



# CCSS Cybersecurity Specialist Operations Training Course

3 – 7 May 2027  
Kuala Lumpur

## CCSS Cybersecurity Specialist Operations Training Course

**Ref:** 750\_157126 **Date:** 3 – 7 May 2027 **Location:** Kuala Lumpur **Fees:** 6500 Euro

### Overview

CCSS Cybersecurity Specialist Operations Training Course is a five-day intermediate course for analysts, security-operations teams, IT administrators, risk and compliance functions, auditors, and technical professionals who leave with a Cybersecurity Specialist Operations Playbook. Participants organize security governance, risk assessment, asset and identity protection, network and endpoint defense, vulnerability management, monitoring, incident response, recovery, and reporting through NIST CSF 2.0 functions. Agile Leaders Training Center develops CCSS cybersecurity specialist operations.

### Who Should Attend

- Cybersecurity-analysis functions responsible for assessing threats, weaknesses, and defensive evidence
- Security-operations functions responsible for monitoring, triage, and incident coordination
- IT-administration functions responsible for identities, endpoints, networks, and secure operations
- Risk and compliance functions responsible for governance, treatment, and control evidence
- Audit and technical-assurance functions responsible for evaluating cybersecurity practices

The course assumes participants work with IT systems, security controls, logs, or risk records and leaves out penetration-testing exploitation, malware development, forensic acquisition, and claims that attendance awards certification.

### Departments and Industries

The course supports departments and industries that need coordinated cyber-risk and defensive operations.

- Cybersecurity and security operations
- IT infrastructure and service management
- Risk, compliance, and internal audit
- Financial services, healthcare, and telecommunications
- Industrial, logistics, and digital-service organizations

### Learning Objectives

By the end of this course, participants will be able to:



- Apply NIST CSF 2.0 functions to cybersecurity operations
- Evaluate cyber risks, assets, identities, and control priorities
- Build network, endpoint, and vulnerability defense workflows
- Analyze security monitoring and detection evidence
- Prioritize incident response and recovery actions
- Build a Cybersecurity Specialist Operations Playbook

## **Course Agenda**

### **Day 1: Govern and Identify Cyber Risk**

- NIST CSF 2.0 Function and Outcome Map
- Cybersecurity Governance Role Matrix
- Asset, Service, and Data Dependency Register
- Threat, Vulnerability, Impact, and Likelihood Worksheet
- Cyber-Risk Treatment and Reporting Dashboard

### **Day 2: Protect Assets and Identities**

- Identity and Privileged-Access Control Matrix
- Network Segmentation and Trust-Boundary Diagram
- Endpoint Security Configuration Baseline
- Data Protection and Handling Control Map
- Security Awareness and Human-Risk Action Plan

### **Day 3: Manage Vulnerabilities and Detect Events**

- Vulnerability Intake and Validation Workflow
- Risk-Based Remediation Priority Matrix
- Security Logging and Telemetry Coverage Map
- Detection Use-Case and Alert Triage Register
- Monitoring Gap and Escalation Checklist

### **Day 4: Respond, Recover, and Report**

- Incident Classification and Severity Matrix
- Incident Containment and Evidence-Preservation Plan
- Response Roles and Communication Workflow
- Recovery Dependency and Restoration Priority Map
- Operational and Management Security Report



## **Day 5: Cybersecurity Specialist Practice**

- Exercise: Profile Cyber Risk and Critical Assets
- Exercise: Design Identity, Network, and Endpoint Controls
- Exercise: Prioritize Vulnerabilities and Detection Gaps
- Exercise: Coordinate Incident Response and Recovery
- Capstone: Cybersecurity Specialist Operations Playbook

## **Practical Exercises**

The course uses suggested activities drawn from financial services, healthcare, telecommunications, industrial operations, logistics, and digital services.

- Suggested activity: map critical assets, dependencies, threats, vulnerabilities, and treatment decisions.
- Suggested activity: design identity, segmentation, endpoint, and data-protection controls for a service.
- Suggested activity: rank vulnerability findings and create detection and escalation priorities.
- Suggested activity: coordinate containment, evidence preservation, communication, recovery, and reporting for an incident.

## **FAQs**

### **Who suits CCSS cybersecurity specialist operations training, and what does it assume?**

Security, IT, risk, compliance, audit, and technical functions suit the training; it assumes work with systems, controls, logs, or risk records.

### **How does CCSS cybersecurity specialist training differ from penetration-testing training?**

CCSS cybersecurity specialist training coordinates governance, risk, protection, monitoring, vulnerabilities, incidents, recovery, and reporting rather than teaching exploitation techniques or offensive testing.

### **How can NIST CSF 2.0 structure cybersecurity specialist operations?**

NIST CSF 2.0 structures operations through Govern, Identify, Protect, Detect, Respond, and Recover outcomes that connect risk decisions to defensive work and improvement.

### **How should cybersecurity specialists prioritize vulnerabilities and alerts?**

Cybersecurity specialists should prioritize vulnerabilities and alerts using asset criticality, exposure, exploitability, observed activity, control coverage, business impact, confidence, and response urgency.



## **What belongs in a Cybersecurity Specialist Operations Playbook?**

A Cybersecurity Specialist Operations Playbook includes governance roles, asset dependencies, risk decisions, protection baselines, vulnerability workflows, telemetry coverage, detection cases, incident actions, recovery priorities, reports, and improvement owners.

## **Conclusion**

Participants take back a Cybersecurity Specialist Operations Playbook supported by risk dashboards, control maps, defense baselines, vulnerability workflows, detection registers, incident plans, recovery maps, and reports. It changes disconnected security tasks into coordinated operational decisions. The playbook provides a repeatable basis for prioritization, escalation, response, recovery, and improvement.