introduction
    A. Security Overview
    B. Using the Simulator
II. Access Control and Identity Management
    A. Access Control Models
    B. Authentication
    C. Authorization
    D. Access Control Best Practices
    E. Active Directory Overview
    F. Windows Domain Users and Groups
    G. Linux Users
    H. Linux Groups
    I. Linux User Security
    J. Group Policy Overview
    K. Hardening Authentication
    L. Hardening Authentication 2
    M. Remote Access
    N. Network Authentication
    O. Identity Management
III. Cryptography
    A. Cryptography
    B. Hashing
    C. Symmetric Encryption
    D. Asymmetric Encryption
    E. Public Key Infrastructure (PKI)
    F. Cryptography Implementations
IV. Policies, Procedures, and Awareness
    A. Security Policies
    B. Manageable Network Plan
    C. Business Continuity
    D. Risk Management
    E. Incident Response
    F. Social Engineering
    G. Certification and Accreditation
    H. Development
    I. Employee Management
    J. Third-Party Integration
V. Physical Security
    A. Physical Security
    B. Hardware Security
    C. Environmental Controls
    D. Mobile Devices
    E. Mobile Device Security Enforcement
    F. Telephony
VI. Perimeter Defenses

Lab Outline

Delivery Methods and Distance Education

Delivery Method: Please list all that apply -Face to face -Online (purely online no face-to-face contact) -Online with some required face-to-face meetings ("Hybrid") -Online course with on ground testing -iTV – Interactive video = Face to face course with significant required activities in a distance modality -Other

Online with some required face-to-face meetings ("Hybrid");
Online (purely online no face-to-face contact);
iTV – Interactive video = Face to face course with significant required activities in a distance modality;
Face to face;

Rigor Statement: Assignments and evaluations should be of the same rigor as those used in the on-ground course. If they are not the same as those noted in the COR on the Methods of Evaluation and out-of-class assignments pages, indicate what the differences are and why they are being used. For instance, if labs, field trips, or site visits are required in the face to face section of this course, how will these requirements be met with the same rigor in the Distance Education section?

All assignments in distance education courses (online, hybrid and iTV) of CSCI C146 are of the same rigor as those in the on-ground course, except that students in purely online sections will submit all of their assignments virtually. Use of industry standard software and a simulation manual which instructs students to complete a series of tasks and provide detailed documentation of their results. The instructor reviews the student's results and provides feedback to the students on skill development and selection of the correct methods. The instructor can provide detailed feedback to students to guide their learning. Instructor evaluation of student work in distance education courses is the same as in the on-ground course, except that evaluation of student work in online is presented virtually. Instead of onsite lectures, hybrid and online courses use a variety of methods including, but not limited to videos, interactive simulations and written lecture notes.

Effective Student-Instructor Contact: Good practice requires both asynchronous and synchronous contact for effective contact. List the methods expected of all instructors teaching the course. -Learning Management System -Discussion Forums -Moodle Message -Other Contact -Chat/Instant Messaging -E-mail -Face-to-face meeting(s) -Newsgroup/Discussion Board -Proctored Exam -Telephone -iTV - Interactive Video -Other (specify)

discussion forums
LMS message
chat
email

Software and Equipment: What additional software or hardware, if any, is required for this course purely because of its delivery mode? How is technical support to be provided?

Ciampa M. (2014). Security+ Guide to Network Security Fundamentals. 5th ed.

Accessibility: Section 508 of the Rehabilitation Act requires access to the Federal government's electronic and information technology. The law covers all types of electronic and information technology in the Federal sector and is not limited to assistive technologies used by people with disabilities. It applies to all Federal agencies when they develop, procure, maintain, or use such technology. Federal agencies must ensure that this technology is accessible to employees and the public to the extent it does not pose an "undue burden". I am using -iTV—Interactive Video only -Learning management system -Publisher course with learning management system interface.

itv

LMS
publisher

Class Size: Good practice is that section size should be no greater in distance ed modes than in regular face-to-face versions of the course. Will the recommended section size be lower than in on-ground sections? If so, explain why.

No Value