Applied Cybersecurity, Certificate

ASACSCERT

Are you passionate about protecting digital systems from intruders and cybercriminals? This program gives you the skills and insight needed to defeat cyber-threats.

Description

The applied cybersecurity certificate program is designed to build competencies in security operations, risk assessment, network security, and governmental and regulatory compliance in an interdisciplinary learning setting. Building upon core skills that students bring with them from their majors, students practice dealing with cyber-threats and resolving issues from multiple perspectives.

The program is offered through a collaboration between the New College of Interdisciplinary Arts and Science, the Ira A. Fulton Schools of Engineering and the W. P. Carey School of Business.

At a glance

- **College/School:** New College of Interdisciplinary Arts and Sciences
- **Location:** Polytechnic, Tempe, West Valley

Program requirements

2024 - 2025 Certificate Map
Certificate Map (Archives)

The certificate in applied cybersecurity consists of 15 credit hours of coursework, of which a minimum of 12 hours must be upper division. Six credit hours must be unique and not count towards a student's undergraduate degree. All courses used to satisfy requirements for the certificate must be passed with a "C" (2.00) or better. Students must select courses from more than one subject to fulfill certificate requirements.

Students must take CSE 365 or IFT 202 and one course each from groups A, B or C, and D; then one course from Group E for a total of five courses or 15 credit hours. It is recommended that the Group A course be taken concurrently with CSE 365 or IFT 202. The Group B or C and D courses must be taken after successful completion of CSE 365 or IFT 202. Group A through D courses must be completed successfully before enrolling in the Group E required course.

Required Course -- 3 credit hours

CSE 365: Information Assurance or IFT 202: Foundations of Information and Computer System Security (3)

Group A - Security Operations and Risk Management -- 3 credit hours

ACO 401 / CIS 401: Managing Cyber Risks in Enterprise Business Processes (3)
ACO 461: Security Operations (3)
IFT 381: Information System Security (3)

Group B - Systems and Network Security OR Group C - Forensics/Cyber Crime -- 3 credit hours

Group B - Systems and Network Security:
ACO 431: Network Security (3)
CSE 466: Computer Systems Security (3)
CSE 468: Computer Network Security (3)
IFT 458: Middleware Programming and Database Security (3)
IFT 475: Security Analysis (3)

Group C - Forensics/Cyber Crime:
ACO 331: Network Forensics Analysis (3)
CSE 469: Computer and Network Forensics (3)
FOR 350: Computer Forensics (3)
IFT 482: Network Forensics (3)

Group D - Policy -- 3 credit hours

ACO 351: Governance, Risk and Compliance (3)
ACO 402 / CIS 402: Privacy, Ethics and Compliance Issues (3)
CSE 467: Data and Information Security (3)
IFT 483: Developing Security Policy (3)

Group E - Project -- 3 credit hours

Students may take more than one semester of the Applied Project but only three credit hours will count towards the certificate.
ACO 484: Internship or ACO 499: Individualized Instruction (3)
CIS 440: Capstone in Information Systems (L) (3)
CSE 485: Computer Science Capstone Project I (L) or CSE 486: Computer Science Capstone Project II (L) (3)
IFT 401: Information Technology Capstone Project I (3)

Prerequisite courses may be needed in order to complete the requirements of this certificate.

Enrollment requirements

To enroll in this certificate program, students should have completed at least 45 credit hours in their declared majors and have a cumulative GPA of 2.00 or better.

Students should pay attention to the prerequisite courses needed for required certificate courses and to make sure to complete them before enrolling in the certificate program.

The prerequisites for CSE 365 Information Assurance are: ACO 240, CIS 235, CIS 236, CSE 220 or CSE 240; and a pre- or corequisite of CSE 310.
The prerequisites for ACO 240 Introduction to Programming Languages are: ACO 102 or CSE 205, or GIS major with GIS 222, or software engineering graduate student.
The prerequisites for CIS 235 Introduction to Information Systems are: CIS 105, 200 or 220; MAT 210, 211, 270 or 271.
The prerequisite for CSE 220 Programming for Computer Engineering is: CSE 205.
The prerequisites for CSE 240 Introduction to Programming Languages are: ACO 102 or CSE 205, or GIS major with GIS 222, or software engineering graduate student.
The prerequisites for IFT 202 Foundations of Information and Computer System Security are: IFT 101, IFT 103 and IFT 166.

A student pursuing an undergraduate certificate must be enrolled as a degree-seeking student at ASU. Undergraduate certificates are not awarded prior to the award of an undergraduate degree. A student already holding an undergraduate degree may pursue an undergraduate certificate as a nondegree-seeking graduate student.

Career opportunities

This program is an ideal supplement for students interested in careers in cybersecurity either in the private sector or within government agencies, such as the FBI, U.S. Department of Homeland Security, the National Security Agency and the U.S. Department of Defense. The certificate in applied cybersecurity provides a solid background for students interested in the following careers:

- chief information security officer
- cyber risk analyst
- information security engineer
- network security engineer
- security operations center analyst

Contact information

School of Mathematical and Natural Sciences | FAB N101
MNSadvising@asu.edu | 602-543-3000