

**Course Code: Information Security Risk Management**

**Semester**

|  |  |
| --- | --- |
| **Credit Hours:** | Enter Credit Hours |
| **Class Details:** | Classroom Location |
|  | Class days / times |
| **Instructor Contact Information:** | Name |
|  | Phone |
|  | Email |
|  | Office: Location and Hours |

**Course Description**

This course will introduce quantitative risk measurement and management methods applicable to a broad spectrum of industries. Principally, it will delve deeply into FAIR (Factor Analysis of Information Risk)—an industry standard risk model—which caters to information security and operational risk. To help contextualize these methods and model, the students will compile a case study that entails: researching a risk topic, scoping an analysis, using the FAIR-U tool to perform the risk analysis, and presenting the results.

**Course Goals**

Students who successfully complete this course will demonstrate an ability to:

* Think critically about risk measurement and management methods
* Define, calculate and analyze risk in a defensible way
* Leverage a probabilistic mindset when evaluating risk
* Demonstrate a working familiarity with the FAIR model
* Translate risk analysis into meaningful business decisions
* Explain how the FAIR model can augment the NIST Cybersecurity Framework (CSF)

**Required Reading Materials**

All books are available on Amazon.com or at the University bookstore.

*The Failure of Risk Management: Why It's Broken and How to Fix It*, Wiley, 2009, by Douglas Hubbard. ISBN 978-0-470-38795-5

<https://www.amazon.com/gp/product/0470387955/ref=oh_aui_detailpage_o00_s00?ie=UTF8&psc=1>

*How to Measure Anything in Cybersecurity Risk,* 1st Edition, Wiley, 2016, by Douglas Hubbard. ISBN 978-1119085294

<https://www.amazon.com/How-Measure-Anything-Cybersecurity-Risk/dp/1119085292>

*Measuring and Managing Information Risk: A FAIR Approach*, Butterworth-Heinemann, 2015, by Jack Freund and Jack Jones. ISBN 978-0-12-420231-3

<http://www.amazon.com/Measuring-Managing-Information-Risk-Approach/dp/0124202314>

Jones, Jack. “NIST CSF & FAIR - Parts 1-5.” Web blog post. *The FAIR Institute Blog*. The FAIR Institute, Mar. 2016. <http://www.fairinstitute.org/blog/nist-csf-fair-part-1>

**Suggested Reading**

Available through The Open Group:

*O-RT Risk Taxonomy Standard*, The Open Group.

<https://www2.opengroup.org/ogsys/catalog/C13K>

*O-RA Risk Analysis Standard*, The Open Group.

<https://www2.opengroup.org/ogsys/catalog/C13G>

**Other technology requirements / equipment / material**

To succeed in this course, students will need access to a computer with internet access, along with Microsoft Word, PowerPoint, and Excel.

**Course Requirements and Assignments**

**Class Participation**

All assigned reading must be completed prior to the start of each class. Students are expected to actively listen, ask questions, and engage in constructive dialogue during class. To maximize the learning experience, students should come to class prepared to share a particular insight based on the readings, and/or bring an article related to the class topic.

In-class exercises will occur intermittently throughout the semester; these exercises will include both individual and group work.

**Case Study**

### The Case Study consists of two deliverables: A Presentation and a Risk Analysis Paper. Presentations will be scheduled within the first few weeks of the semester, then occur throughout the duration of the course. The Risk Analysis Paper is due the last class period (see assignment schedule).

### Each student will be given the opportunity to identify a risk analysis topic; subject to the instructor’s approval. Once a topic is approved, the students are expected to research the topic and then perform a risk analysis in the FAIR-U tool. Access to and instructions for the tool will be provided by the instructor.

### More specific details about the schedule and structure of the Case Study be provided by the instructor via an in-class handout. For an optimal Case Study experience, students are encouraged to seek ongoing consultation with the instructor during the project.

**Note on Exams:**

There are no Midterm or Final exams for this course.

**Grading Chart**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 97-100% | A+ | 87-89.9% | B+ | 77-79.9% | C+ | 67-69.9% | D+ | <60% | F |
| 94-96.9% | A | 84-86.9% | B | 74-76.9 | C | 64-66.9% | D |  |  |
| 90-93.9% | A- | 80-83.9% | B- | 70-73.9% | C- | 60-63.9% | D- |  |  |

**Grading**

Your final grade will be calculated based on the following weights:

|  |  |
| --- | --- |
| Class Participation | 40% |
| Case Study: Risk Analysis Paper | 30% |
| Case Study: Presentation | 15% |
| In-class exercises | 15% |

**University Expectations and Policies**

< Insert any applicable material (e.g. Disability, Academic Honesty, Make-Up Policies etc.) >

**Class Assignment / Reading Schedule\***

*(\*Subject to change; notice of amendments will be provided by instructor.)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Week** | **Date** | **Topic** | **Readings/Assignments** |
| 1 | dd-mmm | Introductions; Syllabus & Class Overview |  |
|  |  | Current Crisis | *Fail*ure, Ch. 1-2 |
| 2 |  | Evaluation Methods | *Failure*, Ch. 3 |
|  |  | The Broken State of Risk Management | *Failure*, Ch. 4-6 |
| 3 |  | Overcoming Bad Practices | *Failure*, Ch. 7-9 |
|  |  | Implementing Improvements | *Failure*, Ch. 10-11 |
| 4 |  | The Risk Community | *Failure*, Ch. 12 |
|  |  | The Primer for Cybersecurity | *How to Measure*, Ch. 1-2 |
| 5 |  | Quantitative Methods to Cybersecurity | *How to Measure*, Ch. 3-4 |
|  |  | Unpacking the Details | *How to Measure*, Ch. 5-6 |
| 6 |  | Estimates and Uncertainties | *How to Measure*, Ch.7-8 |
|  |  | Powerful Models and Metrics | *How to Measure*, Ch. 9-10 |
| 7 |  | Working Together to Move Forward | *How to Measure*, Ch. 11-12 |
|  |  | Introduction to FAIR | *FAIR*, Ch. 1 |
| 8 |  | Basic Risk Concepts | *FAIR*, Ch. 2 |
|  |  | The FAIR Risk Ontology | *FAIR*, Ch. 3 |
| 9 |  | FAIR Terminology | *FAIR*, Ch. 4 |
|  |  | Measurement | *FAIR*, Ch. 5 |
| 10 |  | Analysis Process | *FAIR*, Ch. 6 |
|  |  | Interpreting Results | *FAIR*, Ch. 7 |
| 11 |  | Risk Analysis Examples | *FAIR*, Ch. 8 |
|  |  | Thinking about Risk Scenarios Using FAIR | *FAIR*, Ch. 9 |
| 12 |  | Common Mistakes | *FAIR*, Ch. 10 |
|  |  | Controls | *FAIR,* Ch. 11 |
| 13 |  | Risk Management | *FAIR,* Ch. 12 |
|  |  | Information Security Metrics | *FAIR,* Ch. 13 |
| 14 |  | Implementing Risk Management | *FAIR,* Ch. 14 |
|  |  | FAIR and NIST CSF | “NIST CSF & FAIR - Parts 1-5.” *The FAIR Institute Blog*. |
| 15 |  | Guest Speaker |  |
|  |  | TBA |  |
| 16 |  | Presentations | Reference: in-class Case Study handout |
|  |  | Presentations; Risk Analysis Papers | Reference: in-class Case Study handout |