COURSE SYLLABUS

95-756: Information Security Risk Management II
Spring, 2017

Instructors: James Stevens and Adam Cummings

Office (and office hours): Neither instructor has an office on campus, but we will make ourselves available to meet with students before or after class (when requested).

Email: jfs@andrew.cmu.edu and adamcummings@cmu.edu

TA Information: Eidan Aleidan (ealeidan@cmu.edu)

Course Description:
This course and its predecessor, Information Security Risk Management I (95-755), examine information security as a risk management problem where the organization identifies information security risks, evaluates those risks, and makes risk mitigation and acceptance decisions given its resource constraints. In part one of this class, students will have learned foundational concepts in risk management and economic valuation and will be introduced to standard risk management approaches for identifying, analyzing, and responding to risk, as well as the tools and methodologies for metrics to monitor risk management activities. Part two of the course expands coverage to more quantitative approaches to risk analysis, risk valuation, and risk metrics using Factor Analysis of Information Risk (FAIR) and an associated analysis software toolset called RiskLens.

Number of Units: 6

Prerequisites: 95-752 (preferred) and 95-755 (required)

Class Schedule/Location: Thursdays from 6:00pm to 8:50pm in CIC 1201
Textbook Information: There is one required textbook:


Course Objectives:
- Understand and recall the fundamental terms of risk management and information security
- Extract and summarize the most appropriate risk management terms given a practical scenario
- Apply the FAIR framework to a practical scenario such that the identified risks are appropriately addressed
- Articulate the strengths and weaknesses of common risk management frameworks, such as NIST CSF, OCTAVE, or COBIT.
- Evaluate the proper course of action(s) in order to adequately identify and assess risk
- Design a set of key technology risk indicators that can be used to signal the existence of potentially undesirable conditions

Course Website:
Available in Blackboard (Please let us know immediately if you do not have access to it). The instructors will post announcements informing students of any important changes, such as new reading assignments or dates for deliverables. These announcements may or may not be accompanied by an e-mail notification, but it is your responsibility to check for these announcements and ensure that any changes are understood. Since Blackboard is the primary means of communication for this course, we urge you to check the site often.

Evaluation & Grading:
Though the class average for grades may ebb and flow during the semester, you should not concern yourself with the number associated with a grade absent any other context. Rather, you should be concerned about what aspects of that assignment or exam you did not get correct and how you did against the overall average of the class (which will normally be provided). For example, the average for one homework may be a 92 and the average for a different homework may be an 80. A student receiving a 95
and an 87, respectively, may think they did poorly on the second homework. Rather, they did quite well on both homework assignments, relative to the class as a whole. Work hard, master the material, understand what you missed, and the grades will likely take care of themselves. Appealing a grade will only be considered for one week after the grade has been posted and will not be entertained if the student does not have a coherent reason for the appeal. Final grades will be assessed based on the CMU Graduate student grading standard.

The relative weight of the assignments are as follows:
- HW1 = 10%
- HW2 = 10%
- HW3 = 10%
- HW4 = 10%
- Final Project = 60%

**Late Assignment Policy**
Assignments will always have a stated due date and time, typically by 11:59:59pm (note: not midnight) on the day the assignment is due. Unless stated otherwise, all assignments (papers, labs, homework, case studies) must be submitted via Blackboard before the assigned time in order to avoid assessment of a late penalty. All assignments submitted after the assigned penalty will be assessed a 10% penalty per day until the assignment is turned in or the maximum possible score reaches zero after 10 days. Waiting to submit an assignment until 1 minute before the due date and time may put you at the mercy of any processing and upload time associated with submitting the assignment to Blackboard, so avoid being subject to technical difficulties by managing your time appropriately.

**Course Attendance**
Not mandatory, but lack of attendance (and therefore participation) will not help your grade if you’re on the bubble.

**Laptop Policy**
The expectation is that you’re paying attention and we reserve the right to change the policy to restrict electronic device usage.
Tentative Course Topics and Calendar:

<table>
<thead>
<tr>
<th>WEEK</th>
<th>TOPIC/MODULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (MAR 23)</td>
<td>Intro and the FAIR point of view</td>
</tr>
<tr>
<td>2 (MAR 30)</td>
<td>Risk Identification</td>
</tr>
<tr>
<td>3 (APR 6)</td>
<td>Risk Measurement and Analysis</td>
</tr>
<tr>
<td>4 (APR 13)</td>
<td>Utilizing an Analysis</td>
</tr>
<tr>
<td>5 (APR 20)</td>
<td>Utilizing RiskLens</td>
</tr>
<tr>
<td>6 (APR 27)</td>
<td>Risk Response</td>
</tr>
<tr>
<td>7 (MAY 4)</td>
<td>Open</td>
</tr>
<tr>
<td>8 (MAY 11)</td>
<td>Final group presentations</td>
</tr>
</tbody>
</table>

Take Care of Yourself:
Do your best to maintain a healthy lifestyle this semester by eating well, exercising, avoiding drugs and alcohol, getting enough sleep, and taking time to relax. Despite what you might hear, using your time to take care of yourself will actually help you achieve your academic goals more than spending too much time studying. All of us benefit from support and guidance during times of struggle. There are many helpful resources available on campus. An important part of the college experience is learning how to ask for help. Take the time to learn about all that’s available and take advantage of it. Ask for support sooner rather than later – this always helps.
If you or anyone you know experiences any academic stress, difficult life events, or difficult feelings like anxiety or depression, we strongly encourage you to seek support. Consider reaching out to a friend, faculty or family member you trust for assistance connecting to the support that can help. Counseling and Psychological Services (CaPS) is here for you:

Call 412-268-2922 or visit [http://www.cmu.edu/counseling](http://www.cmu.edu/counseling)

Over 25% of students reach out to CaPS some time during their time at CMU. If you or someone you know is feeling suicidal, call someone immediately, day or night:

CaPS: 412-268-2922  
Re:solve Crisis Network: 888-796-8226  
If the situation is life threatening, call the Police:  
   On campus: CMU Police: 412-268-2323  
   Off campus: 911
CMU Academic Integrity Policy (http://www.cmu.edu/academic-integrity/index.html):

In the midst of self exploration, the high demands of a challenging academic environment can create situations where some students have difficulty exercising good judgment.

Academic challenges can provide many opportunities for high standards to evolve if students actively reflect on these challenges and if the community supports discussions to aid in this process. It is the responsibility of the entire community to establish and maintain the integrity of our university.

This site is offered as a comprehensive and accessible resource compiling and organizing the multitude of information pertaining to academic integrity that is available from across the university. These pages include practical information concerning policies, protocols and best practices as well as articulations of the institutional values from which the policies and protocols grew. The Carnegie Mellon Code, while not formally an honor code, serves as the foundation of these values and frames the expectations of our community with regard to personal integrity.

THE CARNEGIE MELLON CODE

Students at Carnegie Mellon, because they are members of an academic community dedicated to the achievement of excellence, are expected to meet the highest standards of personal, ethical and moral conduct possible.

These standards require personal integrity, a commitment to honesty without compromise, as well as truth without equivocation and a willingness to place the good of the community above the good of the self. Obligations once undertaken must be met, commitments kept.

As members of the Carnegie Mellon community, individuals are expected to uphold the standards of the community in addition to holding others accountable for said standards. It is rare that the life of a student in an academic community can be so private that it will not affect the community as a whole or that the above standards do not apply.
The discovery, advancement and communication of knowledge are not possible without a commitment to these standards. Creativity cannot exist without acknowledgment of the creativity of others. New knowledge cannot be developed without credit for prior knowledge. Without the ability to trust that these principles will be observed, an academic community cannot exist.

The commitment of its faculty, staff and students to these standards contributes to the high respect in which the Carnegie Mellon degree is held. Students must not destroy that respect by their failure to meet these standards. Students who cannot meet them should voluntarily withdraw from the university.

_This policy applies, in all respects, to this course._

Carnegie Mellon University's Policy on Cheating ([http://www.cmu.edu/academic-integrity/cheating/index.html](http://www.cmu.edu/academic-integrity/cheating/index.html)) states the following:

According to the University Policy on Academic Integrity, cheating "occurs when a student avails her/himself of an unfair or disallowed advantage which includes but is not limited to:

- Theft of or unauthorized access to an exam, answer key or other graded work from previous course offerings.
- Use of an alternate, stand-in or proxy during an examination.
- Copying from the examination or work of another person or source.
- Submission or use of falsified data.
- Using false statements to obtain additional time or other accommodation.
- Falsification of academic credentials."

_This policy applies, in all respects, to this course._

Carnegie Mellon University's Policy on Plagiarism ([http://www.cmu.edu/academic-integrity/plagiarism/index.html](http://www.cmu.edu/academic-integrity/plagiarism/index.html)) states the following:
According to the University Policy on Academic Integrity, plagiarism "is defined as the use of work or concepts contributed by other individuals without proper attribution or citation. Unique ideas or materials taken from another source for either written or oral use must be fully acknowledged in academic work to be graded. Examples of sources expected to be referenced include but are not limited to:

- Text, either written or spoken, quoted directly or paraphrased
- Graphic elements
- Passages of music, existing either as sound or as notation
- Mathematical proofs
- Scientific data
- Concepts or material derived from the work, published or unpublished, of another person."

*This policy applies, in all respects, to this course. If the instructors find that you have committed plagiarism, the first penalty will be a 0 (zero) on the assignment and a referral to the appropriate dean (i.e., Heinz or INI).*

Carnegie Mellon University's Policy on Unauthorized Assistance ([http://www.cmu.edu/academic-integrity/collaboration/index.html](http://www.cmu.edu/academic-integrity/collaboration/index.html)) states the following:

According to the University Policy on Academic Integrity, unauthorized assistance "refers to the use of sources of support that have not been specifically authorized in this policy statement or by the course instructor(s) in the completion of academic work to be graded. Such sources of support may include but are not limited to advice or help provided by another individual, published or unpublished written sources, and electronic sources. Examples of unauthorized assistance include but are not limited to:

- Collaboration on any assignment beyond the standards authorized by this policy statement and the course instructor(s).
- Submission of work completed or edited in whole or in part by another person.
● Supplying or communicating unauthorized information or materials, including graded work and answer keys from previous course offerings, in any way to another student.

● Use of unauthorized information or materials, including graded work and answer keys from previous course offerings.

● Use of unauthorized devices.

● Submission for credit of previously completed graded work in a second course without first obtaining permission from the instructor(s) of the second course. In the case of concurrent courses, permission to submit the same work for credit in two courses must be obtained from the instructors of both courses."

This policy applies, in all respects, to this course.

Carnegie Mellon University's Policy on Research Misconduct (http://www.cmu.edu/academic-integrity/research/index.html) states the following:

According to the University Policy For Handling Alleged Misconduct In Research, “Carnegie Mellon University is responsible for the integrity of research conducted at the university. As a community of scholars, in which truth and integrity are fundamental, the university must establish procedures for the investigation of allegations of misconduct of research with due care to protect the rights of those accused, those making the allegations, and the university. Furthermore, federal regulations require the university to have explicit procedures for addressing incidents in which there are allegations of misconduct in research.”

The policy goes on to note that “misconduct means:

● fabrication, falsification, plagiarism, or other serious deviation from accepted practices in proposing, carrying out, or reporting results from research;
● material failure to comply with Federal requirements for the protection of researchers, human subjects, or the public or for ensuring the welfare of laboratory animals; or
● failure to meet other material legal requirements governing research.”
“To be deemed misconduct for the purposes of this policy, a ‘material failure to comply with Federal requirements’ or a ‘failure to meet other material legal requirements’ must be intentional or grossly negligent.”

To become familiar with the expectations around the responsible conduct of research, please review the guidelines for Research Ethics published by the Office of Research Integrity and Compliance.

This policy applies, in all respects, to this course.