CERTIFICATE IN BUSINESS CYBERSECURITY

The undergraduate Certificate in Business Cybersecurity will provide students the knowledge and skills needed to address the challenges associated with information management and security. Cybersecurity and information assurance is a serious concern for any business. Upon completion of this certificate, students will have increased awareness and the ability to assess and secure information technology assets against cybersecurity threats. Students will demonstrate an understanding of cybersecurity terminology, concepts and issues, including the nature of threats, common vulnerabilities, consequences of security failures, and strengths and weaknesses of various cybersecurity models.

Learning Objectives

Upon successful completion students will be able to:

1. Demonstrate the ability to set up and troubleshoot hardware and software for a computer network in Linux and Windows.
2. Compare and contrast various approaches to manage a computer network and learn how to select the best type of network environment to implement in a given situation.
3. Identify system vulnerabilities and common security problems, configure VMWare, perform risk and cost-benefit analysis, configure web protocols, secure servers, configure a firewall, install intrusion detection systems, and understand forensic procedures.
4. Describe the role of cybersecurity in the success of organizations and individuals; demonstrate a fundamental understanding of cybersecurity terminology, concepts, issues, and components.
5. Assess the current security landscape, including the nature of the threat, the general status of common vulnerabilities, and the likely consequences of security failures.
6. Critique and assess the strengths and weaknesses of general cybersecurity models, including the Confidentiality, Integrity and Availability triad.
7. Determine an organization's attitude toward and appetite for risk, by evaluating factors such as the "tone at the top," the organizational culture, the regulatory environment, and the organization's goals & objectives and evaluate their potential impact on the organizations.
8. Evaluate weaknesses in an organization's IT controls, and make recommendations to improve regulatory compliance, reporting, and operational performance.
9. Explain the role of IT audit and the overlap between accounting and IT, particularly with respect to audits of financial statements and of service organizations (e.g., cloud service providers).
10. Evaluate the risk-reward trade-offs of disruptive technologies such as cloud computing, the Internet of Things (IoT), social media, and mobile devices.

Requirements
Effective Fall 2022

Additional coursework may be required due to prerequisites.

Code	Title	Credits
Required:		
CIS 350	Operating Systems and Networks	3
Select two courses from the following:		**6**
CIS 413	Advanced Networking and Security	
CIS 487	Internship [1]	
CIS 563	Information Assurance and Security	
Program Total Credits		**9**

[1] Must be related to cybersecurity.