Change Course CYIS 6720
Specific Course Change type selected: Title
Specific Course Change type selected: Description

1. Existing course prefix and number:
CYIS 6720

2. Proposed course title:
Cybersecurity Governance, Risk Management, and Compliance

3. Existing Banner course title:
IT Governance & Service Mgmt

4. Proposed course title to be entered in Banner:
Cybersec Gov., Risk, and Comp.

A. Please choose Yes or No to indicate if this class is a Teacher Education class:
No

B. Please choose the applicable class level:
Graduate

C. Please respond Yes if this is a current general education course and/or a course being submitted for the new WMU Essential Studies program. Please respond No if it is neither.
No

D. Explain briefly and clearly the proposed improvement.
Change the course title and description for CYIS 6720: IT Governance and Service Management to CYIS 6720: Cybersecurity Governance, Risk Management, and Compliance

E. Rationale. Give your reason(s) for the proposed improvement. (If your proposal includes prerequisites, justify those, too.).
This course was initially developed to focus on general IT Governance and Management, but it has been found that focus on IT Governance and Management, specifically ITIL, requires too much time to cover and interferes with coverage of Cybersecurity-specific governance, risk management, and compliance topics that are necessary for MS students who want to understand frameworks, approaches, and regulations necessary to manage information systems. A change in title and description would remove the focus on general IT governance and management and indicate a specific focus on Cybersecurity governance, risk management, and compliance issues. This change will ensure that MS students gain the requisite knowledge in these areas.

F. List the student learning outcomes for the proposed course or the revised or proposed major, minor, or concentration. These are the outcomes that the department will use for future assessments of the course or program.
--Understand Cybersecurity Governance strategy, goals, and objectives.
--Analyze Cybersecurity Governance processes, procedures, and measurements.
--Apply Cybersecurity Governance program components to organizational environments.
--Understand Risk Management frameworks.
--Analyze Risk Management techniques.
--Apply risk identification, risk assessment, and risk planning to organizational environments.
--Understand the various Cybersecurity regulations.
--Analyze key Cybersecurity compliance components.
--Apply Cybersecurity regulations to a particular industry segment.

G. Describe how this curriculum change is a response to student learning assessment outcomes that are part of a departmental or college assessment plan or informal assessment activities.
N/A

H. Effect on other colleges, departments or programs. If consultation with others is required, attach evidence of consultation and support. If objections have been raised, document the resolution. Demonstrate that the program you propose is not a duplication of an existing one.
None

I. Effect on your department's programs. Show how the proposed change fits with other departmental offerings.
No impact on other offerings. This course is routinely offered once a year.

J. Effects on enrolled students: are program conflicts avoided? Will your proposal make it easier or harder for students to meet graduation requirements? Can students complete the program in a reasonable time? Show that you have considered scheduling needs and demands on students' time. If a required course will be offered during summer only, provide a rationale.
No effect. This course is routinely offered once a year.

The change will help MS students focus more on essential Cybersecurity topics.

K. Student or external market demand. What is your anticipated student audience? What evidence of student or market demand or need exists? What is the estimated enrollment? What other factors make your proposal beneficial to students?
This course is offered as a core class to all MS in Cybersecurity students.

It is one (1) course out of six (6) courses from which students must select five (5).

L. Effects on resources. Explain how your proposal would affect department and University resources, including faculty, equipment, space, technology, and library holdings. Tell how you will staff additions to the program. If more advising will be needed, how will you provide for it?

How often will course(s) be offered? What will be the initial one-time costs and the ongoing base-funding costs for the proposed program? (Attach additional pages, as necessary.)
No required additional resources. This course is routinely offered once a year.

M. With the change from General Education to WMU Essential Studies, this question is no longer used.

For courses requesting approval as a WMU Essential Studies course, a syllabus identifying the student learning outcomes and an action plan for assessing the student learning outcomes must be attached in the Banner Workflow system.
Not Applicable

N. (Undergraduate proposals only) Describe, in detail, how this curriculum change affects transfer articulation for Michigan community colleges. For course changes, include detail on necessary changes to transfer articulation from Michigan community college courses. For new majors or minors, describe transfer guidelines to be developed with Michigan community colleges. For revisions to majors or minors, describe necessary revisions to Michigan community college guidelines. Department chairs should seek assistance from college advising directors or from the admissions office in completing this section.
N/A

O. Current catalog copy:
This course provides foundation-level training for IT professionals to gain an understanding of the ITIL terminology. Students will gain knowledge of the ITIL service lifecycle and the ITIL processes, roles, and functions. Students will also gain an understanding of how the service lifecycle provides effective and efficient IT services that are aligned to, and underpin, business processes.

P. Proposed catalog copy:
This course examines the many challenges of Cybersecurity governance, such as defining risk management strategies and goals, identifying Cybersecurity needs and objectives, establishing and measuring key performance indicators, and creating a continuous monitoring program. The importance of approaching Cybersecurity governance with accountability, consistency, and oversight is stressed throughout. This course will examine, discuss, and apply the various Risk Management Frameworks, such as NIST and ISO/IEC standards. Finally, this course will explore a selection of Cybersecurity regulations in various industries, such as Retail, Healthcare, Energy, and Defense to stress the importance of compliance.

Current Title and Description

CYIS 6720: IT Governance and IT Service Management

Course Prerequisites

Prerequisites: (CIS 5710 or CYIS 5710) and (CS 5710 or CYCS 5710); with a grade of “C” or better in all prerequisites.

Catalog Description

This course provides foundation-level training for IT professionals to gain an understanding of the ITIL terminology. Students will gain knowledge of the ITIL service lifecycle and the ITIL processes, roles, and functions. Students will also gain an understanding of how the service lifecycle provides effective and efficient IT services that are aligned to, and underpin, business processes.

Learning Outcomes

- Understand service management as a practice
- Understand ITIL service life cycle
- Understand generic concepts and definitions of ITIL terminology
- Understand key principles and models of ITIL service life cycle
- Be able to describe the purpose, objectives, and scope of each process in ITIL service life cycle
- Be able to explain the role, objectives, and organizational structures of each Function in ITIL
- Understand the responsibilities of each Role in ITIL

Proposed Title and Description

CYIS 6720: Cybersecurity Governance, Risk Management, and Compliance

Course Prerequisites

Prerequisites: (CIS 5710 or CYIS 5710) and (CS 5710 or CYCS 5710); with a grade of “C” or better in all prerequisites.

Catalog Description

This course examines the many challenges of Cybersecurity governance, such as defining risk management strategies and goals, identifying Cybersecurity needs and objectives, establishing and measuring key performance indicators, and creating a continuous monitoring program. The importance of approaching Cybersecurity governance with accountability, consistency, and oversight is stressed throughout. This course will examine, discuss, and apply the various Risk Management Frameworks, such as NIST and ISO/IEC standards. Finally, this course will explore a selection of Cybersecurity regulations in various industries, such as Retail, Healthcare, Energy, and Defense to stress the importance of compliance.

Learning Outcomes

- Understand Cybersecurity Governance strategy, goals, and objectives.
- Analyze Cybersecurity Governance processes, procedures, and measurements.
- Apply Cybersecurity Governance program components to organizational environments.
- Understand Risk Management frameworks.
- Analyze Risk Management techniques.
- Apply risk identification, risk assessment, and risk planning to organizational environments.
- Understand the various Cybersecurity regulations.
- Analyze key Cybersecurity compliance components.
- Apply Cybersecurity regulations to a particular industry segment.