CertCop

CLOUD SECURITY & FEDRAMP

CERTCOP

CLOUD SECURITY & FEDRAMP

Exam Number : FRCS-CertCop-003

About CertCop

CertCop, a globally integrated knowledge solution company has partnered with leading vendors to provide high-quality and effective professional training solutions in several areas of critical importance to enterprises including Project Management, Open Source, Software and Application Development, Information Security including Biometrics and others. World-class companies continuously examine business processes, and employee performance and aggressively apply solutions to help them improve in training their employees to keep up with the technology and stay effective in an ever-changing technology environment. CertCop can assist you in achieving and maintaining your competitive edge.

1. Certified and highly experienced instructors
2. CertCop Flexible Scheduling (Days, evenings, weekends)
3. Delivery Methods: Virtual Live/In-Class/On-site/1 on 1/ On-Demand
4. CertCop Curriculum is of High Quality, Extensive, and Industry Standard.

MIND THE GAP

Proud to be one of the GLOBAL LEADERS in

CertCop Affiliation

10+

Affiliated Certification Vendors

Upcoming Cyber Security Training

100+

CertCop Certcamps

CertCop Trainings

1000+

Corporate and Govt. Agencies Trained

CERTIFIED CYBERCOP CLOUD SECURITY & FEDRAMP

The Certified CyberCop Cloud Security & FedRAMP program is an in-depth training initiative that prepares cloud service providers (CSPs) and other stakeholders to successfully navigate the complexities of FedRAMP authorization. FedRAMP (Federal Risk and Authorization Management Program) is a U.S. government-wide initiative that standardizes the process for security assessment, authorization, and continuous monitoring of cloud products and services. Achieving FedRAMP compliance can be challenging without proper training, as it requires a deep understanding of regulatory requirements, security frameworks, and assessment processes. This program not only covers FedRAMP requirements but also provides guidance to help CSPs avoid common pitfalls, saving time and resources on the path to government sector growth.

FedRAMP Goals

- Accelerate the Adoption of Secure Cloud Solutions: Streamline the process of using assessments and authorizations to deploy cloud solutions faster.
- Enhance Security Confidence: Improve the security posture of cloud solutions and increase trust in the security assessment process.
- Achieve Consistent Security Authorizations: Utilize a baseline of standards for cloud product approval both within and outside FedRAMP.
- Ensure Uniform Application of Security Practices: Apply established security best practices consistently across all cloud products.
- Promote Automation and Real-Time Monitoring: Enhance continuous monitoring through increased automation and access to near real-time data.

REQUIREMENTS

- Basic knowledge of cloud computing and information systems is required.
- CompTIA Cloud Essentials or Cloud+ training is recommended.
- Basic to intermediate proficiency in Linux is beneficial; candidates are encouraged to learn foundational Linux skills to maximize the course's value.

DURATION

Instructor-Led Training 40 H Training

Alignment with NICE Framework:

The program aligns with the National Initiative for Cybersecurity Education (NICE) framework by focusing on the Knowledge, Skills, and Abilities (KSAs) required for various cloud security roles:

Knowledge Areas Covered:

- Cloud Security Principles: Understanding cloud architectures, secure configuration management, and network security.
- Risk Management: Familiarity with FedRAMP risk management frameworks, including NIST and other regulatory requirements.
- Compliance: Training in achieving regulatory compliance, especially for cloud service providers.

Skills Developed:

- Risk Assessment and Analysis: Conducting security assessments and identifying vulnerabilities.
- Security Operations and Monitoring: Implementing secure development practices, automation, and monitoring.
- Incident Response and Recovery: Establishing response strategies and performing forensic investigations.

Abilities Gained:

- Compliance Planning: Preparing for FedRAMP assessments with comprehensive planning.
- Security Automation: Implementing tools for continuous monitoring and real-time security analysis.
- Security Plan Development: Developing system security plans and control documentation.

7 Pillars of Self-Assessment for CSPs:

The program also covers the 7 pillars of self-assessment, providing a deep understanding of the level of effort needed to complete a FedRAMP assessment, including documentation, implementation, monitoring, and continuous improvement. This structured approach ensures that CSPs can successfully meet FedRAMP authorization requirements while avoiding common mistakes that can delay compliance efforts.

Course Benefits:

By completing the Certified CyberCop Cloud Security & FedRAMP program, participants will gain:

- A thorough understanding of FedRAMP requirements.
- Practical skills to navigate the FedRAMP authorization process.
- Guidance on avoiding common challenges faced during compliance efforts.
- The knowledge to implement secure cloud solutions while adhering to U.S. federal security standards.

The training is ideal for individuals aiming to advance their careers in cloud security and for organizations seeking to expand their cloud services within the U.S. government sector as well as for Government organizations who are seeking Cloud services and deal with Cloud Security and FedRAMP..

Course Overview

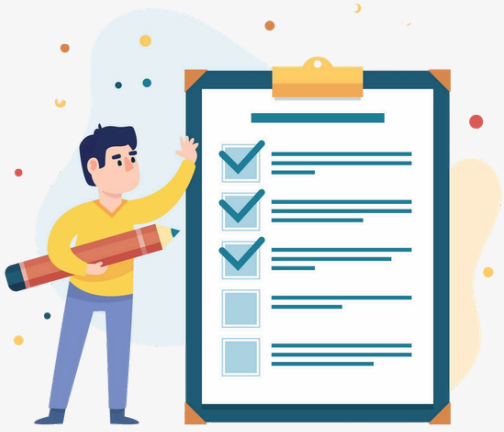
The Certified CyberCop Cloud Security & FedRAMP – Fourth Edition course provides comprehensive training in cloud security, federal cybersecurity requirements, and the FedRAMP certification lifecycle. It covers core cloud concepts, service and deployment models, shared responsibility, Zero Trust, IAM, MFA, encryption, key management, logging, monitoring, threat modeling, and cloud-native security, while also introducing major federal frameworks such as FISMA, FIPS 199, FIPS 200, NIST RMF, NIST SP 800-53 Rev. 5, NIST SP 800-37, and NIST SP 800-171.

The course explains the complete FedRAMP process, including the roles of Cloud Service Providers, 3PAOs, federal agencies, Authorizing Officials, the FedRAMP PMO, and the FedRAMP Board. Learners study authorization reuse, security control implementation, independent assessments, Marketplace listing, continuous monitoring, vulnerability management, remediation, and key authorization documents such as the SSP, SAP, SAR, and POA&M.

The Fourth Edition also includes updated coverage of FedRAMP 20x, CR26, Key Security Indicators, OSCAL, machine-readable security evidence, compliance automation, and continuous certification, along with practical cloud security implementation across AWS, Microsoft Azure, and Google Cloud. The program is designed to prepare learners for both the CertCop Cloud Security & FedRAMP certification exam and real-world cloud security and federal compliance responsibilities

Exam Details

Course Name : Certified CyberCop – FRCS
Required exam – FRCS-CertCop-003
Number of questions – Maximum of 90
Types of questions – Multiple-choice and performance-based
Length of test – 180 minutes
Passing score – 70% – This test has no scaled score; it's pass/fail only.
Languages – English
Retirement – Usually three years after launch
Testing Provider – Online proctoring: ExamIT.com
Certification Exam Voucher – $495 USD



Chapter 1 – Introduction to Cloud Computing
Understand the evolution, characteristics, benefits, risks, and business drivers of cloud computing. Learn government cloud adoption, digital transformation, cloud readiness, and cloud adoption strategy.

Chapter 2 – Cloud Architecture
Explore compute, storage, networking, IaaS, PaaS, SaaS, serverless, containers, hybrid cloud, and multi-cloud architectures. Understand shared responsibility, control inheritance, and secure architecture selection.

Chapter 3 – Cloud Security Fundamentals
Learn how to protect cloud data, applications, identities, and infrastructure using security-by-design principles. Covers CIA, Zero Trust, IAM, MFA, encryption, logging, monitoring, threat modeling, and common cloud threats.

Chapter 4 – Identity & Access Management
Learn identity lifecycle management, authentication, authorization, RBAC, privileged access, service accounts, federation, and least privilege. Understand secure credential, secrets, and privileged-access management.

Chapter 5 – Data Security
Learn data classification, encryption, key management, tokenization, DLP, backup, recovery, storage protection, and database security. Understand how to protect sensitive cloud data.

Chapter 6 – Network Security
Understand VPCs, subnets, routing, firewalls, security groups, segmentation, VPNs, and Zero Trust networking. Learn how monitoring and microsegmentation reduce unauthorized access.

Chapter 7 – Cloud-Native Security
Secure containers, Kubernetes, serverless applications, APIs, microservices, CI/CD pipelines, and Infrastructure as Code. Learn DevSecOps and automated security practices.

Chapter 8 – AWS Security
Learn AWS IAM, Organizations, Security Hub, GuardDuty, Inspector, Config, CloudTrail, encryption, monitoring, and multi-account security.

Chapter 9 – Microsoft Azure Security
Explore Microsoft Entra ID, Defender for Cloud, Sentinel, Azure Policy, Key Vault, Azure Monitor, and Azure Government security capabilities.

Chapter 10 – Google Cloud Security
Learn Google Cloud IAM, Security Command Center, Cloud KMS, Cloud Armor, Audit Logs, Assured Workloads, governance, and compliance.

Chapter 11 – Federal Cybersecurity Framework
Understand FISMA, FIPS 199, FIPS 200, NIST RMF, NIST SP 800-53, NIST SP 800-37, NIST SP 800-171, and the FedRAMP Authorization Act.

Chapter 12 – FedRAMP Fundamentals
Learn FedRAMP purpose, governance, Marketplace, CSP, 3PAO, agency, PMO, FedRAMP Board, and Authorizing Official responsibilities.

Chapter 13 – FedRAMP Security Controls
Study FedRAMP security and privacy controls based on NIST SP 800-53 Revision 5, including control families, implementation, evidence, and assessment.

Chapter 14 – FedRAMP Authorization Process
Understand preparation, readiness, security-control implementation, independent assessment, authorization, and ongoing monitoring.

Chapter 15 – FedRAMP Documentation
Learn the structure and purpose of SSP, SAP, SAR, POA&M, supporting evidence, documentation consistency, and version control.

Chapter 16 – FedRAMP Assessment
Understand how 3PAOs evaluate security controls through examination, interviews, testing, vulnerability scanning, and penetration testing.

Chapter 17 – FedRAMP 20x
Explore continuous, risk-based, and automated certification using Key Security Indicators, certification classes, and machine-readable evidence.

Chapter 18 – Continuous Monitoring
Learn vulnerability scanning, remediation tracking, change management, incident reporting, continuous evidence collection, and ongoing risk management.

Chapter 19 – OSCAL & Automation
Understand OSCAL, machine-readable FedRAMP documentation, compliance automation, evidence validation, and configuration-drift detection.

Chapter 20 – Incident Response
Learn incident preparation, detection, analysis, containment, eradication, recovery, reporting, and post-incident review in cloud environments.

Chapter 21 – Governance, Risk & Compliance
Learn security governance, risk management, risk registers, risk acceptance, compliance management, audit readiness, and continuous improvement.

CLIENTS TESTIMONIALS

I had a fantastic experience with CertCop. Their attention to detail, dedication to their students, and the overall quality of their offerings make them stand out. The company's professionalism and commitment to providing top-tier service are truly commendable. I would recommend CertCop to anyone in the cybersecurity field.

H. Medina - US DoD

CertCop's customer service is exceptional. The team is highly responsive, professional, and dedicated to helping their clients succeed. Whether it's through the provided resources or the overall support, CertCop ensures a positive experience every step of the way. I can't recommend this company enough!

R. Walter - USMC

CertCop is an amazing company that offers not only high-quality services but also incredible support. They provide valuable resources that truly help students excel. The entire team is dedicated to ensuring customer satisfaction, making the learning experience seamless and enjoyable. I would gladly recommend CertCop to anyone looking for a trustworthy and reliable partner.

Helen - US DoD

CertCop is a company that truly prioritizes its clients. Their dedication to providing outstanding support and ensuring that every need is met sets them apart from the rest. The professionalism of their team and their commitment to delivering value make them a trusted partner in the cybersecurity space. I'm extremely satisfied with their service!

Morgan - Developer

50+ Certcamp Location Across the Globe

Certcop

info@certcop.com
www.CertCop.com

CertCop