CERTNEXUS®

CyberSAFE CBS-410
Exam Blueprint

cyberSAFE®

Introduction to CertNexus

CertNexus is a vendor-neutral certification body, providing emerging technology certifications and micro-credentials for business, data, developer, IT, and security professionals. CertNexus' mission is to assist closing the emerging tech global skills gap while providing individuals with a path towards rewarding careers in Cybersecurity, Data Science, Data Ethics, Internet of Things, and Artificial Intelligence (AI)/ Machine Learning.

We rely on our Subject Matters Experts (SMEs) to provide their industry expertise and help us develop these credentials by participating in a Job Task Analysis, Exam Item Development, and determining the Cut Score. We also depend upon practitioners in the field to participate in a survey of the Job Task Analysis and beta testing to ensure that our certifications validate knowledge and skills relevant to the industry.

Acknowledgements

CertNexus was honored to have the following Subject Matter Experts contribute to the development of this exam blueprint.

Drs. Andor Demarteau	Shamrock Information Security	www.ShamrockInfoSec.com	in
Steve Zimmer			in
Greg Childers	Devo Technology	www.devo.com	in
Mohamed Hamdy	Rakict	www.rakict.com	
Claudia Laura Limón Luna	etc ibero america	www.etciberoamerica.com	
Shinesa Cambric	Microsoft	www.microsoft.com	in
Benjamin Franklin	Blue Screen IT	bluescreenit.co.uk	in

CertNexus CyberSAFE® CBS-410 Exam

Exam Information

A single click can lead to a multi-million dollar breach in seconds, and the employee responsible may not even be aware of their mistake. Many end users aren't aware of the dangers accompanying today's most common cybersecurity threats, much less how to detect them. CyberSAFE helps ensure that your end users can identify the common risks associated with using conventional end-user technology, as well as how to safely protect themselves and their organizations from security risks in office or while working remotely.

Candidate Eligibility

The *CyberSAFE (CBS-410)* 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 (CBS-410)* 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 digital technology, such as desktop, laptop, and tablet computers; mobile devices; and basic Internet functions like web browsing and email, whether you are working onsite or from a remote location.

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 CBS-410* course.

Exam Specifications

Passing Score: 80% or 20/25 Items

Duration: Estimated 20-45 minutes, candidates may retake as many times as desired.

Exam Options: Online through the CHOICE platform or via eLearning.

Item Formats: Multiple Choice/Multiple Response

Exam Description

Target Candidate:
This credential is designed for all users of computers, mobile devices, networks, IT services and the Internet to ensure they can use technology safely to minimize security risks while protecting organizational assets.

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 digital technology and safely protect themselves and their organizations from security risks.

To ensure that candidates possess the aforementioned knowledge, skills, and abilities, the *CyberSAFE CBS-410* credential will test them on the following domains with the following weightings:

Domain	% of Examination
1.0 Compliance	16%
2.0 Social Engineering	32%
3.0 Device and Data Protection	24%
4.0 Online Security and Remote Access	28%
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.**

- Types of organizational compliance requirements
  - Password policy
  - Internet usage policy
  - Data protection
  - Personally Identifiable Information (PII)
  - Personal Health Information (PHI)
  - Acceptable Use Policy (AUP)
    - On site vs. remote
    - Equipment
    - Shared resources (passwords, mailboxes, etc.)
    - Job function differentiation
  - Facility policies
    - Employee/visitor access
    - Badge requirements
    - Key policies
  - Ramifications of non-compliance

Objective 1.2 **Identify legal compliance requirements.**

- Types of legal compliance requirements
  - Regulation/law
    - HIPAA
    - SOX
    - GDPR
    - NISD
    - e-privacy directive
  - Legal consequences of non-compliance

Objective 1.3 **Identify industry compliance requirements.**

- Examples of industry compliance requirements
  - PCI DSS
  - ISO 27001
  - NIST

Objective 1.4 **Identify security and compliance resources.**

- Organizational compliance resources
  - Handbooks/websites
  - AUP documentation
    - Updates
    - Location/access
  - Departments
    - Human Resources
    - Information Technology
    - Information Security
  - Incident reporting
- Legal compliance resources

- ◦ Government websites
- ◦ Legal departments
- ◦ Insurance providers
- Industrial compliance resources
  - ◦ Industry associations/professional groups

Domain 2.0   **Social Engineering**

Objective 2.1   **Recognize social engineering attacks.**

- Attack vectors (points of entry)
  - ◦ Username/password
  - ◦ Organizational/personnel information
  - ◦ Physical access
  - ◦ End-user personal information
  - ◦ Email
  - ◦ Mobile device
- Attack goals
  - ◦ Data destruction
  - ◦ Data theft
  - ◦ Financial gain
  - ◦ Financial harm
  - ◦ Political gain
  - ◦ Reputation
  - ◦ Revenge
- High-value targets
  - ◦ C-suite
  - ◦ Accounting personnel
  - ◦ HR personnel
  - ◦ IT personnel
- Attack types
  - ◦ Phishing
    - ▪ Whaling
    - ▪ Spear fishing
  - ◦ Vishing
  - ◦ Smishing
  - ◦ Pharming
  - ◦ Baiting
  - ◦ Pretexting
  - ◦ Impersonation (CEO Fraud)
  - ◦ 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
  - ◦ Continual education/training
  - ◦ Communication
  - ◦ Compliance audit

Domain 3.0   **Device and Data Protection**

Objective 3.1   **Maintain the physical security of devices.**

- Organizational and personal 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
  - ◦ Credentials
  - ◦ Acceptable devices for data storage
  - ◦ Disposal/deletion requirements
- Digital presence
  - ◦ Device logs
  - ◦ Temporary files
  - ◦ Browser history
  - ◦ Cached/saved credentials
  - ◦ IoT devices
  - ◦ Cloud storage
- Device physical security techniques
  - ◦ Proper storage/disposal/recycling
  - ◦ Loss/theft reporting
  - ◦ Locking unattended machines/devices
  - ◦ BYOD controls
    - ▪ Remote wipe functionality
    - ▪ Location detection

Objective 3.2   **Use Secure Authentication Methods.**

- Something you know
  - ◦ Passwords/PINs
    - ▪ Frequent changing
    - ▪ Complexity
    - ▪ Prohibiting reuse/sharing
    - ▪ Memorization vs. recording/documenting
- Something you are
  - ◦ Biometrics
    - ▪ Finger print

- Facial recognition
- Retinal/iris scan
- Something you have
  - Authentication apps
  - Key fob
  - Tokens
  - Smart cards
- Authentication best practices
  - Password managers
  - Covert entry (ensure nobody can watch you enter it)
  - Immediately change following breach/incident
  - Secure storage of passwords
  - Critical importance of protecting email passwords
  - Multi-Factor authentication use when possible
  - Complexity compared to sensitivity of data
  - Unique passwords for all sites and systems
  - Avoiding using easy-to-guess passwords
  - Passphrases

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
  - Alerts for access/ deletion of data
  - Data classification
  - Prohibitions against copying/printing
  - Proper disposal of printed data
  - Prohibitions against removable storage devices
  - Prohibition against mobile devices in designated locations
  - Digital presence considerations
    - Device logs
    - Temporary files
    - Browser History
    - Cached/ saved credentials
    - IoT devices
    - Cloud Storage

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
    - Open Networks
    - Email attachments
    - Links
    - Scripts in data files/software
    - Advertising banners
    - Infected hardware
      - Thumb drives
      - External hard drives
  - Malware prevention techniques
    - Careful reading of emails/dialog boxes/offers/pop-ups/etc.
    - Malware prevention software
    - 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
  - ▪ WPA2/WPA3
  - ▪ 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 and Remote Access**

Objective 4.1   **Browse the web safely.**

- Well-known browsers
  - ◦ Chrome
  - ◦ 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
    - ▪ Shortened (Bitly)
    - ▪ Misspelled
    - ▪ Wrong top-level domain (.com v .net)
    - ▪ Redirect (changed URL)
  - ◦ 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
    - Fake invoices from debt collectors
    - Fake credit card expiry notifications
    - Urgent requests form supervisor/ executive level
  - Malicious attachments
    - High-risk file types
      - ZIP/ Compressed files
      - .exe
      - JavaScript
    - 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/urgency 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 use policy compliance
  - Attachment considerations
    - Approved third-party cloud storage (Dropbox, Box, etc.)
    - Password protected
    - Encrypted

Objective 4.3   **Use social networks securely.**

- Social network security considerations
  - Accidental sharing of sensitive information
  - Combined sources of data (multiple platforms, posts, replies, likes, etc.)
  - Disparaging/revealing comments
    - Representing yourself vs. the organization
    - Sensitive information
  - Lack of control over data and sharing
    - Confidentiality
    - Once posted, always online
    - Consent to data sharing
  - Ambiguous/lengthy confusing security settings
  - Opportunities for social engineering
  - Spoofed accounts
  - Hacked accounts
  - Strong authentication
    - Password
    - Multi-Factor Authentication (MFA)
- 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 credentials
- Social engineering awareness
  - Verify connections
  - Verification of content
    - Fact checking

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)
  - Compromising credentials
  - Data persistence
- IoT device considerations
  - Data collection
- Safe cloud service use techniques
  - Organizational approval for all cloud-based storage
  - Local backups
  - Extra credential vigilance
  - Secure network connection

Objective 4.5   **Working from remote locations securely.**

- Connecting securely
  - VPN
  - Scanning for vulnerabilities (Health check)
    - Anti-Virus Software
- Home Network Security
  - Password sharing
  - Updated router firmware
- Separate professional and personal
  - Separate network
  - Devices
  - Data
  - Cloud storage
- Remote Management / Managed device
- Smart Home Devices
  - Access point for network entry
  - Shut down smart home devices
- Collaboration platforms
  - Personal accounts vs. corporate accounts
  - Background
  - Recording
  - Authentication

- ◦ Access to microphone/ video
- ◦ Sharing settings

Continuing Education Requirements

The *CyberSAFE CBS-410* 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.

CertNexus offers personnel certifications and micro credentials in a variety of emerging technology skills including Cybersecurity, Cyber Secure Coding, the Internet of Things (IoT), IoT Security, Data Science, Artificial Intelligence, and Data Ethics. For a complete list of our credentials visit **https://certnexus.com/certification/**.

CERTNEXUS®