MASTER OF SCIENCE IN CYBERSECURITY MANAGEMENT

The icon appears in the title of traditional courses that are also available as a set of module courses.

Description and Outcomes

The Master of Science in Cybersecurity Management will prepare graduates for leadership roles directing and protecting critical information infrastructures. You will learn to develop, implement, evaluate, and update the cybersecurity policies and practices that allow an organization to effectively respond to the dynamic cybersecurity landscape. Graduates will be adept in the management of information continuity, asset classification and control, compliance management, and the secure administration of IT infrastructure, as well as incident response.

Purdue Global has been designated by the National Security Agency (NSA) and Department of Homeland Security as a National Center of Academic Excellence in Cyber Defense Education (https://www.nsa.gov/resources/students-educators/centers-academic-excellence/#defense) (CAE-CD). More information can be found on the following website: https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/.

Concentrations

In addition to the core program requirements, you may add a concentration to your degree plan, for which you are required to take a minimum of four courses from one of seven concentrations: Amazon Web Services (AWS) cloud technologies, blockchain technologies and apps, critical infrastructure security, data analytics, enterprise architecture systems, project management, or secure software development and quality assurance. Concentrations are not required for completion of the general program.

Program Length

The Master of Science in Cybersecurity Management program consists of a minimum of 60 to 80 quarter credit hours, depending on your choice of the general program or a concentration. Upon successful completion of the program, you will be awarded a master of science degree.

Program Outcomes

1. Theory and Principles: Evaluate theories, principles, and best practices related to the evolving global cybersecurity landscape by assessing and reviewing recent strategies.
2. Industry Research: Demonstrate the scholastic maturity to develop research topics and projects based on underlying cybersecurity principles learned throughout the program.
3. Critical Thinking: Recommend appropriate cybersecurity theories and frameworks to stakeholders to evaluate, mitigate, and manage ongoing risks, threats, and vulnerabilities in contexts of uncertainty.
4. Decision Analysis: Analyze data using accepted best practices for the purpose of synthesizing an effective and ethical cybersecurity solution.

Professional Competencies

In addition to the discipline-specific outcomes, professional competencies are integrated throughout your academic program. You can review the professional competencies associated with your academic program in the Professional Competencies (https://catalog.purdueglobal.edu/graduate/professional-competencies/) section of this Catalog.

Program Availability

For program availability, please refer to the U.S. State and Other Approvals (https://catalog.purdueglobal.edu/policy-information/university-information/accreditation-approvals-memberships/) section and Program Availability Information (https://www.purdueglobal.edu/catalog-program-availability-info.pdf).

Policies

Admissions Requirements

You must meet the below admissions requirements in addition to Purdue Global's general requirements (https://catalog.purdueglobal.edu/policy-information/admissions/).

Students entering the Master of Science in Cybersecurity Management program should already possess an in-depth knowledge of computer systems and networking technology, good mathematical and communication skills, and familiarity with Internet and wireless applications. Required information technology (IT) skillsets should be equivalent to a Bachelor of Science in Information Technology (BSIT), a Master of Science in Information Technology (MSIT), or similar degree, or an appropriate combination of IT professional certifications and experience.

Secure Software Development and Quality Assurance Concentration

To enroll in the secure software development and quality assurance concentration, you must have a minimum of 2 years of programming or software development experience.

Progression Requirements

If, for any reason, you are required to complete additional capstone hours during your program, you may complete them during the normal course of study or you may contact your Student Advisor to secure an extension. IT596 IT Graduate Capstone Extension Course is taken after IT595 Master's Capstone in Cybersecurity Management and is for the specific purpose of providing a means for capstone project completion. Approval of the Dean or the Department Chair is required for enrollment in IT596 IT Graduate Capstone Extension Course. If an extension is granted, the University will not charge tuition for the extension course; however, you will be required to pay the normal resource fee.

Certification, State Board, and National Board Exams

Certification and licensure boards have state-specific educational requirements for programs that lead to a license or certification that is a precondition for employment. Prospective and current students must review Purdue Global's State Licensure and Certifications (https://www.purdueglobal.edu/about/accreditation/licensure-state-authorizations/) site to view program and state-specific licensure information.

Licensure-track programs may limit enrollment to students in certain states; please see Purdue Global's Program Availability Information

(https://www.purdueglobal.edu/catalog-program-availability-info.pdf) to determine enrollment eligibility.

You are responsible for understanding the requirements of optional certification exams. Such requirements may change during the course of your program. You are not automatically certified in any way upon program completion. Although certain programs are designed to prepare you to take various optional certification exams, Purdue Global cannot guarantee you will be eligible to take these exams or become certified. Your eligibility may depend on your work experience, completion of education and/or degree requirements, not having a criminal record, and meeting other certification requirements.

Degree Plan

The icon appears in the title of traditional courses that are also available as a set of module courses. Module course availability may be limited to certain academic calendars. See Course Types *(https://catalog.purdueglobal.edu/policy-information/university-information/approach-to-learning/) for information about module courses.*

Program Requirements

Code	Title	Credits
Core Requirements		
IN505	Security for Analytics	4
IT513	Research and Writing for the IT Professional	4
IT527	Foundations in Data Analytics	4
IT528	Quantitative Risk Analysis	4
IT537	Introduction to Cybersecurity	4
IT540	Management of Information Security	4
IT542	Ethical Hacking and Network Defense	4
IT543	Cryptography Concepts and Techniques	4
IT544	Platforms, Applications, and Data Security	4
IT545	Wireless, Mobile, and Cloud Security	4
IT550	Computer Forensics and Investigations	4
IT590	Legal and Ethical Issues in IT	4
IT591	IT Security Auditing and Assessments	4
MM555	Applied Statistics	4
IT595	Master's Capstone in Cybersecurity Management	4
Total Core Requirements		60
Concentration Requirements		
Concentration Courses (see below)		0-20
Total Concentration Requirements		0-20
TOTAL CREDITS		**60-80**

Concentration Requirements

Students in this program are not required to select a concentration.

Amazon Web Services (AWS) Cloud Technologies

Code	Title	Credits
IN515	AWS Academy Cloud Foundations	4
IN516	AWS Academy Cloud Architecting	4
IN517	AWS Academy Cloud Developing	4
IN518	AWS Academy Data Analytics Lab	4
IN519	AWS Academy Cloud Operations	4
TOTAL CREDITS		**20**

Blockchain Technologies and Apps

Code	Title	Credits
IN530	Introduction to Blockchain	4
IT530	Computer Networks	4
IN531	Blockchain Technologies and Applications	4
IN532	Blockchain Application Development (dApps)	4
IT Elective		4
TOTAL CREDITS		**20**

Critical Infrastructure Security

Code	Title	Credits
IN554	Introduction to Critical Infrastructure Security	4
IN562	Cyber Threat Intelligence	4
IN563	Secure Supply Chain	4
IN564	Critical Infrastructure Sector Security	4
IN565	Critical Urban Infrastructure Security	4
TOTAL CREDITS		**20**

Data Analytics

Code	Title	Credits
IN500	Survey of Modern Data Analytics	4
IN501	Fundamentals of Computer Programming	4
IN502	Python Statistical Tools	4
IN504	Advanced Applications of Python	4
TOTAL CREDITS		**16**

Enterprise Architecture Systems

Code	Title	Credits
IT525	Database Design and Data Modeling	4
IT530	Computer Networks	4
IN560	Open Source Operating System Administration	4
IN561	Cloud Computing	4
IT Elective		4
TOTAL CREDITS		**20**

Project Management

Code	Title	Credits
GM591	Strategic Project Selection and Initiation	4
GM592	Project Planning and the Project Plan	4
GM593	Project Execution With Monitoring and Control	4
GM594	Project Closing, Ethics, and Professional Responsibilities	4
TOTAL CREDITS		**16**

Secure Software Development and Quality Assurance

Code	Title	Credits
IN510	Secure Software Design	4
IN511	Secure Coding	4
IN512	Advanced Secure Coding	4
IN513	System and Security Testing	4
IN514	Secure Development and Operations - SecDevOps	4
TOTAL CREDITS		**20**