CertNexus®

CyberSec First Responder® (CFR-410) Exam Blueprint

Date Issued: 5/1/2021
Date Modified: 2/22/2022
Version: 1.10
Approved by: Scheme Committee

CFR

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, Internet of Things, and Artificial Intelligence (AI)/ Machine Learning.

CertNexus develops its high-stakes exams following the American National Accreditation Board (ANAB) standard for certification development (ISO/IEC 17024:2012). CFR is accredited by ANAB under the ISO/IEC 17024:2012 standard. This standard is a very rigorous, controlled process for initiating, developing, and maintaining our certification programs. We rely on our Subject Matters Experts (SMEs) to provide their industry expertise and help us develop these certifications by participating in a Job Task Analysis, Exam Item Development, and determining the Cut Score. We also depend upon practi-tioners 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.

Dr. Erdal Ozkaya	Comodo Cybersecurity	https://www.comodo.com/	
Tyler Snyder	USAF, AFCERT		
Ashley Pearson		blog.onfvp.com	
William Smith Jr	Johns Hopkins Applied Physics Laboratory	https://www.jhuapl.edu	
Predrag Tasevski		https://predragtasevski.com	
Vanshika Gupta			
Leyla Aliyeva	Proton Technologies Inc.	www.protontechs.com	
Şükrü Durmaz	DIFOSE Digital Forensic Services LLC	www.difose.com	
Dallas Bishoff	MANUS360	https://manus360.com/	
Aaron Sanders	Paychex	https://www.paychex.com/	
Kekai Namauu	Dynamic Advancement	www.dynamicadvancement.com	
Ben Ottoman	Avaus	https://www.avaus.com/	
Paul Janes	Fiserv	https://www.fiserv.com/	
Paul Dumbleton	Gordon Food Service	https://www.gfs.com/en-us	
Brian Copeland	KBR, Inc.	https://www.kbr.com/en	
Adam Danieluk	ISSA Polska	https://www.issa.org.pl/	
Petr McAllister	Tetrate	https://www.tetrate.io/	

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

Alignment with U.S. Department of Defense Directive 8570.01-M

CFR-410 is designed primarily for cybersecurity practitioners preparing for, or who currently perform, job functions related to protecting information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. It is ideal for those roles within federal contracting companies and private sector firms whose mission or strategic objectives require the execution of Defensive Cyber Operations (DCO) or DoD Information Network (DoDIN) operation and incident handling and are seeking personnel to be in compliance with CMMC Incident Response (IR), Audit and Accountability (AU), and Risk Management (RM) domains.

This certification (CFR-410) meets all requirements for personnel requiring DoD directive 8570.01-M position certification baselines:

- CSSP Analyst
- CSSP Infrastructure Support
- CSSP Incident Responder
- CSSP Auditor

CyberSec First Responder® (CFR) Exam CFR-410

Exam Information

A *CyberSec First Responder®* is an IT professional with demonstrated expertise in networking, operating systems, application security, or cloud environments, and their role is to identify, protect, detect, respond, and recover from cybersecurity incidents for their organizations. They have the advanced knowledge, skills, and abilities to deal with an evolving and constantly changing threat landscape, zero-day exploits, and can identify and implement cybersecurity best practices, develop processes for continuous monitoring and detection of potential anomalies, collect and analyze data, accurately report results, are experienced with SIEM and SOAR, and act quickly to mitigate or remediate cyber threats. CyberSec First Responders play a critical role in securing their organization's information, business processes, and intellectual property.

Candidate Eligibility

The *CyberSec First Responder® (CFR)* exam requires no application fee, supporting documentation, or other eligibility verification measures for you to be eligible to take the exam. An exam voucher will come with your training program or can be purchased separately 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 information, 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 you first possess the knowledge, skills, and abilities to do the following:

- Understand the National Institute of Standard and Technology's (NIST) Cybersecurity Framework.

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

- Identify applicable compliance, standards, frameworks, and best practices for privacy and security.
- Understand the cybersecurity threat landscape.
- Assess cybersecurity risk in computing environments within a risk management framework.
- Evaluate an organization's cybersecurity posture.
- Conduct vulnerability assessment processes and identify common areas of vulnerability.
- Perform analysis of network assets.
- Utilize log sources for continuous monitoring and detection of potential anomalies.
- Analyze attacks and post-attack techniques on computing environments.
- Assess and apply organizational cybersecurity policies and procedures.
- Communicate with other stakeholder groups to coordinate incident response processes.
- Prepare for and execute incident response processes when an incident has occurred.
- Implement recovery planning processes and procedures to restore systems and assets affected by cybersecurity incidents.

You can obtain this level of skill and knowledge by taking the following courseware, which is available through training providers around the world, or by attending an equivalent third-party training program:

- *CertNexus CyberSec First Responder® (Exam CFR-410)*

Exam Specifications

Number of Items: 80
Passing Score: 70% or 73% depending on exam form. Forms have been statistically equated.
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 via Pearson OnVUE
Item Formats: Multiple Choice/Multiple Response

Exam Description

Target Candidate:
The CyberSec First Responder® (CFR) exam is designed for individuals with between 2 and 5 years of experience working in a computing environment as part of a CERT, CSIRT, SOC, Command and control (C2) systems, or as an IT professional on the front line of cybersecurity at their organizations, who desire or are required to protect critical information systems before, during, and after an incident which may be a cybersecurity attack.

Exam Objective Statement:
The exam will certify that the successful candidate has the knowledge, skills, and abilities required to effectively identify, detect, protect, respond, and recover from malicious activities involving computing systems. Additionally, the candidate has the foundational knowledge to deal with a changing threat landscape and will be able to assess risk and vulnerabilities, acquire data, perform analysis, continuously communicate, determine scope, recommend remediation actions, and accurately report results.

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

To ensure exam candidates possess the aforementioned knowledge, skills, and abilities, the *CyberSec First Responder® (CFR)* exam will test them on the following domains with the following weightings:

Domain	% of Examination
1.0 Identify	22%
2.0 Protect	24%
3.0 Detect	18%
4.0 Respond	19%
5.0 Recover	17%
Total	**100%**

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

Objectives

Domain 1.0 **Identify**

Objective 1.1 **Identify assets (applications, workstations, servers, appliances, operating systems, and others).**

- Asset identification tools
  - Active
  - Passive
- Tools
  - Nessus
  - Nmap
  - Network monitoring tools
- Operating system information
  - macOS
  - Windows
  - Linux/Unix
  - Android
  - iOS
  - Determine which tools to use for each part of the network

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

- Network topology and architecture information
- Data flow
- Vulnerable ports
- SPAN ports and TAP devices for live packet capture

Objective 1.2 **Identify factors that affect the tasking, collection, processing, exploitation, and dissemination architecture's form and function.**

- Identify relevant policies and procedures
- Collect artifacts and evidence based on volatility level
- Review service level agreements (SLAs)
- Network scanning
- Assets and underlying risks
- Data collection
- Data analytics and e-discovery
- Monitor threats and vulnerabilities
  - CVSS
  - CVE
  - CWE
  - CAPEC
- Threat modeling
- Identify TTPs

Objective 1.3 **Identify and evaluate vulnerabilities and threat actors.**

- Vulnerability scanning tools
- Threat targets
  - Individuals
  - Non-profit associations
  - Corporations
  - Governments
  - Critical Infrastructure
  - Systems
- Mobile
- IoT
- SCADA
- ICS
- PLC
- Threat actors
- Threat motives/reasons
- Threat intent
- Attack phases
- Attack vectors
- Technique criteria

Objective 1.4 **Identify applicable compliance, standards, frameworks, and best practices for privacy.**

- Privacy laws, standards, and regulations
  - GDPR
  - HIPAA
  - COPPA

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

    - GLBA
    - CAN-SPAM
    - National privacy laws
- Frameworks
    - NIST Privacy Framework
    - ISO/IEC 27000 series
    - ISO 29100
    - AICPA Generally Accepted Privacy Principles (GAPP)
- Best practices
    - Federal Trade Commission

Objective 1.5 **Identify applicable compliance, standards, frameworks, and best practices for security.**

- Security laws, standards, and regulations
    - ISO/IEC 27000 series
    - ANSI/ISA-62443
    - NIST Special Publication 800 Series
    - Standard of Good Practice from ISF
    - NERC 1300
    - RFC 2196
    - PCI DSS
    - SSAE 18
- Frameworks
    - NIST Cybersecurity Framework
    - CIS Critical Security Controls
    - COBIT
    - NIST Special Publication 800-61
    - DoD Risk Management Framework (RMF)
    - IT Assurance Framework (ITAF)
- Best practices
    - OWASP
    - MITRE
    - CAPEC
    - CSA

Objective 1.6 **Identify and conduct vulnerability assessment processes.**

- Critical assets and data
- Establish scope
- Determine vulnerability assessment frequency
- Identify common areas of vulnerability
- Users
- Internal acceptable use policies
- Operating systems
- Applications
    - Networking software
- Network operations and management
- Firewall
- Network security applications

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

    - Database software
- Network devices
    - Access points
    - Routers
    - Wireless routers
    - Switches
    - Firewall
    - Modems
    - NAT (Network Address Translation)
- Network infrastructure
    - Network configurations
    - Network services
- DSL
- Wireless protocols
- IP addressing
- Configuration files
- IoT
- Regulatory requirements
- Changes to the system
- Determine scanning criteria
- IoC information
- Perform a vulnerability assessment
    - Determine scanning criteria
    - Utilize scanning tools
    - Identify and assess exposures
    - Generate reports
- Conduct post-assessment tasks
    - Remediate/mitigate vulnerabilities
    - Recovery planning processes and procedures
- Hardening
- Patches
- Exceptions documented
    - Conduct audit/validate action was taken

Objective 1.7 **Establish relationships between internal teams and external groups like law enforcement agencies and vendors.**

- Formal policies that drive these internal and external relationships and engagements
- SLAs
- Communication policies and procedures
- Points of contact and methods of contact
- Vendor agreements, NDAs, and vendor assessment questionnaires
- Privacy rules and laws
- Understanding of relevant law enforcement agencies

Domain 2.0 Protect

Objective 2.1 **Analyze and report system security posture trends.**

- Data analytics

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

- Prioritize the risk observations and formulate remediation steps
- Analyze security system logs, tools, and data
- Threats and vulnerabilities
- Intrusion prevention systems and tools
- Security vulnerability databases
  - CVE
  - CVSS
  - OSVDB
- Discover vulnerabilities in information systems
- Create reports and document evidence

Objective 2.2 **Apply security policies to meet the system's cybersecurity objectives and defend against cyber attacks and intrusions.**

- Cybersecurity policies and procedures
  - Acceptable use policy
  - Network access control (NAC)
  - Disaster recovery and business continuity plans
  - Remote work policies
- Active Directory Group Policy Objects (GPOs)
- Best practices in hardening techniques
- Threats and vulnerabilities
- Security laws, standards, and regulations
- Risk management principles
- Attack methods and techniques
  - Footprinting
  - Scanning
  - Enumeration
  - Gaining access
  - Web attacks
  - Password attacks
  - Wireless attacks
  - Social engineering
  - Man-in-the-middle
  - Malware
  - Out of band
- DoS
  - DDoS
  - Resource exhaustion
  - Forced system outage
  - Packet generators

Objective 2.3 **Collaborate across internal and external organizational lines to enhance the collection, analysis, and dissemination of information.**

- Organizational structure
- Internal teams
- Personnel roles and responsibilities
- Communication policies and procedures
- Knowledge sharing processes

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

- Conflict management
- SLAs
- Relationships with external stakeholders
  - Law enforcement
  - Vendors

Objective 2.4 **Employ approved defense-in-depth principles and practices.**

- Intrusion Prevention or Detection Systems (IDS/IPS)
- Firewalls
- Network Segmentation
- Endpoint Detection and Response (EDR)
- Account Management
  - The Principle of Least Privilege
  - Separation of duties
  - Password policy enforcement
  - Active directory hygiene
- Patch management
- Mobile Device Management (MDM)

Objective 2.5 **Develop and implement cybersecurity independent audit processes.**

- Identify assets
- Cybersecurity policies and procedures
- Data security policies
- Cybersecurity auditing processes and procedures
- Audit objectives
- Network structure
- Compliance standards
- Document and communicate results

Objective 2.6 **Ensure that plans of action are in place for vulnerabilities identified during risk assessments, audits, and inspections.**

- Review assessments, audits, and inspections
- Analyze critical issues for action
- Develop plans of action
- Specify success criteria
- Remediation planning
- Resource implications
- Monitoring procedures

Objective 2.7 **Protect organizational resources through security updates.**

- Cybersecurity policies and procedures
- Software updates
  - Scope
  - Attributes
  - Vulnerabilities
- Firmware updates
  - Scope
  - Attributes
  - Vulnerabilities
- Software patches

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

Objective 2.8 **Protect identity management and access control within the organization, including physical and remote access.**

- Enterprise resources
- Access control
- Authentication systems
- Remote-access monitoring
- Cybersecurity policies and procedures
- Identity management
- Authorization
- Infrastructure/physical security
- Physical security controls
- User credentials

Domain 3.0 **Detect**

Objective 3.1 **Analyze common indicators of potential compromise, anomalies, and patterns.**

- Analyze security system logs, security tools, and data
- IP networking/ IP resolving
- DoS attacks/ DDoS attacks
- Security Vulnerability Databases
- Intrusion Detection Systems
- Network encryption
- SSL decryption
- SIEM
- Firewalls
- DLP
- IPS
- IDS
- Evaluate and interpret metadata
- Malware
- Network topology
- Anomalies
  - False positives
  - Superhuman logins/geo-velocity
  - APT activity
  - Botnets
- Unauthorized programs in the startup menu
- Malicious software
  - Presence of attack tools
- Registry entries
- Unusual network traffic
  - Bandwidth usage
  - Malicious network communication
- Off-hours usage
- New administrator/user accounts
- Guest account usage

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

- Unknown open ports
- Unknown use of protocols
- Service disruption
- Website defacement
- Unauthorized changes/modifications
  - Suspicious files
  - Patches
- Recipient of suspicious emails
- Unauthorized sessions
- Failed logins
- Rogue hardware

Objective 3.2 **Perform analysis of log files from various sources to identify possible threats to network security.**

- Log collection
  - Agent-based
  - Agentless
  - Syslog
- Log auditing
  - Source validation
  - Verification of log integrity
  - Evidence collection
- Log enrichment
  - IP address and hostname resolution
  - Field name consistency
  - Time zones
- Alerts, reports, and event correlation
  - Threat hunting
  - Long tail analysis
  - Intrusion detection
  - Behavioral monitoring
- Log retention
  - Industry compliance/regulatory requirements
- Log aggregator and analytics tools
  - SIEM
- Linux tools
  - grep
  - cut
  - diff
- Windows tools
  - Find
  - WMIC
  - Event Viewer
- Scripting languages
  - Bash
  - PowerShell

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

- Data sources
  - Network-based
  - WAP logs
  - WIPS logs
  - Controller logs
  - Packet capture
  - Traffic log
  - Flow data
  - Device state data
  - SDN
  - Host-based
  - Linux syslog
  - Application logs
- Cloud
  - Audit logs
- Threat feeds

Objective 3.3 **Provide timely detection, identification, and alerting of possible attacks/ intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.**

- Asset discovery methods and tools
- Alerting systems
- Intrusion Prevention or Detection Systems (IDS/IPS)
- Firewalls
- Endpoint Detection and Response (EDR)
- Common indicators of potential compromise, anomalies, and patterns
- Analysis tools
- Document and communicate results

Objective 3.4 **Take appropriate action to document and escalate incidents that may cause an ongoing and immediate impact on the environment.**

- Communication and documentation policies and processes
- Security incident reports
  - Description
  - Potential impact
  - Sensitivity of information
  - Logs
- Escalation processes and procedures
  - Specific technical processes
  - Techniques
  - Checklists
  - Forms
- Incident response teams
- Levels of Authority
- Personnel roles and responsibilities
- Document and communicate results

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

Objective 3.5 **Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks.**

- Post exploitation tools and tactics
  - Command and control
  - Data exfiltration
  - Pivoting
  - Lateral movement
  - Persistence/maintaining access
  - Keylogging
  - Anti-forensics
  - Covering tracks
- Prioritization or severity ratings of incidents
- Communication policies and procedures
- Levels of Authority
- Communicate recommended courses of action and countermeasures

Domain 4.0 **Respond**

Objective 4.1 **Execute the incident response process.**

- Incident response plans and processes
- Communication with internal and external stakeholders
- Personnel roles and responsibilities
- Incident reporting
- Containment Methods
  - Allowlist/blocklist
  - IDS/IPS rules configuration
  - Network segmentation
  - Web content filtering
  - Port blocking
- Containment Tools
  - Firewall
  - IDS/IPS
  - Web proxy
  - Anti-malware
  - Endpoint security solutions
- DLP
- Windows tools to analyze incidents
  - Registry
  - Network
  - File system
  - Malware
  - Processes
  - Services
  - Volatile memory
  - Active Directory tools
- Linux-based tools to analyze incidents
  - Network

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

- File system
- Malware
- Processes
- Volatile memory
- Session management

Objective 4.2 **Collect and seize documentary or physical evidence and create a forensically sound duplicate that ensures the original evidence is not unintentionally modified to use for data recovery and analysis processes.**

- Evidence collection, preservation, and security
  - Digital
  - Physical
- Chain of custody
- Forensic investigation
  - Static analysis
  - Dynamic analysis
- Forensic collection and analysis tools
  - FTK
  - EnCase
  - eDiscovery
  - Forensic Explorer
  - Kali Linux Forensic Mode
  - CAINE
  - SANS SIFT
  - Volatility
  - Binalyze AIR
- Forensically sound duplicates
- Document and communicate results

Objective 4.3 **Correlate incident data and create reports.**

- Logs
- Data analysis
- Intrusion Prevention or Detection Systems (IDS/IPS)
- Forensics analysis
- Correlation analysis
- Event correlation tools and techniques
- Root cause analysis
- Alerting systems
- Incident reports
- Document and communicate results

Objective 4.4 **Implement system security measures in accordance with established procedures.**

- Escalation procedures
  - Chain of command
- Organizational systems and processes
  - Policies
  - Procedures

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

    - Incident response plan
    - Security configuration controls
    - Baseline configurations
    - Hardening documentation
- Document measures implemented

Objective 4.5 **Determine tactics, techniques, and procedures (TTPs) of intrusion sets.**

- Threat actors
    - Patterns of activity
    - Methods
- Tactics
    - Early stages of the campaign
    - Key facts of the infrastructure
    - Artifacts and tools used
- Techniques
    - Technological
    - Non-technological
- Procedures

Objective 4.6 **Interface with internal teams and external organizations to ensure appropriate and accurate dissemination of incident information.**

- Communication policies and procedures
- Internal communication methods
    - Secure channels
    - Out-of-band communications
- External communication guidelines
    - Local law enforcement
    - Stockholders
    - Breach victims
    - Media
    - Other CERTs/CSIRTs
    - Vendors

Domain 5.0 Recover

Objective 5.1 **Implement recovery planning processes and procedures to restore systems and assets affected by cybersecurity incidents.**

- Post-incident
    - Root cause analysis
    - After Action Report (AAR)
    - Lessons learned
    - Reporting and documentation
- Analyze incident reports
- Execute recovery planning processes and procedures
- Document and communicate results

Objective 5.2 **Implement specific cybersecurity countermeasures for systems and applications.**

- Security requirements of systems

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

- System interoperability and integration
- Prevention & mitigation
  - Actions
  - Processes
  - Tools and technologies
  - Devices
  - Systems
- Safeguards
  - Security features
  - Management constraints
  - Personnel security
  - Physical structures, areas, and devices

Objective 5.3 **Review forensic images and other data sources for recovery of potentially relevant information.**

- Memory forensics analysis/tools
  - Volatility
- Data sources and disk images
- Analysis of digital evidence
- Hardware and software tools
- File copying techniques
  - Logical backup
  - Bit stream imaging
- File modification, access, and creation times
- Forensic recordkeeping
  - Automated audit trails
  - Chain of custody
- Forensic investigation
- Forensic collection and analysis tools

Objective 5.4 **Provide advice and input for disaster recovery, contingency, and continuity of operations plans.**

- Recovery planning processes
- Contingency planning
- Systems and assets
- Lessons learned
- Review of existing strategies
- Implement improvements
- Document and communicate reports, lessons learned, and advice for recovery, contingency, and continuity of operations plans

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

Recertification Requirements

The *CyberSec First Responder® (CFR)* certification is valid for 3 years from the date that it is initially granted. In order to maintain a continuously valid certification, candidates can recertify via one of the following options:

1. Retake the most recent version of the exam before their certification expires.
2. Earn and submit enough continuing education credits (CECs) to recertify without retaking the exam.

CyberSec First Responder® (CFR) Acronyms

Acronym	Expanded Form
AAR	After Action Report
AICPA	American Institute of Certified Public Accountants
ANSI	American National Standards Institute
APT	Advanced Persistent Threat
C2	Command And Control
CAINE	Computer Aided Investigative Environment
CAN-SPAM	Controlling The Assault of Non-Solicited Pornography And Marketing Act of 2003
CAPEC	Common Attack Pattern Enumeration And Classification
CERT	Computer Emergency Response Team
COBIT	Control Objectives For Information And Related Technologies
COPPA	Children's Online Privacy Protection Rule
CSA	Cloud Security Alliance
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities And Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DoD	U.S. Department of Defense
DoS	Denial of Service
DSL	Digital Subscriber Line
EDR	Endpoint Detection And Response
FTK	Forensic Toolkit
GAPP	Generally Accepted Privacy Principles
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act
GPOs	Group Policy Objects
HIPAA	Health Insurance Portability And Accountability Act
ICS	Industrial Control Systems
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IoC	Indicator of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

ISA	International Society For Automation
ISO	International Organization For Standardization
IT	Information Technology
ITAF	It Assurance Framework
MDM	Mobile Device Management
NAT	Network Address Translation
NDA	Non-Disclosure Agreement
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standard And Technology
OSVDB	Open Sourced Vulnerability Database
OWASP	Open Web Application Security Project
PCI DSS	Payment Card Industry Data Security Standard
PLC	Programmable Logic Controller
RFC 2196	Site Security Handbook
SCADA	Supervisory Control And Data Acquisition
SDN	Software-Defined Networking
SIEM	Security Information Event Management
SLAs	Service Level Agreements
SOC	Security Operations Center
SPAN	Switch Port Analyzer
SSAE 18	Statement On Standards For Attestation Engagements
SSL	Secure Sockets Layer
TAP	Targeted Attack Protection
TTPs	Tactics, Techniques, And Procedures
WAP	Wireless Access Point
WIPS	Wireless Intrusion Prevention System
WMIC	Windows Management Instrumentation Command-Line

Copyright © 2022 by CertNexus Inc. All rights reserved.
CertNexus CyberSec First Responder® (CFR-410)
Exam Objectives are subject to change without notice.

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/**.

For additional resources on preparing for your certification exam, visit the **Candidate Resources section on our website**.

CERTNEXUS®
3535 Winton Pl, Rochester, NY 14623
1-800-326-8724 | info@certnexus.com
certnexus.com