COURSE NUMBER AND TITLE: BCIS 482 and BCIS 575: Management of Information Security

FACULTY’S NAME: Oliver, Richard L.

OFFICE HOURS AND LOCATION:
- Tuesday 9:00 am – 9:30 am on Adobe Connect
- Thursday 6:00 pm – 6:30 pm on Adobe Connect

TELEPHONE NUMBER: 646-2944

E-MAIL ADDRESS: Richard Oliver in Canvas Conversations

COURSE DESCRIPTION: This course focuses on the managerial aspects of information security and assurance. Topics covered include access control models, information security governance, and information security program assessment and metrics. Coverage on the foundational and technical components of information security is included to reinforce key concepts. The course includes up-to-date information on changes in the field, such as national and international laws and international standards like the ISO 27000 series.
OFFICE HOURS: This section of BCIS482/575 is being delivered as a distance education course. That is, we will not meet face to face in the traditional lecture environment. My office hours are Tuesday morning from 9:00 am to 9:30 am and Thursday evenings from 6:00 pm until 6:30 pm electronically. That is, you can reach me via the web using AdobeConnect every Tuesday and Thursday night! The URL for these office hours is:

http://nmsu.adobeconnect.com/roliverofficehours/  

When you go to this URL with a browser, you will be asked to login to AdobeConnect. To do this, select Guest. You can use any name you want. However, because all of my students from all of my classes are invited to these office hours, it would be helpful if we use the following convention: <Name><CourseNumber>. That is, I would be Richard482 or Richard575. Again, you can use any name you want. So I could be Snoopy482 or Snoopy575 if I wanted! Here is the login screen using the login name Richard338:

COURSE CONDUCT: This course will use a variety of techniques to facilitate your educational experience:

1. I have prepared Narrated PowerPoint Presentations discussing the material from the primary text book. These presentations will be available via Canvas. They are not tiny in terms of file sizes, so please allow them time to download. The power point slides will also be provided in PDF format in Canvas.

2. We will be using Discussions to explore current topics relevant to information surety and information security. Two important reasons for doing this: 1) exposure to very time sensitive topics of importance and 2) practice articulating a position on topics that may well be very new to you. Please remember, there are many right answers, so just pick a reasonable and supportable position and tell us your story!

3. We also use TechNotes in this course. These are videos demonstrations of some new technologies relevant to information surety and information security. Also, we practice presenting a summary of the important content from the videos. Please do remember, your IT staff will very likely LOVE new technologies for their own sake. It will be your task to evaluate the business value of these technologies and provide guidance to your staff as to their applicability and necessity!

4. Vocabulary is a huge hurdle in the information surety and information security space. To help gain a working vocabulary, I have constructed a web-based game patterned after the card game Memory. A set of cards will be displayed and you click on them to turn them over. The idea is to turn over the two cards that match! While this is a game (no scores are assigned) it provides fun drill and kill experience on these key concepts and terms. If you would prefer, I am also preparing an Anki deck with the same key concepts and terms. Please contact me if you would prefer the Anki vocabulary tool.

5. We will use Writings in this class as well. Typically, we will first read a short white paper or a video about new and emergent technologies or problems in the information surety and information security space. Most of these white papers are written by the companies producing these technologies. Thus, we will need to improve our skills to read and think critically as these are likely to be somewhat biased in content. Our goals here are to learn about these technologies, but also to develop our skills to communicate this information in an accurate and appropriate manner in a business setting.

6. Finally, we also use Examinations to assess your learning in the course. These are one hour examinations in the essay format. Typically, I have 8 questions available on the examination and you are asked to answer 4 of them. You leave the other 4 question blank. I will provide a detailed Study Guide before each examination addressing both the specific conduct and content for the examination. Additionally, during our electronic office hours, we will able to address

https://nmsu.instructure.com/courses/812556
specific questions about the examination.

CONTACTING THE INSTRUCTOR:
1. The best way to contact me is through Canvas email. I will be reading and answering Canvas email several times a day.
2. You can use my office phone 575-646-2944. However, I do not check that every day, so there could be a bit of a lag. Please also use Canvas email.

TEXTBOOKS:

LEARNING GOALS:
- Goal 1: Communication (COMM): Students are effective communicators.
  - Objective 1a: Students can write effectively. (write)
  - Objective 1b: Students can make effective oral presentations. (oral)
- Goal 2: Diversity (DIVERSITY): Students can demonstrate knowledge of diversity.
  - Objective 2a: Students can identify stereotypes.
  - Objective 2b: Students can discern between helpful and detrimental stereotypes.
  - Objective 2c: Students can identify individual characteristics that affect social perception and strategies that counter negative influence on social perception.
- Goal 3: Information Technology (TECH): Students are effective users of information technology.
  - Objective 3a: Students can acquire information using relevant information technologies.
  - Objective 3b: Students can use information technology to manipulate information into a form usable in business decision making
  - Objective 3c: Students can use information technology to disseminate information to others
- Goal 4: Critical Thinking: Students can solve problems and think critically.
  - Objective 4a: Students can solve problems. (PROB SOLV)
  - Objective 4b: Students can think critically. (THINK)
- Goal 5: Legal and Ethical: Students can recognize legal and ethical issues.
  - Objective 5a: Students can recognize legal issues. (LEGAL)
  - Objective 5b: Students can recognize ethical issues. (ETHICS)

LEARNING OBJECTIVES:
After completing Chapter 1, you should be able to do the following:
- Describe the importance of the manager’s role in securing an organization’s use of information technology and understand who is responsible for protecting an organization’s information assets
- Enumerate and discuss the key characteristics of information security
- Enumerate and define the key characteristics of leadership and management
- Differentiate information security management from general management
- Identify and implement basic project management practices and technique

After completing Chapter 2, you should be able to do the following:
- Identify the roles in organizations that are active in the planning process
- Explain the principal components of information security system implementation planning in the organizational planning scheme
- Differentiate between strategic organization information security planning and specialized contingency planning
- Enumerate and explain the unique considerations and relationships that exist among the types of specialized contingency planning – IRP, DRP, and BCP

After completing Chapter 3, you should be able to do the following:
- Recognize the need for contingency planning
- Describe the major components of contingency planning
- Create a simple set of contingency plans, using business impact analysis
- Prepare and execute a test of contingency plans
• Explain the unified contingency plan approach

After completing Chapter 4, you should be able to do the following:

• Define information security policy and understand its central role in a successful information security program
• Describe the three major types of information security policy and explain what goes into each type
• Develop, implement, and maintain various types of information security policies

After completing Chapter 5, you should be able to do the following:

• Explain the organizational approaches to information security
• List and describe the functional components of an information security program
• Determine how to plan and staff an organization’s information security program based on its size
• Evaluate the internal and external factors that influence the activities and organization of an information security program
• List and describe the typical job titles and functions performed in the information security program
• Describe the components of a security education, training, and awareness program and explain how organizations create and manage these programs

After completing Chapter 6, you should be able to do the following:

• Describe the dominant information security blueprints, frameworks, and information security management models, including U.S. government–sanctioned models
• Explain why access control is an essential element of information security management
• Select an information security management model and customize it to meet the needs of a particular organization
• Implement the fundamental elements of key information security management practices
• Discuss emerging trends in the certification and accreditation of U.S. federal IT systems

After completing Chapter 7, you should be able to do the following:

• List the elements of key information security management practices
• Describe the key components of a security metrics program Identify suitable strategies for the implementation of a security metrics program
• Discuss emerging trends in the certification and accreditation of U.S. federal IT systems

After completing Chapter 8, you should be able to do the following:

• Define risk management and its role in the organization
• Use risk management techniques to identify and prioritize risk factors for information assets
• Assess risk based on the likelihood of adverse events and the effects on information assets when events occur
• Document the results of risk identification

After completing Chapter 9, you should be able to do the following:

• Recognize and select from the risk mitigation strategy options used to control risk
• Evaluate risk controls and formulate a cost-benefit analysis using existing conceptual frameworks
• Explain how to maintain and perpetuate risk controls
• Describe the OCTAVE Method and other approaches to managing risk

After completing Chapter 10, you should be able to do the following:

• Describe the various access control approaches, including authentication, authorization, and biometric access controls
• Identify the various types of firewalls and the common approaches to firewall implementation
• Enumerate and discuss the current issues in dial-up access and protection
• Identify and describe the types of intrusion detection systems and the two strategies on which they are based
• Explain cryptography and the encryption process, and compare and contrast symmetric and asymmetric encryption

After completing Chapter 11, you should be able to do the following:

• Identify the skills and requirements for information security positions
• List the various information security professional certifications, and identify which skills are encompassed by each
• Discuss and implement information security constraints on the general hiring processes
• Explain the role of information security in employee terminations
• Describe the security practices used to control employee behavior and prevent misuse of information

After completing Chapter 12, you should be able to do the following:

• Differentiate between law and ethics
• Describe the ethical foundations and approaches that underlie modern codes of ethics
• Identify major national and international laws that relate to the practice of information security
• Describe the role of culture as it applies to ethics in information security Identify current information on laws, regulations, and relevant professional organizations

HOW YOUR LEARNING WILL BE MEASURED: Your understanding and ability to explain terminology, advanced information systems concepts, behavioral and organizational issues, international, social and ethical issues will be measured by applying scoring rubrics to your writings, discussion postings, vocabulary exercises, TechNotes, chapter quizzes, and examinations. The rubrics used to score these work products are given in each exercise. Please review these carefully before doing the work and then review the scoring. If you have questions, please do ask immediately!

PERFORMANCE AREAS: The grades will be determined by combining scores in the following required activities: Chapter Quizzes, TechNotes, Discussions, Writings, and Examinations.

<table>
<thead>
<tr>
<th>Performance Activities</th>
<th>Case 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quizzes</td>
<td>15%</td>
</tr>
<tr>
<td>TechNotes</td>
<td>15%</td>
</tr>
<tr>
<td>Discussions</td>
<td>15%</td>
</tr>
<tr>
<td>Writing</td>
<td>15%</td>
</tr>
<tr>
<td>Examinations</td>
<td>40%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

LETTER ASSIGNMENT: At the completion of the scoring for the semester, the numeric score will be converted to a letter grade using the following brackets. Please note that once all of the scoring is complete, these brackets may change to some degree. However, the lower bound will ONLY move down. That is >= 90% will be an A, but that lower bound may be lowered to 88.5% for example.

<table>
<thead>
<tr>
<th>Lower Bound, Upper Bound</th>
<th>Letter Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>90, 100</td>
<td>A</td>
</tr>
<tr>
<td>80, 89.9</td>
<td>B</td>
</tr>
<tr>
<td>70, 79.9</td>
<td>C</td>
</tr>
<tr>
<td>60, 69.9</td>
<td>D</td>
</tr>
<tr>
<td>0, 59.9</td>
<td>F</td>
</tr>
</tbody>
</table>

ACADEMIC INTEGRITY  Academic integrity is the pursuit of scholarly activity free from fraud and deception and is an educational objective of this institution. Academic dishonesty includes, but is not limited to, cheating, plagiarizing, fabricating of information or citations, facilitating acts of academic dishonesty by others, having unauthorized possession of examinations, submitting work of another person or work previously used without informing the instructor, or tampering with the academic work of other students. You should refer to page 3 of the Student Code of Conduct.


for detailed information regarding academic misconduct.

INCOMPLETE GRADES: A grade of "I" (Incomplete) will be assigned only in circumstances in agreement with the current NMSU Undergraduate Catalog. Incomplete grades are to be given only if a student has passed the first half of the course and is unable to complete the course due to circumstances beyond the student's control. (If the circumstances develop during the first half of the course, the student has the opportunity to drop the class.) Examples of appropriate circumstances are documented illness, documented death or crisis in the student's immediate family and similar circumstances. The catalog states that job related circumstances are generally not appropriate grounds for assigning an "I" grade and that this grade is not to be used to avoid assigning a D, F, or U grade.

S/U GRADES: If you are taking this course under the S/U option, you must earn a "C" or better for an undergraduate and
"B" or better for a graduate student to receive a grade of "S."

LATE/INCOMPLETE ASSIGNMENT POLICY: Work products with the exception of the examinations can be submitted up to 48 hours late with a reduction of the possible points by 20%. Projects not submitted by that time will not be accepted.

MAKE-UP ASSIGNMENT POLICY: There will be three examinations during the semester and chapter quizzes. No make-up quizzes will be given. However, the quizzes are available for the entire semester now, thus you need to consult the schedule and manage your time to complete the quizzes early. No make-up examinations are planned, but it is important to contact the instructor as soon as possible to discuss your grade computation should you have to miss an examination for health or family emergency reasons. If you are absent because you are on an official NMSU trip and you are unable to access the LMS, contact the instructor ahead of time or as soon as possible to determine make-up procedures. A University approved excuse will be required for an absence to be excused.

LIBRARY USAGE: Students will use the Internet frequently as an online library.

COMPUTER RESOURCES: You will need access to the following computer resources: Connection to the University’s Canvas system in the cloud. This can be through a home connection (dialup, DSL, cable modem, etc.) or through computers in the University’s computer labs. Go to https://learn.nmsu.edu to connect to Canvas. This page also has links that will test your browser for compatibility with Canvas. The Network Vulnerability Laboratory on the 3rd floor of the Business Complex.

GLOBAL/INTERNATIONAL BUSINESS CONTENT: This course will address many of the technologies that are used to conduct international business. In particular, we will examine the foremost technologies used in international exchange of business information.

ETHICS CONTENT: As appropriate, we will consider ethical issues related to the course content. Information is inherently valuable, and you may well be in professional positions to control access to this resource. I encourage you to consider these ethical issues thoughtfully.

POLITICAL, SOCIAL, LEGAL, REGULATORY, ENVIRONMENTAL AND TECHNOLOGICAL CONTENT: A primary focus of this class is the use of today’s technology to implement business systems using the Internet. Therefore, the technology of the Internet will be discussed daily.

Disabilities and Discrimination:
Section 504 of the Rehabilitation Act of 1973 and the Americans with Disabilities Act (ADA) covers issues relating to disability and accommodations. If a student has questions or needs an accommodation in the classroom (all medical information is treated confidentially), contact:

Trudy Luken
Student Accessibility Services (SAS) –
Corbett Center, Room 244
Phone: 646-6840
Email: sas@nmsu.edu
Website: www.nmsu.edu/~ssd/

NMSU policy prohibits discrimination on the basis of age, ancestry, color, disability, gender identity, genetic information, national origin, race, religion, retaliation, serious medical condition, sex, sexual orientation, spousal affiliation and protected veterans status. Furthermore, Title IX prohibits sex discrimination to include sexual misconduct, sexual violence, sexual harassment and retaliation. For more information on discrimination issues, Title IX or NMSU’s complaint process contact:

Gerard Nevarez or Agustin Diaz
Office of Institutional Equity (OIE) – O’Loughlin House
Phone: 646-3635
Email: equity@nmsu.edu
Website: www.nmsu.edu/~eeo

GRADE APPEALS: In the unlikely event that you wish to file a grievance with some administrative office or faculty
member on campus, check the details of the process in the "General Information" section of the Undergraduate Catalog. Probably the most urgent thing to know about a grade appeal (besides the fact that there is an appeals process) is that you must initiate the process by submitting a written appeal to the faculty member within 30 days of the start of the term following the term in which the grievance occurred. It's not clear whether this includes summer terms, so, to be safe, submit within 30 days of the grievance.

It will be the responsibility of the student to monitor their progress and decide if it is appropriate to withdraw from the class. I will not automatically disenroll students for persistent absences or persistent failure to complete assignments.