

CERTIFICATE IN INFORMATION SECURITY MANAGEMENT



SACRAMENTO STATE

In Workflow

1. CBA College Committee Chair (ramakrishna.dantu@csus.edu)
2. CBA Dean (ptong@csus.edu)
3. Academic Services (catalog@csus.edu)
4. Senate Curriculum Subcommittee Chair (curriculum@csus.edu)
5. Faculty Senate Executive Committee Chair (kathy.honeychurch@csus.edu)
6. Faculty Senate Chair (kathy.honeychurch@csus.edu)
7. Dean of Graduate (s.storms@csus.edu)
8. Dean of Undergraduate (shaw@csus.edu)
9. Provost (maguirem@csus.edu)
10. President (khtudor@csus.edu)
11. Chancellor's Office (s.storms@csus.edu)
12. Board of Trustees (torsetj@csus.edu)
13. WASC (elisa.trimboli@csus.edu)
14. Catalog Editor (catalog@csus.edu)
15. Graduate Studies (jdsmall@csus.edu; mxiong@csus.edu)
16. Registrar's Office (k.mcfarland@csus.edu)

Approval Path

1. Fri, 23 May 2025 20:18:40 GMT
Katie Dickson (katiedickson): Rollback to Initiator
2. 2026-06-02T19:25:22Z
Tota Panggabean (panggabean): Rollback to Initiator
3. 2026-09-25T19:28:05Z
Ramakrishna Dantu (ramakrishna.dantu): Approved for CBA College Committee Chair
4. 2026-09-25T20:17:31Z
Pingsheng Tong (ptong): Approved for CBA Dean

New Program Proposal

Date Submitted: 2026-09-10T18:48:54Z

Viewing: Certificate in Information Security Management

Last edit: 2026-09-10T18:48:53Z

Changes proposed by: Zahra Aivazpour (223025621)

Academic Group: (College)

Business

Academic Organization: (Department)

Information Systems and Business Analytics

Catalog Year Effective:

2027-2028 Catalog

NOTE: This degree major program will be subject to program review evaluation within six years after implementation.

Individual(s) primarily responsible for drafting the proposed degree major program:

Name (First Last)	Email	Phone 999-999-9999
Zahra Aivazpour	zahra.aivazpour@csus.edu	916-278-7123

Program Snapshot**Type of Program:**

Certificate

Title of the Program:

Certificate in Information Security Management

Designation: (degree terminology)

Certificate - Graduate

Delivery Mode:

Fully Face to Face

Hybrid

Fully Online

Support Mode:

Self Support

What is the instructional modality of all courses in this program?

Asynchronous

Synchronous

Both Asynchronous and Synchronous

Please see the CSU/CIP Code Crosswalk: https://www.calstate.edu/csu-system/administration/academic-affairs/academic-programs-innovation-and-faculty-development/Documents/CSU_Codes_to_CIP_2020.pdf

Is this a pilot program?

No

Establishment of a master's degree program should be preceded by a national professional accreditation of the corresponding bachelor's degree major program.

Will this program require accreditation?

No

Provide a clear, concise overview of the program proposal (new or change) and provide a justification. For NEW programs describe the purpose and focus of the program, identify the target student population(s), and highlight key strengths and distinguishing features of the program.

The proposed Certificate in Information Security Management is a specialized program aimed at developing participants' ability to lead and manage organizational security efforts. The curriculum focuses on core areas such as risk management, information security policies, regulatory compliance, incident response, and cybersecurity leadership. The program is designed for IT professionals and managers seeking to transition into information security roles or enhance their cybersecurity expertise. It provides flexibility for working professionals and prepares students for industry certifications such as CISM.

Justification:

High Industry Demand: As cyber threats become more frequent and sophisticated, organizations require skilled professionals to manage and lead their information security programs. This program addresses the critical need for security leadership.

Leadership Focus: While many programs emphasize technical skills, this certificate prioritizes the governance, policy, and strategic aspects of cybersecurity, filling a gap for professionals who manage security from a business perspective.

Career Advancement: The certificate enables professionals to gain the qualifications and skills necessary to pursue advanced roles like Information Security Manager, IT Governance Officer, and CISO, roles that are essential in modern organizations.

Regulatory Pressures: Growing regulations such as GDPR, HIPAA, and ISO/IEC 27001 increase the demand for professionals who can ensure compliance, making this program highly relevant across industries.

University Learning Goals

Graduate (Masters) Learning Goals:

Disciplinary knowledge
Communication
Critical thinking/analysis
Information literacy
Professionalism
Intercultural/Global perspectives

Will this program be 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

Curriculum Alignment and Assessment

Program Goals

Provide a brief statement of the program's overarching goals and priorities: • Describe the program's mission, focus, and intended impact on students. • Identify broad areas of emphasis (e.g., career preparation, research, community engagement, leadership development). • Goals may be aspirational or developmental and do not need to be directly measurable.

Program Goals Statement

The Certificate in Information Security Management aims to prepare students to effectively manage and lead organizational information security efforts. The program emphasizes career and leadership development by building knowledge in risk management, information security policies, regulatory compliance, incident response, governance, and cybersecurity leadership. It seeks to equip students with the managerial and strategic competencies needed for careers in information security management, IT governance, and cybersecurity leadership while introducing them to knowledge areas associated with industry-recognized certifications such as the Certified Information Security Manager (CISM). Through an applied and industry-relevant curriculum, the program aims to strengthen students' ability to align information security initiatives with organizational objectives and address evolving cybersecurity, regulatory, and governance challenges.

Program Learning Outcomes

Provide measurable, program-specific learning outcomes that reflect the most important competencies students will demonstrate upon completion of the program. Programs are expected to assess and use PLOs for continuous improvement.

Program Learning Outcomes

Learning Outcome

Develop cybersecurity and information assurance strategies to current, practical, and important contexts and situations within the field.

Demonstrate ability to integrate cybersecurity and information assurance policies and procedures within development and operations environments.

Articulate an understanding of professional integrity and the ethical and legal implications of the implementation of cybersecurity and information assurance.

Learning Outcomes Display

Course Code	PLO 1	PLO 2	PLO 3
-------------	-------	-------	-------

Please attach a Comprehensive Program Assessment Plan

Assessment_Certificate_Information Security Management .docx

Please attach a Curriculum Map Matrix

Information Security Management_Certificate_SmartPlanner2025.docx

Please attach a Five-Year Budget Projection. For NEW programs, also attach a Budget Narrative.

budget draft_foundations_certificate.xlsx

Please attach the updated roadmap:

Information_Security_Management_Certificate_Roadmap_2025.xlsx

Catalog Description (catalog copy):

The Certificate in Information Security Management is designed to prepare professionals for leadership roles in managing and safeguarding organizational information assets. This program focuses on strategic and managerial aspects of cybersecurity,

equipping participants with the knowledge to develop, implement, and oversee security policies and risk management strategies. Students will explore key areas such as information governance, regulatory compliance, access control, incident response, and business continuity planning.

Admission and Continuation Requirements (catalog copy): minimum GPA and prerequisites (if applicable), required coursework or preparation, portfolio, test scores, and/or letters of recommendation. For graduate programs: expectations for a relevant bachelor's degree (required or preferred disciplines, prerequisite knowledge, or equivalent experience), include evidence that program requirements conform to the minimum requirements for the culminating experience, as specified in Title 5 Section 40510 The Master's Degree and Section 40511 The Doctoral Degree.

Admission to this certificate is open to domestic and international students who meet the following criteria:

1. Academic Standing, Degree, and GPA
Four-year bachelor's degree or equivalent with a minimum GPA of 2.5.
2. Statement of Purpose
Applicants must submit a Statement of Purpose describing their academic background, and professional experience.
3. Résumé
Applicants must submit a current résumé outlining relevant academic preparation, professional experience, and technical skills.
4. Letters of Recommendation
Applicants must submit two letters of recommendation from individuals who can speak to the applicant's academic ability, professional readiness, or potential for success.
5. English Language Proficiency (if applicable)
A foreign language test is required for applicants who earned their undergraduate degree from a country where the official language of instruction is not English. Applicants must submit official English proficiency scores (Institution Code: 4671) from one of the following exams taken within the past two years:
TOEFL iBT (minimum score of 4 on the ETS 1–6 scale)
IELTS: minimum band score of 6.0
PTE Academic: minimum score of 50
6. At least 6 units in financial reporting/audit and telecommunication and networking courses, with minimum grades of "C" or higher, are required for applicants with less than 3 years of cybersecurity-related work experience.

Program Requirements (catalog copy):

List of courses (Total units: 12)

Cores (9 units)

MCM 207 Governance, Cybersecurity Management and Strategy
MCM 208 Cybersecurity Policy, Compliance, and Risk Assessment
MCM 209 Cybercrimes, Forensics and Incident Handling

Electives (3 units)

MCM 211 Security Practices in SDLC
ACCY 212 Forensic Accounting & Fraud Examination
MCM 213 AI and ML Techniques for Cybersecurity
MCM 214 Blockchain Technology
ACCY 216 Accounting Information systems Audit and Control
MCM 217 Data Driven Cybersecurity

Reviewer Comments:

Katie Dickson (katiedickson) (Fri, 23 May 2025 20:18:40 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.

Tota Panggabean (panggabean) (Tue, 02 Jun 2026 19:25:22 GMT): Rollback: Additional review is required as per ADAP office.

Key: 588