



LEAD CYBERSECURITY

PROFESSIONAL CERTIFICATION



LCSPC™ Version 042021

CertiProf®

Lead Cybersecurity Professional Certification LCSPC

Syllabus V062020

Introduction	3
Learning Objectives	3
Exam Format and Duration	3
Eligibility for the Certification	3
Content	4



Introduction

CertiProf® is now offering the professional certification in Cybersecurity, Lead Cybersecurity Professional Certification LCSPC, where you will learn the fundamental concepts of Cybersecurity and implement the practice of protecting systems, networks and programs from digital attacks. These cyber-attacks generally aim to access, change or destroy confidential information; extort money from users; or interrupt normal business processes.

The implementation of effective cybersecurity measures is particularly challenging today because there are more devices than people, and the attackers are becoming more innovative. This certification will help you understand the basic functions of a security framework and the importance of establishing cybersecurity to protect information based on the three pillars of data security.

Learning Objectives

- Fundamental Concepts of Cybersecurity.
- ISO / IEC 27032.
- Introduction to cybersecurity framework.
- Risk management and the cybersecurity framework.
- Implementation of the cybersecurity framework.
- Establish or improve communicative cybersecurity.
- Methodology to protect privacy and civil liberties.
- Self-assessment of cybersecurity risk with the framework.

Exam Format and Duration

The study program has a test that the candidate must pass to obtain the certification in CertiProf Lead Cybersecurity Professional Certification LCSPC.

- Format: Multiple choice. 40 Questions.
- Duration: 60 minutes maximum, for all candidates in their respective language.
- Prerequisite: None.
- Supervised: It will be at the Partner's discretion.
- Open book: No.
- Pass Score: 24/40 or 60 %.
- Delivery: This examination is available online.

Eligibility for the Certification

Know the importance of cybersecurity and learn how to avoid all types of threats, that put at risk the information that is processed, transported and stored on any device.

Content

Fundamental Concepts of Cybersecurity

- Introduction
- The Nature of Cybersecurity
- Approach to Cybersecurity
- Stakeholders in Cyberspace
- Assets in Cyberspace
- Threats in Cyberspace
- Roles of the Stakeholders in Cybersecurity

Cybersecurity Overview

- Cybersecurity Evolution
- The Cybersecurity Skills Gap
- Cybersecurity Objectives
- Cybersecurity Roles
- The Five Core Functions of the Framework
- National Cybersecurity Strategies Evaluation Tool
- Approaches to Implement Cybersecurity
- Cybersecurity Key Terms
- Most Common Types of Cyberattacks
- Cybersecurity Threat Agents
- States as Agents of Threats
- Global Risks Report 2020
- Security Incident Response Policy
- History & Development of the Framework
- Executive Order 13636
- Evolution of the Framework
- Global Cybersecurity Index (GCI)
- Heat Map of National Cybersecurity Commitment
- National Cybersecurity Index

NICE: Cybersecurity Workforce Framework

- NICE: National Initiative for Cybersecurity Education
- NICE Framework Components
- Framework Components
- Framework Components Relationship
- Framework Categories
- Analyze
- Collect and Operate
- Investigate
- Operate and Maintain
- Supervise and Govern
- Protect and Defend
- Safe Provision

Workshop

ISO/IEC 27032

Introduction

Applicability

Introduction

Structure ISO/IEC 27032

ISO 27000 Family

Other Resources in Cybersecurity

Cybersecurity Framework Introduction

Framework Introduction

NIST Cybersecurity Framework (CSF) Reference Tool

The Cyber Security Evaluation Tool (CSET®)

Resources

NIST Translations

Cybersecurity Framework Overview

Framework Overview

Framework Core

Framework Implementation Tiers

Framework Profile

Risk Management and the Cybersecurity Framework

Risk Management and the Cybersecurity Framework

Cybersecurity Framework Basics

Framework Basic Concepts

Cybersecurity Framework Core

Framework Core

Functions

Categories

Subcategories

Informative References

The Five Core Functions of the Cybersecurity Framework

The Five Core Functions of the Framework

Identify

Protect

Detect

Respond

Recover

Informative References: What are they, and how are they used?

Cybersecurity Framework Implementation Tiers

Framework Implementation Tiers

Tier 1: Partial

Tier 2: Risk Informed

Tier 3: Repeatable

Tier 4: Adaptive

Cybersecurity Framework Profile

Framework Profile

Coordination of Cybersecurity Framework Implementation

Coordination of Framework Implementation

How to Use the Framework

How to Use the Framework

Basic Review of Cybersecurity Practices

Basic Review of Cybersecurity Practices

Establishing or Improving a Cybersecurity Program

Establishing or Improving a Cybersecurity Program

Step 1: Prioritize and Scope

Step 2: Orient

Step 3: Create a Current Profile

Step 4: Conduct a Risk Assessment

Step 5: Create a Target Profile

Step 6: Determine, Analyze, and Prioritize Gaps

Step 7: Implement Action Plan

Establishing or Improving a Cybersecurity Program

Communicating Cybersecurity Requirements with Stakeholders

Communicating Cybersecurity Requirements with Stakeholders

Buying Decisions

Buying Decisions

Identifying Opportunities for New or Revised Informative References

Identifying Opportunities for New or Revised Informative References

Methodology to Protect Privacy and Civil Liberties

Methodology to Protect Privacy and Civil Liberties

Self-Assessing Cybersecurity Risk with the Framework

Self-Assessing Cybersecurity Risk with the Framework

Appendix A: Framework Core

Appendix A: Framework Core

Appendix B: Glossary

Buyer

Category

Critical Infrastructure

Cybersecurity

Cybersecurity Event

Cybersecurity Incident

Cybersecurity Incident

Framework

Framework Core

Framework Implementation Tier

Framework Profile

Function

Identify (function)
Informative Reference
Mobile Code
Protect (function)
Privileged User
Recover (function)
Respond (function)
Risk
Risk Management
Subcategory
Supplier
Taxonomy

Appendix C: Acronyms

Appendix C: Acronyms