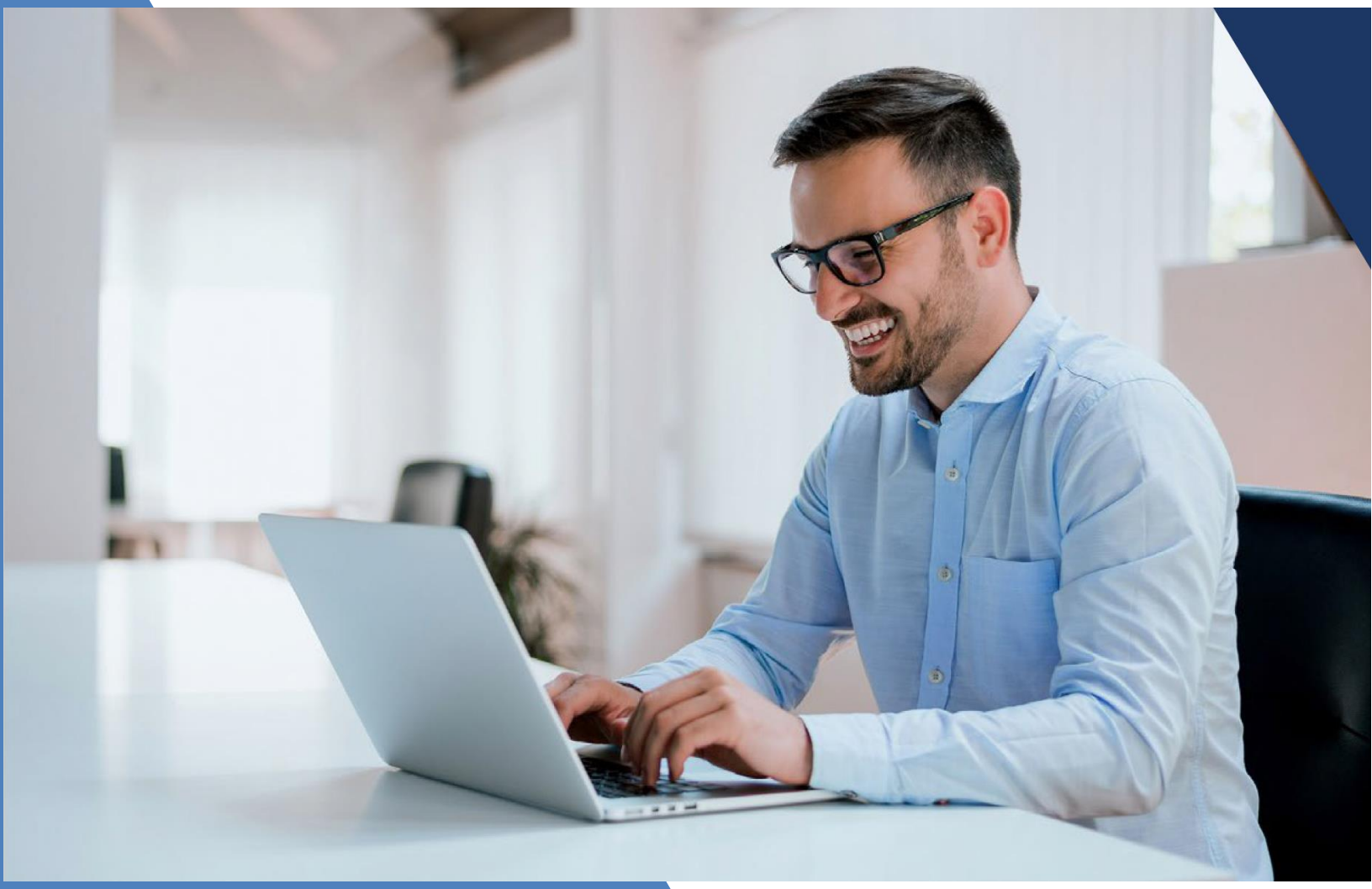
CertNexus® CyberSAFE® Exam CBS-510 Blueprint

Date Issued: 10/10/2025
Version: 1.0



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 (ML).

We rely on our Subject Matter 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.

CertNexus® CyberSAFE® Exam CBS-510

Exam Information

Candidate Eligibility

The CyberSAFE assessment requires no application fee, supporting documentation, or other eligibility verification measures for you to be eligible to take it. Simply purchase an access key for the *CyberSAFE® (Exam CBS-510): Cyber Safety in the Age of AI* course from the CertNexus Store here. This course includes access to the credential process directly through the CHOICE platform.

Exam Prerequisites

Successful candidates should have the knowledge to use computing technology securely and safely in an everyday business context. It is recommended that candidates acquire domain knowledge by attending the CertNexus® *CyberSAFE® (Exam CBS-510): Cyber Safety in the Age of AI* course prior to taking the assessment.

Exam Specifications

Number of Items: 25

Passing Score: 80% or 20/25 Items

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

Exam Delivery: Online through the CHOICE platform or via e-learning.

Item Formats: Multiple Choice/Multiple Response

Upon successful completion, candidates will earn the CertNexus CyberSAFE credential.

Exam Description

Target Audience:

The CyberSAFE assessment is designed for all users of computers, mobile devices, networks, and the Internet, to ensure they can use technology more securely and minimize digital risks, regardless of technical ability.

Exam Objective:

Upon successful completion of the CBS-510 assessment, candidates will demonstrate they can 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 CBS-510 assessment will test them on the following domains with the following weightings:

Domain	% of Examination
1.0 Use Technology Responsibly	20%
2.0 Resist Social-Engineering Attacks	28%
3.0 Secure Devices	24%
4.0 Use the Internet Securely	28%
Total	**100%**

The information that follows is meant to help you prepare for your credential assessment. This information does not represent an exhaustive list of all the concepts and skills that you may be tested on during your assessment. The domains, identified previously and included in the objectives listing, represent the large content areas covered in the assessment. The objectives within those domains represent the specific tasks associated with the job role(s) being tested. 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. All this information represents the industry-expert analysis of the job role(s) related to the credential and does not necessarily correlate one-to-one with the content covered in your training program or on your assessment. We strongly recommend that you study independently to familiarize yourself with any concept identified here that was not explicitly covered in your training program or products.

Domains and Objectives

Domain 1.0 Use Technology Responsibly [20%]

Objective 1.1 Follow compliance requirements.

- Security policies
  - AUP
  - Password policy
  - Internet-usage policy
- Legal compliance
  - HIPAA
  - SOX
  - GDPR
  - EU AI Act
- Industry compliance
  - PCI DSS
  - NIST standards
  - ISO/IEC 27001
- Consequences for non-compliance
  - Disciplinary action from employer
  - Legal fines and imprisonment
  - Loss of reputation and erosion of consumer trust
  - Decline in revenue and market share
- Protect data types
  - PII
  - PHI
- Incident reporting

Objective 1.2 Use generative AI safely.

- Fundamentals
  - Generative AI
  - Agentic AI
- Confabulation/hallucination
- AI-powered scams
  - Gathering/summarizing victim information
  - Crafting convincing messages
  - Voice cloning
- Misinformation and misleading content
  - Crafting propaganda
  - Deepfakes
  - Outdated/obsolete information
- Ethical principles
  - Privacy
  - Accountability
  - Transparency and explainability
  - Fairness and non-discrimination
  - Safety and security
- Legal risks
  - IP rights
  - Restrictions placed on organizations
- Generative AI tools
  - Vendor details and terms of service
  - Quality of output

Domain 2.0 Resist Social-Engineering Attacks [28%]

Objective 2.1 Identify social-engineering attacks.

- Attack goals
  - Data theft
  - Data destruction
  - Financial gain
  - Political gain
  - Revenge
- Attack vectors
  - User name/password
  - Organizational/personnel information
  - Email
  - Mobile device
  - Physical access
- High-value targets
  - C-suite officials
  - Accounting personnel
  - HR personnel
  - IT personnel
- Attack types
  - Impersonation
  - Hoax
  - *Quid pro quo*
  - Pretexting

        - Phishing
            - SMiShing
            - Vishing
            - Spear phishing
            - Whaling
        - Pharming
        - Baiting
        - URL hijacking
        - Spam/spim
        - Shoulder surfing
        - Dumpster diving
        - Tailgating/piggybacking
    - Impact of generative AI on attack effectiveness

Objective 2.2 Defend against social-engineering attacks.

- Resources to defend
    - Organizational hardware/devices
    - Organizational data
    - Network access
    - Premises access
    - User credentials
- Mitigation techniques and best practices
    - Situational awareness
    - Verification of requests
    - Verification of sources
    - Proper disposal/deletion of sensitive data
    - Continual education/training
    - Communication
    - Recognizing generative content

Domain 3.0 Secure Devices [24%]

Objective 3.1 Maintain physical security of devices.

- Organizational requirements for device security
    - BYOD
    - Devices permitted access
    - Required credentials for devices
    - Devices permitted to store data
    - Secure erasure
- Digital presence
    - Device logs
    - Browser history
    - Cached/saved credentials
    - IoT devices
    - Cloud storage
- Security techniques and best practices
    - Proper storage/disposal
    - Loss/theft reporting
    - Locking unattended devices
    - Remote wipe
    - Location detection

Objective 3.2 Use wireless devices securely.

- Wi-Fi network types
  - Open
  - Public
  - Private
- Encryption
- Common wireless-network risks
  - Eavesdropping
  - Insecure public/private networks
  - Rogue APs
  - Evil twins
  - “Remembering” wireless networks
- IoT and smart-device considerations
  - Inherent insecurity
  - Impact on wireless networks
- Security techniques and best practices
  - Avoidance of public networks
  - Password security
  - “Forgetting” wireless networks
  - Recognizing evil twins
  - Disabling Bluetooth discovery

Objective 3.3 Use secure authentication methods.

- Single-factor vs. multi-factor authentication
- Something you know
  - Passwords
  - PINs
  - Patterns
- Something you have
  - Mobile devices
  - Authentication apps
  - Tokens
  - Smart cards
- Something you are
  - Biometrics
- Security techniques and best practices
  - Use of strong passwords
  - Use of password managers
  - Critical importance of protecting email passwords
  - Use of MFA whenever possible
  - Use of unique passwords for each site
  - Entering credentials covertly (to foil shoulder surfers)
  - Reporting account breaches

Objective 3.4 Protect data.

- Confidentiality, integrity, availability
- Data backup
  - Follow policy
  - Discuss with IT
- Mobile-device considerations
  - App permissions
  - Leaking of information

- Security techniques and best practices
  - Alerts for access/deletion of data
  - Data classification
  - Avoidance of removable storage for sensitive data
  - Avoidance of including sensitive data in AI prompts
  - Reviewing output of generative AI for sensitive data
  - Digital-presence considerations
  - Disposal of sensitive documents

Objective 3.5 Defend against malware.

- Malware effects
  - System/data corruption
  - Leaking of sensitive data
  - Annoyance/distraction
- Verified publishers
- Malware types
  - Virus
  - Worm
  - Adware
  - Spyware
  - Trojan horse
  - Rootkit
  - Ransomware
  - Browser hijacker
  - Malvertisement
- Malware sources
  - Trick offers
  - Rogue antivirus
  - Free-software scams
  - Software piggybacking
  - Unknown/untrusted download sites
  - Email attachments
  - Untrusted links
  - Infected hardware

Domain 4.0 Use the Internet Securely [28%]

Objective 4.1 Use email securely.

- Common email risks
  - Fake security alerts
  - Threats of legal/official action
  - Appeals for help
  - Malware removal/IT support offers
  - Free offers
  - Monetary/inheritance scams
- Email attachments
  - Signs of malicious attachments
    - Unknown sender
    - Unsolicited attachment
    - Questionable tone/content of email
  - High-risk file types
    - .htm/.html

        - .zip
        - .exe
        - .js
        - .docm
    - Common phishing techniques
        - Sender name different than email address
        - Spelling/grammar mistakes
        - Subject-line topics
        - Threatening/urgent tone
        - Blank/incomplete/wrong signature
        - Request to update information
        - Use of authority
    - Security techniques and best practices
        - Call back/meet in person before responding/clicking
        - Compliance with email-usage policy
        - Use of approved third-party storage solutions instead of attachments
        - Awareness of unusual requests

Objective 4.2 Browse the web safely.

- URL structure
    - Protocol
    - Hostname
    - Registered domain name
    - TLD
    - Path to resource
- HTTP vs. HTTPS
    - Encryption benefits
    - Visible signs site uses HTTPS
    - Lack of safety guarantees
- Suspicious URLs
    - Similar names/misspellings
    - Unexpected/obfuscated domain or TLD names
    - Numbers at beginning of URL
    - Shortened URLs
- Security techniques and best practices
    - Interpreting URLs
    - Avoidance of unknown add-ins/plugins/extensions
    - Avoidance of clicking/tapping ads/pop-ups
    - Verification of link URLs
    - Bookmarking commonly visited sites
    - Caution when using mobile devices (URL not always visible)

Objective 4.3 Use social networks securely.

- Common social-network risks
    - Accidental sharing of sensitive information
    - Combined sources of data
    - Disparaging/revealing comments
    - Lack of control over data/sharing
    - Opportunities for social engineering
    - Proliferation of AI-powered scams and deepfakes
    - Proliferation of AI-powered misinformation campaigns
- Security techniques and best practices

- Alignment with social-network usage policies
- Configuration of security/privacy settings
- Avoidance of sharing sensitive information
- Awareness of social-engineering attacks
- Awareness of sensational/inflammatory articles/posts
- Corroborating information with other sources

Objective 4.4 Use cloud services securely.

- Common cloud-services risks
  - Trading control for convenience
  - Reliance on a third-party vendor
    - Non-compliance
    - Outsourcing
    - Changes to business
  - Data persistence
  - Compromise/theft of credentials during transmission
  - Spoofing of cloud services
- Security techniques and best practices
  - Organizational approval for cloud storage
  - Use of local backups
  - Use of MFA for cloud services
  - Secure network connections

Objective 4.5 Ensure the security of remote work.

- VPNs
  - Secure tunnel
  - Encrypted traffic
- Remote management
  - Allow organization to manage device
  - Allow organization to manage specific apps
  - Enforcement of IT policies on device
- Collaboration platforms
  - Personal vs. company accounts
  - Access to microphone/video
  - Recording of sessions
  - Sharing settings
- Home networks
  - Password sharing
  - Network segmentation
    - Guest devices
    - Smart devices
    - Work devices
  - Firmware updates for routers
- Security techniques and best practices
  - Separation of personal vs. professional work
  - Up-to-date devices
  - Configuration of strong passwords on home Wi-Fi
  - Blurring/changing video backgrounds for privacy
  - Awareness of smart-home devices on network
  - Adherence to remote-work policies

CyberSAFE Acronyms

Acronym	Expanded Form
AI	Artificial intelligence
AP	Access point
AUP	Acceptable-use policy
BYOD	Bring your own device
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IoT	Internet of Things
IP	Intellectual property
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
MFA	Multi-factor authentication
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
PHI	Protected health information
PII	Personally identifiable information
PIN	Personal identification number
SOX	Sarbanes–Oxley Act
TLD	Top-level domain
URL	Uniform Resource Locator
VPN	Virtual private network

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/.

1150 University Ave, Suite 20, Rochester, NY 14607
1-800-326-8724 | info@certnexus.com
certnexus.com