

**Class Overview**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **General Class Information**  *All fields must be completed and posted in UVaCollab and World Viewable in SIS no later than two weeks prior to registration.* | | | | | | | | |
| **Subject Area &**  **Catalog Number** | BUS 5010 | **Class Title** | Information Security Management (Graduate) | | | | |
| **Credit Type** | **Undergraduate**  **Graduate** | | **Credit**  **Noncredit** | | **Delivery Method** | **P (In-Person)**  **CI (Classroom/Internet)**  **WB (Web-Based)** | |
| **Re-licensure**  **Re-certification Points** |  | | | **Approval Date**  *(For internal use only)* | | |  | |

1. **Class Description (Use the SIS 400 characters from catalog description)**

This foundation course provides managers with the essential framework needed to design and develop an effective information security program. Students explore methods used to raise general security awareness, review current industry practices, and develop expertise needed to adapt policies to safeguard proprietary information. Instruction focuses on key security principles that are critical to protecting information assets and network infrastructure in open access computing environments. The principles of authentication, data integrity, privacy (encryption), access control, trust and non-repudiation are explored in detail.

1. **Learning Outcomes**

ON SUCCESSFUL COMPLETION, THE STUDENT WILL BE ABLE TO:

• UNDERSTAND, OPEN ACCESS AND LIMITED (TRADITIONAL) ACCESS, PERIMETER DEFENSES AND SECURITY, POINT SOLUTIONS AND LIFE CYCLE (HOLISTIC) SECURITY, RISK ANALYSIS AND THREAT ANALYSIS.

• IDENTIFY HACKER STRATEGIES AND ATTACK TOOLS, ATTACK CLASSES, I.E., DISTRIBUTED DENIAL OF SERVICE TOOLS, BACKDOOR PROGRAMS, VIRUS TYPES, SNIFFER PROGRAMS AND TROJAN HORSES.

• GAIN COMPETENCY IN DEVELOPING STRATEGIES AND COUNTERMEASURES FOR THWARTING HACKER EXPLOITS AND TACTICS.

• ESTABLISH AND IMPLEMENT AN INCIDENT RESPONSE TEAM TO ADDRESS INCURSIONS ON ENTERPRISE NETWORKING OPERATIONS.

• HOW TO PLAN, RESPOND TO AND SURVIVE A HACKER ATTACK.

• CONSTRUCT AND ADMINISTER A PLAN FOR HARDENING THE NETWORK’S INFRASTRUCTURE AGAINST HACKER INCURSIONS AND SECURITY BREACHES. FOCUS IS ON ROUTERS, OPERATING SYSTEMS AND FIREWALLS.

• HOW TO PLAN AND COORDINATE THE IMPLEMENTATION OF HOLISTIC SECURITY MEASURES IN MULTIPLE LAYERS WITHIN THE IT NETWORKING ENVIRONMENT.

• DEMONSTRATE PROFICIENCY IN DEVELOPING OPERATING MODELS FOR SECURITY RISK ASSESSMENT AND VULNERABILITY ASSESSMENT.

• DEMONSTRATE PROFICIENCY IN UNDERSTANDING HOW TO APPLY THE VARIOUS OPTIONS AVAILABLE FOR IT SECURITY ARCHITECTURE TO A GIVEN SET OF REQUIREMENTS. FOCUS IS ON FIREWALLS, INTRUSION DETECTION SYSTEMS, AUTHENTICATION AND SINGLE SIGN ON SYSTEMS AND VULNERABILITY EVALUATION TOOLS.

• HOW TO TRACK VULNERABILITIES AND SECURITY INCIDENTS THROUGH PUBLIC WEB SITES AND PLAN FOR APPLYING VENDOR RELATED PATCHES AND UPDATES IN AN ONGOING BASIS.

• DEMONSTRATE PROFICIENCY IN DESIGN AND DEVELOPMENT OF SECURITY RISK ANALYSIS MODELS.

1. **Assessment Components**

STUDENT GRADES WILL BE DETERMINED BY PARTICIPATION ONLINE, COURSE ASSIGNMENTS, EXAMINATIONS, CASE STUDY WORK, POP QUIZZES AND OTHER PROJECTS.

THE MID-TERM CASE STUDY WILL ALLOW STUDENTS THE ABILITY TO DETERMINE THEIR PROGRESS TO DATE AND THE ABILITY TO CONDUCT A PLAN FOR HARDENING AND RESTORING THE NETWORK’S INFRASTRUCTURE AGAINST HACKER INCURSIONS AND SECURITY BREACHES AND MASTERY OF THE CONCEPTS SURROUNDING CRITICAL INFRASTRUCTURE PROTECTION FOR THE 21ST CENTURY.

THE FINAL EXAMINATION WILL BE IN FORM OF AN AGILE FINAL PAPER (E.G. DECISION BRIEF). THIS DETAILED ANALYSIS AROUND UNDERSTANDING THE THREAT ENVIRONMENT ACROSS INDUSTRY, GOVERNMENT, AND ACADEMIA AND THE OVERALL MASTERY OF THE CONCEPTS AND PRINCIPLES OF THIS COURSE IN INFORMATION SECURITY MANAGEMENT AND THE PROFICIENCY IN APPLYING THE CONCEPTS TO ADDRESS REAL WORLD REQUIREMENTS AND SITUATIONS. THIS FINAL ASSESSMENT WILL ALLOW STUDENTS TO DEMONSTRATE MASTERY AROUND IDENTIFYING HACKER STRATEGIES AND ATTACK TOOLS; AND DEVELOP A STRATEGY THAT INCLUDES EMPLOYEE TRAINING AND TECHNICAL COUNTERMEASURES FOR THWARTING HACKER EXPLOITS AND ATTACKS AND AN OVERALL UNDERSTANDING OF THE IT SECURITY MANAGEMENT ROLE AND THREAT ENVIRONMENT FOR PRACTICING THE PRINCIPLES OF GOOD IT SECURITY MANAGEMENT IN THEIR PLACE OF BUSINESS.

ASSESSMENT:

THE FOLLOWING TABLE FEATURES THE PERCENTAGE BREAKDOWN OF EACH ASSIGNMENT AREA TOWARDS THE FINAL GRADE:

INDIVIDUAL CHAPTER ASSIGNMENTS AND CASE STUDIES AND ONLINE PARTICIPATION (FORUMS). 25%

ASSIGNMENTS 35%

ATTENDANCE AND QUALITY OF PARTICIPATION (ONLINE) 15%

FINAL PROJECT/DECISION BRIEF AND PRESENTATION 25%

TOTAL 100%

1. **Required Text (include ISBN, specific edition)**

PANKO, RAYMOND. CORPORATE COMPUTER AND NETWORK SECURITY

PRENTICE HALL, 3RD EDITION. ISBN 0 1303 84712

SECOND EDITION IS ALSO ACCEPTED IF YOU CAN FIND IT AT A REDUCED RATE.

1. **Required Additional Resources and Technical Components**

OTHER RESOURCES WILL BE PROVIDED BY THE PROFESSOR ONLINE

1. **Other Class Expectations (for Classroom/Internet and Web-Based classes, specify any live (synchronous) meetings dates, times, delivery mode)**

Class will be conducted "asynchronously" with optional online meeting sessions each week on Tuesdays from 7-8 pm via the UVA Collab site covering that weeks subjet material. This is an online agile learning environment looking at present day challenges in Information Security Management and using social media sites like LinkedIn to address present day challenges and INFOSEC from both a defensive and offensive nature. We will challenge scenarios through "case study" analysis and class interaction through the use of UVA Collab forums.