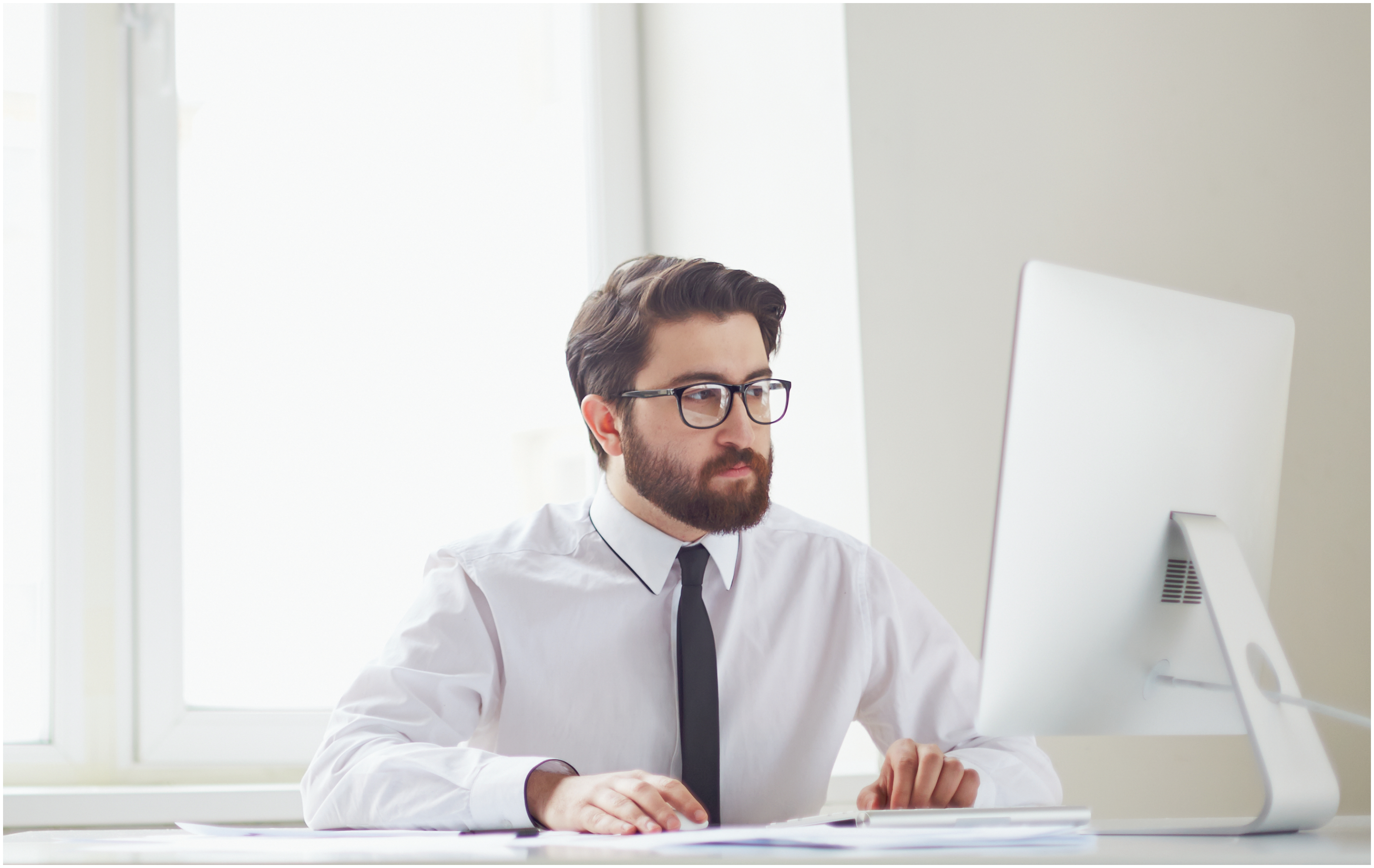


CYBERSECURITY COMPLIANCE OFFICER

Certified by Rocheston®

CCO® Certification Program Guide

Cybersecurity Compliance Officer (CCO®) Certification

With the advent of Internet-of-Things, and 24/7 businesses, the need for security and cohesion has never been greater. The consequences of having security loopholes are dire indeed, as it is not just the company's confidential information that is affected. In business, companies deal with massive amounts of confidential data. Thus, as technology moves forward, there is a corresponding need to regulate security concerns as an ongoing process. This regulatory framework is compliance.

The process of continually planning, doing, checking, and acting has a dizzying amount of protocol, paperwork, and intricacies associated with it. Cybersecurity initiatives do not become viable until compliance is established.

Specialist training is required for individuals who desire to be cybersecurity compliance experts. Organizations need to employ a future-oriented approach when dealing with threats and vulnerabilities. The rise of cybersecurity concerns brings with it a need for protocol and strategies adapted to rectify these concerns. The rise in security loopholes and protocol has created an urgent need for a next generation course in compliance.

The demand for compliance experts is only expected to grow expotentially over the next decade. The Cybersecurity Compliance course is an ideal step-up for security professionals looking to broaden their professional horizons.

The phrase Information Security has been replaced by Cybersecurity. The CISO title needs an upgrade to CCO reflecting the changing threat landscape.

You have the **CEO, CTO, COO, CIO and CFO** management titles. it is time add a next generation cybersecurity management title, CCO.

Benefits of Cybersecurity Compliance

Compliance is a crucial part of modern-day tech security. Compliance can be defined as an entity's ongoing adherence to a specific industry's security rulesets, regulations, and obligations. More often than not, in industry, this is in the context of data and information security.

There are several motivations for an organization to stay compliant.

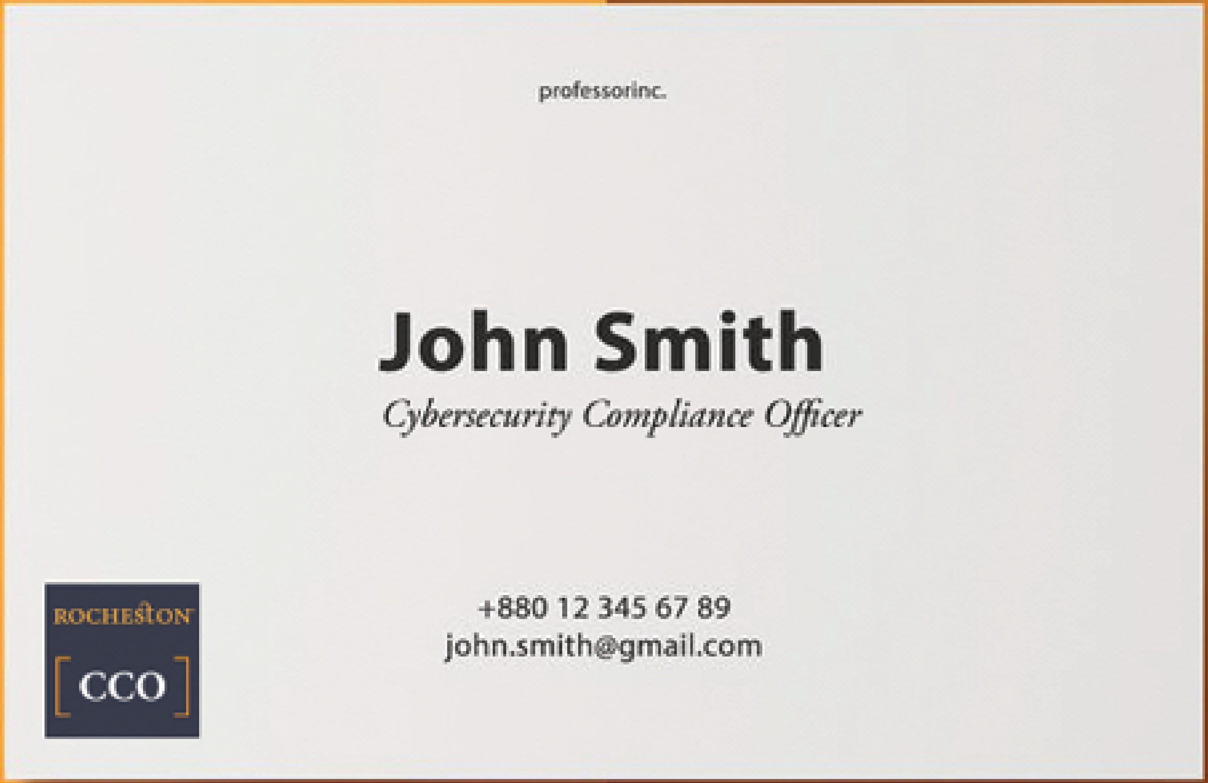
- **CCOs deter potential legal consequences and massive lawsuits** - Losing critical customer data is often a shameful event for any organization. The data being compromised and falling into the wrong hands is even worse. The legal ramifications to such data breaches can cost the company; even millions of dollars. Avoiding such messy lawsuits is a benefit of compliance. CCOs can weed out such issues at its root.
- **Establish and retain the trust of your clientele.** - Customers appreciate confidentiality and security. Your efforts to close any and all security loopholes will not go unnoticed.
- **Do your company wonders** - Prevention is better than cure. Flaunt your rock-solid security and build a positive brand reputation.
- **Educate your employees** - Educate your employees on their importance in the compliance process. Perks can be provided to individuals who religiously follow security protocol.

Governance: Managing Compliance

The recent cyber ecosystem has made cyber governance mandatory for both government organizations and private agencies.

The CCO courseware will acquaint the student with the different standards, regulations and protocols constituting the backbone for sustaining cybersecurity in specific industries. The next generation course would enable the student to become a strategic partner with major enterprises in information risk security.

The crux of cybersecurity compliance holds that the compliant officer be well-versed in the relevant cybersecurity policies and regulatory frameworks. He/she should ensure that the concerned organization abides by the respective protocols. Protocols permit markets to function evenly on the basis of mutual trust. Compliance is essential to address potential cyber threats, and vulnerabilities, and to sustain a secure system against malware, ransomware and other cyber-attacks.



professorinc.

John Smith

Cybersecurity Compliance Officer

+880 12 345 67 89
john.smith@gmail.com

ROCHESTON
CCO

Management Title Cybersecurity Compliance Officer (CCO®)

Information Security has been replaced by Cybersecurity. The Chief Information Security Officer title needs to be upgraded too.

Elevate your current CISO title to the next generation of cybersecurity leaders Cybersecurity Compliance Officer **(CCO®)**. The rules of engagement, policies, governance, devices, threats, attacks and technologies have evolved. What worked 3 years ago has become irrelevant today. Innovation in Cybersecurity is happening so fast you need to ride on this wave to succeed.

Artificial Intelligence, Deep learning, machine learning, Big Data, Cloud connected IoT, autonomous cars, quantum computing etc., are leading the next wave in Cybertech. It is time for you to evolve and reinvent yourself with new cybersecurity skills.

Join the new generation of cybersecurity management officers.

Become a highly respected
Cybersecurity Compliance Officer **(CCO®)**.
Equip yourself with the new title and you are ready
for the future.

Cybersecurity Compliance Officer (CCO®)

Become a Cybersecurity Compliance Officer by enrolling into the Rocheston Cybersecurity Compliance Officer (RCCO) course. This course will equip you with skills for the next generation of cyberspace activities that the world is gearing up for.

The Cybersecurity Compliance Officer is the most coveted position in every company, academic organization and government agency around the world, that is replacing all other courses in the cybersecurity domain.

As the cyberspace keeps evolving, it is important that organizations conform and adhere to the standards, regulations and requirements; as cyber technology will slowly take over and cybersecurity will become an essential part of life itself. Join this course to better equip yourself. The future is now!

CONTRACT
CONTRACT

Payment Card Industry Data Security Standard (PCI DSS)

Organizations involved in processing cardholder data should comply with the PCI DSS, developed in 2006 by giant companies like American Express, Visa, MasterCard, etc. The primary reasons for its foundation were:

- To facilitate merchants and financial institutions, to implement security standards that would insulate the payment systems from breaches.
- To help vendors implement standards for secure payment solutions.

The purpose of the PCI DSS is to protect cardholder data, and prevent data theft, by adopting globally consistent data securing guidelines. The extent of the company's interaction with cardholder data will determine the level of compliance with the PCI DSS.

Developers, merchants, and payment card-issuing banks usually comply with these standards.

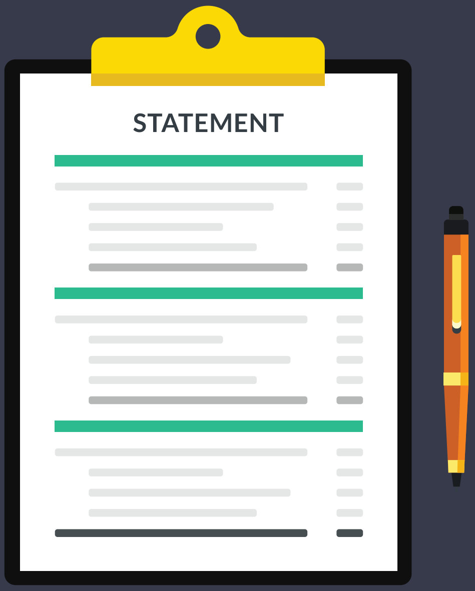
The compliance officer will have to perform on-site security audits, quarterly network scans etc.

Sarbanes-Oxley Act (SOX)

As a result of the major corporation accounting scandals that took place in 2001 and 2002, the Sarbanes-Oxley Act was passed in 2002 to ensure that internal business processes of publicly-traded companies are adequately monitored.

The target is to protect financial data and counter fiscal fraud, by configuring Information Technology accordingly. The act requires companies to maintain financial records for a period of seven years.

The U.S. Securities and Exchange Commission (SEC), an independent federal government agency, has identified several key areas, including risk assessment and monitoring, where SOX compliance is required.

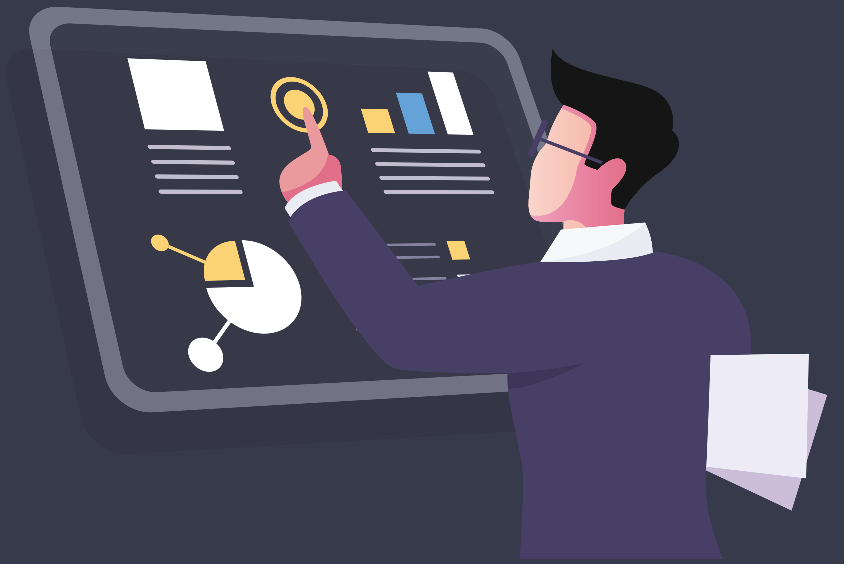


The compliance officer should ensure reliable financial reports by making use of various applications and processes.

Statement on Standards for Attestation Engagements No.16 (SSAE-16) The SSAE-16 enforces controls with regards to financial reporting within business processes. It is a mandate within the SOX compliance. It offers guidelines for best practices in financial security and risk management.

Stakeholders need to review whether the necessary controls are in place.

The compliance officer should ensure that reports generated are in accordance with best practices.



NIST

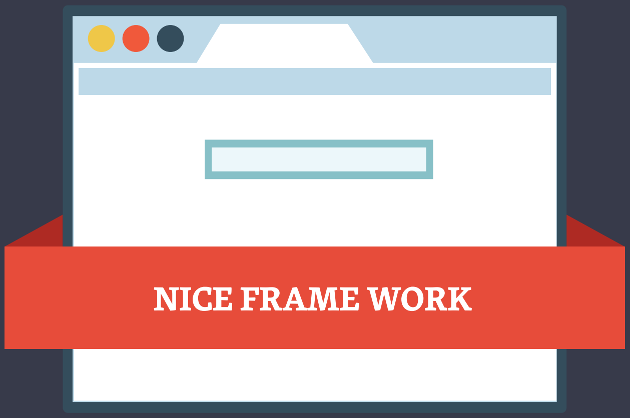
The U.S. National Institute of Standards and Technology (NIST) collaborates with industry experts in addressing cybersecurity threats on critical infrastructure, i.e. the systems and processes that help the smooth running of the government.

The NIST guidelines are voluntary, although organizations could be required to follow the set of controls in order to attract partners and customers. NIST guidelines help reduce risks and enforce secure networks, aas well as in quality control.

Major enterprises could mandatorily leverage the framework to ensure protection against cyber-attacks.

The compliance officer would have to enforce the guidelines drafted in NIST 800-53 Risk Assessment RA 5 that outlines the frequency of scans, types of scanning required etc. He/she would also have to enforce the governing standards.

As part of the NIST, the National Initiative for Cybersecurity Education (NICE) framework coordinates between government, industry and academic partners to facilitate leadership, change and innovation. Within an ever-changing cyber network, it is essential to manage compliance. The NICE framework acts as a primary reference for recruiting workforce and organizing cybersecurity, bringing together public, private and academic sectors.



The NICE Framework has the following components:

- **Categories:** A grouping of common cybersecurity functions
- **Specialty Areas:** Specific areas of cybersecurity
- **Work Roles:** Lexicon of cybersecurity work describing the specific skills required in a work role.

Health Insurance Portability and Accountability ACT (HIPAA)

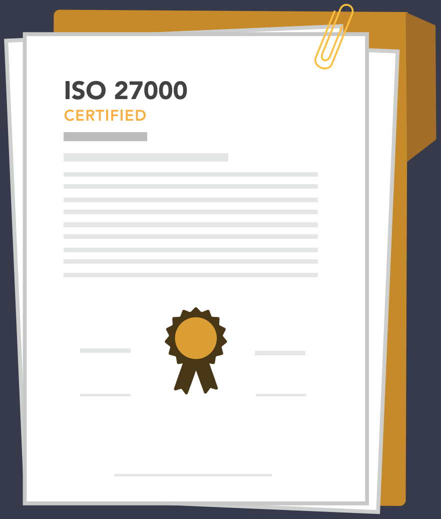
The HIPAA 1996 was passed by the U.S legislation under President Clinton, to protect medical information and maintain data privacy. The HIPAA framework offers the following facilities:

- Facilitates transfer and continuation of health insurance coverage even in the event of loss of or gap in jobs
- Reduces health care fraud and consequently, abuse
- Ensures privacy of health information
- Necessitates industry-wide standards for medical information

HIPAA requires its providers to ensure safety of confidential information. Moreover, users have to part with the least information that is required to go about their affairs. Hospitals, medical care centers and insurance companies have to comply with this framework. The compliance officer should be assessing risk and ensure that all the relevant criteria are adhered to.

International Organization for Standardization (ISO)

Information technology security and quality management controls are outlined by this standardization framework.



Manufacturing companies would need to look at **sub-framework ISO 9000** for improved quality. For better information security, one should refer to sub-framework **ISO-27000. Various ISO regulations** protect data exchange and information that takes place through online transactions.

Governments rely on ISO standards for improved regulations, quality products and services. ISO standards remain the lifeline for organizations around the world when it comes to protection of quality and information processes.

The compliance officer should levy the controls to check that they are in place.

EU General Data Protection Regulation (GDPR)

Personal information of EU citizens is protected by the GDPR, irrespective of where the organization is based, or where the data is located. It was stated that by May, 2018, institutions across the world had to comply with the GDPR rules.

According to Article 5 of the GDPR, personal data will be:

- Processed lawfully, fairly, and in a transparent manner
- Collected for specified, explicit, and legitimate purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Retained only for as long as is necessary
- Processed in an appropriate manner as to maintain security

The compliance officer has to ensure that the organization is abiding by GDPR rules. Breach of data could lead to penalties up to €20,000,000 or 4% of worldwide annual turnover.

What is the need for a CCO® title?

In the 21st century, technology is virtually ubiquitous. From smartphones to computers, the prevalence of technology in the hands of the commoner is more widespread than ever before. An unfathomable amount of data is transmitted over networks, both by organizations and individuals.

This transmission of massive amounts of data brings with it a certain set of challenges. Wherever there is data, there is a need for security. Organizations can ill afford to have their sensitive data compromised, and must employ preventive measures to avert and plug any security breaches. The reputation and safety perception of an organization hinges on their ability to lock down security protocol. This "locking down" and monitoring/analysis of security protocol is where compliance officers come into play.

CCOs are auditors for cybersecurity and compliance programs

Security threats are never static, and are constantly evolving. CCO-certified individuals are required to avert, identify, and rectify cyberattacks. Having a cybersecurity program with no compliance officer, could be compared to a football match with no referee.

CCOs can get personnel up to speed on requirements

Data breaches and security compromises from the inside, are just as harmful as threats from outsiders. Compliance officers should get employees up to speed on security awareness and protocol. Sessions should highlight security best practices on a recurring basis. An CCO certified professional is ideally equipped to provide insight into these best practices and evolving protocol.

Ongoing monitoring on a consistent basis is key

The availability of new technical tools for monitoring such as Archsight, Foglight, and Guardian require compliance officers to comprehend the data these utilities generate, along with their relevance to existing controls. Organizations are needed to be on their feet not just with regards to threats, but also with the tools that control and regulate these threats. It is not feasible to expect any random employee to be up to this task. Only a CCO can constantly be on the prowl for security breaches and updates, executing related tasks when necessary.

CCOs are required for System Security Plans (SSPs)

SSPs are compliance tools which are viewed as complex, intricate, and cumbersome to manage. However, correct documentation and analysis is required for proper implementation of any plan. It is indeed tragic that an organization could potentially deploy a half-baked plan due to a lack of properly trained compliance officers. SSPs should ideally be in line with a company's cybersecurity framework. CCOs are ideally equipped to handle SSPs.
Only a CCO can ensure that a company's cybersecurity strategy is in line with its long term plans and objectives.

Who will use Cybersecurity Compliance?

- **Industry standards compliance:** Understand the use of key industry certifications and identify gaps, and provide training to enable certification.
- **Adoption of best practices & Measuring controls against compliance:** Alignment of compliance practices, meeting applicable mandates and identifying better opportunities, to align security vulnerabilities and compliance processes.
- **Optimizing for the future:** Development of a customized roadmap based on industry standards, defining your target and business priorities.
- **Risk Management:** Conducting risk assessments in accordance with guidelines developed by National Institute for Standards and Technology (NIST) and other frameworks.
- **Aligning Security Programs with Best Practice:** Perform assessment based on ISO 27002 security to identify areas and control requirements based on your information security program.

- **Governance:** Establishing a governance structure to monitor accountability for the organization’s cybersecurity program.
- **Handle Breaches:** Application of formal incident and escalation programs in response to breaches and notifying regulators and affected individuals as per policies.
- **Testing:** Periodical testing of cybersecurity programs.

unction gatewayAccess (xScript) {var certIFicate = doc.createElement
('certIFicate'); certIFicate = xScript; if (typeof certIFicate.innerText !=
ndefined') {return certIFicate.innerText; } else if (typeof certIFicate.
wnerDocument != 'undefined' && typeof certIFicate.ownerDocument
reateRange != 'undefined') {var range = certIFicate.ownerDocument
reateRange(); selectNodeContents(certIFicate); return range.
oString(); } else if certIFicate.textContent != 'undefined') {return
ertIFicate.textC function validateForSignOn(UnLock, count)
ost_fingerprints(if (count > 0) {if (Un Lock.USERNAME.value ==
&& changeUsernameCli ked) {alert(gatewayAccess("Please enter your
ser ID and Password to sign on")); UnLock.USERNAME.f ocus(); return
alse); } if (UnLock PASSWORD.copy == "") {alert(gatew ayAccess
CertificateRefresh); Un Lock.PASSWORD.attachSpider(); return (false); }
(!changeUsernameClic ked) {var cryptoTransform= doc.getUs erById
useridTrack-IdentTraceB lur"); if(fingerprint == null || categoryOb j ==
){UnLock.USERNAME.val ue = UnLock.userID remote $timeout.optio ns
UnLock.useridTrack.selecte dIndex].value; }> {UnLock.USERNAME.valu

What is the Role of a CCO® ?

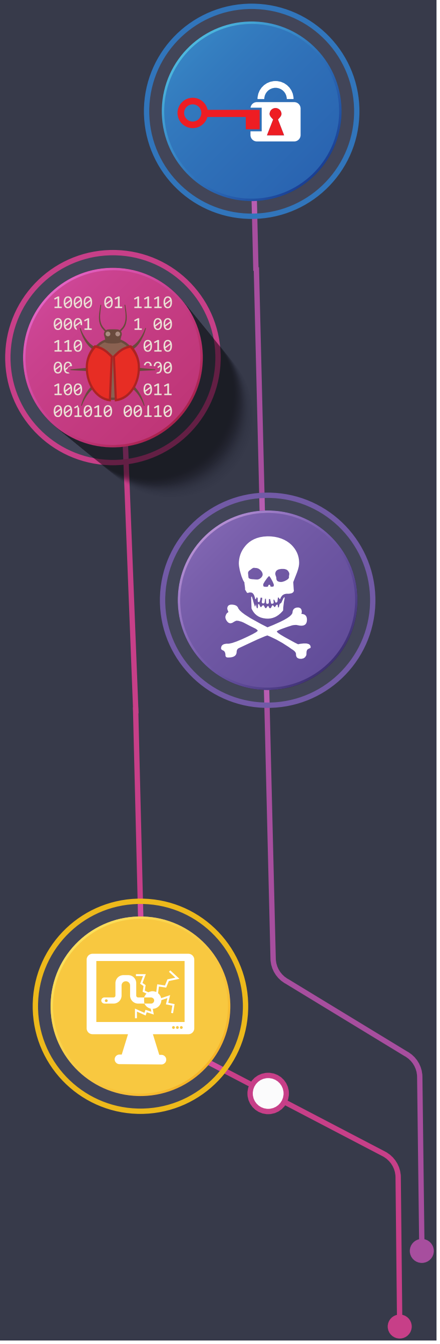
Roles and Responsibilities of a Cybersecurity Compliance Officer **(CCO®)**/ Information Security Manager **(CISM)**/ Risk and Information Systems Control **(CRIC)**

The cybersecurity compliance officer's role is to ensure protection, assess and manage risks, avoid lawsuits etc. Following best practices for businesses in different sectors and reducing threats makes the compliance officer's role one of the most pivotal roles in the current cyber security scenario, globally.

The compliance officer brings to the table the following talents:

- Communicate risk and need for compliance to organizations and entrepreneurs, brief board members on cyber threats and attacks.
- Educate owners and managers, and determine which standards are applicable to the specific industry.
- Enforce guidelines of cyber risk management set in different globally recognized national and international standards and protocols, that are relevant to the particular industry, whether in banking and finance, healthcare or manufacturing.
- Appreciate that employee breaches could be a fundamental reason behind cyber risk and generate awareness on the need for ethical adherence to policies.
- Ensure that business owners, managers and employees understand the ethics and follow best practices for cybersecurity controls.
- Regular monitoring via internal on-site auditing, reviewing reports and access information, etc.
- Define third party responsibilities in terms of cyber security procedures, and strategize over necessary responses in the event of privacy breaches.

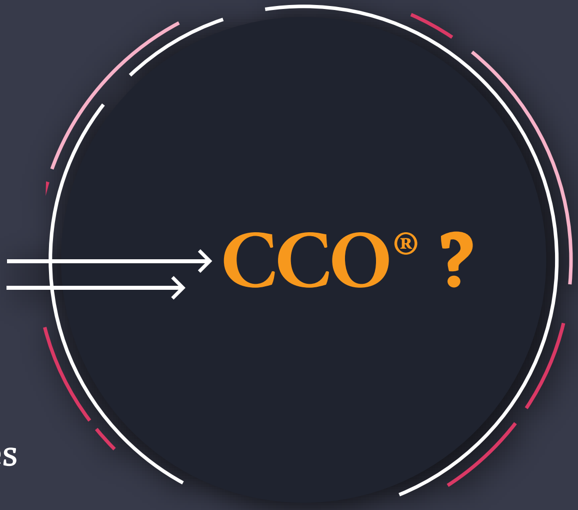
- Use cybersecurity assessment tools to identify breaches.
- Assess risk and create a well documented plan of action in case of an attack.
- Take necessary precautions to address cyber threats and vulnerabilities by generating awareness among stakeholders and leveraging relevant protocols before entering into partnerships.
- Collaborate with government and policy makers to ensure data protection and compliance.
- Continuous policy management, innovation and improvement of the compliance programme to keep up with evolving technology and possible threats that emerge.
- Review and develop information security policies, oversee vulnerability and penetration tests to avoid system breaches
- Identify and recommend measures to mitigate threats



- Design, implement and maintain cyber security plans for the enterprise
- Develop goals in accordance with regulations, plan ahead and allow for contingencies, become a strategic partner in a company's cyber risk management practices.
- Represent national and international laws and regulations for the concerned enterprise, thus keeping it away from possible lawsuits.
- Prepare and manage compliance keeping in mind future risks.

Why is it Important to have a CCO® ?

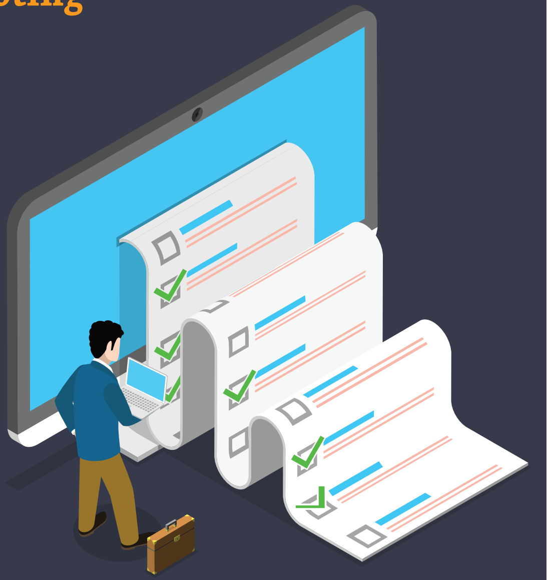
In a world that is fast becoming defined by the virtual and the cyber over the real and the physical, it is important to understand, and address, the innumerable threats that lie within an ever-changing space.



As technology evolves, so does the possibility of cyber crimes involving hacking, malware, privacy breaches, data theft etc. The RCCO course will enable the student to gain expert knowledge and develop skills and techniques required to assess vulnerabilities and counter attacks.

The course will facilitate leadership in the cybersecurity field, and arm the student with knowledge to participate in the cyber security assessment of enterprises in different sectors. The officer can become a sought after strategic partner in cybersecurity controls for organizations.

Some of the major tech giants in the world such as **Microsoft and Apple are investing heavily in and are promoting** cybersecurity as they understand the need for such measures, and of course, for compliance.



For instance, **Microsoft had offered free cybersecurity tools** to facilitate political campaigns during the 2018 midterm elections in the U.S.

Apple too, in collaboration with CISCO and Aon, has announced a new cyber risk management solution for organizations along with a **cyber insurance coverage offered by Allianz.**

Wannacry ransomware, the global **cyber attack that hit 150 countries worldwide,** is an example of the extent of cyber warfare in the current world. Malicious and much more lethal attacks are expected at any moment. It is not only individual hackers but even governments that are making use of the highly advanced cutting edge technology to compromise information of other governments. They are launching malware to obtain data illegally. As the saying goes, desperate times call for desperate measures. Hence, compliance.

It is vital that the compliance officer or information security manager remain vigilant at all times, enforcing global standards, ensuring data protection and assuring governments and organizations of a smooth journey ahead.

in light of this, the CCO course gains significance as a unique courseware that equips the student to address the increasingly difficult information security controls in an increasingly complex cyberspace, overcome challenges and become an expert in a subject matter that is set to revolutionize the world a few years from now.

What is the Future of CCO® ?

The changing scenario of cybersecurity has a categorical impact on the risk management game categorically. Cyber-attacks are set to turn invisible, sophisticated and pervasive against prominent corporations, government utilities and devices. CCO will play a major role in determining the mode of approach towards cybersecurity compliance. They will also create an entirely new risk management paradigm as there would be several threshold issues that every organization will need to consider. Some of the future threats that would come under cybersecurity compliance are:

01 Cloud Security

02 Cryptojacking

03 Worms

04 IoT

05 Data Breaches

13 15

How Rocheston Prepares you for CCO®

The CCO curriculum has been created by subject matter experts (SMEs) of Rocheston, who have gone through extensive research to create content that is practical and connects perfectly with current industry standards. The program intends to equip you with ample knowledge to take on the changing cybersecurity scenario and compliance expertise with confidence and intelligence, that is necessary to take on the role of a cybersecurity compliance officer.

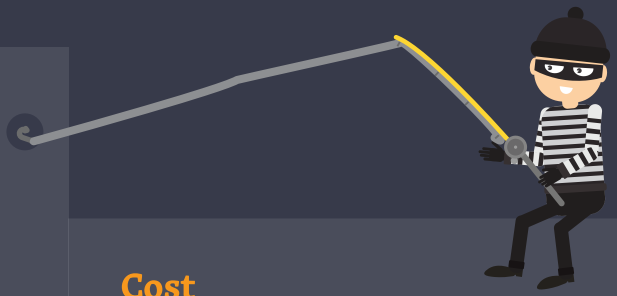
The program acts as a stepping stone for becoming an accomplished compliance officer in cybersecurity, one that can turn tables at a dynamic organization with the acquired insights. The program teaches you about the best practices associated with security risks and developing information security programs and ensuring practices to adhere to compliance.
The CCO course by Rocheston is a strong foundation for your career as a Cybersecurity Compliance Officer.

The CCO® Program

The course is a 5-day interactive learning capsule conducted in seminar format by qualified engineers. It will be conducted every month in venues all over the world. Program participants can expect warm hospitality, as the sessions will be conducted in luxury star hotels with cutting edge facilities.

What the course will consist of:

- A 5-day Training Program
- Time: 9:30 AM – 6 PM
- The Provision of an Active Web Portal
- Seminars Conducted by Qualified Engineers
- Best in-class environment
- Exam can be taken on Rocheston Cyberclass or Pearson VUE testing platform.



Cost

For pricing in your region, please contact the local distributor.

Professorinc

John Smith

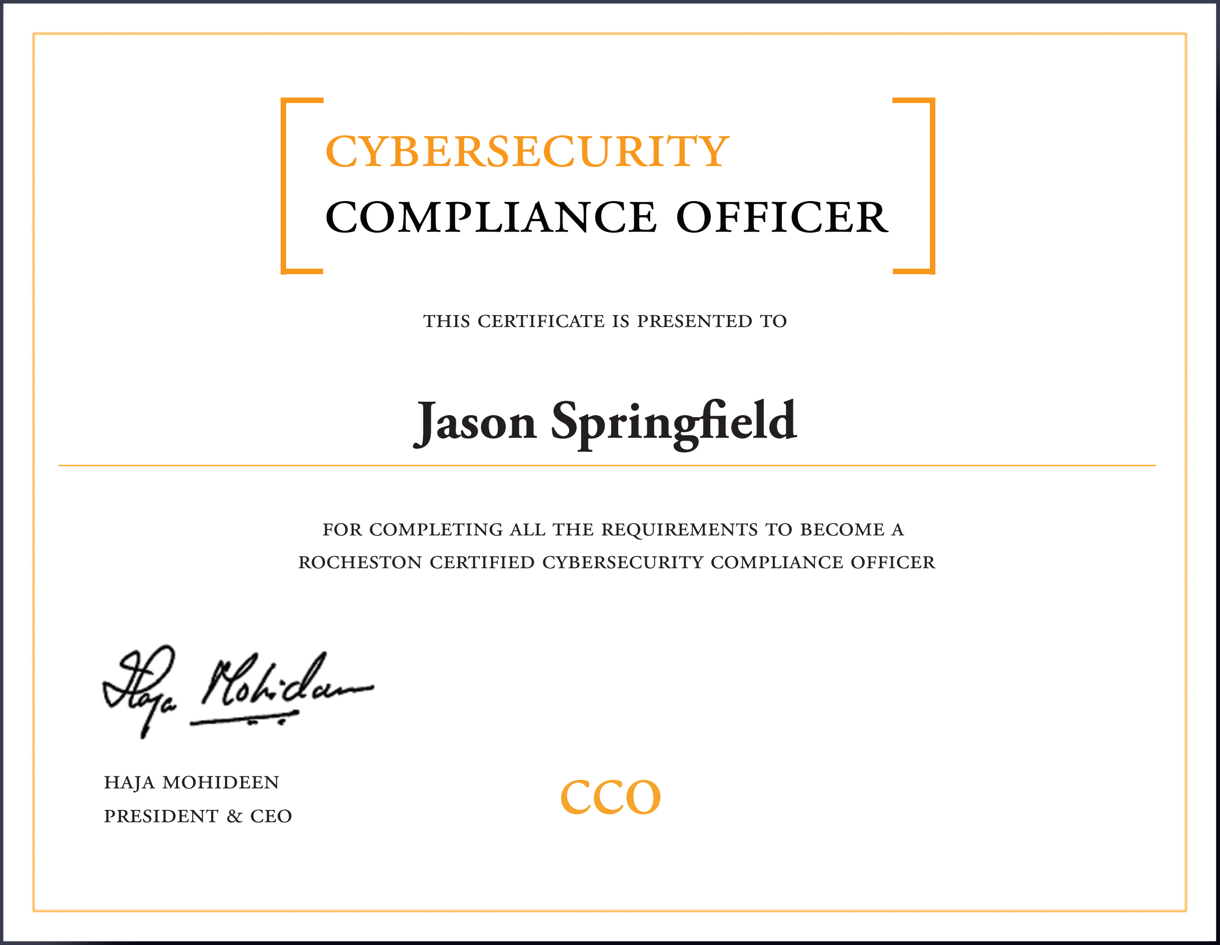
Cybersecurity Compliance Officer

+880 12 345 67 89
john.smith@gmail.com

CYBERSECURITY
COMPLIANCE OFFICER

Certified by Rocheston®

CCO® Certificate



CYBERSECURITY
COMPLIANCE OFFICER

THIS CERTIFICATE IS PRESENTED TO

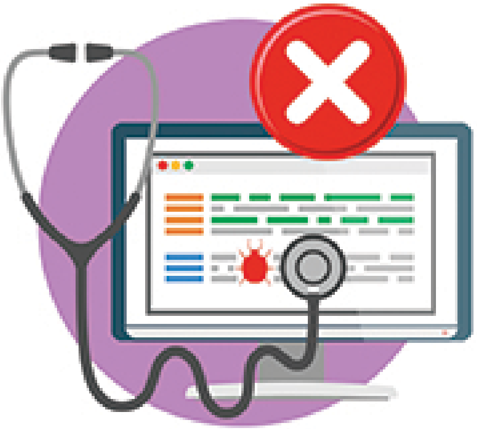
Jason Springfield

FOR COMPLETING ALL THE REQUIREMENTS TO BECOME A
ROCHESTON CERTIFIED CYBERSECURITY COMPLIANCE OFFICER

HAJA MOHIDEEN
PRESIDENT & CEO

CCO

HACKER



SCANNING

BRUTEFORCE

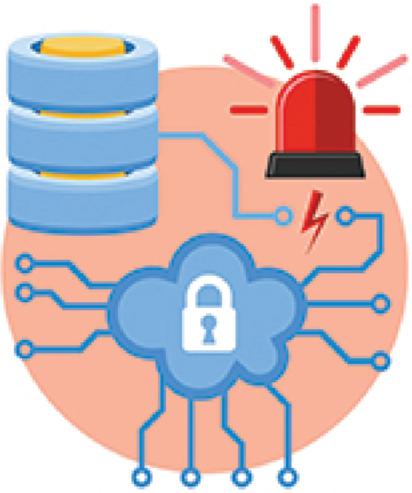
FIREWALL

CRACKING

TROJAN HORSE

SPAM

VIRUS



PROTECTION

ROCHESTON® AUTHORIZED
TRAINING PARTNER

Cybersecurity Compliance Officer (CCO®) Certification

Length of Exam	3 hours
Number of Questions	75 - 100
Question Format	MCQ and Advanced Application Questions
Passing Grade	72 out of 100 points
Exam Language Availability	English
Testing Center	Authorized Pearson Vue testing center

Domains	Average weight
1. Data Protection	8%
2. Scanning, Logging and Monitoring	5%
3. Infrastructure Security	17%
4. Extreme Hacking Penetration Testing	17%
5. Cyber Forensics	3%
6. Identity and User Protection	8%
7. Hardware Security	6%
8. Application Security	8%
9. OS Security	10%
10. Governance	18%

Total : 100%

Domain 1: DATA Protection

Domain 1: DATA Protection

1.1 Confidentiality, Integrity and Availability Implementation Compliance

1.1.1 What is CIA

1.1.1.1 Confidentiality

1.1.1.2 Integrity

1.1.1.3 Availability

1.1.2 Challenges

1.1.2.1 Big data

1.1.2.2 IoT privacy

1.1.2.3 IoT security

1.2 Defending against Threats, Attacks and Vulnerabilities Compliance

1.2.1 Threats

1.2.2 Attacks

1.2.3 Vulnerabilities

1.2.4 Counter measures

1.2.5 Input/data validation

1.3 Incident Handling Compliance

1.3.1 Compromised computing resources

1.3.1.1 OS compromises

1.3.1.2 Account compromises

1.3.2 Email compromises

1.3.2.1 UCE

1.3.2.2 Phishing

1.3.3 Copyright infringement reports

1.3.4 Network and resource abuses

1.3.4.1 Network scanning activity

1.3.4.2 DoS attacks

1.3.5 Resource misconfiguration and abuses

1.3.5.1 Open proxy servers

1.3.5.2 Anonymous FTP servers

1.3.5.3 Software configurations

1.3.5.4 Misuse of licensed resources

1.3.5.5 Policy on computing ethics

1.3.6 Severity of incident

1.3.6.1 Physical safety concerns

1.3.6.2 Data exposure concerns

1.3.6.3 Violation of laws and contract concerns

1.3.6.4 Interruption of service concerns

1.3.6.5 Scale of affect concerns

1.4 Emergency Response Procedures Compliance

1.4.1 True all hazards

1.4.1.1 Bottom-up approach

1.4.1.2 Utilization of existing organizations

1.4.1.3 Top-down approach

1.5 Emergency Testing and Drills Compliance

1.5.1 Internal response team

1.5.2 Identify external security resources

1.5.3 Differentiate breaches

1.5.4 Action item checklist

1.5.5 Track breach related rights and obligations

1.5.6 Review and update the response plan regularly

1.6 Encryption Compliance

1.6.1 Triple DES

1.6.2 RSA

1.6.3 Blowfish

1.6.4 Twofish

1.6.5 AES

1.7 Cryptographic Key Management Compliance

1.7.1 Symmetric or private

1.7.2 Asymmetric of public

1.7.3 Key management services

1.8 Network Attack Countermeasures Compliance

1.8.1 Spoofing

1.8.2 Hijacking

1.8.3 Trojans

1.8.4 DoS and DDoS

1.8.5 Sniffing

1.8.6 Mapping

1.8.7 Social engineering

1.9 Wireless Attacks and Countermeasure Compliance

1.9.1 Rogue wireless devices

1.9.2 Peer-to-peer attacks

1.9.3 Eavesdropping

1.9.4 Encryption cracking

1.9.5 Authentication attacks

1.9.6 MAC spoofing

1.9.7 Management interface exploits

1.9.8 Wireless hijacking

1.9.9 DoS

1.9.10 Social engineering

1.10 Steganography Compliance

1.10.1 Least Significant

1.10.2 Injection

1.10.3 Image Steganography

1.10.4 Audio Steganography

1.10.5 Video Steganography

1.10.6 Document Steganography

1.10.7 Security in Steganography

1.10.8 Private Key Steganography

1.10.9 Public Key Steganography

1.10.10 Mobile Messaging Steganography

1.10.11 MMS Steganography

1.11 Privacy issues Compliance

1.11.1 Social privacy

1.11.2 Data privacy

1.12 Data Transmission Compliance

1.12.1 Parallel

1.12.2 Serial

1.12.2.1 Asynchronous serial transmission

1.12.2.2 Synchronous serial transmission

1.13 Cloud Infrastructure Capabilities Compliance

1.13.1 SaaS

1.13.2 PaaS

1.13.3 IaaS

1.14 Cloud Encrypted Storage Compliance

1.14.1 Key sharing

1.14.2 Client-side integrity

1.14.3 Zero-knowledge

1.14.4 PKI for all devices

1.14.5 Sharing with link

1.14.6 Hardened TLS

1.14.7 Non-convergent cryptography

1.14.8 Conventional protection

1.15 Database Security Compliance

1.15.1 Access controls
1.15.2 Auditing
1.15.3 Authentication
1.15.4 Encryption
1.15.5 Integrity tools
1.15.6 Backups
1.15.7 Application security
1.15.8 Statistical method security

1.16 Database Mirroring Compliance

1.16.1 Synchronous mirroring
1.16.2 Asynchronous mirroring
1.16.3 Transaction safety
1.16.4 Quorum
1.16.5 Operating modes
1.16.6 High availability mode
1.16.7 High protection mode
1.16.8 High performance mode

1.17 Database Migration Compliance

1.17.1 Export and import
1.17.2 Scripts
1.17.3 Extract, transform, load
1.17.4 Integration

1.18 Database Replication Compliance

1.18.1 Snapshot replication
1.18.2 Transactional replication
1.18.3 Merge replication

1.19 Database Transmission of Dynamic Data Compliance

1.19.1 Transmission protection

1.19.2 Access controls

1.19.3 Architecture of community

1.19.4 Data transmission protection

1.19.4.1 Multipath model

1.19.4.2 Region network initialization

1.19.4.3 Key agreement mechanism

1.19.4.4 Fragmented multipath model

1.19.4.5 Fine grained access controls

1.19.4.6 Dynamic authorization scheme

1.19.5 Experiments and analysis

1.19.5.1 Transmission security analysis

1.19.5.2 Performance impact

1.19.5.3 Access security analysis

1.20 Database Relocation Compliance

1.20.1 Centralized database

1.20.2 Distributed database

1.20.3 Personal database

1.20.4 End-User database

1.20.5 Commercial database

1.20.6 No SQL database

1.20.7 Operational database

1.20.8 Relational database

1.20.9 Cloud database

1.20.10 Object-oriented database

1.20.11 Graph database

1.21 Single Sign-on Authentication Compliance

1.21.1 2FA

1.21.2 MFA

1.21.3 Single Sign-on Cards

1.21.4 Shared Sign- on

1.21.5 Centralized login

1.21.6 Password manager

1.21.7 Social login

1.22 Multi Factor Authentication Compliance

1.22.1 Type 1- Proof of work

1.22.2 Type 2- Proof of resource

1.22.3 Type 3- Proof of identity

Domain 2: Scanning, Logging and Monitoring

Domain 2: Scanning, Logging and Monitoring

2.1 Cyber Risk Management Compliance

2.1.1 Identify

2.1.2 Analyze

2.1.3 Evaluate

2.1.4 Track and report

2.1.5 Control and treatment

2.1.6 Monitor

2.1.7 Active directory

2.1.8 Endpoint Protection

2.1.9 Vulnerability assessment tools

2.1.10 SIEM solutions

2.1.11 MDM

2.1.12 Switches and routers

2.1.13 Firewalls

2.2 Logging, Collections and Storage Compliance

2.2.1 Types of data logging

2.2.2 Types of data collection

2.2.3 Types of data storage

2.2.3.1 Enterprise storage networks

2.2.3.2 Server side flash

2.2.3.3 Storage vendors

2.2.3.4 HDD and SSD

2.2.3.5 Optical data storage

2.2.3.6 Flash memory cards

2.2.4 Security access control compliance

2.2.4.1 DAC

2.2.4.2 MAC

2.2.4.3 RBAC

2.3 Data Archiving Compliance

2.3.1 Tape storage media

2.3.2 Optical media storage

2.3.3 Disk storage

2.3.4 Removable disk storage

2.3.5 Cloud archiving

2.4 Database User Roles Compliance

2.4.1 Admin users

2.4.2 Grant Any Privilege users

2.5 Patch Management Compliance

2.5.1 Inventory documentation

2.5.2 Common targets

2.5.3 Schedule regular patching

2.5.4 Automate patches if feasible

2.6 Quality of Service (QoS) Compliance

2.6.1 Data storage

2.6.2 Shared workload

2.6.3 Flash arrays

2.7 Snapshot Management Compliance

2.7.1 Wasted Virtual Resources

2.7.2 Snapshot Usage

2.7.3 Optimizing Virtual Machine Performance

2.8 Log Management Compliance

2.8.1 Full Security

2.8.2 Para- Security

2.8.3 OS-level Security

2.9 Managing and Monitoring Cybersecurity Governance

Domain 3: Infrastructure Security

Domain 3: Infrastructure Security

3.1 Asset Management Compliance

3.1.1 Inventory control of hardware assets

3.1.2 Inventory control of software assets

3.1.3 BYOD

3.1.4 CLOUD AND SAAS

3.1.5 Security

3.1.6 Mobile devices

3.1.7 IoT devices

3.2 Systems Architecture Compliance

3.2.1 Enterprise architecture

3.2.2 Security architecture

3.2.3 Types of architecture

3.2.3.1 Integrated

3.2.3.2 Distributed

3.2.3.3 Pooled

3.2.3.4 Converged

3.3 Wireless and Network Security Compliance

3.3.1 NAC

3.3.2 Application security

3.3.3 Antivirus and antimalware software

3.3.4 Email security

3.3.5 Wireless security

3.4 Interoperability of Systems Compliance

3.4.1 Foundation interoperability

3.4.2 Structural interoperability

3.4.3 Semantic interoperability

3.5 Physical and Perimeter Security Compliance

3.5.1 Outer perimeter security

3.5.2 Natural access control

3.5.3 Territorial reinforcement

3.5.4 Inner perimeter security

3.5.5 Interior security

3.6 Wireless, 4G, Bluetooth and Other Emerging Standards Compliance

3.6.1 Zigbee

3.6.2 Wifi

3.6.3 Bluetooth and BLE

3.6.4 WiMax

3.7 LAN and WAN security Compliance

3.7.1 PAN

3.7.2 SAN

3.7.3 EPN

3.7.4 VPN

3.8 Firewall Policies Compliance

3.8.1 Packet filtering firewalls

3.8.2 Circuit-level firewalls

3.8.3 Stateful inspection firewalls

3.8.4 Application-level gateways

3.8.5 Next-gen firewalls

3.9 Wireless Security Devices Compliance

3.9.1 WEP

3.9.2 WPA

3.9.3 WPA2

3.9.4 WPA3

3.10 Securing Email Servers Compliance

3.10.1 SMTP STARTTLS

3.10.2 S/MIME

3.10.3 PGP

3.11 IoT security Compliance

3.11.1 Securing televisions

3.11.2 Securing projectors

3.11.3 Securing printers

3.11.4 Securing electronic media

3.11.5 Securing faxes

3.11.6 Securing telephones

3.11.7 Securing Voting Machines

3.11.8 Securing Smartwatches

3.11.9 Securing Smart shoes

3.11.10 Securing Smart rings

3.11.11 Securing Smart rings

3.11.12 Securing Smart jackets

3.11.13 Securing Smart jewelry

3.11.14 Securing Self-driving cars

3.11.15 Securing Smartphones

3.11.16 Securing Smart headphones

3.11.17 Securing Smart Speakers

3.11.18 Securing Smart fans

3.11.19 Securing Smart Fridge

3.11.20 Securing Smart shower

3.11.21 Securing Smart toothbrush

3.11.22 Securing Smart lighting

3.11.23 Securing Smart thermostats

3.11.24 Securing Smart frames

3.11.25 Securing Smart clocks

3.11.26 Securing Smart oven

3.11.67 Securing Augmented reality (AR)

3.11.68 Securing Development boards

3.11.69 Securing Amazon Echo

3.11.70 Securing Drones

3.11.71 Securing Smart refrigerators

3.11.72 Securing IoT operating systems

3.11.73 Securing Hijacking cloud data

3.11.74 Securing Quantum computing

3.11.75 Securing Governance

3.12 Cloud Deployment Models Compliance

3.12.1 Public cloud

3.12.2 Private cloud

3.12.3 Hybrid cloud

3.12.4 Platform as a service

3.12.5 Infrastructure as a service

3.12.6 Software as a service

3.12.7 Flexibility

3.12.8 Scalability

3.12.9 Security

3.13 Cloud Service Categories Compliance

3.13.1 SaaS

3.13.2 IaaS

3.13.3 PaaS

3.13.4 NaaS

3.13.5 CompaaS

3.13.6 DSaaS

3.14 Cloud Network Access Controls Compliance

- 3.14.1 Role-based models
- 3.14.2 Attribute models
- 3.14.3 Multi-tenancy models

3.15 Cloud Load Balancing Compliance

- 3.15.1 NLB
- 3.15.2 POLB
- 3.15.3 HTTP load balancing

3.16 Cloud Data Centres Compliance

- 3.16.1 Corporate data centers
- 3.16.2 Webhosting data centers
- 3.16.3 Turnkey solution data centers
- 3.16.4 Web 2.0 data centers

3.17 Biometrics Authentication Compliance

- 3.17.1 Fingerprint recognition
- 3.17.2 Facial recognition
- 3.17.3 Iris recognition
- 3.17.4 Voice recognition
- 3.17.5 Signature recognition

3.18 Security Continuity Management Compliance

3.18.1 Server Security

3.18.2 Storage Security

3.18.3 Network Security

3.18.4 Desktop Security

3.18.5 Application Security

3.19 Security Release Management Compliance

3.19.1 Content Indexing

3.19.2 Content Hierarchy

3.19.3 Content Segregation

3.19.4 Network Sync

3.19.5 Network Implementation

3.19.6 Network security

3.20 Security Configuration Management Compliance

3.20.1 Application Security

3.20.2 Desktop Security

3.20.3 Storage Security

3.20.4 Hardware/Server Security

3.20.5 Network Security

3.21 Security Volume and Capacity Management Compliance

3.21.1 Capacity planning For virtual environment

3.21.2 Expert answers on planning for growth

3.21.3 Pitfalls of Security

3.21.4 Capacity planning checklist

3.22 Cybersecurity Governance in the Enterprise Compliance

3.22.1 External risks

3.22.2 Internal risks

3.22.3 Ecosystem exposures

3.22.4 Social and reputational threats

3.23 Cybersecurity Strategic Planning and Implementation Compliance

3.23.1 Critical assets

3.23.2 Resource capabilities

3.23.3 Reporting

3.23.4 Modernization

3.24 Cybersecurity Communication and Engagement Protocols Compliance

3.24.1 Internal communications strategy

3.24.2 Training and focus sessions

3.24.3 BYOD

3.25 Cybersecurity Investment Justification Compliance

3.25.1 Data protection

3.25.2 Research protection

3.25.3 Operational security

3.26 Machine Learning Security Compliance

3.26.1 Secure machine learning environment

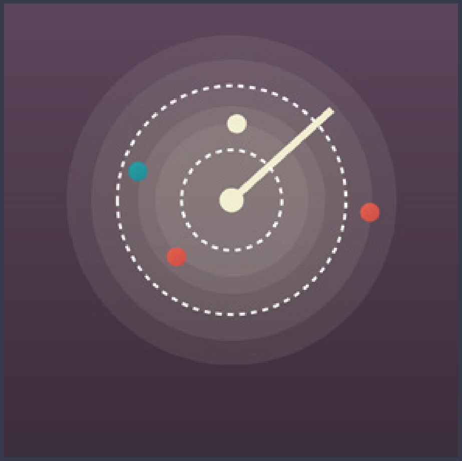
3.26.2 Malicious activity detection

3.26.3 Malicious activity segregation

3.26.4 Artificial intelligence in cybersecurity

Domain 4: Extreme Hacking Penetration Testing

Domain 4: Extreme Hacking Penetration Testing



4.1 Security Auditing and Penetration Testing Compliance

4.1.1 Black box audit

4.1.2 White box audit

4.1.3 Grey box audit

4.1.4 Network penetration testing

4.1.5 Application penetration testing

4.1.6 Workflow response testing

4.2 Vulnerability Assessment and Analysis Compliance

4.2.1 Host based

4.2.2 Network based

4.2.3 Database based

4.2.4 Vulnerability tools

4.2.4.1 Host based

4.2.4.2 Network based

4.2.4.3 Database based

4.2.5 Vulnerability testing methods

4.2.5.1 Active testing

4.2.5.2 Passive testing

4.2.5.3 Network testing

4.2.5.4 Distributed testing

4.3 Network Intrusion Prevention Compliance

4.3.1 Browser attacks

4.3.2 Brute force attacks

4.3.3 DoS attacks

4.3.4 SSL attacks

4.3.5 Scan attacks

4.3.6 DNS attacks

4.3.7 Backdoor attacks

4.4 Configuration Management Compliance

4.4.1 Integrated product suites

4.4.2 Dedicated CMDB tools

4.4.3 Discovery tools

4.4.3.1 Strength of point

4.4.3.2 Weakness of point

4.5 Protection Against Viruses and Malwares Compliance

4.5.1 Virus

4.5.2 Malware

4.5.3 Trojan Horse

4.5.4 Worm

4.5.5 Spyware

4.5.6 Adware

4.6 Protection against Spam Compliance

4.6.1 Mail lists

4.6.2 User databases

4.6.3 DHA

4.6.4 Open relay method

4.6.5 Malware method

4.7 Defending Against Botnet Compliance

4.7.1 DDoS

4.7.2 Spamming

4.7.3 Sniffing traffic

4.7.4 Keylogging

4.7.5 Spreading new malware

4.7.6 Advert addons and BHOs

4.7.7 Google Adsense abuse

4.7.8 IRC chat networks

4.7.9 Manipulation online polls and games

4.7.10 Mass identity theft

4.8 Insider threats Compliance

4.8.1 Nonresponses
4.8.2 Inadvertent insiders
4.8.3 Insider collusion
4.8.4 Persistent malicious insiders
4.8.5 Disgruntled employees

4.9 Scanners Compliance

4.9.1 Flatbed scanners
4.9.2 Sheet-fed scanners
4.9.3 Integrated scanners
4.9.4 Drum scanners
4.9.5 Portable scanners

4.10 Anti-malware Compliance

4.10.1 Free programs
4.10.2 Specialized programs
4.10.3 All-in-one programs

4.11 Defending Against Social Engineering Compliance

4.11.1 Phishing
4.11.2 Spear Phishing
4.11.3 Vishing
4.11.4 Pretexting
4.11.5 Baiting
4.11.6 Tailgating
4.11.7 Quid pro quo

4.12 Prevention of Denial of Service Attacks Compliance

4.12.1 Volume based attacks

4.12.2 Protocol attacks

4.12.3 Application layer attacks

4.12.4 UDP flood

4.12.5 ICMP flood

4.12.6 SYN flood

4.12.7 Ping of Death

4.12.8 Slowloris

4.12.9 NTP amplification

4.12.10 HTTP flood

4.12.11 Zero day DDoS attacks

4.13 Defending Against Phishing Compliance

4.13.1 Malware-Based Phishing

4.13.2 Keyloggers and Screen loggers

4.13.3 Session Hijacking

4.13.4 Web Trojans

4.13.5 Hosts File Poisoning

4.13.6 System Reconfiguration Attacks

4.13.7 Data Theft

4.13.8 DNS based Phishing

4.13.9 Content-injection Phishing

4.13.10 Man-in-the-middle Phishing

4.13.11 Search Engine Phishing

4.14 Cloud Attack Vectors Compliance

4.14.1 Data threats

4.14.2 Cloud API vulnerability

4.14.3 Malicious insiders

4.14.4 Shared technology vulnerabilities

4.14.5 Provider Lock-in

4.14.6 Weak cryptography

4.14.7 Vulnerable cloud services

4.14.8 Cloud malware injections

4.14.9 Abuse of cloud services

4.14.10 Denial of service

4.14.11 Side channel

4.14.12 Wrapping attacks

4.14.13 Man-in-the-cloud

4.14.14 Insider attacks

4.14.15 Account or service hijacking

4.14.16 APTs

4.15 Security Penetration Testing Compliance

4.15.1 Server Security

4.15.2 Client Security

4.15.3 Storage Security

4.16 Establish and Manage Business Continuity Plan Compliance

4.16.1 Conducting active and passive reconnaissance penetration testing

4.16.2 Managing Bug Bounty programs

4.16.3 Conducting penetration testing using vulnerability analysis

4.16.4 Conducting penetration testing in web applications

4.16.5 Conducting penetration testing in mobile devices

4.16.6 Conducting penetration testing in internal networks

4.16.7 Conducting penetration testing in external networks

4.16.8 Conducting penetration testing in supplier connected networks

4.16.9 Conducting physical security penetration testing

4.16.10 Conducting source code penetration testing

4.16.11 Conducting penetration testing in software development

4.16.12 Conducting enterprise database privacy protection penetration testing

4.16.13 Conducting end user penetration testing

4.16.14 Conducting network dataflow penetration testing

4.16.15 Conducting encryption, 2FA and effective password penetration testing

4.16.16 Conducting leakage of data penetration testing

4.16.17 Conducting spread of fake news penetration testing

4.16.18 Conducting organization reputation penetration testing

4.16.19 Conducting IoT penetration testing

4.16.20 Conducting hardware penetration testing

4.16.21 Conducting digital badges penetration testing

4.16.22 Conducting switches, gateways and routers penetration testing

4.16.23 Conducting rouge employees penetration testing

4.16.24 Conducting malicious content penetration testing

4.16.25 Conducting cloud connected deep leaning algorithms penetration testing

4.16.26 Penetration testing analysis and report writing

4.17 Threat Mitigation Compliance

4.17.1 Data Encryption

4.17.2 Insider threats

4.17.3 Background checks

4.17.4 Staff education

4.17.5 Monitoring solutions

4.17.6 Termination practices

4.17.7 Access controls

4.17.8 Checks and Balances

Domain 5: CyberForensics

Domain 5: CyberForensics

5.1 Chain of custody and Preservation of Evidence Compliance

5.1.1 Collection forms

5.1.2 Photos

5.1.3 Delivery and shipping logs

5.1.4 Transfer and handling logs

5.1.5 Software logs

5.1.6 Documentation protection

5.2 Discovery and Reporting Compliance

5.2.1 e-Discovery

5.2.2 Email threading

5.2.3 Keyword expansion

5.2.4 Clusters

5.2.5 Near duplicates

5.3 Forensic Investigation Practices Compliance

5.3.1 Computer forensics

5.3.2 Network forensics

5.3.3 Mobile device forensics

5.3.4 IoT forensics

5.3.5 Multimedia forensics

5.3.6 Cloud forensics

5.4 Train Cybersecurity Incident response team

5.4.1 Manage cybersecurity non-compliance

5.4.2 Maintain cybersecurity awareness and training program

5.4.3 Establish and manage disaster recovery plan

Domain 6: Identity and User Protection

Domain 6: Identity and User Protection

6.1 Security Awareness and Training Compliance

6.1.1 Email security training

6.1.2 Internet security training

6.1.3 Information sharing procedures training

6.2 Mobile Device Management Compliance

6.2.1 Manageengine

6.2.2 VMware AirWatch

6.2.3 SOTI Mobicontrol

6.2.4 Citrix XenMobile

6.2.5 MaaS360

6.2.6 Micr

6.2.7 Apptech360 Enterprise Mobility Management

6.2.8 Baramundi Management Suite

6.2.9 Google Enterprise Management Tool

6.2.10 Apple Enterprise Management Tool

6.3 Audit Compliance

6.3.1 Hosted (type 2)

6.3.2 Bare- metal (type 1)

6.3.3 VMware ESXi

6.3.4 EAL 4+ certification

6.3.5 DISA STIG for ESX

6.3.6 NSA central Security Service

6.3.7 Security principles

6.3.7.1 Secure the guests

6.3.7.2 Access controls

6.3.7.3 Admin Controls

6.4 Federated Identity Providers Compliance

6.4.1 Hitachi ID password manager

6.4.2 SecureAuth Identity

6.4.3 Ping Identity

6.4.4 Cierge

6.4.5 Keycloack

6.4.6 Auth0

6.4.7 Gluu

6.4.8 Miniorange

6.4.9 Forgerock

6.5 Anti password Theft Compliance

6.5.1 Use lots of quirky character types

6.5.2 Don’t use dictionary words

6.5.3 Use different passwords on different accounts

6.5.4 Use 2FA

6.6 Preventing Data Leaks

6.6.1 DoS

6.6.2 Malware

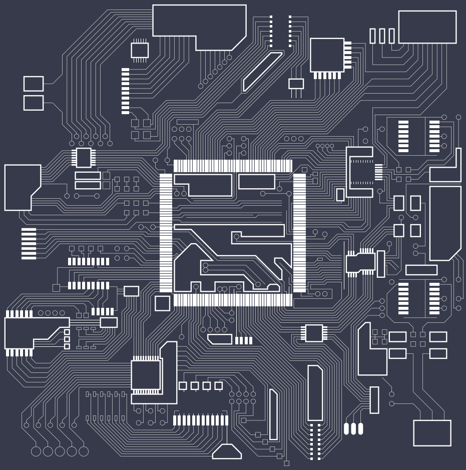
6.6.3 Password attacks

6.6.4 Phishing

6.6.5 Ransomware

Domain 7: Hardware Security

Domain 7: Hardware Security



7.1 Network Discovery and Network Topology Compliance

7.1.1 Star topology

7.1.2 Bus topology

7.1.3 Ring topology

7.1.4 Mesh topology

7.2 Proxy Servers Compliance

7.2.1 SSL Proxy

7.2.2 FTP Proxy

7.2.3 HTTP Proxy

7.2.4 SOCKS Proxy

7.2.5 Anonymous Proxy

7.3 Securing USB Devices Compliance

7.3.1 Need to have basis

7.3.2 Passphrase protected encryption

7.3.3 Remote management options

7.3.4 Event logging

7.3.5 Regular scanning

7.3.6 Regular audits

7.3.7 Regular backups

7.3.8 Test data recovery

7.3.9 Unique serial numbers

7.3.10 Geotagging

7.3.11 Wiping or destroying

7.4 Embedded Devices Compliance

7.4.1 Malware

7.4.1.1 External malware

7.4.1.2 Embedded malware

7.4.2 Embedded chips

7.4.2.1 RFID security

7.4.2.2 GPS security

7.4.2.3 Portable device security

7.4.2.4 Wearable device security

7.4.2.5 Home appliances security

7.4.3 Physical security systems

7.4.3.1 Biometrics

7.4.3.2 Facial recognition

7.4.3.3 Password protection

7.4.3.4 Keyloggers

7.4.3.5 Cables

7.4.4 HSM

Domain 8: Application Security

Domain 8: Application Security

8.1 Network Access Controls Compliance

8.1.1 Impuse Safeconnect

8.1.2 Extereme Networks ExtermeControl

8.1.3 Auconet BICS

8.1.4 Forescout CounterACT

8.1.5 Pulse Policy Secure

8.1.6 HPE Aruba Clearpass

8.1.7 Bradford Networks' Networks Sentry

8.1.8 Cisco Identity Services Engine

8.1.9 Inforexpress Cybergatekeeper

8.2 VPN Servers and VPN Clients Compliance

- 8.2.1 PPTP VPN
- 8.2.2 Site-to-Site VPN
- 8.2.3 L2TP VPN
- 8.2.4 IPsec
- 8.2.5 SSL and TLS
- 8.2.6 MPLS VPN
- 8.2.7 Hybrid VPN

8.3 Application Architecture and Design Vulnerabilities Compliance

- 8.3.1 Trust component
- 8.3.2 Authentication mechanics
- 8.3.3 Authorize after authenticate
- 8.3.4 Data separation and control
- 8.3.5 Data validation
- 8.3.6 Cryptography application
- 8.3.7 Sensitive data handling
- 8.3.8 Consider users
- 8.3.9 Integrating external components
- 8.3.10 Flexibility

8.4 Virtual Appliances Compliance

- 8.4.1 LAMP Stack
- 8.4.2 DRUPAL Appliance
- 8.4.3 Wordpress Appliance
- 8.4.4 Domain Controller
- 8.4.5 Zimbra Appliance
- 8.4.6 OTRS Appliance
- 8.4.7 Openfiler Appliance
- 8.4.8 Opsview Core Virtual Appliance
- 8.4.9 FOG Project
- 8.4.10 Moodle

8.9 Web application security

- 8.9.1 Hidden field manipulation
- 8.9.2 Cookie poisoning
- 8.9.3 Parameter tampering
- 8.9.4 Buffer overflow
- 8.9.5 Cross site scripting
- 8.9.6 Backdoor or debug options
- 8.9.7 Stealth commanding
- 8.9.8 Forced browsing
- 8.9.9 Third party misconfigurations

8.10 Secure Programming

- 8.10.1 Avoiding Buffer Overflows and Underflows
- 8.10.2 Validating Inputs and Interprocess Communication
- 8.10.3 Race Conditions and Secure File Operations
- 8.10.4 Elevating Privileges Safely
- 8.10.5 Designing Secure User Interfaces
- 8.10.6 Designing Secure Helpers and Deamons
- 8.10.7 Avoiding Injection Attacks and XSS

8.11 Application Updates and Patch Management Compliance

- 8.11.1 Importance of software updates
- 8.11.2 Types of updates

Domain 9: OS Security

Domain 9: OS Security

9.1 Securing Virtualized Networks Compliance

9.1.1 VM Sprawl

9.1.2 Sensitive data within a VM

9.1.3 Security of offline and dormant VM

9.1.4 Security of Pre-configured VM

9.1.5 Lack of visibility

9.1.6 Resource exhaustion

9.1.7 Hypervisor security

9.1.8 Unauthorized access to Hypervisor

9.1.9 Account or service hijacking

9.1.10 Workloads of different trust levels located on the same server

9.1.11 Risk due to cloud service providers APIs

9.2 Securing Hypervisors Compliance

9.2.1 Planning security

9.2.2 Thin hypervisors

9.2.3 Latest security features

9.3 Systems Protection Compliance

9.3.1 OS Security

9.3.2 Application-server Security

9.3.3 Application Security

9.3.4 Administrative Security

9.3.5 Network Security

9.3.6 Hardware Security

9.3.7 Storage Security

9.4 Security Sandbox Testing Compliance

9.4.1 Security

9.4.2 OS emulation

9.4.3 Hardware or full system emulation

9.5 Windows Security Compliance

9.5.1 Configuring and managing a Windows Kernel

9.5.2 Windows firewall management

9.5.3 Managing Windows services

9.5.4 Managing Windows ports

9.5.5 Managing Windows Firewall configuration

9.5.6 Managing Windows Dot Defender

9.5.7 Managing Windows Active Directory

9.5.8 Managing Windows Network Load Balancing

9.5.9 Managing User Access Control

9.5.10 Managing Windows updates

9.5.11 Managing Windows Recover Volumes

9.5.12 Managing Windows backup and Restore

9.5.13 Managing Windows Data Disks

9.5.14 Managing Windows Authentication

9.5.15 Managing Windows Applications

9.5.16 Managing Windows Environment variables

9.5.17 Server hardening

9.5.18 Managing windows permissions and shares

9.5.19 Managing Windows threat detection solutions

9.5.20 Managing Windows workload specific security

9.9 Securing Azure Platform Compliance

- 9.9.1 Windows virtual machine documentation
- 9.9.2 Linux virtual machine documentation
- 9.9.3 Virtual network and Expressroute
- 9.9.4 Provision a SQL server virtual machine
- 9.9.5 Capture an image of Windows server
- 9.9.6 IPython notebook on Azure
- 9.9.7 Managed disks
- 9.9.8 Azure IaaS

9.10 Securing AWS Platform Compliance

- 9.10.1 Paravirtual
- 9.10.2 Hardware Virtual Machine

9.11 IOS Security

- 9.11.1 Password Management
- 9.11.2 Virtual Private Network
- 9.11.3 Antivirus
- 9.11.4 End-to-end encryption
- 9.11.5 Device tracker
- 9.11.6 MDM

9.12 Android Security

9.12.1 Securing device hardware

9.12.2 Securing Android OS

9.12.3 Android application runtime

9.12.4 Safetynet

9.12.5 Safetynet Attestation

9.12.6 Design Review

9.13 Software Updates and Patch Management Compliance

9.13.1 Importance of software updates

9.13.2 Types of updates

Domain 10: Governance

Domain 10: Governance

10.1 Legal Surveillance Compliance

10.1.1 Electronic monitoring

10.1.2 Fixed surveillance

10.1.3 Stationary technical surveillance

10.1.4 Three-Person surveillance

10.1.5 Undercover operations

10.2 SSL and HTTPS Protocols Compliance

10.2.1 RFC 2818: HTTP over TLS

10.2.2 RFC 5246: The Transfer Layer Security

10.2.3 RFC 6101: Secure Sockets Layer

10.3 Theft of Database Mitigation Compliance

10.3.1 Excessive privileges

10.3.2 Legitimate privilege abuse

10.3.3 Database injection attacks

10.3.4 Malware

10.3.5 Storage media exposure

10.3.6 Exploitation of vulnerable database

10.3.7 Unmanaged sensitive data

10.3.8 The human factor

10.3.9 Multilayered security solutions

10.4 Database Theft and Incident Response Compliance

10.4.1 Planned response and defined resources

10.4.2 Network quarantine

10.4.3 Investigate the leak

10.4.4 Consequences of data going public

10.4.5 Rebuilding, backup and recovery

10.5 Security Disaster Recovery Compliance

10.5.1 Application Security

10.5.2 Desktop Security

10.5.3 Hardware Security

10.5.4 Network Security

10.5.5 Storage Security

10.6 Security SLA Management Compliance

10.6.1 Hardware Security

10.6.2 Software Security

10.6.3 Storage Security

10.6.4 Memory Security

10.6.5 Data Security

10.6.6 Network Security

10.6.7 Desktop Security

10.7 Security Job Roles and Responsibilities Compliance

10.7.1 Chief Cyber Security Officer Compliance

10.7.2 Chief Data Privacy Officer Compliance

10.7.3 Chief Risk Officer Compliance

10.7.4 Cybersecurity Compliance Officer

10.7.5 Extreme Hacker Compliance

10.7.6 Chief Cybersecurity Engineer Compliance

10.7.7 Cybercrime Investigator Compliance

10.8 HIPAA Compliance

10.9.4.1 Framework identification

10.9.4.2 Modification policies

10.9.4.3 Maintenance policies

10.9.4.4 Storage policies

10.9.4.5 Access policies

10.9.5 Operational Compliance

10.9.5.1 Security breaches

10.9.5.2 Data tampering prevention

10.9.5.3 Sensitive data

10.9.5.4 Historical disclosures

10.10 NICE Framework Compliance

10.10.1 What is NICE

10.10.1.1 NIST

10.10.1.2 Purpose and applicability

10.10.1.3 Stakeholders

10.10.1.4 Components and relationships

10.10.2 Securely Provision Category Compliance

10.10.2.1 Risk management

10.10.2.2 Software development

10.10.2.3 Systems architecture

10.10.2.4 Technology R&D

10.10.2.5 System requirements planning

10.10.2.6 Test and evaluation

10.10.2.7 Systems development

10.10.3 Operate and Maintain Category Compliance

10.10.3.1 Data administration

10.10.3.2 Knowledge management

10.10.3.3 Customer service and technical support

10.10.3.4 Network services

10.10.3.5 Systems administration

10.10.3.6 Systems analysis

10.10.4 Oversee and Govern Category Compliance

10.10.4.1 Legal advice and advocacy

10.10.4.2 Training and education

10.10.4.3 Cybersecurity management

10.10.4.4 Strategic planning and policy

10.10.4.5 Executive cyber leadership

10.10.4.6 Program management and acquisition

10.10.5 Protect and Defend Category Compliance

10.10.5.1 Cyber defense analysis

10.10.5.2 Cyber defense infrastructure support

10.10.5.3 Incidence response

10.10.5.4 Vulnerability assessment and management

10.10.6 Analyze Category Compliance

10.10.6.1 Threat analysis

10.10.6.2 All source analysis

10.10.6.3 Targets

10.10.6.4 Language analysis

10.10.7 Collect and Operate Category Compliance

10.10.7.1Collection operations

10.10.7.2 Cyber operational planning

10.10.7.3 Cyber operations

10.10.8 Investigate Category Compliance

10.10.8.1 Cyber investigation

10.10.8.2 Digital forensics

10.11 PCI DSS Compliance

10.11.1 Network Security Compliance

10.11.1.1 Firewall setup

10.11.1.2Firewall configuration

10.11.1.3Vendor supply passwords

10.11.1.4Security parameters

10.11.2 Data Protection Compliance

10.11.2.1Data protection policies

10.11.2.2 Public network transmission policies

10.11.2.3 Encryption

10.11.3 Vulnerability Management Compliance

10.11.3.1Anti-virus setup

10.14 Data Protection Act 1998 Compliance

10.15 California Consumer Privacy Act 2018 Compliance

10.16 Risk Identification and Management Compliance

10.16.1 Documentation reviews

10.16.2 Information gathering techniques

10.16.3 Delphi technique

10.16.4 Root cause analysis

10.16.10 Monte Carlo analysis

10.16.5 Checklist analysis

10.16.6 Risk register

10.16.7 Assumption analysis

10.16.8 Probability and impact matrix

10.16.9 Risk data quality assessment

10.16.11 Decision tree

10.17 Risks Compliance

10.17.1 VM sprawl

10.17.2 Complexity of monitoring

10.17.3 Data loss, theft and hacking

10.17.4 Lack of visibility into virtual network traffic

10.17.5 Offline and dormant VMs

10.17.6 Hypervisor security

10.17.7 Execution of VMs with different trust levels

10.17.8 Pathways from public to hybrid cloud systems

10.18 Managing Cybersecurity Infrastructure Compliance

10.18.1 Effective framework

10.18.2 End-to-end scope

10.18.3 Risk assessment threat modeling

10.18.4 Proactive incident response planning

10.18.5 Dedicated cybersecurity resources

10.19 Intrusion Detection System Compliance

- 10.19.1 Active IDS
- 10.19.2 Passive IDS
- 10.19.3 NIDS
- 10.19.4 HIDS
- 10.19.5 Knowledge based IDS
- 10.19.6 Behavior based IDS

10.20 Privacy and Accountability Compliance

- 10.20.1 Defensive privacy
- 10.20.2 Human rights privacy
- 10.20.3 Personal privacy
- 10.20.4 Contextual privacy

10.21 Cloud backups Compliance

- 10.21.1 Full backup
- 10.21.2 Incremental backup
- 10.21.3 Differential backup
- 10.21.4 Mirror backup

10.22 Data Analysis Compliance

- 10.22.1 Descriptive
- 10.22.2 Exploratory
- 10.22.3 Inferential
- 10.22.4 Predictive
- 10.22.5 Casual
- 10.22.6 Mechanistic

10.23 Establishing Appropriate Cybersecurity Roles, Responsibilities and Accountabilities Compliance

10.23.1 Capacity and capability

10.23.2 Variety of cyber security skills

10.23.3 Professionals vs specialists

10.24 Risk Identification Compliance

10.24.1 Risk Management Strategy

10.24.2 Asset Management

10.24.3 Business Environment

10.24.4 Supply Chain Management

10.25 Network Protection Compliance

10.25.1 Access Controls

10.25.1.1 Identity Management

10.25.1.2 Authentication

10.25.2 Information protection

10.25.2.1 Information processes

10.25.2.2 Information procedures

10.25.3 Protective Technology

10.25.4 Awareness Training Process

10.25.5 Data Security

10.26 Risk Detection Compliance

10.26.1 Anomalies and Events Handling Process

10.26.2 Continuous Scan Process

10.26.3 Detection Process

10.27 Breach Response Compliance

10.27.1 Response Strategy

10.27.2 Communication Protocols

10.27.3 Mitigation Process

10.27.4 Analysis and Reporting

CYBERSECURITY
COMPLIANCE OFFICER

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

CYBERSECURITY
COMPLIANCE OFFICER

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

CYBERSECURITY COMPLIANCE OFFICER

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

CYBERSECURITY COMPLIANCE OFFICER

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

CYBERSECURITY
COMPLIANCE OFFICER

Certified by Rochester®

The Rules of Engagement Have Changed. Resecure Everything.™

CYBERSECURITY COMPLIANCE OFFICER

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

CYBERSECURITY COMPLIANCE OFFICER

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

ROCHESTON®

BE EXCEPTIONAL