Logical Operations CyberSec First Responder: Threat Detection and Response (CFR) Exam CFR-110

Exam Information

Candidate Eligibility:

The *CyberSec First Responder: Threat Detection and Response (CFR)* exam requires no special fee, supporting documentation, or other eligibility verification measures for you to be eligible to take the exam. Simply purchase an exam voucher here, then Logical Operations will send you an email containing the information you need to register to take the exam through Pearson VUE, or purchase directly from Pearson VUE. If your voucher came bundled with your CFR training program, you will receive this information from your trainer or training administrator. Once you have obtained your voucher information, you can register for an exam time here. By redeeming your exam voucher, you agree to our Candidate Agreement.

Exam Prerequisites

While Logical Operations (LO) requires no formal prerequisites for you to register for and schedule a *CFR* exam time, LO strongly recommends you possess the following knowledge, skills, and experience prior to preparing for the exam:

- At least two years of experience in computer network security technology or a related field.
- The ability to recognize information security vulnerabilities and threats in the context of risk management.
- A working knowledge of common computer operating systems.
- A working knowledge of the concepts and operational frameworks of common assurance safeguards in computing environments (including, but not limited to: basic authentication and authorization, resource permissions, and anti-malware mechanisms).
- A working knowledge of common networking concepts, such as routing and switching.
- A working knowledge of the concepts and operational frameworks of common assurance safeguards in network environments (including, but not limited to: firewalls, intrusion prevention systems [IPSs], and virtual private networks [VPNs]).

You can obtain this level of skill and knowledge by taking the following Logical Operations courses or by passing the associated exams:

- *CompTIA A+: A Comprehensive Approach (Exams 220-901 and 220-902)*
- *CompTIA Network+ (Exam N10-006)*
- *CompTIA Security+ (Exam SY0-401)*

Once you have obtained the recommended level of skill and knowledge, LO also strongly recommends that you prepare for the *CFR* exam by taking Logical Operations' *CyberSec First Responder: Threat Detection and Response* course.

Exam Specifications

Number of Items: 126

Duration: 180 minutes

Exam Options: In person (PearsonVUE)

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

Exam Description

Target Candidate:

This exam is designed for cybersecurity practitioners who perform job functions related to protecting and defending information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. The exam focuses on the knowledge, ability, and skills necessary to provide for the restoration of those information systems in a cybersecurity context including protection, detection, investigation, reaction, response, and auditing capabilities.

Domain	% of Examination
1.0 Assessing Information Security Risk	10%
2.0 Creating an Information Assurance Lifecycle Process	7%
3.0 Analyzing Threats to Computing and Network Environments	19%
4.0 Designing Secure Computing and Network Environments	15%
5.0 Operating Secure Computing and Network Environments	5%
6.0 Assessing the Security Posture Within a Risk Management Framework	10%
7.0 Collecting Cybersecurity Intelligence Information	5%
8.0 Analyzing Cybersecurity Intelligence Information	5%
9.0 Responding to Cybersecurity Incidents	7%
10.0 Investigating Cybersecurity Incidents	10%
11.0 Auditing Secure Computing and Network Environments	7%
Total	**100%**

Objectives:

Domain 1: Assessing Information Security Risk

- Identify the Importance of Risk Management

- Assess Risk

- Mitigate Risk

- Integrate Documentation into Risk Management

Domain 2: Creating an Information Assurance Lifecycle Process

- Evaluate Information Assurance Lifecycle Models

- Align Information Security Operations to the Information Assurance Lifecycle

- Align Information Assurance and Compliance Regulations

Domain 3: Analyzing Threats to Computing and Network Environments

- Identify Threat Analysis Models

- Assess the Impact of Reconnaissance Incidents

- Assess the Impact of Systems Hacking Attacks

- Assess the Impact of Malware

- Assess the Impact of Hijacking and Impersonation Attacks

- Assess the Impact of DoS Incidents

- Assess the Impact of Threats to Mobile Security

- Assess the Impact of Threats to Cloud Security

Domain 4: Designing Secure Computing and Network Environments

- **Information Security Architecture Design Principles**

- **Design Access Control Mechanisms**

- **Design Cryptographic Security Controls**

- **Design Application Security**

- **Design Computing Systems Security**

- **Design Network Security**

Domain 5: Operating Secure Computing and Network Environments

- **Implement Change Management in Security Operations**

- **Implement Monitoring in Security Operations**

Domain 6: Assessing the Security Posture Within a Risk Management Framework

- **Deploy a Vulnerability Management Platform**

- **Conduct Vulnerability Assessments**

- **Conduct Penetration Tests on Network Assets**

- **Follow Up on Penetration Testing**

Domain 7: Collecting Cybersecurity Intelligence Information

- **Deploy a Security Intelligence Collection and Analysis Platform**

- **Collect Data from Security Intelligence Sources**

Domain 8: Analyzing Cybersecurity Intelligence Information

- **Analyze Security Intelligence to Address Incidents**

- **Use SIEM Tools for Analysis**

Domain 9: Responding to Cybersecurity Incidents

- Deploy an Incident Handling and Response Architecture

- Perform Real-Time Incident Handling Tasks

- Prepare for Forensic Investigation

Domain 10: Investigating Cybersecurity Incidents

- Create a Forensics Investigation Plan

- Securely Collect Electronic Evidence

- Identify the Who, Why, and How of an Incident

- Follow Up on the Results of an Investigation

Domain 11: Auditing Secure Computing and Network Environments

- Deploy a Systems and Processes Auditing Architecture

- Prepare for Audits

- Perform Audits Geared Toward the Information Assurance Lifecycle

Continuing Education Requirements

The *CyberSec First Responder: Threat Detection and Response (CFR)* certification is valid for 3 years from the time the certification is granted. You must re-take the most up-to-date version of the exam prior to the 3-year period's end to maintain a continuously valid certification.

You can purchase a voucher to take the exam by clicking here.