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. This certificate is an ideal supplement for students interested in careers in cybersecurity in both the private sector and within government agencies (FBI, Homeland Security, NSA, DOD) in positions such as:

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

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 campus, Tempe campus, West campus

Program Requirements

Certificate Map (Archives)
- 2020 - 2021 Certificate Map
The certificate in applied cybersecurity consists of 15 credit hours; a minimum of 12 upper-division credit hours must be earned at ASU. 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 prefix 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 Courses -- 3 credit hours**

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

**Electives -- 9 credit hours**

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

ACO 461: Security Operations (3)
CIS 401: Managing Cyber Risks in Enterprise Business Processes (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:
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)
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 or IFT 402: Information Technology Capstone Project II (3)

Depending on a student's undergraduate program of study, 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 prerequisites needed for required certificate courses and make sure to complete prerequisite courses prior to enrolling in the certificate program.

- CSE 365 Information Assurance has prerequisites of ACO 240, CIS 235, CSE 220 or CSE 240.
- Prerequisites for ACO 240: ACO 102 or CSE 205, or GIS major with GIS 222, or software engineering graduate student
- Prerequisites for CIS 235: CIS 105, 200 or 220; MAT 210, 211, 270 or 271
- Prerequisites for CSE 220: CSE 205
- Prerequisites for CSE 240: ACO 102 or CSE 205, or GIS major with GIS 222, or software engineering graduate student

- IFT 202 Foundations of Information and Computer System Security has prerequisites of 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.

**Contact Information**