

MS IN CYBERSECURITY 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. 2026-06-02T19:25:33Z
Tota Panggabean (panggabean): Rollback to Initiator
2. 2026-09-25T19:27:56Z
Ramakrishna Dantu (ramakrishna.dantu): Approved for CBA College Committee Chair
3. 2026-09-25T20:15:58Z
Pingsheng Tong (ptong): Approved for CBA Dean

New Program Proposal

Date Submitted: 2026-09-16T14:31:12Z

Viewing: MS in Cybersecurity Management

Last edit: 2026-09-16T14:31:09Z

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

Academic Master Plan Projection

Has this degree been approved for inclusion in the Academic Master Plan?

Yes

Attach Projected Degree Proposal form:

ProjectedDegreeProposalMCM.docx

New degree major proposals must receive prior approval for inclusion in the Academic Master Plan before a New Program proposal can be submitted to Workflow. Submissions to the AMP can be made through the Miscellaneous Request form.

Program Snapshot

Type of Program:

Major

Title of the Program:

MS in Cybersecurity Management

Designation: (degree terminology)

Master of Science

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

Does this major plan to include any formal options, concentrations, or special emphases?

No

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

TMC Templates: <https://c-idssystem.org/transfer-efforts/>

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?

Yes

Anticipated date of accreditation request:

will include in our next AACSB review (2032)

Provision for meeting specialized accreditation requirements, where applicable:

NA

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 Master of Science in Cybersecurity Management is designed to equip students with both technical and managerial skills to combat evolving cyber threats. The program emphasizes a balanced approach, offering coursework in cloud and IoT security, ethics, governance, forensics, secure software development, and risk management. Through practical learning experiences, students will develop the expertise needed for key roles like cybersecurity analyst, security architect, and Chief Information Security Officer.

(CISO). The program will prepare graduates to secure information systems, design robust cybersecurity frameworks, and ensure regulatory compliance in diverse industries.

Justifications:

High Industry Demand: Cybersecurity professionals are in high demand across industries due to the increasing frequency of cyberattacks and data breaches. This program will help meet the urgent need for skilled professionals.

Comprehensive Curriculum: The integration of both technical and managerial aspects ensures students are well-prepared to address multifaceted cybersecurity challenges, making them competitive in the job market.

Hands-On Learning: Offering real-world simulations, capstone projects, and certifications provides students with practical skills that enhance employability.

Career Versatility: Graduates will be equipped to fill various high-paying, in-demand roles across sectors such as finance, healthcare, government, and technology.

Global Relevance: With increasing regulatory requirements worldwide (e.g. GDPR, HIPAA), this program ensures graduates are well-versed in compliance, making them essential assets for organizations needing to navigate legal and ethical obligations.

Enrollment Projections

Demonstrate realistic, evidence-based enrollment expectations. • Provide projected enrollment (headcount) for Year 1, Year 3, and Year 5 after implementation. • Describe the evidence and assumptions used to develop the above projections. • Provide a summary of at least three years of enrollments (new and total) for existing programs within the department that are academically related to, or likely to share student populations, curricular resources, or instructional capacity with, the proposed program.

1st Year Enrollment: 20; 3rd Year Enrollment: 30; 5th Year Enrollment: 30

Evidence and assumptions behind the projections

- A commissioned third-party feasibility study (UPCEA, June 2024) surveyed Sacramento State undergraduate business alumni. Of 93 completed surveys, 23 respondents identified the MS in Cybersecurity Management as the proposed master's degree of greatest interest to them. Within that group, 11 respondents (48%) were extremely or very interested in the program and 5 (24%) said they were extremely or very likely to enroll in a cybersecurity management master's within two years. We report counts alongside percentages because the interested subgroup is small.
- Fifteen regional opinion leader interviews (CISOs, cyber risk specialists, and IT managers in the energy, utilities, government, and cybersecurity sectors) confirmed employer demand for management track cybersecurity graduates and interest in sponsoring employees. A third of surveyed alumni report employer tuition reimbursement benefits for master's degrees.
- Near absence of regional supply. Only two master's completions in the relevant cybersecurity CIP codes were recorded in the 12 county primary region across 2018 to 2022, and UPCEA identified only one competitor program in the primary region, the University of the Pacific's online MS in Cybersecurity.
- The projections are deliberately conservative relative to these demand indicators. They reflect a new program ramp and cohort capacity in a management focused format built for working professionals.

Three-year enrollment history of related department programs

Declared undergraduate majors in the corresponding baccalaureate concentration (BS in Business Administration, Management Information Systems) show steady growth:

- 2023: 241 declared majors
- 2024: 275 declared majors
- 2025: 311 declared majors, a 29% increase over the period

The MS in Business Analytics (MSBA) is the department program most likely to share student populations, curricular resources, and instructional capacity with the proposed program.

Enrollment and Admissions: Fall 2023: 25 new enrollments, 58 total enrollments, 50 complete applications, and 43 admits;

Fall 2024: 24 new enrollments, 144 total enrollments, 166 complete applications, and 122 admits;

Fall 2025: 30 new enrollments, 110 total enrollments, 106 complete applications, and 77 admits.

Degrees Confirmed: Academic Year 2022–23: 28;

Academic Year 2023–24: 31;

Academic Year 2024–25: 31.

University Learning Goals

Graduate (Masters) Learning Goals:

Disciplinary knowledge

Communication
 Critical thinking/analysis
 Information literacy
 Professionalism
 Intercultural/Global perspectives
 Research (optional)

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 Master of Science in Cybersecurity Management aims to prepare students to effectively address complex cybersecurity challenges through the integration of technical, managerial, and strategic competencies. The program emphasizes career preparation and leadership development by building advanced knowledge in areas such as cloud and IoT security, cybersecurity governance, digital forensics, secure software development, risk management, ethics, and regulatory compliance. Through applied learning experiences, the program seeks to develop students' ability to secure information systems, assess and manage cybersecurity risks, design effective security frameworks, and align cybersecurity initiatives with organizational objectives. The program prepares graduates for a broad range of technical and leadership roles, including cybersecurity analyst, security architect, cybersecurity manager, and Chief Information Security Officer (CISO). Through a comprehensive and industry-relevant curriculum, the program aims to develop cybersecurity professionals capable of leading organizational security efforts and responding to evolving technological, regulatory, and ethical challenges across diverse industries.

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

PLO 1: Integrate and apply knowledge and skills of cybersecurity and information assurance to current and practical contexts and situations.

PLO 2: Communicate analytics findings to decision makers in a variety of formats appropriate to the audience.

PLO 3: Demonstrate the ability to think creatively, analytically, and critically when confronted with business problems.

PLO 4: Communicate key knowledge of cybersecurity and information assurance with clarity and purpose, within the field and broader business contexts.

PLO 5: Our graduates demonstrate an understanding of professional integrity and the ethical and legal implications of the application of cybersecurity and information assurance.

PLO 6: Develop business analytics implementations that represent multicultural perspectives and global awareness.

Learning Outcomes Display

Course Code	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5	PLO 6
-------------	-------	-------	-------	-------	-------	-------

Strategic Case for the Program

Provide specific evidence of alignment: • Explain how the program advances CSU Forward priorities. • Describe alignment with campus mission, strategic plan, and/or academic priorities. • Identify the institutional, regional, or system-level need or gap this program addresses. • Explain how the program complements existing CSU programs.

How the Program Advances CSU Forward Priorities

The program supports CSU Forward's priorities of economic mobility, sustainable affordability, and statewide impact. It provides an efficient pathway for recent graduates and working professionals to develop career-ready skills. The applied curriculum prepares graduates for high-demand technical and leadership positions while strengthening California's cybersecurity workforce.

Alignment with Campus Mission, Strategic Plan, and Academic Priorities

The program advances Sacramento State's emphasis on learning with an academic and community return on investment by preparing students for strong employment outcomes in a rapidly growing field. It also supports the University's priorities related to student success and applied learning. The program directly aligns with the College of Business Strategic Plan through its focus on digital innovation, high-demand graduate education, and experiential learning. Flexible delivery supports access for working professionals and historically underserved students, and the program's innovative focus strengthens Sacramento State's regional impact and national reputation.

Institutional, Regional, and System-Level Need

The program addresses the growing need for professionals who combine technical cybersecurity knowledge with expertise in management, governance, risk, ethics, and regulatory compliance. Nationally, employment of information security analysts is projected to grow 21% from 2025 to 2035, with approximately 14,100 openings annually. CyberSeek documented 514,359 job listings for dedicated cybersecurity positions and adjacent technical positions requiring substantial cybersecurity skills between May 2024 and April 2025, including 44,344 listings in California. CyberSeek also calculated a national supply–demand ratio of 74%, indicating a continuing gap between the potential supply of cybersecurity workers and perceived employer demand. This need is particularly important in the Sacramento region, where government agencies, healthcare organizations, financial institutions, educational institutions, and technology firms manage sensitive information and require professionals capable of connecting cybersecurity operations with organizational strategy and regulatory requirements. The program addresses a gap in graduate-level cybersecurity management education at Sacramento State and supports regional and statewide workforce needs.

How the Program Complements Existing CSU Programs

Although several CSU campuses offer cybersecurity-related master's degrees—including San José State University, California State University, San Bernardino, and San Diego State University—the M.S. in Cybersecurity Management at Sacramento State differs from similar programs offered by other CSU campuses and neighboring institutions in several ways:

Local Focus: The program primarily serves students from Sacramento and surrounding communities, with a curriculum designed to address regional workforce needs.

Flexible Delivery: The program offers flexible course-delivery options to accommodate different learning preferences, work commitments, and schedules.

Public-Sector Connections: The program draws on Sacramento State's proximity to state government and its connections with public-sector organizations, providing students with opportunities to collaborate on applied projects, gain practical experience, and develop professional networks.

Demonstrate workforce demand for the program using verifiable labor market data and documented employer input: • Identify 3–5 key occupations aligned with this program. • Summarize demand at the regional and/or state level (national data may supplement but not replace regional analysis) and how the data support the need for this program. Include: • Projected job growth • Median or entry-level wages • Current employment levels (if relevant) • Specific data sources (e.g., CA EDD, BLS, Lightcast) • Describe employer or industry input used to validate demand. • Provide evidence of student demand (if available).

Key occupations aligned with the program

- Information Security Analysts (SOC 15-1212)
- Computer and Information Systems Managers (SOC 11-3021)
- Computer Systems Analysts (SOC 15-1211)
- Computer Network Architects (SOC 15-1241)
- Database Administrators (SOC 15-1242)

Regional demand: 12 county Sacramento primary region (UPCEA/Lightcast 2024.1)

- There were 27,291 jobs across the select occupations in 2024, projected to grow 7% (1,858 additional jobs) by 2034, with 1,984 average annual openings driven largely by replacement demand.
- Information Security Analysts are the fastest growing select occupation regionally at 26% growth from 2024 to 2034, with a regional median wage of \$127,352. Computer and Information Systems Managers are projected to grow 14% with a median of \$148,728. Median annual earnings across the select occupations are \$103,426 regionally, above the size adjusted national average of \$94,793.
- Employer effort is visible in postings. There were 26,224 total postings (7,560 unique) for the select occupations in the primary region in calendar 2023, of which 2,038 explicitly mentioned a master's degree. Top regional employers posting these roles include the University of California, Intel, the California State University, and PG&E. The largest employing industries are computer systems design services (14.6%) and state government excluding education and hospitals (14.0%). State government is a distinctive and stable source of demand in the capital region.

Statewide and national corroboration

- BLS Occupational Outlook Handbook: employment of information security analysts is projected to grow roughly 29% from 2024 to 2034, about seven times the average across all occupations, from a 2024 base of approximately 182,800 jobs, with about 16,000 openings per year and a May 2024 median wage near \$124,910.
- CyberSeek (NIST/CompTIA): approximately 514,000 U.S. cybersecurity job openings in the 12 months ending March 2026, with a supply to demand ratio near 74%, meaning roughly one in four posted cybersecurity roles goes unfilled. State and metro level figures for California and the Sacramento area are available on the CyberSeek heat map and can be appended.

Employer and industry input

- UPCEA conducted 15 structured interviews with regional opinion leaders including CISOs, senior cyber risk specialists, and IT managers. Sentiment on demand for master's level cybersecurity management professionals was positive. Leaders reported persistent difficulty filling roles, especially senior roles requiring both technical depth and leadership, and identified communication, strategic thinking, risk management, and leadership as the crucial differentiators the proposed program targets.
 - Several interviewees indicated they would encourage employees to enroll, citing tuition reimbursement programs and Sacramento State's regional reputation relative to online alternatives. Interviewees also emphasized that the program must be deliverable outside normal business hours, which the proposed format accommodates.
- Evidence of student demand
- From the alumni survey described in Q1: 11 of 23 interested respondents (48%) were extremely or very interested in the program, 5 (24%) extremely or very likely to enroll within two years, and 10 (44%) rated stackable graduate certificates extremely or very valuable, which supports the stackable credential design described in Q3.

Describe the program's value to students, how it is meaningfully differentiated from existing offerings, and how it will be sustained and remain current over time:

- Describe the factors expected to attract and serve students.
- Describe how this program will be meaningfully differentiated from existing offerings.
- Describe how the curriculum, pedagogy, and program structure will remain responsive to evolving disciplinary, workforce, technological, and student needs over time.
- How will the program prepare students to work ethically and effectively in environments increasingly shaped by AI and emerging technologies?

Factors expected to attract and serve students

- A management focused degree at the intersection of cybersecurity and business, housed in an AACSB accredited college. The program prepares students for leadership roles in security management, governance, risk, and compliance, audit, and assurance rather than duplicating purely technical programs.
- A clear return on investment for working professionals. Regional medians run from \$127,352 for information security analysts to \$148,728 for information systems managers, and a third of surveyed alumni have access to employer tuition reimbursement.
- A format built for working professionals. The program offers face to face, hybrid, and online options with evening delivery, a cohort structure, and curriculum relevant to the professional certifications employers named, including CISA and CISM.
- Stackable graduate certificates that allow professionals to earn a credential on the way to the degree, or to begin without committing to the full program at the outset.
- CSU level affordability relative to the identified competition. The one competitor program in the primary region costs approximately \$38,400, and the average profiled competitor program approximately \$37,363.

Meaningful differentiation from existing offerings

- There is effectively no regional supply. Only two master's completions in the relevant CIP codes were recorded in the primary region over 2018 to 2022, and there is a single competitor program, which is technically oriented and offers no certificates or specializations. No CSU or UC program in the capital region combines cybersecurity with management education.
- Differentiators identified by employers and built into the design: an explicit business and cybersecurity intersection; a governance, risk, and compliance orientation that interviewed employers said they rarely see in the region; stackable graduate certificates, favored by both employers and alumni; recognition of relevant professional certifications and experience; and curriculum developed with industry input.
- Position in the state capital. The program is well placed to serve public sector cybersecurity needs, which supports the campus Anchor University strategy.

Remaining current over time

- The curriculum is governed by the College's AACSB continuous improvement and Assurance of Learning processes, with program level learning goals assessed on a regular cycle and closed loop revisions.
- The MISBA industry advisory board, which is already established, reviews the curriculum annually against the evolving threat landscape, including cloud security, zero trust architecture, supply chain risk, and IoT, and against current certification frameworks.
- Modular course design and the elective and certificate architecture allow individual topics to be refreshed without a full program revision.

Preparing students for environments shaped by AI and emerging technologies

- AI is treated as both subject and tool. The curriculum includes AI use in cybersecurity management as a core topic area, covering AI driven threats such as AI enabled malware and social engineering, AI governance and emerging regulation, and the responsible use of AI in security operations.
- Ethical practice is assessed at the program level. PLO 5 requires graduates to demonstrate an understanding of professional integrity and the ethical and legal implications of the application of cybersecurity and information assurance, and it is measured through the College's Assurance of Learning cycle.
- Industry data show AI is among the largest skills gaps cybersecurity employers report, and a growing share of cybersecurity postings reference AI skills. The program's governance, risk, and ethics core is aimed directly at that gap.

Please attach a Comprehensive Program Assessment Plan

Assessment_MSinCSMgmt.docx

Please attach a Curriculum Map Matrix

MSinCybersecurityMgmt_Smart Planner 2025 - Copy.docx

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

budget draft_MSin CSgmt.xlsx

Please attach the updated roadmap:

MS_in_Cybersecurity_Management_Roadmap_2025.xlsx

Catalog Description (catalog copy):

The Master of Science in Cybersecurity Management is a comprehensive graduate program designed to equip students and professionals with advanced skills in protecting digital assets and managing the ever-evolving landscape of cyber threats. This program focuses on both the technical and managerial aspects of cybersecurity, offering deep insights into risk management, ethical hacking, cryptography, network security, and information assurance. Students will learn to secure information systems, protect infrastructure, and ensure compliance with global cybersecurity standards.

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 the MS in Cybersecurity Management 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, professional experience, and interest in Cybersecurity Management.

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: 30)****Core Courses (Required; 21 units)**

MCM 204 Cloud, IoT and Enterprise Security

MCM 205 Cybersecurity Foundations

MCM 206 Cybersecurity & Ethics

MCM 207 Governance, Cybersecurity Management and Strategy

MCM 208 Cybersecurity Policy, Compliance, and Risk Assessment

MCM 209 Cybercrimes, Forensics and Incident Handling

MCM 500 Culminating Experience: Advanced Topics in Cybersecurity and Information Assurance

Elective Courses (3 electives; 9 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

Please attach the Curriculum Overview

MS_Cybersecurity_Management_Curriculum_Overview.docx

Student Pipeline and Access

• Describe how the program will recruit and enroll its target student population. • Identify primary student sources (e.g., first-time, transfer, adult learners). • Describe recruitment strategies and outreach efforts. • Identify key feeder programs, pathways, or partnerships.

Primary student sources

- Working professionals in the capital region, particularly in state government, which accounts for 14% of regional employment in the aligned occupations, along with utilities and energy, health care, and financial services, who are seeking movement into security leadership roles.

- Sacramento State business alumni, especially graduates of the MIS and Accountancy concentrations, which were the two largest alumni segments expressing interest in the program, supported by a growing MIS pipeline of 311 declared majors in 2025.

- Recent graduates of regional undergraduate programs in business, information systems, and computer science, at Sacramento State and at area community colleges, seeking a management track credential.

Recruitment strategies and outreach

- Recruitment and marketing are led by the College of Business Graduate Programs Office, working in collaboration with the College of Continuing Education given the self-support structure of the program.

- Employer channel recruitment through information sessions and cohort arrangements with major regional employers identified in the posting data, including state agencies, UC and CSU, PG&E, Intel, and regional health systems, taking advantage of the roughly one third of employers offering tuition reimbursement.

- Targeted digital marketing to the regional professional workforce, alumni network campaigns, and presence at regional industry groups such as the Sacramento chapters of ISACA and ISSA.

- MISBA advisory board members serve as recruitment ambassadors. Feasibility study interviewees indicated a willingness to refer employees.

Feeder programs, pathways, and partnerships

- An internal pathway from the BSBA, particularly the MIS and Accountancy concentrations, and from other business majors.

- Stackable graduate certificates as an on-ramp for professionals not yet ready to commit to the full degree.

- Pathways with regional community college cybersecurity programs, and recognition of industry certifications and professional experience toward admission or acceleration.

• Describe how the program will support student success. • Describe academic support services available to students. • Describe career and experiential learning support. • Identify program-specific supports (e.g., advising, cohort models, mentoring). • Explain how students will access services based on delivery modality. For fully online programs (required): • Describe how advising, tutoring, library, and career services are delivered remotely. • Explain how student engagement and access are ensured.

Academic support

- A graduate program director and a staff graduate advisor will be assigned to the program, providing advising from admission through graduation. Orientation and academic standing early alert processes run through the College's Graduate Programs Office.

- Students have access to university wide support including library research consultations, writing support, and tutoring.

Career and experiential learning

- Career coaching and employer events through College career services and the University Career Center.

- Applied capstone projects with regional employers, and internship and project placements facilitated through College employer partnerships and the MISBA advisory board.

- Certification preparation aligned with coursework, with attention to the credentials employers named, including CISA and CISM.

Program-specific supports

- A cohort model that builds a peer network among working professionals.

- Mentoring connections with MISBA advisory board practitioners.

- Certificate stacking, so students earn recognized credentials on the way to the degree.

Access by delivery modality

- The program is offered in face to face, hybrid, and online formats. Advising is delivered in person and by Zoom with evening availability for working students, and all student services functions including advising, registration, and financial aid are accessible remotely.

- For students in the online pathway, advising and tutoring are available by Zoom and through the University's online tutoring platform, with full remote access to library databases, e-reserves, and librarian consultations, and virtual career services including remote coaching and virtual employer sessions.

- Engagement is supported through the cohort structure, synchronous session components, online faculty office hours, and learning management system engagement monitoring with proactive outreach to students who fall behind.

Resources for Implementation

Curriculum Resource Implications

• Describe resource implications of curriculum development and delivery. • Identify the number and level of new courses required (if any). • Describe the purpose and development timeline for new courses. • Explain how curriculum design aligns with available faculty and instructional resources.

Resource Implications of Curriculum Development and Delivery

All required courses have already been developed by faculty in the Management Information Systems and Business Analytics (MISBA) Department and the Accounting Department. The corresponding Form A proposals have been submitted through the CourseLeaf system.

Number and Level of New Courses Required

The program consists of 13 newly developed graduate-level courses. All course proposals have already been submitted for approval through CourseLeaf system.

Purpose and Development Timeline for New Courses

The courses were developed to provide an integrated curriculum covering the technical, managerial, strategic, ethical, and regulatory dimensions of cybersecurity. The curriculum includes cloud and IoT security, cybersecurity foundations, governance and strategy, ethics, policy and compliance, risk assessment, cybercrime, digital forensics, incident response, electives, and a culminating experience.

Alignment with Faculty and Instructional Resources

The curriculum was designed around the expertise of existing faculty in the MISBA and Accounting departments. The program will not change the number of faculty needed, and current faculty resources are sufficient to deliver the curriculum. Existing classroom facilities are also adequate. Courses may use HyFlex-enabled classrooms in the College of Continuing Education's current self-support facility.

Below, we list the faculty members who may potentially teach courses in the program.

Faculty and Staffing

List faculty members, with rank, appointment status, highest degree earned, date and field of highest degree, and professional experience (including publications if the proposal is for a graduate degree), who would teach in the proposed program:

Name	Rank	Appointment Status	Highest Degree Earned	Year of Highest Degree Earned (YYYY)	Publications/Professional Experience
Zahra Aivazpour	Assistant Professor	Full Time	Doctorate	2020	Certified in Cybersecurity, numerous related publications: Aivazpour, Z., & Beebe, N. L. (2025). Understanding the role of justification mechanisms in cyberbullying: Relative acceptability, postponed justification, and comparative justification. <i>Computers in Human Behavior Reports</i>, 19, 100704. Aivazpour, Zahra, and Chino Rao. "A Replication Study of the Impact of Impulsivity on Risky Cybersecurity Behaviors." <i>AIS Transactions on Replication Research</i> 8.1 (2022): 3. Aivazpour, Zahra, Rohit Valecha, and Rajarshi Chakraborty. "Data Breaches: An Empirical Study of the Effect of Monitoring Services." <i>ACM SIGMIS Database: the DATABASE for Advances in Information Systems</i> 53.4 (2022): 65-82. Aivazpour, Z., and Rao, V. S. (2020). Information Disclosure and Privacy Paradox: The Role of Impulsivity. <i>ACM SIGMIS Database: the DATABASE for Advances in Information Systems</i>, 51(1), 14-36.

Joseph Taylor	Associate Professor	Full Time	Doctorate	2016	Previous executive responsible for IT Governance, publications: Taylor, J., Dantu, R., & Wells, T. (2024). Promoting guest satisfaction: Digital platforms as a means to encourage economic development in hospitality. <i>International Journal of Hospitality & Tourism Administration</i>, 25(2), 406-435. Taylor, J., Sahaym, A., & Vithayathil, J. (2023). Do CIOs matter in the face of exogenous shocks? An examination through upper Echelon theory. <i>International journal of innovation and technology management</i>, 20(02), 2350005.
Sadaf Ashtari	Associate Professor	Full Time	Doctorate	2016	Numerous related publications: Ashtari, S., & Taylor, A. D. (2022). The internet knows more than my physician: qualitative interview study of people with rare diseases and how they use online support groups. <i>Journal of medical Internet research</i>, 24(8), e39172. Ashtari, S., & Taylor, A. (2023). Patients with rare diseases and the power of online support groups: implications for the medical community. <i>JMIR formative research</i>, 7, e41610.
Ramakrishna Dantu	Assistant Professor	Full Time	Doctorate	2016	Member of ISACA, numerous publications: Taylor, J., Dantu, R., & Wells, T. (2024). Promoting guest satisfaction: Digital platforms as a means to encourage economic development in hospitality. <i>International Journal of Hospitality & Tourism Administration</i>, 25(2), 406-435. For love or money? Examining reasons behind OSS developers' contributions. <i>Information systems management</i> 39 (2), 122-137

Evren Eryilmaz	Associate Professor	Full Time	Doctorate	2011	Publications: Ahmed, Z., Eryilmaz, E., Kumar V., & K. U. (2025) Control Balancing in Offshore Information Systems Development: Extended Process Model. Communications of the Association for Information Systems, 56(1), 31. (A Level Journal on the ABDC Journal List) (Acceptance Rate 7%) Eryilmaz, E., Thoms, B., & Ahmed, Z. (2024) Theory-guided multiclass text classification in online academic discussions. Journal of Computer Information Systems (2024): 1-12 (A Level Journal on the ABDC Journal List) (Acceptance Rate 8%)
----------------	---------------------	-----------	-----------	------	---

Xiaolin Lin	Assistant Professor	Full Time	Doctorate	2022	1. Wang, X., Lin, X.*, & Shao, B. (2025). Security and privacy protection in developing ethical AI: A mixed-methods study from a marketing employee perspective. <i>Journal of Business Ethics</i>, 200, 373-392. (*Corresponding author) (FT50, ABS 3, ABDC: A) 2. Lin, X., Sarker, S., Featherman, M., & Wang, X. (2025). A multiplatform study of social commerce success: Theoretical development and empirical validation. <i>International Journal of Electronic Commerce</i>, 29(1), 4-38. (ABS 3, ABDC: A) 3. Lin, X. (2025). Honest Information Sharing in Social Commerce based on ethical perceptions. <i>Journal of Computer Information Systems</i>, 65(1), 1-14. (ABDC: A) 4. Lin, X., Wang, X., Shao, B. & Taylor, J. (2024). How Chatbots Augment Human Intelligence in Customer Services: A Mixed-Methods Study. <i>Journal of Management Information Systems</i>, 41(4), 1016-1041. (FT50, ABS 4, ABDC: A*, AIS Basket of 8) 5. Wang, X., Lin, X.*, Zhang, C., & Macias, J. (2024). Establishing Consumer Trust in Social Commerce: Cognitive and Affective Appraisal. <i>Journal of Computer Information Systems</i>. (*Corresponding author) (ABDC: A) 6. Wang, X., Lin, X., & Gonzales, A. (2024). The impacts of social media on job satisfaction: Task-oriented use and relationship-oriented use. <i>International Journal of Human-Computer Interaction</i>, 40(14), 3732-3747. (*Corresponding author) (ABDC: B)
-------------	---------------------	-----------	-----------	------	--

Grace Mubako	Associate Professor	Full Time	Doctorate	2012	Strong audit background, publications: Mubako,G., Mazza T. (2023). The use of the internal audit function as management training ground and internal audit quality. <i>International Journal of Accounting, Auditing and Performance</i>, Vol. 19, No. 4, 2023 Roberts, R., Jang, D., & Mubako, G. (2023). Pandemic risk disclosure in integrated reports: after COVID#19 is hindsight 2020?. <i>Accounting & Finance</i>, 63(2), 1739-1758. Mubako, G., Bagchi, K., Udo, G., & Marinovic, M. (2020). Personal Values and Ethical Behavior in Accounting Students. <i>Journal of Business Ethics</i>, 1-16. Mubako, G., & Muzorewa, S. C. (2019). Interaction between internal and external auditors—insights from a developing country. <i>Meditari Accountancy Research</i>. Mubako, G. (2019). Internal audit outsourcing: A literature synthesis and future directions. <i>Australian Accounting Review</i>, 29(3), 532-545. Francis, R. N., Mubako, G., Olsen, L. M. (2018) Archival research considerations for CRSP data. <i>Accounting Research Journal</i> Mubako, G., & O'Donnell, E. (2018). Effect of fraud risk assessments on auditor skepticism: Unintended consequences on evidence evaluation. <i>International Journal of Auditing</i>, 22(1), 55-64. Mubako, G., Mazza, T. (2017). An Examination of Internal Auditor Turnover Intentions. <i>Managerial Auditing Journal</i>, 32(9). Rodgers, W., Mubako, G. N., & Hall, L. (2017). Knowledge management: The effect of knowledge transfer on professional skepticism in audit engagement planning. <i>Computers in Human Behavior</i>, 70, 564-574.
--------------	---------------------	-----------	-----------	------	--

Tota Panggabean	Associate Professor	Full Time	Doctorate	2015	Strong Accounting/ IS background; publications: The role of visual attention in the managerial Judgment of Balanced#Scorecard performance evaluation: Insights from using an eye# tracking device Journal of accounting research 54 (1), 113-146 Panggabean, T., & Jermias, J. (2020). MITIGATING AGENCY PROBLEMS USING THE BALANCED SCORECARD. Journal of theoretical accounting research, 15(2).
Fernanda Maciel	Assistant Professor	Full Time	Doctorate	2020	Statistics consulting and expertise Araujo Maciel, F. (2026). Unintended educational consequences of the Bolsa Família program in Brazil. International Journal of Social Economics, 1-16. Maciel, F. A., & Duarte, D. (2023). The impact of cash transfer participation on unhealthy consumption in Brazil. Health Policy OPEN, 4, 100087.

Ajmal Aminee	Lecturer	Part Time	Doctorate	2022	Current practitioner Kaiser Permanente (Group Leader, 05-2017 to 05-2022 and Product Manager - Quality, 02-2024 to date) American Technology Solutions, LLC., (Technical Director, 01-2018 to date) Planned Parenthood (Director of Analytics and Reporting, 03-2022 to 12-2023) Generative AI Uses and Challenges in Society - A Macro-level Analysis, Ajmal Aminee and Joseph Taylor. International Journal of Technology, Knowledge and Society 22 (1): 99-124 https://doi.org/10.18848/1832-3669/CGP/v22i01/99-124 Differences in Readmission and Length of Stay between Income Communities Before and During Covid-19, Ajmal M Aminee, Grand Canyon University, ProQuest Dissertations & Theses, 2022. 28971397.
--------------	----------	-----------	-----------	------	---

Enrollment and faculty positions should be shown for all discipline categories which will increase because of the new program and for all discipline categories which will decrease because of the new program. If faculty positions are to be transferred into the new program from other areas, the reductions in faculty positions should be shown on the appropriate discipline category or categories:

N/A - this program does not change the number of faculty needed to teach

Any special characteristics of the additional faculty or staff support positions needed to implement the proposed program:

Additional support staff will be provided through our Graduate Programs office as needed for student support.

Facilities and Infrastructure

Space and facilities that would be used in support of the proposed program: Show how this space is currently used and what alternate arrangements, if any, will be made for the current occupants.

CCE Classrooms; no limit for online classes; Facilities will be used in our current self-support building

Library resources to support the program, specified by subject areas, volume count, periodical holdings, etc.:

Current resources are sufficient

Equipment and other specialized materials currently available:

Current resources are sufficient; Hyflex learning classrooms are provided in our teaching facility

Additional Facilities and Infrastructure

The amount of additional lecture and/or laboratory space required to initiate and sustain the program over the next five years: Indicate any additional special facilities that will be required. If the space is under construction, what is the projected occupancy date? If the space is planned, indicate campus wide priority of the facility, capital outlay program priority, and projected date of occupancy.

Teaching will be done in existing class facilities.

Additional library resources needed: Indicate the commitment of the campus to purchase or borrow through interlibrary loan these additional resources.

NA

Additional equipment or specialized materials that will be 1) needed to implement the program and 2) needed during the first two years after initiation: Indicate source of funds and priority to secure these resource needs.

NA

External Partnerships (if applicable)

Describe partnerships that are essential to program delivery, student learning, or workforce alignment. • Identify external partners (e.g., industry, community organizations, clinical sites, school districts) that play a direct role in the program. • Describe how each partner contributes to program delivery (e.g., internships, clinical placements, co-teaching, curriculum input). • Indicate the status of partnerships (i.e., established, in development, or planned). • Describe how partnerships will be sustained over time, if critical to program success.

NA

Note: Include only partnerships that are directly tied to program implementation or student experience.

Please attach any additional files not requested above:

EMAIL-CSConsult.pdf

FollowUpConsultationMSCybersecurityProgram.pdf

Reviewer Comments:

Tota Panggabean (panggabean) (Tue, 02 Jun 2026 19:25:33 GMT): Rollback: Additional review is required as per ADAP office.

Key: 586