CYPD 632. Cybersecurity Compliance Methodologies II. 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
Prerequisite:	CYSE 630 or equivalent; or permission of the instructor
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 develop the competencies to utilize the NIST RMF, Steps 4-6: Implementation, Authorization and Monitoring /FedRAMP, Steps 3-4. Students analyze how these steps relate to the CMMC accreditation process.

Assessment Objectives:

- Ability to produce the Security Assessment Plan
- Ability to conduct a Security Assessment
- Ability to produce a Security Assessment Report (SAR)
- Ability to produce a Plan of Action and Milestones (POA&M)
- Ability to compile an Authorization to Operate (ATO)
- Ability to develop an Information Security Continuous Monitoring (ISCM) Strategy
- Ability to develop a System Decommissioning Strategy

Course Outline:
Weekly projects will enable students to learn, analyze and apply the methods of the NIST RMF, Steps 4-6. The following is a tentative list of topics to be covered in the course:

1. Security Assessment Plan
2. Security Assessment Report (SAR)
3. POA&M
4. ATO Package
5. ISCM Strategy
6. System Decommissioning
7. Interrelationship among the steps of the NIST RMF, NIST 800-171 compliance and CMMC compliance

Grading

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%

(back)