CCO®

ROCHESTON CERTIFIED
CYBERSECURITY
COMPLIANCE OFFICER

Silotech
Academy

Program Guide

ROCHESTON CERTIFIED CYBERSECURITY COMPLIANCE OFFICER CERTIFICATION

Rocheston Certified Cybersecurity Compliance Officer Certification is a comprehensive program designed to equip IT professionals with the knowledge and skills necessary to ensure their organizations' compliance with applicable cybersecurity regulations and standards. Participants will gain an in-depth understanding of the compliance requirements of common industry standards such as PCI-DSS, HIPAA, EUNISA, GDPR, NIST-53 (National Institute of Standards and Technology Cybersecurity Framework), SOC2 (Service Organization Controls 2) and ISO/IEC 27000, COBIT.

REGULATIONS AND STANDARDS

This program will provide participants with an understanding of the importance of cybersecurity compliance and the various regulations and standards that need to be addressed. Through lectures, hands-on activities, and discussions, participants will explore the components of a cybersecurity compliance program, including risk assessment and management, policy and control establishment, and incident response. Participants will learn best practices for monitoring and auditing compliance, as well as methods for responding to audit findings and regulatory violations.

THE DEMAND FOR CYBERSECURITY PROFESSIONALS

The demand for cybersecurity professionals is growing rapidly due to the increasing number of cyber threats and the need to protect sensitive data. As a result, organizations are looking for qualified and experienced professionals who can help them protect their networks and systems against cyber threats.

The demand for CCO® is growing because many organizations are recognizing the need to protect their systems and data from cyberthreats. CCOs are often in high demand because they are knowledgeable about the various cybersecurity regulations and can help organizations implement the necessary security measures. Additionally, they often have the skills and knowledge necessary to understand the various cyber threats and how they can be addressed.

Overall, the demand for qualified and experienced cybersecurity professionals is growing, and the need for CCOs is no exception. As organizations recognize the need to protect their networks and data, they are increasingly turning to CCOs to help them meet their security requirements.

WHAT DOES THE CCO® PROGRAM COVER?

The CCO® Certification program provides an in-depth look into the various compliance standards and best practices related to cybersecurity. With the ever-increasing demand for secure digital networks, organizations must remain on the cutting edge of compliance standards. This program provides participants with the skills and knowledge to stay ahead of the curve and ensure the safety of their digital assets.

The certification covers the most important compliance standards such as the Payment Card Industry Data Security Standard (PCI-DSS), the Health Insurance Portability and Accountability Act (HIPPA), the National Institute of Standards and Technology (NIST-53), Service Organization Control 2 (SOC2), and the International Organization for Standardization (ISO), GDPR, ISO/IEC 27000, COBIT, etc.

Throughout the course, participants will gain an extensive understanding of each standard, as well as the related best practices. Topics will include an introduction to the standards, an overview of the associated requirements, and best practices for implementation and maintenance. Participants will learn the importance of compliance documentation and how to audit, monitor, and report on security compliance.

EMERGING CYBERSECURITY TECHNOLOGIES

The certification also covers risk management, incident response, and how to create and manage a robust cybersecurity program. Participants will become familiar with emerging security trends and be able to devise and implement plans to maintain compliance with the various standards.

At the end of the program, participants will have the knowledge and skills to effectively manage and monitor the security of their organization.

You will master topics such as the fundamentals of cybersecurity compliance, risk management, information security and assurance, SOC, Zero-trust, DevSecOps, cybercrime investigations, data privacy and protection, incident response, audit and compliance, cloud security and legal aspects of compliance.

Students will develop the skills and knowledge necessary to identify, assess, and mitigate risks associated with data protection, compliance, and cybersecurity.

THE JOB ROLE OF A CCO

A Certified Cybersecurity Compliance Officer (CCO®) is responsible for ensuring that a company's cybersecurity policies and procedures are compliant with industry and government regulations. This person must be knowledgeable in the areas of laws and regulations related to network security, data protection, and privacy.

The CCO® is responsible for developing and maintaining a comprehensive cyber security strategy that is aligned with the organization's overall business strategy. This includes creating plans to reduce cyber security risks, implementing cyber security controls, and ensuring that the organization is in compliance with relevant laws and regulations. The CCO® is also responsible for managing the organization's cyber security programs, such as security awareness training, policy enforcement, and threat detection. They must identify and assess cyber security risks and develop and implement measures to mitigate them. The Certified Cybersecurity Compliance Officer must also monitor the effectiveness of the cyber security program and update it regularly.

The CCO® must also have a strong understanding of cyber security technology and tools, including encryption and authentication technologies, firewalls, intrusion detection and prevention systems, and other security measures. The CCO® must also be familiar with cyber security laws and regulations, such as the Health Insurance Portability and Accountability

Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and the Sarbanes-Oxley Act (SOX), NIST-53, GDPR, CCPA, etc.

The CCO® must also be knowledgeable about cybersecurity best practices, such as patch management, vulnerability management, cloud security, devsecops, penetration testing, threat intelligence and user access management. The CCO® must also be able to communicate effectively with other departments and stakeholders in order to ensure that the organization's cyber security policies and procedures are being followed. The CCO® must be able to provide guidance and advice to the organization on cybersecurity matters.

The CCO® will be responsible for the following tasks:

1. Developing and maintaining a cybersecurity compliance program that is compliant with industry and government regulations

2. Developing and implementing policies, procedures, and processes to ensure compliance

3. Identifying and assessing potential risks associated with cybersecurity and compliance

4. Coordinating with departments and teams to ensure compliance with cybersecurity policies and procedures

5. Analyzing and monitoring cybersecurity threats and vulnerabilities
   Investigating potential security breaches

6. Establishing and maintaining relationships with external partners and vendors

7. Working with the IT department to ensure security controls are in place

8. Developing and delivering training programs for employees on cybersecurity policies and procedures

9. Working with the legal department to ensure compliance with applicable laws and regulations

10. Preparing and presenting reports to senior management on the status of cybersecurity compliance

11. Ensuring that security audits are conducted regularly and any issues are addressed in a timely manner

12. Collaborating with other departments to ensure that all systems, networks, and applications are secure
    Staying up-to-date with changes in industry regulations and best practices to ensure compliance.

WHY YOU NEED THE CCO CERTIFICATION

By enrolling in the CCO® Certification Program, you will gain a comprehensive understanding of the latest cybersecurity compliance regulations, standards, and best practices and the tools and strategies to ensure the safety of your digital assets and data. You will also have the opportunity to develop your cybersecurity expertise and earn a recognized certification that will be recognized by employers and institutions in the industry.

1. **Understand the Latest Cybersecurity Compliance Requirements:** The CCO® Certification Program is designed to provide you with the latest information on the current and emerging cybersecurity compliance regulations, standards, and best practices. You will gain a deep understanding of the regulations and guidance from the National Institute of Standards and Technology (NIST), the Federal Trade Commission (FTC), and other leading organizations and institutions.

2. **Learn How to Implement a Cybersecurity Compliance Program:** The CCO® Certification Program will teach you how to develop, implement, and manage a comprehensive cybersecurity compliance program that meets the requirements of the latest cybersecurity regulations, standards, and best practices. You will learn techniques for assessing your organization's risk, developing security policies and procedures, and

implementing appropriate controls and measures to protect your data and systems.

3. **Develop Your Cybersecurity Expertise:** The CCO® Certification Program includes comprehensive training materials, workshops, tools, templates, interactive exercises, and real-world case studies to help you expand your knowledge and gain hands-on experience in the field. You will have the opportunity to discuss and debate the latest developments in cybersecurity with experts from the industry and refine your skills through practical application.

4. **Earn a Recognized Certification:** Once you complete the CCO® Certification Program, you will receive a certificate and a Rocheston's seal of approval that will be recognized by employers and institutions in the industry. This certification will demonstrate to employers that you have the technical knowledge and experience to effectively manage and protect their digital assets and data. This certification will open up new opportunities in the field and can set them apart from other applicants.

5. **Network with Industry Professionals:** The CCO® Certification Program provides a platform for networking with other cybersecurity professionals and experts in the industry. You will be able to share best practices and discuss the latest developments in the field, as well as gain valuable contacts and insights into the industry.

6. **Latest regulations:** The CCO® Certification program provides comprehensive training in all aspects of cybersecurity compliance, including the latest regulations and best practices. This program gives individuals a thorough understanding of the complexities of cybersecurity compliance and the strategies and tools needed to meet compliance objectives.

7. **Compliance requirements:** Participants in the program will develop a deep knowledge of the legal and regulatory requirements of cybersecurity compliance and the ability to effectively design and implement a compliance program. They will also gain an understanding of the different types of compliance requirements, such as data privacy, data security, and incident response.

8. **In-depth topics covered:** The program covers a variety of topics, from risk management to data governance, and provides hands-on training in the latest cybersecurity compliance tools. Participants will also learn how to create policies, procedures, and reports, as well as how to conduct audits and assess compliance.

9. **Upon completion of the program**, participants will be well-prepared to lead teams and organizations in developing and implementing effective cybersecurity compliance programs. They will also be able to identify and manage risks, as well as develop strategies

for mitigating those risks.

10. **Delivery formats:** The program is offered in a variety of formats, including onsite and online courses, allowing participants to learn at their own pace and in their own time. There is also the option of completing the program in a group setting or receiving one-on-one training.

11. **Experienced instructors:** The program is taught by experienced cybersecurity professionals in the field who are dedicated to providing the highest quality of instruction and support. Participants will benefit from their extensive knowledge and experience, and will get the opportunity to network with like-minded professionals.

The Rocheston Certified Cybersecurity Compliance Officer Certification program is an excellent choice for anyone looking to gain the skills and knowledge necessary to work in the field of cybersecurity compliance. It is a worthwhile investment for those looking to further their career in this rapidly growing area.

WHO SHOULD ATTEND THE CCO® PROGRAM

The CCO® Certification is an ideal program for anyone looking to take their cybersecurity career to the next level. This program is best suited to experienced cybersecurity professionals, such as Chief Information Security Officers (CISOs), IT security managers, security architects, security analysts, and IT compliance professionals.

This certification program provides invaluable information and insight into the latest trends, best practices, and techniques for cybersecurity compliance. Professionals who attend this program will gain a comprehensive understanding of the fundamentals of cybersecurity compliance, including risk assessment and management, incident management and response, and data security.

They will also learn about the legal, regulatory, and organizational structures that support cybersecurity compliance and gain an understanding of the various tools and technologies used to implement and maintain a secure environment. In addition, attendees will build a comprehensive portfolio of cybersecurity compliance documents, such as policies and procedures, security incident response plans, and security audits.

3 YEARS EXPERIENCE RECOMMENDED

The program is designed to equip participants with the knowledge and skills to become successful cybersecurity compliance officers. It is open to anyone with a minimum of three years of experience in the field of cybersecurity, and the necessary qualifications to demonstrate a high level of knowledge and expertise in the subject matter.

The program is also suitable for IT professionals looking to transition into a cybersecurity role, such as IT security analysts, security engineers, and IT managers. Participants who already have a degree in Computer Science, Information Technology, or a related field may find this certification beneficial in improving their career prospects.

The CCO® Certification Program is an excellent choice for experienced cybersecurity professionals who are eager to take their careers to the next level. It provides participants with the skills and knowledge needed to become successful cybersecurity compliance officers and offers a comprehensive portfolio of documents that can be used to implement and maintain a secure environment.

CCO

THE CCO CERTIFICATE

Upon successful completion, participants will receive their Rocheston Certified Cybersecurity Compliance Officer Certification, which is recognized by industry associations and organizations worldwide.

The program culminates with a final exam, the Rocheston Certified Cybersecurity Compliance Officer Exam. Once students have successfully completed the program, they will receive their CCO® certificate and be eligible to begin their careers as Cybersecurity Compliance Officers.

CCO EXAM INFORMATION

1. **Exam Title:** Certified Cybersecurity Compliance Officer

2. **Exam Code:** RCT-90

3. **No. of Questions:** 50

4. **Exam Format:** Scenario Based MCQ

5. **Passing Score:** 70%

6. **Duration:** 3 hours

7. **Exam mode:** Online using Rocheston Ramsys Exam Proctoring System

HOW TO PREPARE FOR THE CCO EXAM

You can prepare for CCO® exam using Rocheston CCO® self study guide. The Rocheston Certified Cybersecurity Compliance Officer (CCO) exam is an important certification for those aspiring to become cybersecurity professionals. The exam is designed to test the knowledge and understanding of the various components of cybersecurity compliance. Preparation for the RCT-90 CCO exam requires a comprehensive understanding of the topics covered in the exam guide book.

The CCO® exam guide book contains thousands of mcq practice questions, which can be used to prepare for the exam. First, it is important to read through the entire guide book and become familiar with the topics and questions covered. Secondly, create study plans that focus on the important topics and sections of the exam. Thirdly, use the practice questions provided in the guide book to reinforce the concepts and understand the different types of questions that may be asked on the exam. By following these steps and using the CCO® exam guide book, you should be able to pass the RCT-90 exam with flying colors. Good luck!

CCO CERTIFICATION DOMAINS

The CCO® exam covers the following cybersecurity compliance domains

Domain 1: Cybersecurity Principles and Ethics

Domain 2: Cybersecurity Models and Frameworks

Domain 3: Cybersecurity Legal Regulatory Governance and Compliance

Domain 4: Cybersecurity Policies and Procedures

Domain 5: Asset Discovery, Classification and Management

Domain 6: Risk Assessment

Domain 7: Identity and Access Management

Domain 8: Cybersecurity Design and Architecture

Domain 9: Network Security Compliance

Domain 10: Audits and Compliance Checks

Domain 11: Cyberthreat Intelligence

Domain 12: Security Operations Center (SOC)

Domain 13: Incident Handling and Response

Domain 14: System and Database Security

Domain 15: Business Continuity and Disaster Recovery

Domain 16: Physical and Biometrics Security

Domain 17: Secure Coding and Devsecops

Domain 18: Data Protection and Cryptography

Domain 19: Cybersecurity Awareness Training

Domain 20: Cybersecurity Performance Metrics

Domain 21: Supply Chain Risk Management

Domain 22: Zero-Trust Architecture

Domain 23: Cloud Security Compliance

Silotech Academy

[**CYBERSECURITY**
COMPLIANCE OFFICER]

Certified by Rocheston®

https://www.silotech-academy.com/rocheston