NOCTI

Foundational Credential Blueprint

Cybersecurity Fundamentals

Code: 4324 / Version: 01

General Assessment Information

Blueprint Contents

General Assessment Information
Written Assessment Information
Specific Competencies Covered in the Test
Sample Written Items

Test Type: The Cybersecurity Fundamentals industry-based credential is included in NOCTI's Foundational assessment battery. Foundational assessments measure occupational awareness and fundamental competencies within a specific field, providing insight into a learner's progress toward job readiness. Foundational assessments include a written component only and can be used at the secondary and post-secondary levels. Foundational assessments can be delivered in an online or paper/pencil format.

Revision Team: The assessment content is based on input from secondary, post-secondary, and business/industry representatives from the states of Florida, Georgia, Pennsylvania, South Carolina, Virginia, West Virgina.

11.1003 – Computer and Information System Security/Auditing/ Information Assurance

Career Cluster - Information Technology

15-1122.00 – Information Security Analysts

The Association for Career and Technical Education (ACTE), the leading professional organization for career and technical educators, commends all students who participate in career and technical education programs and choose to validate their educational attainment through rigorous technical assessments. In taking this assessment you demonstrate to your school, your parents and guardians, your future employers and yourself that you understand the concepts and knowledge needed to succeed in the workplace. Good Luck!

NATIONAL COLLEGE CREDIT RECOMMENDATION SERVICE
University of the State of New York - Regents Research Fund

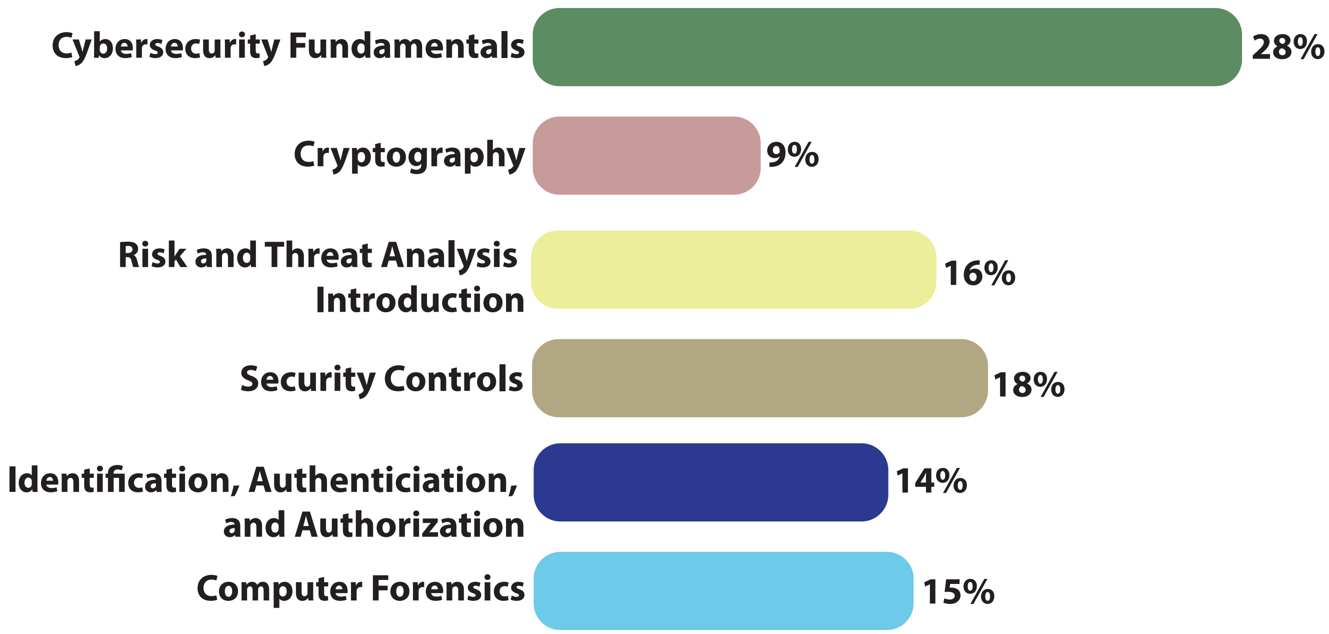
In the lower division baccalaureate/associate degree category, 2 semester hours in Cybersecurity, Information Technology or Computer Information Systems.

Written Assessment

NOCTI written assessments consist of questions to measure an individual's factual theoretical knowledge.

Administration Time: 2 hours
Number of Questions: 98
Number of Sessions: This assessment may be administered in one, two, or three sessions.

Areas Covered



Specific Standards and Competencies Included in this Assessment

Cybersecurity Fundamentals

- Identify different types of cybercrimes
- Communicate incident handling and the response process
- Identify risk (e.g., categorize, mitigate, accept)
- Identify basic cybersecurity terminology
- Recognize network security basics

Cryptography

- Identify different types of cryptography
- Distinguish between steganography and cryptography
- Describe different encryption and decryption methods

Risk and Threat Analysis Introduction

- Identify attackers through threat modeling
- Describe vulnerabilities in information systems and file systems
- Describe procedures necessary for finding and containing malware and viruses
- Interpret current laws and regulations to provide updates to organizational security policies

Security Controls

- Identify different types of attacks and applicable responses
- Apply procedural concepts necessary to configure security systems and validate security
- Understand importance of hardware and software updates and patches
- Define social engineering
- Describe an access control list

(Continued on the following page)

Specific Standards and Competencies (continued)

Identification, Authentication, and Authorization

- Identify different methods of identification, authentication, and authorization
- Describe different biometric devices
- Identify the appropriate placement of biometric devices

Computer Forensics

- Apply procedural concepts required to use forensic tools
- Determine the important content of event logs in forensics
- Recognize that devices are kept in the same state as they were found
- Apply procedural concepts required to discover evidence on different file systems and operating systems
- Identify the chain of custody and implement the proper handling of evidence

Sample Questions

Denial of access or of misusing websites or computer networks is known as

A. spoofing
B. skipping
C. hacking
D. spyware

A security incident is <u>best</u> described as

A. compromise of local hard drive resources
B. activity by tailgating
C. inappropriate web surfing
D. violation of a company security policy

Running outdated or older software increases the chances of

A. not being able to upgrade hardware
B. system crashing
C. system overheating
D. exploitable vulnerabilities

When a software update is released, it should be

A. installed immediately to get the new features
B. tested before being installed companywide
C. ignored if the OS is functioning properly
D. installed during non-peak hours

When a user uses one authentication to gain access to all network resources, this is known as

A. single sign-on
B. authorization
C. network login
D. credentials