Syllabi

CYPD 630. Cybersecurity Compliance Methodologies I. 3 credits

Credits:	3
Classroom:	Online
Class Hours:	Weekly online engagement, 20 hours; biweekly virtual seminars alternate Saturdays 10AM – 12:00 PM, ET
Office Hours:	Virtual, by appointment
Instructor:	TBD
Phone:	TBD
Email:	TBD
Prerequisites:	N/A
Text:	Mastering the Risk Management Framework Revision 2 by James Broad
Materials:	NIST SP 800-53, NIST SP 800-171 and FedRamp documentation

Course Description and Objectives:
Students review and analyze the concepts and interrelationships underlying cybersecurity compliance methodologies, including the NIST Risk Management Framework (RMF); Federal Risk and Authorization Management Program (FedRAMP; NIST 800-171; CMMC; NIST Cyber Security Framework (CSF); and NIST 800-53. Students develop competencies to utilize NIST RMF Steps 1-3/FedRAMP Steps 1-2.

Assessment Objectives:

- Ability to apply risk management compliance methods to categorize the risk exposure of a system
- Ability to identify the controls required to achieve the system risk categorization
- Ability to conduct privacy analysis and produce a privacy assessment
- Ability to develop a continuous monitoring strategy

Course Outline:
Weekly projects will enable students to learn, analyze and apply the methods of the NIST RMF, Steps 1- 3. The following is a tentative list of topics to be covered in the course:

1. NIST RMF/ FedRAMP Comparison
2. FIPS 199 System Categorization
3. NIST Security Control Selection
4. Privacy Threshold Analysis (PTA)
5. Privacy Impact Assessment (PIA)
6. Preliminary System Security Plan (SSP)
7. Preliminary Information Systems Continuous Monitoring (ISCM) Strategy

Grading:

The grading will be based on course engagement, assignments, and projects. The final grade will be determined by weighing each component as follows:

- Asynchronous engagement: 40%
- Virtual seminar engagement: 12%
- Assignments: 24%
- Projects: 24%