



CAPELLA UNIVERSITY

Master of Science (MS) in **Information Assurance and Cybersecurity**
with a specialization in

Network Defense

Master of Science (MS) in Information Assurance and Cybersecurity with a specialization in

Network Defense

Capella University has been designated by the National Security Agency (NSA) and the Department of Homeland Security (DHS) as a National Center of Academic Excellence in Information Assurance/Cyber Defense (CAE IA/CD) for academic years 2014-2021.



Knowledge gained through work experience and industry certifications may help you earn academic credit toward your degree through Capella's Prior Learning Assessment process, offering you potential savings on tuition and time to completion.*

In this specialization, you have the option to earn a Network Defense Graduate Certificate as well as NSA Focus Area digital badges in Network Security Administration, Network Security Engineering, and System Security Engineering.

The Network Defense master's specialization prepares information security professionals to assess, develop, and implement solutions to safeguard the information assets and enterprise IT infrastructures of an organization. Learners examine the technical and managerial controls critical to the success of a network defense specialization, including network security controls and testing, telecommunication, cryptography, penetration testing, visualization, risk assessment, and information security regulation standards.

A University on Top of IT Industry Trends

With the emergence of globalization and outsourcing, the field of information technology poses new challenges to IT professionals who want to advance in their careers. Previously it was enough simply to stay focused on "hard" skills through IT certifications and training. Today, organizations are looking for IT professionals who also understand the business needs of the enterprise, the creative possibilities of technology, and how to integrate that technology into complex enterprise-wide systems. Capella is aware of these trends and continues to adjust its curricula to keep up with the needs of this rapidly changing, dynamic field.

*Residents of Washington may receive credit for prior learning only in the bachelor's and MBA programs.

This guide is intended to provide an overview of the specialization and is subject to change. Your enrollment counselor can provide updates, details, and Capella's official *University Catalog* that specifies your program requirements.

Career Information

Capella's Career Center proactively assists learners and alumni in developing and implementing their unique career management goals. The Career Center staff is committed to helping you move forward in your career.

RELATED EMPLOYMENT SETTINGS TO EXPLORE

- Government agencies (such as National Security Agency and US Cyber Command)
- Government system integrators
- Military
- Consulting firms
- Defense contractors
- Corporations in the following industries:
 - Publicly traded companies
 - Technology
 - Finance
 - Health care
 - Retail
- Land-based or online college or university
- Community college

RELATED JOB TITLES TO EXPLORE*

- Network security analyst
- Internet security analyst
- Exploitation analyst
- Network intelligence analyst
- Information security analyst
- Security management specialist
- Computer systems analyst
- Network and computer systems administrator
- Auditor
- Security manager
- Intelligence analyst
- Cyber security engineer
- Consultant (cyber security)
- Chief security officer
- Chief information security officer
- Adjunct or part-time faculty

SPECIALIZATION OUTCOMES

- Analyze the scope and areas of responsibility of a network defense professional
- Analyze the existing categories of network defense tool
- Apply network defense tools that will meet identified network defense needs
- Assess network defense challenges from a legal and ethical perspectives
- Analyze the network defense skills necessary for an independent contractor in the network defense field
- Appraise relationships among customers, stakeholders, legal entities, and sub-contractors in the network defense field

*Many positions require/prefer a certification (e.g. CISSP, CCSA) along with an advanced degree. We encourage you to research requirements for your job target and career goals.

Curriculum

TRANSFER CREDIT

A maximum of 12 quarter credits from previous graduate coursework may be transferred and applied to your program's requirements.

ADMISSION REQUIREMENTS

Bachelor's degree from an institution accredited by a U.S. Department of Education-recognized accrediting agency or an internationally recognized institution

Grade point average of 2.3 or higher on a 4.0 scale

This specialization is offered in the GuidedPath delivery model.

The core curriculum in this program includes and expands on the International Organization for Standardization ISO 27001 and includes the domains of knowledge represented in several leading security certifications, including CISSP®.

Learners in this specialization gain the knowledge required to sit for the Certified Ethical Hacker (CEH) and Certified Network Defense Architect (CNDA) exams.

- 12 required courses
- Total program credits: 48 quarter credits

CORE COURSES

IAS5002	Communication Skills for Today's Information Security Professional	4 quarter credits
IAS5010	Information Technology Security Fundamentals	4 quarter credits
IAS5015*	Network Security Fundamentals and Cryptography.	4 quarter credits
IAS5020*	Information Security Regulatory and Legal Environment.	4 quarter credits
IAS5025*	Network and Operating System Defense	4 quarter credits
IAS5030*	Identifying and Managing Risk.	4 quarter credits

SPECIALIZATION COURSES

IAS5210	Data Communications.	4 quarter credits
IAS5220	Network Security Controls and Testing	4 quarter credits
IAS5230	Secure Network Design and Engineering	4 quarter credits
IAS5130	Programming for Security Professionals	4 quarter credits
IAS5200	Network Architecture and Cyberoperations	4 quarter credits

CAPSTONE COURSE

Taken during the learner's final quarter:

IAS5900*	IAS Capstone	4 quarter credits
----------	------------------------	-------------------

*Denotes courses that have prerequisite(s). Refer to the course descriptions for further details.

The courses in this program may require live web conferencing activities and/or learner audio/video recordings. Learners who require assistive technology or alternative communication methods to participate in these activities should contact Disability Services to request accommodations.

Core Course Descriptions

Learners enrolled in the Master of Science in Information Assurance and Cybersecurity degree program have the option to complete multiple specializations in IAS.

IAS5002 Communication Skills for Today's Information Security Professional

4 QUARTER CREDITS

This course establishes foundational knowledge of the methodologies, nomenclature, communication skills, principles, and practices related to information assurance and security. This course also introduces current and future technological tools and practices designed to assess vulnerabilities while protecting information technology assets and intellectual property. **Must be taken during the first quarter by learners who have been admitted to the MS in Information Assurance and Cybersecurity degree program. Cannot be fulfilled by transfer or prior learning assessment.**

IAS5010 Information Technology Security Fundamentals

4 QUARTER CREDITS

In this course, learners examine the technology life cycle and identify the security principles that apply throughout system and product lifecycles. Learners identify the basic and network components in an information technology system, how they interact, and their role in system operation. Learners explore the basic role and function of network devices including routers, switches, firewalls, VPNs, and intrusion detection, and the underlying protocols and controls that contribute to their operation. Learners demonstrate skill using network security tools including operating system installation and setup and network mapping through the use of hands-on activities.

IAS5015 Network Security Fundamentals and Cryptography

4 QUARTER CREDITS

Learners apply foundational concepts of cyber-defense and information assurance to select the appropriate information security policies, procedures and controls. Learners assess specific points of vulnerability that are mitigated through the use of information security tools and policies. Finally, learners examine the mathematical theory behind cryptography and the range of information security controls and methods that use cryptography or encryption as a factor in how they function. **Prerequisite(s): IAS5010 or ITEC5010.**

IAS5020 Information Security Regulatory and Legal Environment

4 QUARTER CREDITS

Learners apply cyber-defense and information assurance controls in context of the rules and guidelines that influence them and with an understanding of the security standards, responsibilities, rules, regulations, and issues that impact a particular organization. Learners identify laws and policies related to cyber-defense and how they relate to the storage and transmission of data. Learners also study basic concepts of audit, evidence collection, and chain of custody rules. **Prerequisite(s): IAS5015.**

IAS5025 Network and Operating System Defense

4 QUARTER CREDITS

Learners identify the basic security issues in operating system (OS) design and implementation. Learners articulate the steps necessary for hardening the OS with respect to various applications and describe the various concepts in network defense. Finally, learners demonstrate network security defense techniques through hands-on activities. **Prerequisite(s): IAS5015.**

IAS5030 Identifying and Managing Risk

4 QUARTER CREDITS

Learners identify common information security risk analysis methodologies, their characteristics, pros and cons, and applications by selecting an appropriate methodology to apply to a specific organization. Learners examine the qualities, characteristics, and motivation of hackers and cyber-criminals and their attacks on information assets, with an emphasis on malware. Learners also identify vulnerabilities in hardware, software, locations, and procedures that provide an opening to criminals and create risk to organizations that collect and store data. Learners demonstrate risk assessment techniques through hands on application of software vulnerability testing tools. **Prerequisite(s): IAS5015.**

Specialization Course Descriptions

In this specialization, you will learn to manage real-time responses to security breaches using Nessus to perform vulnerability assessments, including system sanitizing and hardening in Capella's virtual lab environment.

IAS5210 Data Communications

4 QUARTER CREDITS

Learners examine architecture and issues associated with analog communication systems, as well as the protocols and methodologies used in modern digital communication systems. Learners also develop a working knowledge of the hardware, communications, management, and programming environments associated with mobile technologies, as well as a basic understanding of radio frequency communications.

IAS5220 Network Security Controls and Testing

4 QUARTER CREDITS

Learners study cryptographic algorithms, protocols, and how they protect information in various states. Learners apply methodology to detect, analyze, and mitigate vulnerabilities and threats within a network environment, and examine the latest network technologies and security issues involved in network communications. Finally, learners identify and demonstrate ways of exploiting vulnerabilities to gain access to a system through penetration testing and network forensics techniques.

IAS5230 Secure Network Design and Engineering

4 QUARTER CREDITS

Learners study abstract data types and how to apply them in solving cyber security problems related to network design and engineering. Learners also acquire knowledge of the processes and regulations associated with the analysis and evaluation of operational systems, and identify the authorities and processes needed for the approval of their operation. Finally, learners articulate how virtualization is implemented, deployed, and used, and describe the implications that interfaces between major components of virtualized systems have on security.

IAS5130 Programming for Security Professionals

4 QUARTER CREDITS

Learners in this course create scripts and programs to automate and perform simple operations, including basic security practices. Learners develop and demonstrate the skills necessary to program low level languages, perform low level operations, and develop complex, low level software, typically in the C or assembly programming language. Learners apply these skills by programming and testing assembly-based, stand-alone, secure network management tools.

IAS5200 Network Architecture and Cyberoperations

4 QUARTER CREDITS

Learners in this course study common security architectures to help identify potential vulnerabilities in architectures, and learn to design secure architectures. Learners identify issues related to the design and implementation of operating system concepts, components and interfaces, and design and implement significant architectural changes to an existing operating system. Learners also examine the authorities, roles, and steps associated with cyber operations, and develop a working knowledge regarding the security issues associated with building complex systems out of third-party components of unknown origin.

Capstone Course Description

IAS5900 IAS Capstone

4 QUARTER CREDITS

Learners demonstrate their mastery of the program and specialization objectives through application of information security and assurance tools and methodologies. **For MS in Information Assurance and Cybersecurity learners only. Must be taken during the learner's final quarter. Prerequisite(s): Completion of all required coursework. Cannot be fulfilled by transfer or prior learning assessment.**

Recommended Course Sequence

This recommended course sequence assumes learners take two courses per quarter. Some learners elect to take fewer or more based on workload and the amount of time available for graduate study.

YEAR 1	COURSES	
Q1	IAS5002	Communication Skills for Today's Information Security Professional
Q2	IAS5010	Information Technology Security Fundamentals
	IAS5015	Network Security Fundamentals and Cryptography
Q3	IAS5020	Information Security Regulatory and Legal Environment
	IAS5025	Network and Operating System Defense
Q4	IAS5030	Identifying and Managing Risk
	IAS5200	Network Architecture and Cyberoperations

YEAR 2	COURSES	
Q5	IAS5210	Data Communications
	IAS5220	Network Security Controls and Testing
Q6	IAS5230	Secure Network Design and Engineering
	IAS5130	Programming for Security Professionals
Q7	IAS5900	IAS Capstone

Tuition and Fees

This tuition estimate is effective July 10, 2017, and is subject to change. For current pricing, visit the Capella University website at www.capella.edu.

	TUITION/FEE
Tuition per credit	\$682
Resource kit per quarter	\$175

Digital course materials covered by the quarterly resource kit fee offer advantages such as immediate mobile access to books; fast, easy full-text search of materials; digital note-taking; and peer collaboration through note sharing.

Financial Aid

Capella University offers assistance to learners who qualify and would like to secure educational funding to help finance their academic program. A number of options are available, given the diverse needs and backgrounds of prospective learners. Options include:

- Federal Direct Stafford Loan Program
- Federal Direct PLUS Loan Program
- Non-federal loans through preferred lenders and financial institutions
- Capella scholarships
- External scholarships
- Veterans' educational benefits and U.S. armed forces discounts
- Corporate and higher education alliances
- Employer tuition reimbursement

Regarding loan programs, interest rates for Stafford student loans are low compared to other types of consumer loans, and repayment can be deferred until after graduation. In compliance with federal and state laws, Capella University has established policies for all learners regarding satisfactory academic progress, which is necessary for financial aid eligibility.

There are many financial aid options available to help you offset tuition costs.

Contact an enrollment counselor at **1.888.CAPELLA (227.3552)** to discuss your financial aid opportunities.

Academic Leadership

Rhonda Capron, EdD

Dean

Dr. Rhonda Capron is an accomplished leader with remarkable business acumen, extensive academic experience and professional relevance within the confluence of today's transformative marketplace. She brings a unique blend of background and experience to Capella as a seasoned executive and higher education leader with more than 15 years of experience successfully leading strategic initiatives and operations within high-tech businesses. She also has 10 years in higher education, including extensive, hands-on experience teaching; faculty and staff leadership; academic programming; curriculum development; and strategic planning. Dr. Capron joined Capella in 2016. She was previously the academic dean of the School of Business at University of Phoenix. Prior to that position, she held a number of academic leadership roles at William Jessup University in Rocklin, California. In addition she has an extensive background in both the business sector and the military. Rhonda was vice president of support services and software as a service at Oracle Corporation, and she served as the deputy director for operations within the Departments of Army and Energy.

Bill Dafnis, PhD

Associate Dean

Dr. Bill Dafnis is the associate dean of technology in Capella University's School of Business and Technology and faculty chair for undergraduate technology. Bill joined Capella in 2014 to serve as faculty chair in the ABET-accredited BS in IT program. Prior to joining Capella, Bill served in faculty and academic leadership roles at other academic institutions. Preceding his academic career, Bill traversed a distinguished 20-year profession with the Chicago-based media conglomerate Tribune Company in leadership roles inclusive of information technology, project management, and operations management. Bill holds a PhD in Information Systems from Nova Southeastern University, Master of Science in Information Technology with a security focus from Carnegie Mellon University, Master of Business Administration from Lake Forest College, and Bachelor of Arts from the University of Illinois and is certified as a Project Management Professional (PMP). His research interests include the intersection of disruptive change and innovation planning, cloud computing economic models, business process modeling, project management, and information security.

Melissa Zgola, MS

Faculty Chair

Melissa Zgola joined Capella University in 2007 as an adjunct faculty member for the School of Technology and became a core faculty member in 2008, teaching courses in networking technology and software architecture. In 2012, she was named faculty chair for the Bachelor of Science in Information Technology program in the School of Business and Technology and served in that role until 2014 when she became faculty chair for the Master of Science in Information Systems and Technology Management and the MS in Analytics programs. Prior to joining Capella, Melissa spent several years as an online facilitator, instructor, and program director with The Art Institute Online, the Pittsburgh Technical Institute and ITT Technical Institute. She also served as an engineering technician for the Department of Labor, and senior system analyst for the University of Pittsburgh. She holds a BA in Psychology and an MA in Counseling from West Virginia University, and an MS in Information Science from the University of Pittsburgh.

Move Forward with Capella University

Important Information
about the educational debt,
earnings, and completion
rates of students who
attended this program: [http://
capellaresults.com/assets/
includes/gainfulemployment/
cta/GE/GE15/masters/MS_IAS_
Network_Defense_gedt.html](http://capellaresults.com/assets/includes/gainfulemployment/cta/GE/GE15/masters/MS_IAS_Network_Defense_gedt.html).

WORKING SCHOLARS

Capella provides an online, flexible learning environment for working adults who are also determined scholars. That connection between academic and professional work infuses the entire Capella experience—from the faculty we recruit to the course projects you complete. The theories discussed in the courseroom are designed to develop working knowledge for everyday situations.

AN ACCREDITED UNIVERSITY

Our accreditation* is an assurance to students, employers, and the public that Capella University meets established standards for quality of faculty, curriculum, and learner services. It is also an important factor in the ability to transfer credits among higher education institutions. Regional accreditation, the type held by Capella, is the most common type for major public, state, and private institutions in the United States.

VALUING YOUR KNOWLEDGE AND EXPERIENCE

Adults bring a wealth of experience and learning to their education. Capella courses are designed to bring out your perspectives just as you gain from others' ideas. Your knowledge can also be worth time and money: An enrollment counselor can help you estimate how much of your prior learning may apply toward your Capella degree program.



CAPELLA UNIVERSITY

Capella Tower
225 South Sixth Street, Ninth Floor
Minneapolis, MN 55402

1.888.CAPELLA (227.3552)
www.capella.edu

*ACCREDITATION

Capella University is accredited by the Higher Learning Commission.

HIGHER LEARNING COMMISSION
<https://www.hlcommission.org>
800.621.7440

© 2018 Capella University. All rights reserved.