Date Issued: 2/1/2019
Date Modified: 1/29/2020
Version: 1.3

CertNexus CyberSAFE 2019 Exam CBS-310

Exam Information

Candidate Eligibility:

The *CyberSAFE 2019* credential requires no fee, supporting documentation, or other eligibility verification measures for you to complete the credential process. Simply purchase an access key for the *CyberSAFE 2019* course from the CertNexus Store here. This course includes access to the credential process directly through the CHOICE platform.

Exam Prerequisites

While there are no formal prerequisites to complete the CyberSAFE credential process, it is recommended that you have experience with the basic use of conventional end-user technology, such as desktop, laptop, and tablet computers; mobile devices; and basic Internet functions, like web browsing and email.

Once you have obtained this level of skill and knowledge, or if you already possess it, CertNexus also strongly recommends that you prepare for the CyberSAFE credential by taking the CertNexus' *CyberSAFE 2019: Exam CBS-310* course.

Exam Specifications

Number of Items: 10

Passing Score: 8 out of 10 (80%)

Duration: There is no formal time limit for taking the CyberSAFE credential. However, you should expect to be able to complete the assessment within approximately 15-30 minutes.

Exam Options: Online via the CHOICE LMS—the assessment is open-book

Item Formats: Multiple Choice/Multiple Response/True-False

Exam Description

Target Candidate:

This credential is designed for all end-users of computers, mobile devices, networks, and the Internet to ensure they can use technology safely to minimize security risks.

Exam Objective Statement:

The assessment will certify that the successful candidate has the knowledge, skills, and abilities required to identify the common risks associated with using conventional end-user technology and safely protect themselves and their organizations from security risks.

To ensure that candidates possess the aforementioned knowledge, skills, and abilities, the *CyberSAFE 2019* credential will test them on the following domains with the following weightings:

Domain	% of Examination
1.0 Compliance	12%
2.0 Social Engineering	20%
3.0 Device and Data Protection	37%
4.0 Online Security	31%
Total	**100%**

The information that follows is meant to help you prepare for your CertNexus credential assessment. This information does not represent an exhaustive list of all the concepts and skills that you may be tested on during the assessment. The domains, identified previously and included in the objectives listing, represent the large content areas covered on the test. The objectives within those domains represent the specific tasks associated with the safe use of computing devices you will be tested on. The information beyond the domains and objectives is meant to provide examples of the types of concepts, tools, skills, and abilities that relate to the corresponding domains and objectives. These examples do not necessarily correlate one-to-one with the content covered in your training program or on your test. CertNexus strongly recommends that you independently study to familiarize yourself with any concept identified here with which you are unfamiliar before taking the assessment.

Objectives:

Domain 1.0 Compliance

Objective 1.1 Identify organizational security compliance requirements

- Sources of organizational compliance requirements
  - Password policy
  - Internet usage policy
  - Data privacy
  - Personally Identifiable Information (PII)
  - AUP
    - On site vs. remote
    - Equipment
    - Shared resources (passwords, mailboxes, etc.)
    - Exceptions and waivers

        - Escalation paths/incident reporting
    - Facility policies
        - Employee/visitor access
        - Badge requirements
        - Key policies
    - Ramifications of non-compliance

Objective 1.2 Identify legal compliance requirements

- Sources of legal compliance requirements
    - Regulation/law
        - HIPAA
        - SOX
        - PCI DSS
        - Local ordinances
    - Legal consequences of non-compliance

Objective 1.3 Identify security and compliance resources

- Organizational and legal compliance resources
    - Organizational handbooks/websites
    - AUP documentation
        - Updates
        - Location/access
    - Organizational departments
        - Legal
        - HR
        - Health Information Management
        - IT
    - Industry associations/professional groups
    - Government websites

Domain 2.0 Social Engineering

Objective 2.1 Recognize social engineering attacks

- Attack vectors
    - User name/password
    - Organizational/personnel information
    - Physical access
    - End-user personal information
- Attack goals
    - Data destruction
    - Data theft
    - Financial gain
    - Political gain
    - Reputation

        - Revenge
    - High-value targets
        - C-suite
        - Accounting personnel
        - HR personnel
        - IT personnel
    - Attack types
        - Phishing
            - Whaling
            - Spear fishing
        - Vishing
        - Pharming
        - Baiting
        - Pretexting
        - Impersonation
        - Quid pro quo
        - Tailgating/piggybacking
        - Shoulder surfing

Objective 2.2 Defend against social engineering attacks

- Resources to defend
    - Organizational hardware/devices
    - Organizational data
    - Network access
    - Premises access
    - User credentials
- Mitigation techniques
    - Situational awareness
    - Badging systems/security checks
    - Door locks
    - Verification of requests
    - Proper disposal/deletion of sensitive information
    - Education/communication

Domain 3.0 Device and Data Protection

Objective 3.1 Maintain the physical security of devices

- Devices containing potentially sensitive data
    - Laptops/computers
    - Mobile phones
    - Tablets
    - Removable storage
- Organizational device-security requirements

        - Limiting the devices that have access to sensitive data
        - Acceptable devices for data storage
        - Disposal/deletion requirements
    - Digital presence
        - Device logs
        - Temporary files
        - Browser history
        - Cached/saved credentials
    - Device physical security techniques
        - Proper storage/disposal/recycling
        - Loss/theft reporting
        - Locking unattended machines/devices

Objective 3.2 Use passwords securely

- Passwords/PINs
    - Frequent changing
    - Complexity
    - Prohibiting reuse/sharing
    - Memorization vs. recording/documenting
- Biometrics
- Multifactor authentication vs. two-step authentication
- Password managers
- Password/PIN security techniques
    - Covert entry (ensure nobody can watch you enter it)
    - Immediately change following breach/incident
    - Secure storage of passwords
    - Critical importance of protecting email passwords
    - Multifactor authentication use when possible
    - Complexity compared to sensitivity of data
    - Unique passwords for all sites and systems
    - Avoiding using easy-to-guess passwords

Objective 3.3 Adhere to data and sensitive data protection best practices

- Data backups/storage locations
- Mobile device considerations
    - Information leakage through always-on app functionality
    - Accidental or intentional recording of sensitive data
        - Camera
        - Microphone
- Data security techniques
    - Prohibitions against copying/printing
    - Proper disposal of printed data

    - Prohibitions against removable storage devices
    - Prohibition against mobile devices in meetings

Objective 3.4 Identify potential sources of malware and prevent infection

- Malware effects
    - System corruption
    - Spying/logging
    - Distracting/annoying
    - Device performance degradation
    - Data hijacking/ransoming
    - Data destruction
    - Blackmail
    - Advertising
- Malware types
    - Key logger
    - Ransomware
    - Adware/spyware
    - Trojan horse
    - Virus
    - Worm
    - Browser hijacker
- Malware sources
    - Trick offers
    - Rogue antivirus
    - Free software scams
    - Software piggybacking
    - Confusing or obscured options (custom installations)
    - Unknown/untrusted download sites
    - Email attachments
    - Links
    - Scripts in data files/software
    - Infected hardware
        - Thumb drives
        - External hard drives
- Malware prevention techniques
    - Careful reading of emails/dialog boxes/offers/pop-ups/etc.
    - IT approval for software installation
    - Inspection of links before selecting
    - Benefit/risk analysis when installing software
    - General system behavior awareness
    - Use of only known vendors and devices

        - Verified publishers

Objective 3.5 Use wireless devices securely

- Common wireless network risks
    - Eavesdropping
    - Unsecure networks
        - Private
        - Public
        - Open
    - Rogue access points
    - Evil twins
    - “Remembering” wireless networks
- Secure wireless device use techniques
    - Public network use prohibitions
    - Encryption
        - WEP/WPA/WPA2
        - Securing Wi-Fi passwords
    - Wireless network “forgetting”
    - Evil twin avoidance
        - Misspelled network names
        - Lack of password requirements when they are expected
        - Multiple networks with similar names

Domain 4.0 Online Security

Objective 4.1 Browse the web safely

- Well-known browsers
    - Chrome
    - Internet Explorer
    - Edge
    - Firefox
    - Safari
- URL construction
    - HTTP vs. HTTPS
        - Non-encryption vs. encryption
    - Top level domains
    - Domain names
    - Suspicious/spoofed URLs
        - Close spellings/misspellings
- Safe web browsing techniques
    - Current and updated web browser use
    - Deciphering web addresses
    - Unknown add-in, plug-in, toolbar avoidance

- Not clicking/tapping ads and pop-ups
- Protocol verification
- URL verification when using links
- Typing vs. clicking
- Bookmarking common sites
- Caution when using mobile devices (URLs not always visible)

Objective 4.2 Use email securely

- Common email use risks
  - Frequent social engineering attacks
    - Security concern alerts
    - Requests for user credentials
    - Malware removal/IT support offers
    - Free offers
    - Monetary/inheritance scams
    - Requests for information
  - Malicious attachments
    - High-risk file types
    - Attachment policy/regulation compliance
- Safe email use techniques
  - Imposter identification
    - Sender name vs. email address
    - Subject line topics
    - Tone/voice/grammar of sender
    - Signature lines
    - Unusual/atypical requests from seemingly valid sources
      - "Bank" asking for password in email
      - "IT" asking for personal info via email
  - Sender verification
    - Call back/meet in person before responding/clicking
  - Email us policy compliance
  - Attachment considerations

Objective 4.3 Use social networks securely

- Social network security considerations
  - Accidental sharing of sensitive information
  - Disparaging comments
    - Representing yourself vs. the organization
  - Lack of control over data and sharing
    - Confidentiality
    - Once posted, always online
  - Confusing security settings

        - Opportunities for social engineering
        - Spoofed accounts
    - Safe social networking techniques
        - Alignment with organizational social networking usage and policies
        - Thorough research and configuration of security and privacy settings
        - Caution with sharing any potentially sensitive or reputation-damaging information
        - Security of admin credentials
        - Social engineering awareness

Objective 4.4 Use cloud services securely

- Cloud service risks
    - Cloud service spoofing
    - Vendor changes
        - Acquisitions/mergers
        - Out of business
    - Mixing up work and private accounts (digital storage location)
- IoT device considerations
- Safe cloud service use techniques
    - Organizational approval for all cloud-based storage
    - Local backups
    - Extra credential vigilance

Continuing Education Requirements

The *CyberSAFE 2019* credential is valid for 1 year from the time the certificate is granted. You must take the Recertification Credential for CyberSAFE or take the most up-to-date version of the CyberSAFE credential prior to the 1-year period's end to maintain a continuously valid certification.