Cybersecurity and Information Assurance Program Plan

The cybersecurity program is rigorous and offers a comprehensive coverage of fundamental technical and non-technical concepts, including cybersecurity policy, software assurance, network defense, and programming including scripting. The curriculum prepares learners to identify key business assets, associated threats and vulnerabilities, identify security controls and defense tools, methods, and components. Students are required to demonstrate the conceptual and practical aspects of Cybersecurity. Additionally, successful students will receive six CompTIA certifications as part of the curriculum. Providing these certifications to the students as part of the curriculum makes WGU unique.

PROGRAM LEARNING OUTCOMES:

1) The graduate will be able to evaluate security of a given system design according to defined security goals.
2) The graduate will be able to mitigate security concerns related to network, cellular, mand wireless technologies.
3) The graduate will be able to evaluate the effectiveness of an organization's cyber operations to protect and preserve data.
4) The graduate will be able to conduct digital forensics as part of an incident response plan.
5) The graduate applies core information technology skills in IT systems, operating systems, networking, security, scripting and programming,* and web development to support organizational functions.

1. **CREDITS**
   - Total Credits for degree: 61 CU
   - Gen Ed credits: 21 CU (15 from USNCC, 6 WGU)
   - WGU Certificate (Network and Cyber Defense Foundations) credits: 20 CU
   - Other Required Credits (20 CU): AS degree will also allow the student to achieve four CompTIA certificates (A+, Net+, Security+, and CySA+). Once students earn these four certs, CompTIA grants two additional stackable certs Secure Infrastructure Specialist and Security Analytics Professional for a total of six certifications.

2. **Transfer Credit Allowed:** 45 CUs max (including the USNCC 15 CUs)

3. **Residency Requirement**

   Credits that must be earned at WGU: (16 CUs)

4. **The five Naval Studies certificate courses satisfy the WGU GenEd requirements for Critical Thinking: Reason & Evidence 3CU, Introduction to Physical & Human Geography 3CU, American Politics and the US Constitution 3CU, Introduction to Communication: Connecting with Others 3CU, and Ethics in Technology 3CU.**

5. **WGU GENERAL EDUCATION AND OTHER REQUIREMENTS (40 CREDITS):**

WGU GEN ED COURSES (6 Credits)

Required Gen Ed Course	**Credits**	**General Education Area**
Technical Communications	3	Communication and Composition
Composition: Writing with a Strategy	3	Communication and Composition
Additional Gen Ed Elective Requirements: None		

OTHER REQUIRED COURSES FOR AS DEGREE (20 Credits)

Other Required Courses	**Credits**	**Notes**
IT Foundations	4	
IT Applications	4	Prepares students for CompTIA A+
Networks	4	Prepares students for CompTIA Network+
Network and Security - Applications	4	Prepares students for CompTIA Security+
Cyber Defense and Countermeasures	4	Prepares students for CompTIA CySA+

WGU PROFESSIONAL CERTIFICATE (20 CREDITS): Network and Cyber Defense Foundations Certificate

The 20 credits below will be tracked towards a stand-alone Professional Certificate Program.

For AS degree tracking purposes, the professional certificate program should also be nestled along with the Naval Studies 15 credit requirements marked above + the Gen Ed requirements noted in the section above

Professional Certificate Required Courses (20 CREDITS)

Introduction to IT	4
Fundamentals of Information Security	3
Web Development Foundations	3
Network and Security – Foundations	3
Digital Forensics in Cybersecurity	4
Scripting and Programming Foundations	3
Additional Professional Certificate Elective Requirements: None	

6. WGU Certificate Course Descriptions & Learning Outcomes:

a. Introduction to IT

Introduction to IT examines information technology as a discipline and the various roles and functions of the IT department as business support. Students are presented with various IT disciplines including systems and services, network and security, scripting and programming, data management, and business of IT, with a survey of technologies in every area and how they relate to each other and to the business.

This course covers the following competencies:

- The graduate describes IT as a discipline and discusses the history and future of computing as well as the currently used infrastructure.
- The graduate describes information technology systems and their role in converting data to organizational knowledge.
- The graduate identifies the role of different types of software in a computing environment and explains the fundamentals of software development.
- The graduate recognizes and describes functions of basic computer hardware components.
- The graduate describes the structure, function, and security associated with networks.
- The graduate identifies common software architectures, development techniques, and the relationship between software and its environment.
- The graduate explains the structure and function of databases.
- The graduate explains the role of technology in today’s business environment and describes basic concepts of project management.
- The graduate evaluates ethical concerns involved in the use of technology.

b. Fundamentals of Information Security

This course lays the foundation for understanding terminology, principles, processes, and best practices of information security at local and global levels. It further provides an overview of basic security vulnerabilities and countermeasures for protecting information assets through planning and administrative controls within an organization.

This course covers the following competencies:

- The graduate defines security principles and cyber defense concepts to support security practices within an organization.
- The graduate identifies how security principles and cyber defense concepts impact organizational policies and practices.
- The graduate identifies security principles and cyber defense concepts that have been violated in common security failures.

● The graduate identifies security principles and cyber defense concepts to protect an organization’s assets.
● The graduate identifies how confidentiality, integrity, and availability define security requirements for an organization.
● The graduate identifies guidelines in privacy and compliance as applied to cybersecurity.

c. Web Development Foundations

This course introduces students to web design and development by presenting them with HTML5 and Cascading Style Sheets (CSS), the foundational languages of the web, by reviewing media strategies and by using tools and techniques commonly employed in web development.
This course covers the following competencies:
● The graduate creates web pages using a graphic user interface (GUI) editor as well as basic HTML5 and CSS 3 elements.
● The graduate develops a plan for creating and maintaining a website that addresses specific business needs while maintaining industry and ethical standards.

d. Network and Security – Foundations

Network and Security - Foundations introduces students to the components of a computer network and the concept and role of communication protocols. The course covers widely used categorical classifications of networks (e.g., LAN, MAN, WAN, WLAN, PAN, SAN, CAN, and VPN) as well as network topologies, physical devices, and layered abstraction. The course also introduces students to basic concepts of security, covering vulnerabilities of networks and mitigation techniques, security of physical media, and security policies and procedures.
This course covers the following competencies:
● Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.
● The graduate identifies fundamental networking concepts to support an organization.
● The graduate identifies the fundamentals of network security concepts to support an organization.
● The graduate determines appropriate network security operations to protect an organization’s assets.

e. Digital Forensics in Cybersecurity

Digital forensics, the science of investigating cybercrimes, seeks evidence that reveals who, what, when, where, and how threats compromise information. This course examines the relationships between incident categories, evidence handling, and incident management. Students identify consequences associated with cyber threats and security laws using a variety of tools to recognize and recover from unauthorized, malicious activities.

This course covers the following competencies:
- The graduate identifies types of digital evidence, digital evidence examination rules, and digital evidence consideration by crime category.
- The graduate describes digital forensics procedures from the initial recognition of an incident through the steps of evidence gathering, preservation, analysis, and through the completion of legal proceedings.
- The graduate identifies laws, rules, policies, and procedures that affect digital forensics.
- The graduate conducts analysis on gathered evidence using forensic cyber tools to determine the nature of a security breach.
- The graduate executes recovery procedures for deleted data.
- The graduate identifies steganography and its techniques as it relates to concealed data.
- The graduate identifies common methods and concepts for password cracking, email tracking, file logging, and mobile forensics.

f. Scripting and Programming Foundations

Scripting and Programming - Foundations provides an introduction to programming, covering basic elements such as variables, data types, flow control, and design concepts. The course is language-agnostic in nature, ending in a survey of languages and introduces the distinction between interpreted and compiled languages. This course covers the following competencies:
- The graduate examines basic computer programming elements, including data types, constants, variables, operators, and expressions.
- The graduate determines how to achieve programming goals through functions and control structure.
- The graduate interprets algorithms.
- The graduate describes steps of the software design process.
- The graduate compares various scripting and programming languages.

The non-certificate course descriptions and competencies are:

a. IT Foundations

IT Foundations is the first course in a two-part series that will prepare you for the CompTIA A+ exam, Part I. This course focuses mostly on hardware and will afford you the skills you need to support five core components: Mobile Devices; Networking; Hardware; Virtualization and Cloud Computing; and Network and Hardware Troubleshooting. These are essential skills to set up and troubleshoot any system. Whether you work in a data center or an office, most of your work as an IT professional will execute in a hardware platform; understanding the hardware layer of the IT infrastructure will allow you to work more efficiently, provide solutions for business requirements, and be a key contributor in your company. This course covers the following competencies:
- The graduate configures client-side virtualization to meet organizational requirements.

- The graduate determines appropriate diagnostic and repair strategies for common personal computer hardware, access to network resources, and network connectivity.
- The graduate recommends appropriate strategies for classifying, installing, configuring, optimizing, upgrading, and troubleshooting laptops and mobile devices.
- The graduate recommends appropriate strategies for classifying, installing, configuring, optimizing, and upgrading basic network types.
- The graduate demonstrates an understanding of personal computer components and their function in a desktop system.

b. IT Applications

IT Applications provides students with an understanding of personal computer components and their functions in a desktop system. Also covered is computer data storage and retrieval including classifying, installing, configuring, optimizing, upgrading, and troubleshooting printers, laptops, portable devices, operating systems, networks, and system security. Other areas include recommending appropriate tools, diagnostic procedures, preventative maintenance, and troubleshooting techniques for personal computer components in a desktop system. The course then finishes with strategies for identifying, preventing, and reporting safety hazards and environmental/human accidents in a technological environment, and effective communication with colleagues and clients as well as job-related professional behavior. This course is designed to build the skills to support 4 core components: Operating Systems, Security, Software Troubleshooting, and Operational Procedures. These are core competencies for IT professionals from cloud engineers to data analysts, and will empower you with a better understanding of the tools used during your career. This course covers the following competencies:

- The graduate determines appropriate tools, diagnostic procedures, preventive maintenance, security, malware removal, and troubleshooting techniques for common personal computer and mobile operating systems (mobile and personal computer) and applications.
- The graduate determines appropriate strategies to implement documentation, change management and disaster recovery, and explain common safety, environmental concerns; explain addressing prohibited content; use professional communication techniques.
- The graduate determines appropriate strategies for classifying, installing, configuring, optimizing, upgrading, and troubleshooting computer operating systems.
- The graduate determines appropriate strategies for classifying, controlling access, setting permission, configuring, optimizing, and upgrading basic system security.

c. Networks

Networks for undergraduates focuses on the general concepts and applications of computer operating systems and network topologies. The fundamental knowledge and skills gained in this course prepares students for the CompTIA Network+ (N10-007) certification exam. Network and Security is a prerequisite for this course and should be completed prior to beginning Networks. This course covers the following competencies:

- The graduate configures basic networking components to support an organization’s operations.

- The graduate manages a network infrastructure to support an organization's operations.
- The graduate manages networks to support an organization's operations.
- The graduate troubleshoots network issues in support of an organization's operations.
- The graduate manages network security to protect an organization.

d. Composition: Writing with a Strategy

Composition: Writing with a Strategy introduces candidates to the types of writing and thinking that are valued in college and beyond. Candidates will practice writing in several genres with emphasis placed on writing and revising academic arguments. Instruction and exercises in grammar, mechanics, research documentation, and style are paired with each module so that writers can practice these skills as necessary. Composition: Writing with a Strategy is a foundational course designed to help candidates prepare for success at the college level. There are no prerequisites for Composition: Writing with a Strategy. This course covers the following competencies:

- The graduate applies appropriate grammatical rules, sentence structure, and writing conventions.
- The graduate selects appropriate rhetorical strategies that improve writing and argumentation.
- The graduate appropriately uses a given writing style.
- The graduate uses appropriate writing and revision strategies.
- The graduate integrates credible and relevant sources into written arguments.
- The graduate composes an appropriate narrative for a given context.
- The graduate composes an appropriate argumentative essay for a given context.

e. Network and Security - Applications

Network and Security - Applications prepares students for the CompTIA Security+ certification exam. Successfully completing the course ensures the student will demonstrate the knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations. The following course is a prerequisite: Networks. This course covers the following competencies:

- The graduate examines the impact of threats, attacks, and vulnerabilities to organizational security.
- The graduate configures network hardware and software to support organizational security.
- The graduate implements secure system design to secure organization networks.
- The graduate executes identity and access management controls to prevent unauthorized access to organizational resources.
- The graduate executes data security and privacy practices to manage organizational risk.
- The graduate manages security settings to secure organization networks.

f. Cyber Defense and Countermeasures

Traditional defenses such as firewalls, security protocols, and encryption sometimes fail to stop attackers determined to access and compromise data. This course provides the fundamental skills to handle and respond to the computer security incidents in an information system. The course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats. Students learn how to leverage intelligence and threat detection techniques, analyze and interpret data, identify and address vulnerabilities, suggest preventative measures, effectively respond to and recover from incidents handle various types of incidents, risk assessment methodologies, and various laws and policy related to incident handling. This course prepares students for the CompTIA Cybersecurity Analyst (CySA+) certification exam. This course covers the following competencies:

- The graduate identifies key concepts of information security and incident categories.
- The graduate describes the principles of incident recovery and continuity planning in order to evaluate business impact.
- The graduate distinguishes the purpose and elements of a security policy in order to comply with the laws and regulations related to handling a security incident.
- The graduate applies NIST’s risk assessment methodology to conduct IT risk assessment.
- The graduate describes steps in incident response and handling procedures.
- The graduate defines the purpose, protocol, and functions of a Computer Security Incident Response Team (CSIRT).
- The graduate describes security incident types and procedures for handling them.
- The graduate describes malicious codes and methods of its incident containment and prevention.
- The graduate describes steps in detecting and preventing insider threats.
- The graduate describes the role of forensics analysis in incident response and prevention plan.
- The graduate describes the purpose, key elements, and procedure for creating an incident report.

g. Technical Communication

This course covers basic elements of technical communication, including professional written communication proficiency; the ability to strategize approaches for differing audiences; and technical style, grammar, and syntax proficiency. This course covers the following competencies:

- The graduate integrates basic elements of professional discourse, including audience analysis, the writing process, correct grammar, and appropriate design elements, into technical communication artifacts.
- The graduate makes strategic and appropriate communication decisions based on the audience.
- The graduate creates various technically written artifacts using appropriate technical communication concepts.

7. Course Sequence (including Naval Studies courses)

	Competency Based Sequence of Course(s)

	(Note: 3 WGU courses followed by 1 USNCC Course then repeat
	Introduction to IT 4CU Composition: Writing with a Strategy 3 CU Fundamentals of Information Security 3 CU NAV 101 – Naval Ethics and Leadership 3CU Network and Security 3CU Scripting and Programming Foundations 3CU IT Applications 4CU NAV 102 – Modern Naval History 3CU IT Foundations 4CU Technical Communications 3CU Networks 4CU *NAV 103 – Naval Force Design 3CU* Network and Security Applications 4CU Digital Forensics in Cybersecurity 4 CU Web Development Foundations 3CU NAV 104 – Civil/Military Organization and Politics 3 CU Cyber Defense and Countermeasures 4 CU NAV 105 – Introduction to the Geopolitical Environment 3 CU

	Total credits earned =61