Agenda Item #16-12
Effective: Fall 2017

Eastern Illinois University

New/Revised Course Proposal Format

(Approved by CAA on 4/3/14 and CGS on 4/15/14, Effective Fall 2014)

Banner/Catalog Information (Coversheet)

1. **__X__ New Course or _____Revision of Existing Course**
2. **Course prefix and number:** _____CYB 5550_____
3. **Short title:** _____Cybersecurity Seminar
4. **Long title:** _____Cybersecurity Professional Seminar__
5. **Hours per week:** __3_ Class _0_ Lab __3_ Credit
6. **Terms:** ___ Fall ___ Spring ___ Summer _X_ On demand
7. **Initial term**: _X__ Fall ___ Spring ___ Summer Year: 2017
8. **Catalog course description:** Review of content and procedures of the recommended professional cybersecurity certifications in the U.S. market.
9. **Course attributes:**

   General education component: __None _____

   ___ Cultural diversity ___ Honors ___ Writing centered ___ Writing intensive ___Writing active
10. **Instructional delivery**
    Type of Course:

    _X_ Lecture ___ Lab ___ Lecture/lab combined ___ Independent study/research

    ___ Internship ___ Performance ___ Practicum/clinical ___ Other, specify: _____

    Mode(s) of Delivery:

    __ Face to Face __X_ online ___ Study Abroad

    __ Hybrid, specify approximate amount of on-line and face-to-face instruction: _____
11. **Course(s) to be deleted from the catalog once this course is approved.** _____None_____
12. **Equivalent course(s):** __None_____

    a. Are students allowed to take equivalent course(s) for credit? ___ Yes _X_ No
13. **Prerequisite(s):** _TEC 5353, MIS 4850

    a. Can prerequisite be taken concurrently? ___ Yes _X_ No

    b. Minimum grade required for the prerequisite course(s)? _C_

    c. Use Banner coding to enforce prerequisite course(s)? _X_ Yes __ No

    d. Who may waive prerequisite(s)?

___ No one _X_ Chair _ Instructor ___ Advisor ___ other (specify)

14. **Co-requisite(s):** _____NONE_____

15. **Enrollment restrictions**

    a. **Degrees, colleges, majors, levels, classes which <u>may</u> take the course:** _Enrollment on Cohort or permission by the chair

    b. **Degrees, colleges, majors, levels, classes which may <u>not</u> take the course:** Undergrad Students

16. **Repeat status:** __X_ May not be repeated ___ May be repeated once with credit

17. **Enter the limit, if any, on hours which may be applied to a major or minor:** _3__

18. **Grading methods:** _X_ Standard ___ CR/NC __ Audit ___ ABC/NC

19. **Special grading provisions:**

    ___ Grade for course will <u>not</u> count in a student's grade point average.

    ___ Grade for course will <u>not</u> count in hours toward graduation.

    ___ Grade for course will be removed from GPA if student already has credit for or is registered in: _____

    ___ Credit hours for course will be removed from student's hours toward graduation if student already has credit for or is registered in: _____

20. **Additional costs to students:**
    Supplemental Materials or Software: Each student will be required to buy practice test (current test) for both exams totaling an investment of about $200. Average cost of materials is about $100 dollars per test

    Course Fee ___No _X Yes, Explain if yes: <u>Exam might be updated by the time this course is offered for first time, students must buy CD with practice test or enroll in practice tests.</u>_

21. **Community college transfer:**

    ___ A community college course may be judged equivalent.

    _X__ A community college may <u>not</u> be judged equivalent.

    Note: Upper division credit (3000+) will <u>not</u> be granted for a community college course, even if the content is judged to be equivalent.

Rationale, Justifications, and Assurances (Part I)

1. _X Course is required for the major(s) of : Master of Science in Cybersecurity
   ___Course is required for the minor(s) of _____
   ___Course is required for the certificate program(s) of _____
   ___ Course is used as an elective
2. **Rationale for proposal** :

   The United States Department of Defense (DOD) and most private companies require select cybersecurity certifications as a pre-requisite for employment. Students in the M.S. in Cybersecurity will be trained and advised on current U.S. market certifications in order to improve the likelihood of their passing the certification exams. This course prepares our students in the mechanics, content and details of those certifications. After this course our student will have a higher chance to pass these certifications. Preparing for this course outside EIU, will give them a cost-benefit advantage, due to the fact that similar courses cost between $3500 and $5000 in the open market.
3. **Justifications for (answer N/A if not applicable)**

   Similarity to other courses: NONE

   Prerequisites: Satisfactory completion of TEC 5353 and MIS 4850 are required. This is a graduate level course that requires students to have a solid knowledge and understanding of cybersecurity and systems security concepts prior to enrollment.

   Co-requisites: None

   Enrollment restrictions: This is a graduate level course and restricting it to graduate students only helps ensure those taking the class are adequately prepared. If there are any seats left for other graduate students in our programs with the proper pre-requisites, the chair of the School of Technology might allow them to sign up for this course.

   Writing active, intensive, centered: No
4. **General education assurances (answer N/A if not applicable)**

   General education component: N/A

   Curriculum: N/A

   Instruction: N/A

   Assessment: N/A
5. **Online/Hybrid delivery justification & assurances (answer N/A if not applicable)**

   Description: This course builds upon content covered in TEC 5353 and MIS 4850 and reviews materials covered in the U.S. Department of Defense required cybersecurity certifications. All reviews, homework submissions, special topic discussions and practice

exams can properly be taught in an online format. The actual certification exams are administered via computers, so the online/computer format for instruction is most appropriate.

Instruction: The course employs structured web discussions focused on reading assignments and topics drawn from the materials provided.
In this format the assignments require students to apply the course material to their own experiences as a means of enhancing learning and assuring integrity. The course employs email, web-based discussions, and exploration of off-site internet resources, chats, video/audio activities, practice exams, and web-based presentations in order to ensure similar academic exposure to materials, instructor collaboration and practices.
Any instructors of technology-delivered courses/sections must submit proof of having completed the Online Course Development Institute (OCDI), Illinois Online Network's "Master Online Teacher" certificate or another documented and equivalent training activity before teaching the courses/sections for the first time.

Integrity:

- Students will have personalized questions during exams, although group study and group work will enhance their certification preparation. Questions in each exam will come from a database which will ensure that students will have a different set/order of questions for a particular exam (question selection will be randomized).

- Each student will have his/her own credentials and her/his own particular file when authenticating remotely to exams and homework assignments. Written submissions will be tested using Turnitin or similar plagiarism software detection to have an initial review of plagiarism.

Interaction:

- The course employs email, web-based discussions, exploration of off-site Internet resources, chats and synchronous video/audio activities, and web-based presentations. Chats with students, e-mail, group discussion, online synchronous interaction (i.e. Skype, Messenger and/or chats), and a LMS system will be used extensively either in a synchronous or asynchronous fashion.

If students with disabilities register for the course, and depending upon the disability, different accommodations can be made for the students (longer exam times, larger fonts, he/she can submit online exams if needed) including but not limited to the assistive technology @ EIU offered by the office of disability services.

Model Syllabus (Part II)

Please include the following information:

1. Course number and title: CYB 5550 , "Cybersecurity Professional Seminar"

2. Catalog description: Review of content and procedures for the recommended professional cybersecurity certifications on the U.S. market.

3. Learning objectives. Upon completion of this course, all students will be able to:

#	**Objectives**	Graduate Learning Goals
1	Describe and explain the content of the most current required cybersecurity certifications in the U.S. market.	a. Depth of content knowledge b. Effective critical thinking and problem solving c. Effective oral and written communication
2	Practice and prepare for cybersecurity certifications by completing mock exams.	a. Depth of content knowledge b. Effective critical thinking and problem solving c. Effective Oral and Written communication
3	Review and synthetize the academic concepts included in the most current cybersecurity certifications.	a. Depth of content knowledge b. Effective critical thinking and problem solving
4	Complete a self-assessment of how well prepared they are to pass the certification.	a. Depth of content knowledge b. Effective critical thinking and problem solving c. Effective oral and written communication

4. Course materials.

- "Principles of Computer Security CompTIA Security+ and Beyond (Exam SY0-301), 3rd Edition (Official CompTIA Guide)" by Arthur Conklin and Gregory White. McGraw Hill 2012
- "CISSP All-In-One Exam Guide [With CDROM] Hardcover", October 18, 2012 by Shon Harris, John Wiley and Sons.
- "CISSP Practice Exams" 3rd Edit.: March 2, 2015 by Shon Harris, John Wiley and Sons.
- Materials developed by the instructor(s)

5. Weekly outline of content.

WEEK	Topic
1	Network Security
2	Compliance and Operational Security
3	Threats and Vulnerabilities
4	Application, Data and Host Security
5	Access Control and Identity Management
6	Security Exam: Cryptography
7	Final Practice
8	Security and Risk Management
9	Protecting Security Assets
10	Security Engineering
11	Communication and Network Security
12	Identity Access and Management
13	Security Assessment and Testing
14	Security Operations and Software Security
15	Final Practice

6. Assignments and evaluation, including weights for final course grade.

Assignments and evaluations, including weights for final course grades are summarized below

- Quizzes – 30%
- Homework assignments – 30%
- Essay and discussion reflection about the certification exams – 5%
- Two mock Comprehensive Exams – 15% and 20%

7. Grading scale.

Final grades are based on the following scale:

- Percentage ≥ 90 A
- $80 \leq$ Percentage < 90 B
- $70 \leq$ Percentage < 80 C
- $60 \leq$ Percentage < 70 D
- Percentage < 60 F

8. Correlation of learning objectives to assignments and evaluation.

#	Objectives for all Students	Discussion/ Reflection	Quizzes	Homework Assignments	Comprehensive Exams
1	Describe and explain the content of the most current key cybersecurity certifications in the U.S. market.	X			
2	Practice and prepare for cybersecurity certifications by doing mock exams.	X	X	X	X
3	Review and synthetize the academic concepts included in the most current cybersecurity certifications.		X	X	
4	Complete a self-assessment of how well prepared they are to pass the certification	X	X		X

Date approved by the department or school: NOVEMBER 6/2015
Date approved by the college curriculum committee: JANUARY 22/2016
Date approved by CGS: