NOCTI

Foundational
Credential Blueprint

Cybersecurity Fundamentals

Code: 4224 / Version: 01

General Assessment Information

Blueprint Contents

Test Type: The Cybersecurity Fundamentals industry-based credential is included in NOCTI's Foundational assessment battery. Foundational assessments measure technical skills at the occupational level and include items which gauge factual and theoretical knowledge. 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, Michigan, Pennsylvania, and Virginia.

CIP Code

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

Learning that works for America CTE™

Career Cluster 11- Information Technology

O*NET™ in*it

15-1122.00 – Information Security Analysts

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

Association for Career and Technical Education ACTE®

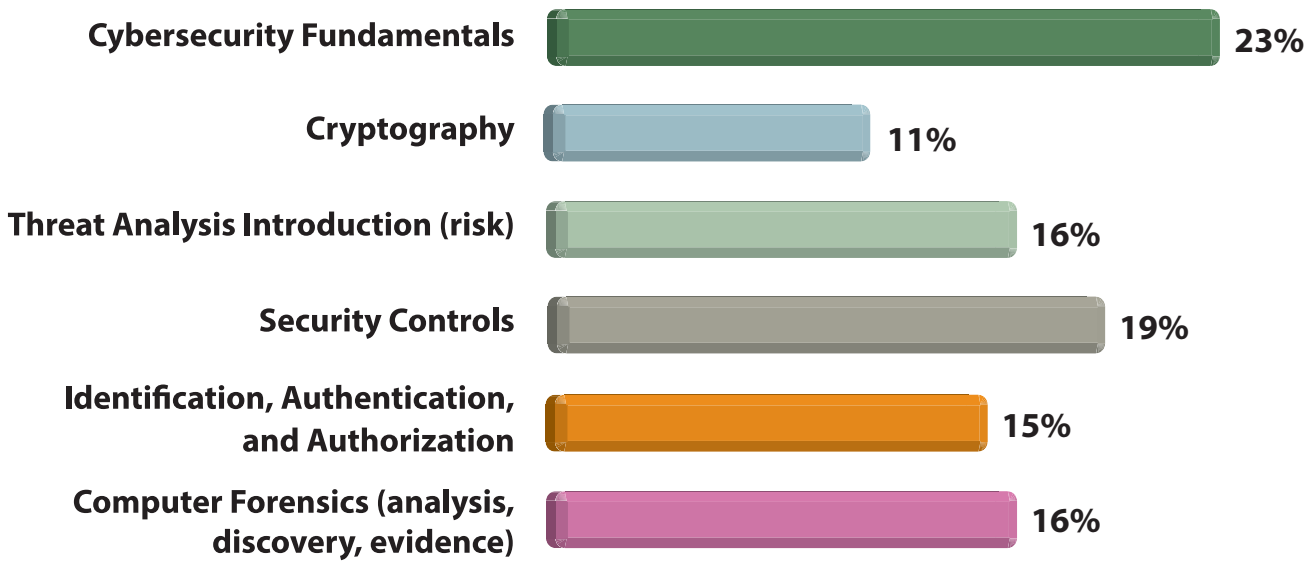
The Association for Career and Technical Education (ACTE), the leading professional organization for career and technical educators, commends all students who participate in career and technical education programs and choose to validate their educational attainment through rigorous technical assessments. 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!

Written Assessment

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

Administration Time: 2 hours
Number of Questions: 100
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, defer)
- Identify basic cybersecurity terminology

Cryptography

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

Threat Analysis Introduction (risk)

- 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

(Continued on the following page)

Specific Standards and Competencies (continued)

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

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 (analysis, discovery, evidence)

- Apply procedural concepts required to use forensic tools (e.g., hashes)
- 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

(Continued on the following page)

Sample Questions

The act of shutting down or misusing websites or computer networks is known as

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

What is an important aspect of evidence gathering?

A. backing up all log files
B. monitoring user access to compromised systems
C. purging transaction logs
D. restoring damaged data from backup media

A security incident is best described as

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

Which cipher rearranges the letters in the message?

A. monolithic
B. substitution
C. transposition
D. static

Running outdated or older software increases the chances of

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

Sample Questions (continued)

Virus files contain bits of code that, when broken down, display certain patterns called

A. autographs
B. images
C. signatures
D. portfolios

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

To assist in granting or denying a user's access to the network, set the Access Control List in the

A. firewall
B. host
C. system
D. server

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

Only _____ should have access to a secure evidence container.

A. the primary investigator
B. the system administrator
C. the investigators in the group
D. senior-level management