

MCM 208: CYBERSECURITY POLICY, COMPLIANCE, AND RISK ASSESSMENT

In Workflow

1. CBA College Committee Chair (panggabean@csus.edu,joseph.taylor@csus.edu)
2. CBA Dean (ptong@csus.edu)
3. Academic Services (catalog@csus.edu)
4. Senate Curriculum Subcommittee Chair (curriculum@csus.edu)
5. Dean of Undergraduate and Graduate (Dean of Undergraduate and Graduate@csus.edu)
6. Catalog Editor (catalog@csus.edu)
7. Registrar's Office (k.mcfarland@csus.edu)
8. PeopleSoft (PeopleSoft@csus.edu)

Approval Path

1. Fri, 23 May 2025 20:19:32 GMT
Katie Dickson (katiedickson): Rollback to Initiator
2. 2026-06-02T19:10:25Z
Tota Panggabean (panggabean): Approved for CBA College Committee Chair
3. 2026-06-23T20:24:45Z
Pingsheng Tong (ptong): Approved for CBA Dean

New Course Proposal

Date Submitted: 2026-05-18T19:06:59Z

Viewing: MCM 208 : Cybersecurity Policy, Compliance, and Risk Assessment

Last edit: 2026-05-18T19:06:58Z

Changes proposed by: Zahra Aivazpour (223025621)

Contact(s):

Name (First Last)	Email	Phone 999-999-9999
Ajmal Aminee	aminee@csus.edu	916-278-7124

Catalog Title:

Cybersecurity Policy, Compliance, and Risk Assessment

Class Schedule Title:

Compliance & Risk Assessment

Academic Group: (College)

CBA

Academic Organization: (Department)

Information Systems and Business Analytics

Will this course be offered through the College of Continuing Education (CCE)?

Yes

Please specify:

CCE Only

Catalog Year Effective:

Fall 2027 (2027/2028 Catalog)

Subject Area: (prefix)

MCM - Master of Cybersecurity Management

Catalog Number: (course number)

208

Course ID: (For administrative use only.)

TBD

Units:

3

Is the ONLY purpose of this change to update the term typically offered or the enforcement of existing requisites at registration?

No

In what term(s) will this course typically be offered?

Fall, Spring, Summer

Does this course require a room for its final exam?

Yes, final exam requires a room

Does this course replace an existing experimental course?

No

This course complies with the credit hour policy:

Yes

Justification for course proposal:

The Cybersecurity Policy, Compliance, and Risk Assessment course is a critical addition to the newly proposed Master of Science in Cybersecurity Management at California State University, Sacramento. This course responds directly to the growing demand for cybersecurity professionals who not only possess technical expertise but also understand the broader organizational, legal, and regulatory environments in which cybersecurity operates.

As cyber threats continue to evolve in scale and complexity, organizations are increasingly required to comply with a wide range of standards and regulations (such as NIST, ISO 27001, and industry-specific frameworks). Consequently, there is a clear need for professionals who can interpret these frameworks, implement compliant security practices, and assess organizational risk in a structured and defensible manner.

Course Description: (Not to exceed 90 words and language should conform to catalog copy.)

Cybersecurity Policy, Compliance, and Risk Assessment provides an in-depth exploration of cybersecurity governance, regulatory compliance, and risk management. Students will analyze industry standards (e.g. NIST, ISO/IEC 27001), legal frameworks (e.g. GDPR, HIPAA, SOX), and best practices for risk mitigation. The course covers incident response planning, auditing procedures, and enterprise security policy development. Through case studies and hands-on projects, students will gain practical insights into cybersecurity governance, enabling them to implement effective security policies and ensure compliance in dynamic business environments.

Are one or more field trips required with this course?

No

Fee Course?

No

Is this course designated as Service Learning?

No

Is this course designated as Curricular Community Engaged Learning?

No

Does this course require safety training?

No

Does this course require personal protective equipment (PPE)?

No

Does this course have prerequisites?

Yes

Prerequisite:

Admission to the MS in Cybersecurity Management program

Prerequisites Enforced at Registration?

Yes

Does this course have corequisites?

No

Graded:

Letter

Approval required for enrollment?

No Approval Required

Course Component(s) and Classification(s):

Seminar

Seminar Classification

CS#05 - Seminar (K-factor=1 WTU per unit)

Seminar Units

3

Is this a paired course?

No

Is this course crosslisted?

No

Can this course be repeated for credit?

No

Can the course be taken for credit more than once during the same term?

No

Description of the Expected Learning Outcomes and Assessment Strategies:

List the Expected Learning Outcomes and their accompanying Assessment Strategies (e.g., portfolios, examinations, performances, pre-and post-tests, conferences with students, student papers). Click the plus sign to add a new row.

	Expected Learning Outcome	Assessment Strategies
1	Acquire, synthesize, and apply both fundamental and advanced expertise in cybersecurity and information assurance.	Exams, quizzes, case study reports, projects
2	Exhibit the ability to gather, evaluate, and analyze information from various sources to develop effective cybersecurity and information assurance policies and procedures.	Exams, quizzes, case study reports, projects
3	Create cybersecurity policies aligned with industry standards and regulatory requirements to enhance organizational security.	Exams, quizzes, case study reports, projects

Attach a list of the required/recommended course readings and activities:

MCM 208 - Syllabus.docx

For whom is this course being developed?

Majors in the Dept

Is this course required in a degree program (major, minor, graduate degree, certificate?)

Yes

Has a corresponding Program Change been submitted to Workflow?

Yes

Identify the program(s) in which this course is required:**Programs:**

MS in Cybersecurity Management

Does the proposed change or addition cause a significant increase in the use of College or University resources (lab room, computer)?

No

Will there be any departments affected by this proposed course?

Yes

Indicate which department(s) will be affected by the proposed course:

Department(s)
Computer Science

Attach evidence of consultation with the affected department

EMAIL-CSConsult.pdf

I/we as the author(s) of this course proposal agree to provide a new or updated accessibility checklist to the Dean's office prior to the semester when this course is taught utilizing the changes proposed here.

I/we agree

Attach Accessibility Checklist: (Optional at submission. Fulfills requirement to file with Dean's office.)

Accessibility Checklist.docx

University Learning Goals

Graduate (Masters) Learning Goals:

Disciplinary knowledge
Communication
Critical thinking/analysis
Information literacy

Is this course required as part of a teaching credential program, a single subject, or multiple subject waiver program (e.g., Liberal Studies, Biology) or other school personnel preparation program (e.g., School of Nursing)?

No

Is this a Graduate Writing Intensive (GWI) course?

No

Reviewer Comments:

Katie Dickson (katiedickson) (Fri, 23 May 2025 20:19:32 GMT): Rollback: In preparation for the summer 2025 Curriculum Workflow software update, all course and program proposals have been moved out of Workflow. Submissions to Workflow will resume Monday, August 11, 2025. Please contact Academic Services at catalog@csus.edu with any questions.

Key: 15275