Eastern Illinois University
New/Revised Course Proposal Format
(Approved by CAA on 9/30/21 and CGS on 11/16/21)

Banner/Catalog Information (Coversheet)

1. **__X__ New Course or _____Revision of Existing Course**
2. **Course prefix and number:** ___MBA 5870_____
3. **Short title:** ____InfoSec and Risk Management _____
4. **Long title:** _____ Information Security and Risk Management_____
5. **Hours per week:** _3_ Class _0_ Lab _3_ Credit
6. **Terms:** ___ Fall ___ Spring ___ Summer _X_ On demand
7. **Initial term**: ___ Fall _X_ Spring ___ Summer Year: _2024_
8. **Catalog course description:** ___ Study of theories, principles and techniques of information security and risk management. The course covers security threats and countermeasures, operational and organizational security, infrastructure security, risk assessment and risk management, business continuity and disaster recovery.__
9. **Course attributes: N/A**

   General education component: _____

   ___ Cultural diversity ___ Honors ___ Writing centered ___ Writing intensive ___Writing active

   ___ Department Capstone as Senior Seminar

10. **Instructional delivery**

    Type of Course:

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

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

    Mode(s) of Delivery:

    _X_ Face to Face __ Online Synchronous _X_ Online Asynchronous ___ Study Abroad

    _X_ Hybrid, specify approximate amount of on-line and face-to-face instruction__ A maximum of 49% of the course will be online with the remainder face-to-face _

11. Course(s) to be deleted from the catalog once this course is approved:
___N/A_____

12. Equivalent course(s):
__N/A_____

a. Are students allowed to take equivalent course(s) for credit? ___ Yes _X_ No

13. Prerequisite(s): __ Graduate standing, BUS 3500 with a grade of C or better, or MBA 5670, or permission of the Chair, School of Business **_**

a. Can prerequisite be taken concurrently? __ Yes _X__ No

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

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): _____

15. Enrollment restrictions

a. Degrees, colleges, majors, levels, classes which <u>may</u> take the course: ___All_____

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

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 _____NONE_____

Course Fee _X_No ___Yes, Explain if yes_____

21. Community college transfer:

___ A community college course may be judged equivalent.

_X_ A community college may not be judged equivalent.

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

Rationale, Justifications, and Assurances (Part I)

1. ___Course is required for the major(s) of _____

___Course is required for the minor(s) of _____

___Course is required for the certificate program(s) of _____

_X_ Course is used as an elective _____in the MBA program _____

2. Rationale for proposal: The US Bureau of Labor Statistics lists cybersecurity among its fastest-growing career areas. With an expected 32% growth over the coming decade, Cybersecurity has over six times the growth rate for all jobs. This course prepares students with relevant knowledge and technical skills to understand and help address information security threats and risk management issues.

3. Justifications for (answer N/A if not applicable)

Similarity to other courses: _____ N/A_____.

Prerequisites: ___The listed pre-requisites will prepare students for the class__.

Co-requisites: N/A

Enrollment restrictions: N/A

Writing active, intensive, centered: N/A

Capstone as Senior Seminar: N/A

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)

Online or hybrid delivery justification: This course may be offered in online or hybrid formats in order to make this class as accessible to a broad range of students. This approach is being used to assist in the recruitment and retention of students, as it allows for more

flexibility in scheduling for working professionals. In addition, the course content focuses on understanding different perspectives and opinions of people with diverse backgrounds. As such, an online platform allows for a broader range of diverse students to enroll in the course, and therefore share their ideas with other classmates, allowing for richer discussions

Instruction: Lectures of the instructor will be recorded, in order to replicate the type of learning that occurs in a face-to-face class. Other course materials, such as the textbook, videos, readings and discussions will also be available online. Students will submit assignments and participate in discussion board posts online. All instructors will have completed OCDi (or equivalent) training.

Integrity: Students will take quizzes and exams through an online platform with a video monitoring system.

Interaction: At the discretion of the faculty, provisions and requirements would vary but generally will utilize Email, Web-Based Discussions, and Web-conferencing

Model Syllabus (Part II)

Please include the following information:

1. **Course number and title:** MBA 5870 – Information Security and Risk Management
2. **Catalog description:** Study of theories, principles and techniques of information security and risk management. The course covers security threats and countermeasures, operational and organizational security, infrastructure security, risk assessment and risk management, business continuity and disaster recovery.
3. **Learning objectives:**

Upon successful completion of the course, students will be able to:

1) Implement principles of information security. (Graduate 1,2)
2) Evaluate the various types of intrusions and attacks against computers and network systems. (Graduate 1,2)
3) Analyze and choose the tools and technologies used for providing security. (Graduate 1,2)
4) Evaluate business continuity and disaster recovery plans, and computer forensics. (Graduate 1,2)
5) Conduct risk assessment. (Graduate 1,2)

4. Course materials.
   - *Corporate Computer Security* by Randall Boyle and Raymond R. Panko, 5th edition, Pearson, 2021, ISBN-13: 9780135822784
   - Current academic literature on information systems' security such as:
     - Humayum et a. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study, Computer Engineering and Computer Science, 45, 3171-3189
     - Li, Y. and Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports, Volume 7, 8176-8186.

- Bhaskar, R. (2022). Better Cybersecurity Awareness Through Research, ISACA, Volume 3 available at https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/better-cybersecurity-awareness-through-research

5. Weekly outline of content.

Week	**Topic**	**75-minute class period equivalents**
1	Introduction to computer and network security	2 periods
2	Security goals and the Plan-Protect-Respond cycle	2 periods
3-4	Managing the *security* function (control principles, risk analysis, vulnerability testing)	4 periods
5-6	Incident and disaster response management	4 periods
7-8	Access control and site security	4 periods
9	Attack methods	2 periods
10	TCP/IP Internetworking	2 periods
11-12	Tools and technologies for providing computer and network security	4 periods
13-14	Cryptography and cryptographic systems	4 periods
15	Application security: electronic commerce and email	2 periods
16	Final Exam	2 hours
	Total	**Thirty 75-minute periods + Two hours of final exam**

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

Grade weighting may vary by instructor, but it is generally considered as follows:

- Exams (40% of total grade)
- Assignments (20% of total grade)
- Research Project/Case Study (25% of total grade)

  Sample Research Project/Case Study: Students will analyze a given information security infrastructure in light of what they have learned in class in order to discover and layout the strengths and weaknesses of the infrastructure. They will also search academic and professional literature in order to write a research paper providing a theoretical background about the weaknesses found and proposing possible solutions that can be adopted to mitigate risks of attacks.
- Final (15% of total grade)

7. Grading scale.

90% or better	A
80-89%	B
70-79%	C
60-69%	D
Less than 60%	F

8. Correlation of learning objectives to assignments and evaluation.

The students' achievement of the stated course objectives will be assessed as follow:

Objectives	Exams	Assignments	Project/Case Study	Final
1	X	X		X
2	X	X	X	X
3	X	X	X	X
4	X	X	X	X
5	X			X

Date approved by the department or school: 12/5/2022
Date approved by SBUS graduate committee: 1/31/2023
Date approved by the college curriculum committee: 2/9/2023
Date approved by the Honors Council *(if this is an honors course):*
Date approved by CAA: CGS: