# CERTNEXUS®

# Cyber Secure Coder™ (CSC-210) Exam Blueprint

*Date Issued: 1/21/2020*
*Date Modified: 1/31/2023*
*Version: 1.3*

C{S}C

## 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 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.

| | | | |
|---|---|---|---|
| Christine Bresnahan | Ivy Tech Community College | https://www.ivytech.edu | in |
| Andrea Cogliati | LighTopTech Corp | https://lightoptech.com | in |
| Armando Pantoja | HireMatch.io | | in |
| Rick Matter | M&T Bank | https://www3.mtb.com | in |

# CertNexus Cyber Secure Coder™ (CSC) Exam CSC-210

## Exam Information

*The Cyber Secure Coder™ (CSC)* is an industry-validated certification which helps professionals differentiate themselves from other job candidates by demonstrating their ability to impart secure coding into software applications. Developers are tasked with ensuring that the software that they create includes coding that results in protected applications. Specialists holding the Cyber Secure Coder certification have proven that they can follow safe practices throughout the creative process. This certification validates that candidates can identify security vulnerabilities and remediate them throughout all of the phases of software development, from conception through to final product.

## Candidate Eligibility

The *Cyber Secure Coder™ (CSC)* exam requires no application fee, supporting documentation, or other eligibility verification measures for you to be eligible to take the exam. Your exam voucher will come bundled with your training program, which can be purchased here. Once purchased, you will receive more information about how to register for and schedule your exam through Pearson VUE. You can also purchase a voucher directly through Pearson VUE. Once you have obtained your voucher, you can register for an exam time here. By registering, you agree to our Candidate Agreement included here.

## Exam Prerequisites

While there are no formal prerequisites to register for and schedule an exam, we strongly recommend that you first possess the knowledge, skills, and abilities to do the following:
- Develop applications using multiple programming languages and coding environments while following generally accepted coding best practices.
- Develop applications for a variety of platforms: web, cloud, mobile, and desktop.
- Write and analyze use cases, technical requirements, specifications, and other application documentation.
- Work with common tools, such as analysis, debugging, encryption, and penetration testing tools.

You can obtain this level of skill and knowledge by taking the following courseware, which is available through training providers located around the world, or by attending an equivalent third-party training program:
- *CertNexus Certified Cyber Secure Coder™ (Exam CSC-210)*

## Exam Specifications

**Number of Items:** 80

**Passing Score:** 60%

**Duration:** 120 minutes (**Note:** Exam time includes 5 minutes for reading and signing the Candidate Agreement and 5 minutes for the Pearson VUE testing system tutorial.)

**Exam Options:** In person at Pearson VUE test centers or online with Pearson OnVUE online proctoring

**Item Formats:** Multiple Choice / Multiple Response

## Exam Description

**Target Candidate:**
This certification exam is designed for software developers, testers, and architects who may develop in multiple programming languages for any type of platform and who desire or are required to develop highly secure applications for business and organizational use. Candidates will also have a need to author or analyze specifications and technical requirements and develop applications that meet them.

**Exam Objective Statement:**
This exam will certify that the successful candidate has the knowledge, skills, and abilities to design and develop a variety of applications for various platforms, analyze security concerns outside of specific languages and platforms, use a number of testing and analysis tools, and mitigate against common threats to data and systems.

To ensure exam candidates possess the aforementioned knowledge, skills, and abilities, the *Cyber Secure Coder™ (CSC)* exam will test them on the following domains with the following weightings:

| Domain | % of Examination |
|---|---|
| 1.0 Common Secure Application Development Terminology and Concepts | 15% |
| 2.0 Job and Process Responsibilities Related to Secure Application Development | 15% |
| 3.0 Architecture and Design | 18% |
| 4.0 Risk Assessment and Management | 17% |
| 5.0 Application Implementation | 35% |
| Total | 100% |

## Objectives

**Domain 1.0**  **Common Secure Application Development Terminology and Concepts**

**Objective 1.1**  **Understand basic security principles**

- Encryption
- Division of resources/categorization of components
- The CIA Triad
- AAA
- Least privilege
- Least common mechanism
- Defense in Depth
- Fail safe
- Weakest link
- Separation of duties
- Monitoring

**Objective 1.2**  **Identify common hacking terminology and concepts**

- Black hat, gray hat, white hat
- Builders and breakers
- Social engineering
- Vulnerability
- Exploits and attacks

**Domain 2.0**  **Job and Process Responsibilities Related to Secure Application Development**

**Objective 2.1**  **Explain the software development lifecycle**

- SDLC phases
- Secure SDLC

**Objective 2.2**  **Understand the role of the designer/architect in creating secure applications**

- Design deliverables
- Whiteboarding
- Compliance assurance and adherence to organizational requirements

**Objective 2.3**    **Explain the role of the developer in creating secure applications**

- Development deliverables
- Debugging tools
- Use of standard libraries and APIs

**Objective 2.4**    **Understand the role of the code reviewer in creating secure applications**

- Review deliverables
- Static analysis tools
- Dynamic code analysis tools

**Objective 2.5**    **Understand the role of the application tester in creating secure applications**

- Testing deliverables
- Penetration testing

# Domain 3.0    Architecture and Design

**Objective 3.1**    **Interpret use and abuse cases**

- Design intentions
- Attacks

**Objective 3.2**    **Understand architecture and design industry best practices**

- Modular design
- Design methodologies
- Software design patterns
- Security design patterns
- Requiring strong passwords
- Identity management process
- Design of monitoring/logging system

**Objective 3.3**    **Identify common regulations that relate to secure software development**

- HIPAA
- PCI DSS
- ISO 27001
- SOX
- Country-specific privacy laws

**Objective 3.4**    **Explain the importance of organizational requirements to the development of secure software applications**

- Internal organizational processes
- Internal organizational policies

# Domain 4.0    Risk Assessment and Management

**Objective 4.1**    **Classify common threats and vulnerabilities in terms of their impact on applications**

- OWASP Top 10
- CWE/SANS Top 25
- Attack vectors
- Assets
- Risks
- Threat types
- Countermeasures

---

- Impacts
- Probability

**Objective 4.2** **Compare and contrast common risk assessment and management best practices**

- Quantitative risk assessment
- Qualitative risk assessment
- Policy adjustments/updates
- Architectural review

# Domain 5.0 Application Implementation

**Objective 5.1** **Implement input validation**

- Input vulnerabilities
- Input validation techniques

**Objective 5.2** **Restrict the output of sensitive data**

- Output vulnerability
- Output security techniques

**Objective 5.3** **Implement cryptography**

- Crypto libraries
- Key management
- Algorithm implementation
- Secure storage of data

**Objective 5.4** **Implement authentication and access control**

- Password verification
- Roles, permissions, groups
- Implementation of secure session management
- Account lockouts
- Password recovery

**Objective 5.5** **Implement error handling and logging**

- Error message logging
- Security exception logging
- Log centralization

**Objective 5.6** **Implement communication security**

- SSL/TLS
- Encrypted tunnels
- Mobile app considerations
- IoT app considerations
- Security of web services

**Objective 5.7** **Implement application security parameters and configure security settings**

- Parameterizing security properties and settings
- Configuration file protection
- Default passwords on third-party applications

**Objective 5.8** **Implement secure database access**

- Elimination of string concatenation for database queries
- Database connection access control

## Recertification Requirements

*The Cyber Secure Coder™ (CSC)* certification is valid for 3 years from the date that it is initially granted. You must retake the most recent version of the exam before the certification's 3-year period expires in order to maintain a continuously valid certification.

## Cyber Secure Coder™ (CSC) Acronyms

| Acronym | Expanded Form |
|---------|---------------|
| AAA | authentication, authorization, and accounting |
| CIA | confidentiality, integrity, and availability |
| DoS | Denial of Service |
| GDPR | General Data Protection Regulation |
| HIPAA | Health Insurance Portability and Accountability Act |
| IoT | Internet of Things |
| IPsec | Internet Protocol security |
| ISO | International Organization for Standardization |
| LDAP | Lightweight Directory Access Protocol |
| OS | operating system |
| OWASP | Open Web Application Security Project |
| PASTA | Process for Attack Simulation and Threat Analysis |
| PCI DSS | Payment Card Industry Data Security Standard |
| SDLC | software development lifecycle |
| SOX | Sarbanes-Oxley Act |
| SSH | Secure Shell |
| SSL/TLS | Secure Sockets Layer/Transport Layer Security |
| SQL | Structured Query Language |
| VPN | virtual private network |
| XML | Extensible Markup Language |
| XSS | cross-site scripting |
| XXE | XML External Entity |

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/**.