Certification Training

CCSA℠ Certified Cyber Security Architect

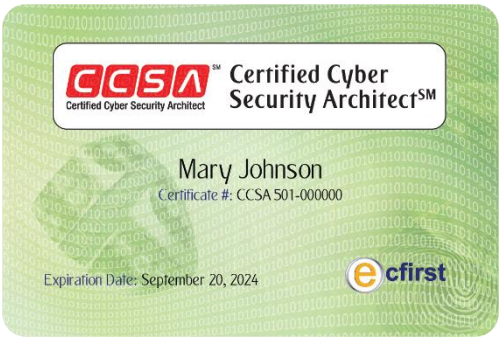
CEU 8 Hours

Course Outline

- CCSA℠ is an instructor-led 1-day program.
- The program validates knowledge and skill sets in cybersecurity with focus on the NIST Cybersecurity Framework, and the U.S. DoD cybersecurity mandate, CMMC.
- Core topics emphasized include establishing a credible, evidence-based enterprise cybersecurity program and developing a comprehensive incident response plan.

Learning Objective

- Examine how to establish a cybersecurity program based on the NIST Cybersecurity Framework.
- Step through key areas that must be addressed in a credible incident response plan.
- Walk through core components, organization and CMMC Maturity Levels.
- Examine CMMC domains and CMMC capabilities required for organizations.



Skills

CMMC Framework | Cyber Policies | Cybersecurity Framework | Cybersecurity Program | Encryption | Penetration Testing | Security Incident | Risk Assessment | Vulnerability Assessment | NIST

Target Audience

- Information Security Officers
- Security Practitioners
- Privacy Officers
- Senior IT Professionals
- Compliance Professionals & Managers

Course Content

Module 1 - Cybersecurity Framework

- Framework Profile
- Framework Implementation Tiers
- Framework Core Functions
- Functions, Categories & Sub-Categories

Module 2 - CMMC Framework: A U.S. DoD Mandate

- Introduction
- CMMC Key Facts
- CMMC Module Framework
- CMMC Levels
- CMMC Domains and Process Maturity

Module 3 - NIST SP 800-171 R2

- Purpose
- Target Audience
- Controlled Unclassified Information (CUI)
- Security Requirements

Module 4 - Security Incident Management

- Fundamentals
- Serious Incident Management
- Incident Management Recommendations

Module 5 - Vulnerability Assessment & Penetration Testing

- Vulnerability Scans
- Wireless Assessment
- Pen Test Methodology
- External & Internal Pen Test
- Exploitable Vulnerabilities
- Detect & Prevent Intrusions
- Change-Detection Mechanism
- Firewall/DMZ Assessment
- Enterprise Risk Assessment

Module 6 - Essential Cyber Policies

- Information Security Policies
- Organization of Information Security
- Risk Assessment
- Risk Management
- Audit Controls
- Mobile Devices
- Breach Notification
- Information Security Incident Management
- System Acquisition, Development and Maintenance
- Supplier Relationships

Module 7 - Encryption

- Encryption Assessment: Cloud, Mobile & More
- Mandates: Standards & Regulations
  - ISO 27001
  - PCI DSS
  - NIST
  - HIPAA and HITECH
- Encryption Strategy
  - Policy
  - Checklist
  - Cybersecurity Framework

Module 8 - Establishing a Cybersecurity Program

- Prioritize and Scope
- Orient
- Create a Current Profile
- Conduct a Risk Assessment
- Create a Target Profile
- Determine, Analyze, and Prioritize Gaps
- Implement Action Plan

Digital Badge

ecfirst also offers a Digital Badge with your certification. There is no fee for this service and acceptance is totally up to you.

- A web-enabled version of your certification that can be shared online.
- A more efficient way of posting to social media platforms.
- Labor market insights that relate your skills to jobs.
- A trusted method for real-time certification verification.