CYBERSECURITY POLICY AND RISK MANAGEMENT (M.S.)

https://cps.unh.edu/online/program/ms/cybersecurity-policy-risk-management

Description

This program is offered online.

The M.S. in Cybersecurity Policy and Risk Management (CPRM) program cultivates strategic thinking, policy development, and risk-management skills for students interested in careers in business or government. The program features full-time faculty and industry experts who help blend strategy and policy with preparedness, incident response, recovery, and resilience – the heart of our security studies discipline.

Students may come from business, public administration, healthcare, finance, homeland defense and security, retail, law, insurance, and a myriad of technical and engineering disciplines. Prior experience or undergraduate degrees in technical fields are not required.

This is an online only program, taught over five 8-week terms per academic calendar year.

Requirements

The degree requires a minimum **30 graduate credits** made up of nine core courses and culminating with a required capstone experience. The capstone involves a project custom-designed by each student (in cooperation with an advisor) to address real-world or work-related challenges in cybersecurity. Students research into the chosen challenge/problem, and then synthesize and apply their knowledge to recommend solutions or other deliverables that help address the problem.

Code	Title	Credits
Core Courses (All Required)		
CPRM 810	Foundations of Cybersecurity Policy	3
CPRM 820	Policy Development and Communication	3
CPRM 830	Security Measures I	3
CPRM 840	Cybersecurity Standards, Regulations, and Laws	3
CPRM 850	Security Measures II	3
CPRM 860	Incident Response and Investigation	3
CPRM 870	Cybersecurity Risk Management	3
CPRM 880	Cybersecurity Metrics and Evaluation	3
CPRM 890	Organizations, Change Management, and Leadership	3
Concluding Experience		
CPRM 898	Capstone Project	3
Total Credits		**30**

Accelerated Master's

UNH students may be considered for "Accelerated Master's" (AM) dual degree status which permits you to begin studying for a master's degree while still finishing your bachelor's degree.

When taking courses in AM status, you earn course credit toward both your undergraduate and graduate degrees.

This saves time and money and gives a boost to your career prospects and workplace advancement.

See the Graduate School site for AM application requirements and support.

The AM option for MS CPRM is open to UNH students at Durham and Manchester campuses.

Undergraduate degrees

The MS CPRM program accepts students from all undergraduate degrees, both non-technical and technical. Students may come from business, public administration, healthcare, finance, homeland defense and security, retail, law, insurance, and a myriad of technical and engineering disciplines. Prior experience or education in technical fields is not required.

The AM program for MS CPRM also aligns with UNH's minor in Cybersecurity Policy, which means that you can earn the Cybersecurity Minor alongside your chosen major.

Timeline

- **Junior year**: Apply for the MS CPRM program under the "Accelerated Master's" (AM) option.
- **Senior year**: If accepted as an AM student, begin taking the approved classes (see below) and receive credit toward both your undergraduate and graduate degrees. For MS CPRM, you may start taking classes only in Fall or in Spring. Students **must** begin with CPRM 810 Foundations of Cybersecurity Policy as their first class.

Program Rules

All CPRM courses are taught asynchronously online in our intensive 8-week term structure and at the graduate level only. There are two consecutive terms in the Fall semester and two in the Spring.

AM students may start their MS CPRM studies only at the beginning of Fall or Spring (first taking CPRM 810 Foundations of Cybersecurity Policy). A Summer start is not permitted.

AM students are not permitted to take more than one CPRM class per term without prior approval by the CPRM program coordinator.

This rule is put into place because AM students will be starting CPRM classes while also completing bachelor degree requirements in the senior year (typically including demanding classes such as capstones or other challenging classes), and we want to preserve the best option for student success in both your undergraduate and graduate pursuits.

To complete the MS CPRM degree, students must fulfill all requirements for the program (p. 1).

Courses

While in AM status, you may take **up to 12 credits of the following courses**. These credits will apply to both your undergraduate and MS CPRM degree.

You must begin with CPRM 810 Foundations of Cybersecurity Policy (which is offered in Term 1 in the Fall and Term 3 in the Spring).

Code	Title	Credits
CPRM 810	Foundations of Cybersecurity Policy	3
CPRM 820	Policy Development and Communication	3
CPRM 830	Security Measures I	3

CPRM 840	Cybersecurity Standards, Regulations, and Laws	3
CPRM 850	Security Measures II	3
CPRM 890	Organizations, Change Management, and Leadership	3

Example Schedules

These are only examples. Once accepted into the AM option for MS CPRM, you will work with your MS CPRM advisor to establish a schedule that works best for you.

Fall Start

Course	Title	Credits
Fall		
Junior Year		
	Apply for the MS CPRM program under the "Accelerated Master's" (AM) option	
Fall of Senior Year		
CPRM 810	Foundations of Cybersecurity Policy (Term 1)	3
CPRM 830	Security Measures I (Term 2)	3
Spring of Senior Year		
CPRM 850	Security Measures II (Term 3)	3
CPRM 840	Cybersecurity Standards, Regulations, and Laws (Term 4)	3
After Bachelor's Degree Awarded		
	Transition to normal graduate student status and continue with the remaining requirements for the MS CPRM program. See important comments below re: this transition.	
	Credits	**12**
	Total Credits	**12**

Spring Start

Course	Title	Credits
Spring		
Junior Year		
	Apply for the MS CPRM program under the "Accelerated Master's" (AM) option	
Fall of Senior Year		
	Take only your undergraduate courses per your bachelor's study plan	
Spring of Senior Year		
CPRM 810	Foundations of Cybersecurity Policy (Term 3)	3
CPRM 830	Security Measures I (Term 4)	3
Summer of Senior Year		
	If you are still pursuing your bachelor's degree (e.g., will graduate in September rather than May), you may elect to take CPRM 850 in Term 5 of the summer semester.	
CPRM 850	Security Measures II (Term 5)	3
After Bachelor's Degree Awarded		
	Transition to normal graduate student status and continue with the remaining requirements for the MS CPRM program. See important comments below re: this transition.	
	Credits	**9**
	Total Credits	**9**

Transition to normal graduate student status

Upon completion and award of your undergraduate degree, you will no longer be an "AM" student but will transition to normal graduate student status.

It is important to plan for this transition in advance, as there will be both academic and financial implications to consider.

Be sure to reach out to all available advisors to help you plan for a smooth transition.

Student Learning Outcomes

- Describe & explain the conceptual framework of cybersecurity and its role in risk management; and discuss the history and various approaches to cybersecurity.
- Analyze the conceptual framework of cybersecurity, and identify & integrate the standards and other resources for the professional development, implementation, and management of cybersecurity policies and methods.
- Reflect on the organizational structures, information, and skillsets required for ongoing evaluation & revision of cybersecurity in a variety of real-world organizations.
- Communicate professionally and effectively with upper management, regulators, partners, colleagues, clients, and other end-users regarding cybersecurity planning and incident management.
- Explain & justify the needs for cybersecurity policy development, implementation, and management (within or across businesses, agencies, other organizations, industries, sectors, and nations).
- Strategize & customize cybersecurity risk management policies and processes for private or public organizations, with balanced consideration of organizational goals, regulatory mandates, industry best practices, and professional ethics.