Common Course Outline
CSIT 161
Introduction to Information Assurance
3 Semester Hours

The Community College of Baltimore County

Description

CSIT 161- 3 Credits - Introduction to Information Assurance discusses the principles of information assurance through the lens of information assurance management. Information assurance is not just a technology concern but a management issue. Future organizations will expect the next generation of employees to be able to have the right combination of skills and experience to anticipate and troubleshoot multifaceted information assurance matters. This course will provide the students with the ability to identify threats and vulnerabilities in present systems as well as expand techniques to design and develop secure information systems as needed.

3 credits:
Co-requisite: CSIT 101

Overall Course Objectives

Upon successfully completing this course students will be able to:

1. define information assurance and related concept terms;
2. explain the critical characteristics of information components – software, hardware, data, people, procedures and networks;
3. identify information assurance system development life cycle;
4. explain the reasons for information assurance;
5. identify information business assurance needs;
6. identify security threats by defining and distinguishing between compromises to hardware and software components;
7. differentiate and define computer attacks;
8. explain the legal, ethical and professional issues in information assurance;
9. demonstrate knowledge of risk management, risk identification, risk assessment, and risk control strategies;
10. create risk management strategies using quantitative or qualitative risk controls;
11. develop an information assurance plan;
12. recognize the importance of firewalls, VPNs and remote connections protection;
13. define and differentiate between cryptography terminology of cipher methods and cryptographic algorithms;
14. identify security and personnel practices in enterprise organizations;
15. explain information assurance maintenance models; and
16. discuss the importance of security examinations to corporate and personal computer usage.

Major Topics

I. Introduction to Information Assurance
II. The Need for Information Assurance
III. Legal, Ethical, and Professional Issues in Information Assurance
IV. Risk Management
V. Planning for Information Assurance
VI. Security Technology: Firewalls, VPNs, and Wireless
VII. Security Technology: Intrusion Detection, Prevention Systems and Tools
VIII. Cryptography
IX. Physical Security
X. Implementing Information Assurance
XI. Security and Personnel

Course Requirements

Grading/Exams: Grading will be determined by the individual faculty member, and will include but not limited to the following assessments of the student's ability to demonstrate an understanding of the above stated Overall Course Objectives:

- Skills Assessment: At least two assessment measures such as lab projects, cases, and skills evaluations where the student can display the knowledge obtained from course materials.
- Concept Assessment: At least two tests and/or quizzes. Individual faculty will notify students of the testing procedures to be used.
- Oral/Written Report on a current Information Assurance issue affecting society.
- Comprehensive Final Exam: The course will include a comprehensive final exam.

Other Course Information:

This course is required for the Information Technology program at CCBC. Student may take CSIT 161 concurrently with CSIT 101.

Updated 8/2014