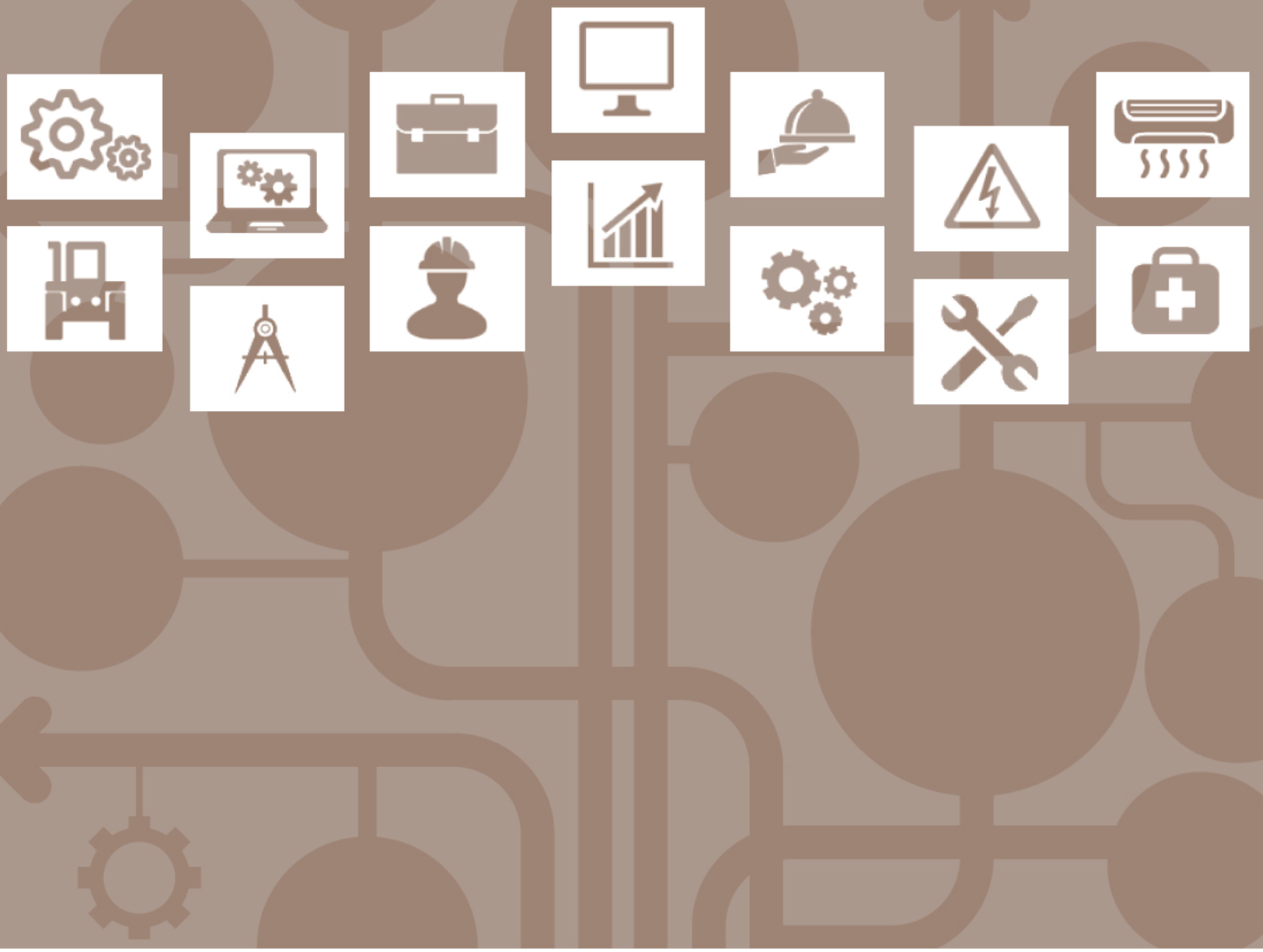
Nocti Business Solutions®
Your Corporate Assessment Provider
www.noctibusiness.com

Entry Level Assessment Blueprint

Cybersecurity Fundamentals



Test Code: 4224 / Version: 01

Specific Competencies and Skills Tested 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

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

Cybersecurity Fundamentals (continued)

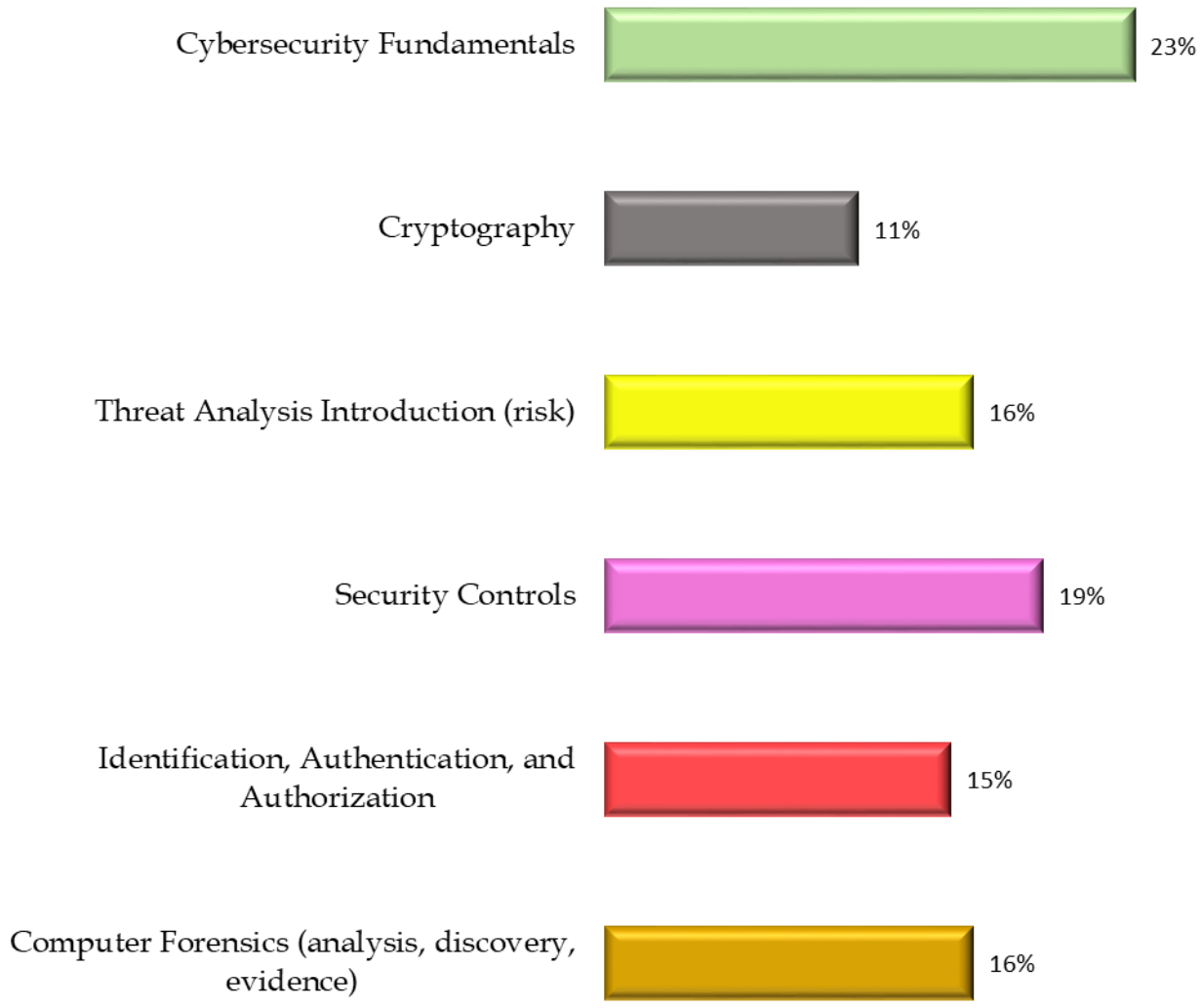
Computer Forensics (analysis, discovery, evidence)

- 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

Written Assessment:

Administration Time: 3 hours
Number of Questions: 100

Areas Covered:



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)

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