CAPITOL COLLEGE

1927

Critical Infrastructures and Cyber Protection Center (CICPC)
Professional Development Programs

FISMA Compliance Review Program
Sample Syllabus

FISMA

ICP-086-Pxx

(class dates)
Live on Weekdays
Lunchbox Training Sessions: 11:30 AM – 1:00 PM

Program Director: Prof. Charles L. Cayot Jr.
Email: clcayot@capitol-college.edu
Phone: 518-781-3300

Office hours: by appointment
Fax: 518-781-3302
Number of Live Meetings: 10

Course Description:

The E-Gov Act of 2003, specifically the Federal Information Security Management Act (FISMA), requires information assurance (IA) professionals and managers throughout the federal government to comply with a defined set of policies, procedures and security countermeasures to protect sensitive information and critical infrastructures. Federal and corporate IA professionals must understand and comply with requirements that include system categorization, identification, installation and maintenance of baseline IA countermeasures, system testing, and certification and accreditation.

The FISMA training program developed by the CICPC will provide IT/IA professionals the required training and understanding of current requirements published by the National Institute of Standards and Technology (NIST). This comprehensive program leverages the experience of selected instructors with vast experience in Information Assurance, Risk Management, the DoD Certification and Accreditation Process and other related professions. Those who complete successfully the CICPC FISMA training course will receive a CICPC Certificate of Completion.

The FISMA program consists of 11 separate subject modules broken into 17 individual instructional periods. The program will include one practical exercise in system categorization and controls mapping, a comprehensive review session and a course exam administered during the last live session. Successful completion of the exam is required for the issuance of the course completion certificate.

Due to the subject matter and projected student audiences this course is offered as a “Lunch Box” training program. Contents of the various subject modules are presented live over 17 consecutive lunch time sessions. Other presentation options can be arranged based on student and organization requirements to accommodate unique situations and individual needs. In each training session we will cover topical areas that together provide a comprehensive presentation of the critical areas to establish a solid framework that will assist you in successfully complying with your FISMA requirements. An alternative presentation schema is available for those not desiring a “lunch box” course.

Course Objectives:

1. Provide a comprehensive review of the FISMA program
2. Present and discuss legal and regulatory compliance requirements
3. Identify the various IA compliance requirements including source derivative documents
4. Review and discuss the functional components of IA and security control requirements
5. Review applicable NIST documentation (FIPS / 800 series SPs)
6. Insure understanding of basic Risk Management procedures
7. Discuss and review Certification and Accreditation

Principle Topics Covered:

1. FISMA Primer – A Program Overview
2. System Life Cycle and security implications throughout the entire lifecycle
3. Legal and Management Issues
4. Information Assurance Basics
5. Security Categorization of Information Systems and Networks
6. Category Mapping
7. Security Controls for Information Systems
8. Testing and Assessment of Security Controls
9. Certification and Accreditation (C&A)
10. Security Plans
11. Risk Management
12. Industrial Control System Security (ICS)

Required Texts / Training Reference Materials:

- **FIPS Publication 199** (Standards for Security Categorization of Federal Information and Information Systems)
- **FIPS Publication 200** (Minimum Security Requirements for Federal Information and Information Systems)
- **NIST Special Publication 800-18** (*Guide for Developing Security Plans for Federal Information Systems*)
- **NIST Special Publication 800-30** (*Risk Management Guide for Information Technology Systems*)
- **NIST Special Publication 800-37** *(Guide for the Security Certification and Accreditation of Federal Information Systems)*
- **NIST Special Publication 800-53** (*Recommended Security Controls for Federal Information Systems)*
- **NIST Special Publication 800-53A** (*Guide for Assessing the Security Controls in Federal Information Systems*)
- **NIST Special Publication 800-59** (Guidelines for Classifying Information Systems as a National Security System)
- **NIST Special Publication 800-60** (Guide for Mapping Types of Information and Information Systems to Security Categories)
- **NIST Special Publication 800-82** (Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, 2nd Draft 09/07)
- **MITRE Technical Report (MT070050),** Addressing Industrial Control Systems in NIST SP 800-53

Instructional Methods:

The basic mode of instruction will include live classes and individual research learning. Live classes will be conducted with audio. Your instructor presents the live classes. Students can visit the classroom at any time for additional preparation and review of previous lessons, including the playback of recorded lectures. Both individual and small groups may participate by utilizing the features of Blackboard to collaborate, respond to questions and clarify the subject matter as necessary. Live (synchronous) sessions will be used for module / subject matter presentation, class discussions, and question and answer periods. Make sure that you take the time to familiarize yourself with the software and instructions that were provided by Capitol College and CentraOne. If you have any technical questions about Capitol Online or CentraOne and your system, the Capitol College helpdesk staff will be happy to assist you.

Live Sessions:

Instructors present the Live sessions. All students are encouraged to attend Live "synchronous sessions".

Live "synchronous sessions" are intended to clarify and strengthen the material students have covered in the reading and other research. An active rather than passive role by the student is essential in "online" education. The sessions will consist of discussion and review of assigned material. Discussions will focus upon those areas and issues where comprehension is substantially enhanced by additional elaboration or illustration and those of a controversial nature. The instructor will attempt to emphasize the points and factors that are most important and, in this way, focus on the test taking strategy objectives for this course.

CentraOne has full-time "live mic" capability. Please keep the following in mind:

1. Only one person should "speak" at a time.
2. Students should raise their "electronic hand" as if they were in a classroom. The Professor will call on students who have raised their hand to make a comment or ask a question. Questions/comments will be addressed in the order they were received.
3. Centra also has text "chat" capability. When using text chat enter your comment in short phrases. If you want to comment or ask a question simply send a "Text chat" message to the Professor or raise your "electronic" hand.
4. Following these rules will assist in making the eLearning environment as productive as possible.

FISMA Certification Program
Lunch Box Presentation Schedule

Live on weekdays: (11:30 AM – 1:00 PM)
(**L**) = Live Session (with the Instructor) (**A**) = Asynchronous / Blackboard (without the Instructor)

Date	Session	Module	Functional Area	Instructor	Readings/URL/Topics
	Session 00		Preparation	Students	Download Syllabus, Lecture Slides, and any Additional Readings
Day 1	Session 01	MOD 1	FISMA Primer	TBA	Communications Check, and Orientation and Introduction. Compliance with NIST Standards Slide Set: – Module 1 Reading: E-Gov Act; Title III - FISMA
Day 2	Session 02	MOD 1	FISMA Primer	TBA	Compliance with NIST Standards General Responsibilities C&A Slide Set: – Module 1 Reading: E-Gov Act; Title III - FISMA
Day 3	Session 03	MOD 2	Legal and Management Issues	TBA	Legal and Regulatory Obligations Reporting Requirements Reporting Tools Slide Set: – Module 3 Reading: Privacy Act; OMB Cir A-130; PDDs/HSPDs; SP800-59
Day 4	Session 04	MOD 2	Legal and Management Issues	TBA	Legal and Regulatory Obligations Reporting Requirements Reporting Tools Slide Set: – Module 3 Reading: Privacy Act; OMB Cir A-130; PDDs/HSPDs; SP800-59
Day 5	Session 05	MOD 3	Information Assurance Basics	TBA	Goals of Security The Art of IA Slide Set: – Module 3
Day 6	Session 06	MOD 4	Security Categorization	TBA	Security Categorization Min Sec Controls Slide Set: – Module 4 Reading: FIPS 199; FIPS 200; SP800-59
Day 7	Session 07	MOD 5	Category Mapping	TBA	Mapping Standards Types of Information Minimum Security Reqts Slide Set: – Module 5 Reading: FIPS 199; FIPS 200; SP800-60
Day 8	Session 08	MOD 6	Security Controls	TBA	Selecting and specifying controls Assessment methodologies Slide Set: – Module 6 Reading: FIPS 199; FIPS 200; SP800-53

Date	Session	Module	Functional Area	Instructor	Readings/URL/Topics
ay 9	Session 09	Practical Exercise	Categorization of Information and Mapping of IA Controls	TBA	Students will complete a practical exercise in system categorization, selection and mapping of applicable IA controls from the previous modules.
Day 10	Session 10	MOD 7	Testing and Assessment of Security Controls	TBA	Test and Evaluation Programs SDLC and Security Controls Slide Set: – Module 7 Reading: SP800-53A; SP800-42; NIST ITL Bulletin Nov 2003-
Day 11	Session 11	MOD 8	Certification and Accreditation	TBA	C&A Basics Roles in C&A NIST program for Certifying System Certifiers Slide Set: – Module 8 Reading: SP800-37; SP800-53A
Day 12	Session 12	MOD 9	Security Plans	TBA	Security Plans Policies Training and Security Documentation Assessing Policies & Guidelines Slide Set: – Module 9 Reading: SP800-18, Rev1
Day 13	Session 13	MOD 10	Risk Management	TBA	Risk Management Framework Risk Management Programs Slide Set: – Module 10 Reading: FIPS 199 & 200; SP800-53, 53A, 30, 18, 37
Day 14	Session 14	MOD 10	Risk Management	TBA	Risk Management Framework Risk Management Programs Slide Set: – Module 10 Reading: FIPS 199 & 200; SP800-53, 53A, 30, 18, 37
Day 15	Session 15	MOD 11	Industrial Control Systems Security (ICS)	TBA	SCADA & DCS Systems Importance of protecting critical infrastructure Slide Set: – Module 11 Reading: SP800-53; SP800-82; MITRE Tech Report (MT070050) Addressing ICS in NIST SP 800-53
Day 16	Session 16	MOD X	Course Review	TBA	Recap and Review of FISMA and major components and requirements necessary for compliance
Day 17	Session 17	MOD X	Course Exam	TBA	Comprehensive Exam covering course materials and content