COURSE INFORMATION

COURSE TITLE
CNG131: Principles of Information Assurance

COURSE DESCRIPTION
Provides skills and knowledge required to survey key issues associated with protecting information assets, determine the levels of protection and response to security incidents, and design a consistent, reasonable information security system, with appropriate intrusion detection and reporting features. Students learn to inspect and protect information assets, detect and react to threats to information assets, and examine pre- and post-incident procedures, and technical and managerial responses. Students learn about information security planning and staffing functions.

CREDIT HOURS
3

CCCOnline Course Policies
The CCCOnline Course Policies page contains information about the student's role in the classroom, grading policies, and rights and responsibilities.
COURSE MATERIALS

Your textbook is available online as an eText. You do not need to purchase any additional materials. For specific information on refund policies and the optional black and white textbook available for purchase please contact the CCCOnline bookstore.

MINIMUM COMPUTER REQUIREMENTS

To complete this course, you will need regular access to a computer from which you can get to the internet and use email. In order to ensure that your course functions properly, you must run the System Check. This is a CRITICAL STEP, and taking the time to do it now will eliminate a tremendous amount of frustration for you later. To run the System Check, click Tools in the course NavBar and then click System Check.

REQUIRED eText

MAIN eText

The assigned readings introduce concepts and terminology necessary for effective participation in class discussions and completion of assignments, including the Practice Certification Exam at the end of the course.


DIGITAL MATERIALS ACCESS AND SETUP

This course uses uCertify digital content which contains the ebook and as well as interactive multimedia study tools, homework and labs (also named eText - you do not need to purchase it separately).

Visit the uCertify Course Start page for details on first access of the materials.

To make sure your computer is set up correctly to access the eText and other digital content, review the uCertify Technical Support page, also linked in the Technical Support Module.
**Course Competencies and Outcomes**

**Student Competencies**

The competencies you will demonstrate in this course are as follows:

A. Define key terms and explain critical concepts.
B. Explain the managerial and technical aspects of information security for information systems.
C. Examine the legal, ethical, and professional issues in information security.
D. Identify, assess, and reduce risk to an acceptable level and implement effective control measures to maintain that level of risk.
E. Describe authentication and access control methods.
F. Describe accepted security models and frameworks and examine the planning processes that support business continuity, disaster recovery, and incident response.
G. Use intrusion detection, prevention systems, and other security tools.
H. List architectures and implementations of cryptosystems.
I. Examine the elements that are critical to implementing a security plan.
J. Develop security policies for personnel.
K. Maintain information security policies and procedures.

The module outcomes that will permit you to demonstrate course competencies are:

**Module 1**

<table>
<thead>
<tr>
<th>Outcomes</th>
<th>Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Define terms related to security and risk management.</td>
<td>A, I</td>
</tr>
<tr>
<td>2 Apply security governance principles to real-world situations.</td>
<td>A, B, C, I</td>
</tr>
<tr>
<td>3 Identify issues with ethical, legal and regulatory risk.</td>
<td>A, C, I</td>
</tr>
<tr>
<td>4 Identify security policies and procedures.</td>
<td>A, C, D, I</td>
</tr>
<tr>
<td>5 Discuss geographical threats.</td>
<td>A, D, F, I</td>
</tr>
<tr>
<td>6 Identify security risks in the supply chain.</td>
<td>A, B, F, I</td>
</tr>
</tbody>
</table>

**Module 2**

<table>
<thead>
<tr>
<th>Outcomes</th>
<th>Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Define terms related to asset security, architecture and engineering.</td>
<td>A</td>
</tr>
</tbody>
</table>
**Module 3**

**Outcomes**
1. Define terms related to network security and access processes.
2. Examine prevention and mitigation of access control threats.
3. Describe security protocols and services.
4. Discuss Identity as a Service (IDaaS) implementation.
5. Describe access control threats and solutions.

**Competencies**
- A
- A, B, D, E, I
- A, B, D, E, I
- A, B, D, E
- A, B, D, E, I

**Module 4**

**Outcomes**
1. Define terms related to security assessment, testing, and operations.
2. Apply logging and monitoring activities.
3. Examine the impact of assessment and testing on overall security of systems and servers.
4. Describe analysis and report test outputs.
5. Identify and assess security audits.
6. Discuss types of computer investigations and related software.
7. Define processes and plans for change management, disaster recovery, business continuity and personnel.

**Competencies**
- A
- A, B, E, G, I, K
- A, B, C, F, I, J, K
- A, B, G, I, K
- A, B, G
- (A, B, C)
- A, B, C
- A, B, C, D, F, J

**Module 5**

**Outcomes**
1. Define terms related to software development and security.
2. Identify software development life cycles.
3. Assess software security effectiveness.
4. Discuss risk assessment practices in the workplace.

**Competencies**
- A
- A, E, F
- A, B, D, E, F
- A, B, C, D, E, G
GRADING AND EVALUATION

METHODS
Evaluation includes a combination of discussion participation, assignments, and other evaluations. Rubrics are provided for assignments and discussions.

GRADING POLICIES
Mark all module due dates on your calendar for this class. You may submit assignments AHEAD of schedule. Late assignments will not be accepted without prior approval.

SUMMARY OF GRADING

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Points</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discussions (10 @ 20 points each)</td>
<td>200</td>
<td>20%</td>
</tr>
<tr>
<td>Labs (8 @ 25 points each)</td>
<td>200</td>
<td>20%</td>
</tr>
<tr>
<td>Flash Cards (8 @ 15 points each)</td>
<td>120</td>
<td>12%</td>
</tr>
<tr>
<td>Quizzes (8 @ 25 points each)</td>
<td>200</td>
<td>20%</td>
</tr>
<tr>
<td>Final Paper</td>
<td>100</td>
<td>10%</td>
</tr>
<tr>
<td>Capstone: uCertify Practice Certification Exam</td>
<td>180</td>
<td>18%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>1000</td>
<td>100%</td>
</tr>
</tbody>
</table>

Grading Scale
A = 90 to 100%  B = 80 to 89%  C = 70 to 79%  D = 60 to 69%  F = 59% and below

DISCUSSIONS
The discussion will consist of three or more posts. The first post will be based off the assignment topic and will consist of 1-2 paragraphs. You will then need to post the following two types of replies:

1. **Reply 1:** Additional Research and Innovation - The purpose of your first reply is to verify and expand the topic. As with all ideas, they can always be improved or added on to. You need to find two ways to improve the discussion topic. You will need to add two additional resources to the topic if possible.

2. **Reply 2:** Analysis - The purpose of the 2nd reply is to critically analyze the topic being discussed. This is to be done professionally. If you can, find one potential flaw, security concern, or issue that might be a risk to a company, school, home, or any other entity that uses the internet. Please include at
least one source of reference that backs your reply and cite this reference in APA format (use a Citation Machine on the web if necessary for format). Do not put “Great post” only and feel this will be suffice as a reply.

LABS
Labs are completed through uCertify in a Windows-10 simulation or virtual machine that steps you through the processes. These will familiarize you with terms presented in the readings through real-world scenarios. You may complete the labs as many times as you like.

FLASH CARDS
Flash Cards are completed through uCertify and are a great way to study before a quiz. You can access these at any time throughout the course.

QUIZZES
Quizzes are completed through uCertify and relate directly to the readings. You may take the quizzes as many times as you like and the highest score will be recorded.

FINAL PAPER
The Final Paper is a multi-page essay consisting of a minimum one and a half pages of body text. Additional pages containing the conclusion, abstract, title-page, and references should be included but do not count towards the one and a half pages required. In this paper, you will analyze the vulnerabilities of the Internet of Things. You will be provided with questions to to build an informative paper, but you are also expected to extend the topic with your own questions and thoughts on the subject.

CAPSTONE: PRACTICE CERTIFICATION EXAM
The Capstone of this course is the Practice Certification Exam. You have two attempts on this exam and the highest score will be recorded. It is highly recommended to go back through all the Flash Cards before taking this exam. For more practice, you may also take the Practice Test B, which is a different version of the practice certification exam. Scores will not be recorded for Practice Test B.
COURSE SCHEDULE

The Schedule is subject to change as needed.

This page summarizes all of the graded assignments, discussions, quizzes, and reading assignments for the course. If you want, you can print it out and post it somewhere handy.

All assignments are described in detail on the Module Assignment pages. If you have questions check there and/or send me an e-mail.

This course is not self-paced and is not open-exit. All assignments, quizzes, discussions, etc., are to be completed by no later than 11:59 pm MST/MDT of the due date.

NOTE: Important CCCOnline semester dates (e.g., drop/withdraw/term end) appear on the CCCOnline calendar.

MODULE 1

Reading/Assignments/Exams                          Due Dates
Read Chapter 1 of the eText – Security and Risk Management
Read Module 1 Exploration: Security with Inventions
Participate in M1 Discussion 1: Student Introductions
Participate in M1 Discussion 2: Geographical Threat
Complete Chapter 1 Labs
Complete Chapter 1 Flash Cards
Complete Chapter 1 Quiz

MODULE 2

Reading/Assignments/Exams                          Due Dates
Read Chapter 2 of the eText – Asset Security
Read Module 2 Exploration: Public & Private Key
Participate in M2 Discussion 1: Info & Assurance Handling Requirements
Complete Chapter 2 Labs
Complete Chapter 2 Flash Cards
Complete Chapter 2 Quiz
Read Chapter 3 of the eText – Security Architecture and Engineering
Participate in M2 Discussion 2: Using Public Key Infrastructure Encryption
Complete Chapter 3 Labs
Complete Chapter 3 Flash Cards
Complete Chapter 3 Quiz
**Module 3**

**Reading/Assignments/Exams**
- Read Chapter 4 of the eText – Communications and Network Security
- Read Module 3 Exploration: Social Engineering
- Participate in M3 Discussion 1: Quantum Cryptography
- Complete Chapter 4 Labs
- Complete Chapter 4 Flash Cards
- Complete Chapter 4 Quiz
- Read Chapter 5 of the eText – Identity and Access Processes
- Participate in M3 Discussion 2: Identity as a Service (IDaaS)
- Complete Chapter 5 Labs
- Complete Chapter 5 Flash Cards
- Complete Chapter 5 Quiz

**Module 4**

**Reading/Assignments/Exams**
- Read Chapter 6 of the eText – Security Assessment and Testing
- Read Module 4 Exploration: Change Management Process
- Participate in M4 Discussion 1: Security Validation Testing
- Complete Chapter 6 Labs
- Complete Chapter 6 Flash Cards
- Complete Chapter 6 Quiz
- Read Chapter 7 of the eText – Security Operations
- Participate in M4 Discussion 2: Computer Investigations
- Complete Chapter 7 Labs
- Complete Chapter 7 Flash Cards
- Complete Chapter 7 Quiz

**Module 5**

**Reading/Assignments/Exams**
- Read Chapter 8 of the eText – Software Development Security
- Read Module 5 Exploration: Auditing Network Infrastructure
- Participate in M5 Discussion 1: Security Controls and Development
- Complete Chapter 8 Labs
- Complete Chapter 8 Flash Cards
- Complete Chapter 8 Quiz
- Submit Final Paper: IoT Vulnerability
- Complete Capstone – Practice Certification Exam - Security
- Participate in M5 Discussion 2: Class Feedback

_Last modified 8/8/2019 tlt_