NITROXIS
Training Catalog 2025 – V5.6

Table of Contents

Who are we? **3**

Our values **4**

Our B+ approach **5**

Study at your own pace **6**

Mentoring **7**

TRECCERT Trainings **10**

Artificial Intelligence **11**
- **ISO/IEC 42001 Practitioner (2 Days)** 11
- **ISO/IEC 42001 Lead Implementer (4 Days)** 12
- **ISO/IEC 42001 Lead Auditor (4 days)** 14

Business Continuity **15**
- **ISO/IEC 22301 Foundation (2 Days)** 15
- **ISO/IEC 22301 Lead Implementer (4 Days)** 17
- **ISO/IEC 22301 Lead Auditor (4 Days)** 19

Compliance **21**
- **ISO 37301 Foundation (2 Days)** 21
- **ISO 37301 Lead Implementer (4 Days)** 23
- **ISO 37301 Lead Auditor (4 Days)** 25

Data Protection **28**
- **GDPR Essentials (1 day)** 28
- **GDPR Professional (3 days)** 30
- **Data Protection Impact Analysis Specialist (1 day)** 32

Digital Operational Resilience ACT (DORA) **34**
- **DORA Essentials (2 Days)** 34

Environmental Social Governance (ESG) **36**
- **ESG Essentials (1 Day)** 36

Information Security **38**
- **ISO/IEC 27001 Foundation (2 Days)** 38
- **ISO/IEC 27001 Lead Implementer (4 Days)** 39
- **ISO/IEC 27001 Lead Auditor (4 Days)** 41

Risk Management **43**
- **ISO 27005 Risk Professional (3 Days)** 43
- **ISO 31000 Risk Practitioner (2 Days)** 45

Nitroxis Trainings **48**

Introduction Training **48**

Cybersecurity Training **48**
- **NIST CSF 2.0 – (3 Days)** 48

CIS Critical Security controls (v8) (3 Days) 53

Preparation for certifications (Bootcamps) **57**

ISACA **58**

CISA® (Certified Information Systems Auditor) (5 Days) 58

CISM® 16th Edition (Certified Information Security Manager) (4 Days) 62

CRISC® 7th Edition (Certified in Risk and Information System Control) (4 Days) . 65

(ISC)2 ..... **69**

CISSP (Certified Information Systems Security Professional) (5 Days) 69

CCSP (Certified Cloud Security Professional) (5 Days) 73

PCI-DSS **76**

PCI-DSS v4 (2 days) 78

PCI-DSS v4 (4 days) 80

Who are we?

NITROXIS SRL is a consulting company founded in 2011 and specialized in Information Security and Governance. Nitrox is a term frequently used in the diving community to refer to any mixture of nitrogen and oxygen. “IS” stands for Information Security, Information Systems, Infrastructures. The use of NITROX has the advantage of increasing dive time and safety, it also provides well-being during and after diving.

This is why we apply the same standards used in scuba diving to each of our missions.

Stability

Reach the maximum stability and durability for your project

Optimization

Optimize planning and risk management

Relationship

Build a trustful relationship that increases mutual satisfaction

Resources

Optimize resources management

With Nitrox, we provide:

A longer security curve for the same diving depth

A shorter decompression-stop for a same diving duration

A shorter surface interval between two dives

We benefit from longer and successive dives (missions) with reduced decompression.

Our values

Without planification or security or risk management, It management (as scuba diving) can be deadly.

Buoyancy Control Device « BCD »: We are aiming at the maximum stability and durability for your project by deploying different control systems: preventive, deterrent, detective, corrective.

Never dive alone: Trust is an essential factor regarding IT Governance projects. We are also aware that some projects require very specific skills. You can count on our trusted partners' network to provide you with a wide range of expertise.

Plan or dive: Nitroxis never engages in a mission without careful planning and a full internal/external factors assessment. That's the key to our success.

Transparency: Like in diving it's better when your sight is clear. Web ring all the facts to your knowledge with no sugarcoating or camouflage.

Discovery: Because the IT world is in perpetual evolution, we dedicate ourselves to a continuous learning and training program.

Enthusiasm: Each project and each dive is a unique adventure. We enjoy and share both our IT & Diving passions with our partners. Divers are always happy and ready for the next dive. They share their knowledge and experience with their community.

We are doing the same with you.

Our B+ approach

In a liquid, the bodies are subject to buoyancy. There are three kinds of buoyancy : positive (up), negative (down), neutral. Unmanaged buoyancy in projects causes up and down and frustrations, increase resource consuming (money, time) and fails to focus on the objective (risk to surface at all cost).
A perfect buoyancy increases the optimization at the planned depth (mission, project), brings satisfaction (buddies, customers, and Nitroxis), decreases resources consuming and stays focused on the objectives (dive plans).

While the excellence refers to an A+, we only provide you with our B+ notation (our optimized buoyancy approach)

Study at your own pace

Why ?

-Adaptable to your needs in terms of flexibility (content, time, budget)
-Budget restrictions have a negative impact on training budgets, and it is essential to stay up to date with the acceleration of digital transformation.
-In order to give you a perfect buoyancy (B+ Approach).
-You remain billable while you study or prepare for a certification and your company can better deliver on its goals.
-Sometimes some classes do not take place, due to a lack of sufficient participants

For Who

-Consultants
-freelances (senior, with at least 5 years of experience)
-individuals with already a good knowledge of the subject.

Certification

At the end of the training, you receive a certificate of participation of the total hours of training followed, it is ideal for those who must maintain CPE/CPD/PDU (proof of maintenance of knowledge for a particular certification). We can register you directly for the exam (it is then included in our price).

Description

If you are looking for a new way to be trained or to prepare for certification, this is the most efficient way to start or continue your training journey.

With a personalized training, and taking the necessary time, we make sure that you are comfortable with the subject.

It is also a unique chance to learn from the comfort of your home and to join a community of certified professionals.

We prepare the session together in advance to identify the points you want to review in addition to the important points of the training and / or the exam.

We review the course questions and exercises together to prepare for the exam, generally this is done interactively through a SAAS application for which a session number will be communicated to you.

Each dive is unique, each course is different. Studying at your own pace with a certified trainer who will show you the most interesting parts of the course is a guarantee of success.

Product	Essentials	Found.	Pro	Lead
Example of Content	Iso Management System ; Audit ; DORA; DPIA; ESG; ISMS Transition (2013-2022); ISSRW; Data protection	ISO (9001; 14001; 22301; 27001; 37001; 37301; 42001)	ISO (27005; 31000); GDPR; Management System Lead Auditor	ISO (9001; 14001; 22301; 27001 ; 37001; 37301 ; 42001) Lead Implementer or Auditor
Standard	199 €	299 €	399 €	599 €
Premium (2h coaching)	499 €	599 €	699 €	899 €
Start my journey	Discover	Build	Become an Expert	Become a Leader
CPE Credits	8	16	24	32

Mentoring

Why ?

-Adaptable to your needs in terms of flexibility (content, time, budget)
-Budget restrictions have a negative impact on training budgets, and it is essential to stay up to date with the acceleration of digital transformation.
-In order to give you a perfect buoyancy (B+ Approach).
-You remain billable while you study or prepare for a certification and your company can better deliver on its goals.
-Sometimes some classes do not take place, due to a lack of sufficient participants

For who ?

-Consultants
-Freelances (senior, with at least 5 years of experience)
-Individuals with already a good knowledge of the subject
-Seniors who will take benefit of the summary of two different trainings

Certification

At the end of the training, you receive a certificate of participation of the total hours of training followed, it is ideal for those who must maintain CPE/CPD/PDU (proof of maintenance of knowledge for a particular certification).

Depending on the course chosen, we can register you directly for the exam (it is then included in our price), or you must do it yourself (and this represents an additional cost, not managed by our invoicing department).

Description

It is often said that what cannot be seen does not exist. Nowadays, with digital transformation if there is no video or trace of an event, there is no event. Since the start of the COVID-19 pandemic we have carried out various sessions for different companies and freelancers. This demand continues to grow with the new rules brought about by the pandemic.

We estimate together the material and the number of hours you need. Mentoring goes beyond preparation for certification, as it allows us to answer more specific questions outside the scope of the exam.

Our NDA forces us to keep identities of clients a secret but know that they do exist.

Some examples of training:

-2h of CISM course for a final revision and preparation of a CISO for an exam

-10 CISSP sessions of 4 hours at a pace of 1x per month for one person

-Blended learning of an ISO 27001 session and 2 CISA sessions for a large French bank with review of the most important points of the PDCA (Plan – Do – check – Act), and audit points and interactive MCQ to facilitate attention and participation (remote or face-to-face).

-We provided our partners with review sessions to prepare for passing both the ISO 27001 Lead Implementer and Lead Auditor Exams.

-2h of monthly cybersecurity awareness sessions.

-2h of onboarding sessions for banking staff (Luxembourg) and Cybersecurity Awareness.

-2h of onboarding sessions for banking staff (Luxembourg) and GDPR.

-3 Days of CISA focusing on the Sampling Methodologies and Technical parts for a Financial Company in Luxembourg

-Our team also works weekends, public holidays and in shift schedule depending on requests.

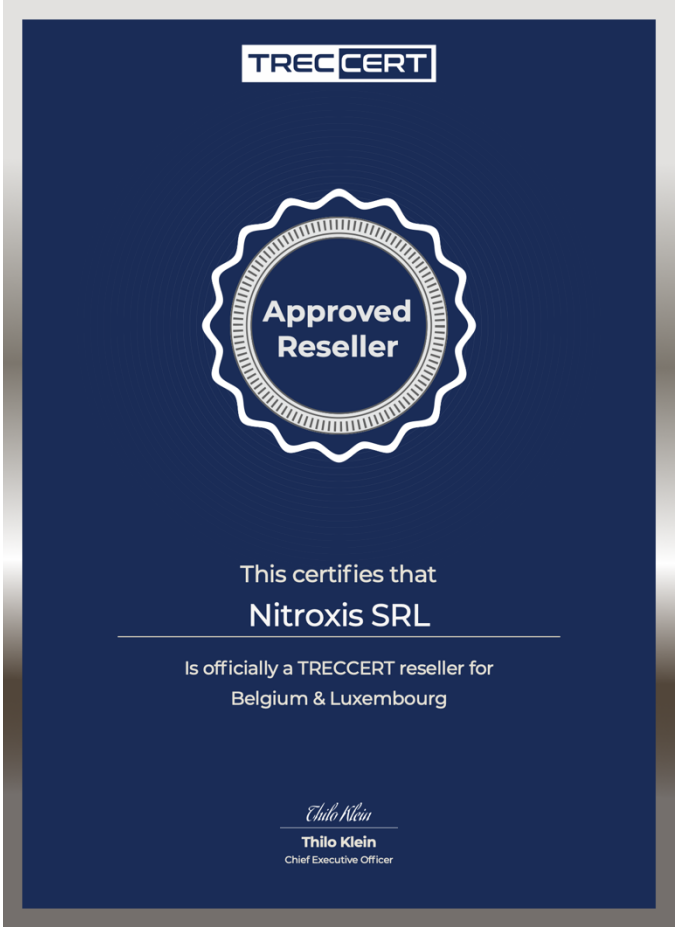
TRECCERT Trainings

TRECCERT is a certification body for people, providing certifications that promote professional development by improving the practice of IT decision-makers.

These certifications are part of continuous improvement to deepen their knowledge of the performance of IT.

Nitroxis is official Distributor for Belgium-Luxembourg, Reseller and Trainer.

Given our DNA, this does not prevent us from forging new partnerships beyond our borders to meet a growing demand for distance learning.



Artificial Intelligence

ISO/IEC 42001 Practitioner (2 Days)

Course Overview

TRECCERT ISO/IEC 42001 Practitioner is an introductory-level course developed to provide individuals with fundamental knowledge of artificial intelligence management system best practices, standards, tools, and techniques. The training course provides the fundamental information, terminology, and concepts related to AIMS and the benefits of introducing good AI governance practices within the working environment.

Course Outline

AIMS Establishment requirements

Overview of ISO/IEC 42001 / Context of the organization / Leadership /Planning /Support /Operation /Performance Evaluation /Improvement

AI Controls

Policies related to AI /Internal organization /Resources for AI systems /Assessing impact of AI systems /AI system life cycle /Data for AI systems /Information for interested parties of AI systems /Use of AI systems /Third party relationships

Learning Objectives

Know and understand Artificial Intelligence fundamental concepts, elements, and functions. Know and understand ISO/IEC 42001 requirements and controls and describe their function and operation. Know, understand, and be able to participate in Artificial Intelligence MS implementation projects and related activities. Know, understand, and be able to participate in AIMS audits and related activities.

Target Audience

The ISO/IEC 42001 Practitioner training course is developed for individuals interested in gaining basic competency in AI management system frameworks, tools, and techniques, for example: Executives or Business Owners, Information, Security Managers, Cybersecurity Managers, Risk Managers, Entry-level employees of the private and public sector.

Exam

50 MCQ online (60% to pass)

ISO/IEC 42001 Lead Implementer (4 Days)

COURSE OVERVIEW

TRECCERT ISO/IEC 42001 Lead Implementer is an expert-level course developed to equip trainees with a practical understanding of the Artificial Intelligence Management System (AIMS) implementation approach based on the requirements of the ISO/IEC 42001 standard. The training course provides a comprehensive overview of the AIMS implementation based on the Plan-Do-Check-Act model and related concepts, processes, methods, and techniques.

COURSE OUTLINE

1. Introduction to AIMS

Introduction to AI / AI Management System Overview / AI Governance Frameworks and Best Practices

2. ISO/IEC 42001 Requirements

Context of the organization / Leadership / Planning / Support / Operation / Performance Evaluation /Improvement

3. AI controls

Policies related to AI / Internal Organization / Resources for AI systems /Assessing impacts on AI systems /AI system life cycle /DATA for AI systems /Information for interested parties of AI systems /Use of AI systems /Third party relationships

4. AIMS initiation

Develop the Project Charter /Ensure Management Commitment /Identify the interested parties /Conduct a Gap Analysis /Prepare the PDCA Cycle

5. Establishment Phase

Establish the Context of the Organization /Define the AIMS Scope /Establish the Objectives, Processes and Procedures /Establish the AIMS Policy /Define the Risk Assessment Approach /Create the AIMS implementation Plan /Management Authorization to Implement ad Operate the AIMS

6. Implementation and Operation Phase

AI Risk Management /Implement the AI Management Policies and Procedures / Manage AIMS Operations /Awareness and Training /Resource Management and Documented Information

7. Monitor and Review phase

Monitor the AIMS /Conduct Internal Audits /Review the AIMS

8. Maintenance and Improvement Phase

Implement the Identified improvements /Corrective and Preventive Actions / Communicate the Actions and improvements /Ensure Continual Improvement of AIMS

LEARNING OBJECTIVES

Know and understand artificial intelligence management fundamental concepts, standards, best practices and laws/regulations.

Know and understand ISO/IEC 42001 requirements, and describe their function and operation.

Know, understand and be able to define a framework for implementing a AI Management System (AIMS) within an organization.

Know, understand and be able to interpret ISO/IEC 42001 controls and implement the AIMS based on the defined framework.

Know, understand and be able to support the implementation team to continually improve the implemented management system.

TARGET AUDIENCE

The ISO/IEC 42001 Lead Implementer training course is developed for professionals who are involved in AI management, including:

Head of Compliance or Risk / AI Governance Analyst, Consultant, Manager / IT Manager, Compliance Officer, Risk Manager

ISO/IEC 42001 Lead Auditor (4 days)

COURSE OVERVIEW

TRECCERT ISO/IEC 42001 Lead Auditor is an expert-level course developed to equip trainees with a practical understanding of the Artificial Intelligence Management System (AIMS) audit approach based on the requirements of the ISO/IEC 42001 and ISO 19011 standards. The training course provides a comprehensive overview of the AIMS audit following the ISO 19011 guidelines for MS auditing and related concepts, processes, methods and techniques.

COURSE OUTLINE

1. Introduction to AIMS

Introduction to AI /AI Management System Overview /AI Governance Frameworks and Best Practices

2. ISO/IEC 42001 Requirements

Context of the organization /Leadership /Planning /Support /Operation /Performance Evaluation /Improvement

3. AI controls

Policies related to AI /Internal Organization /Resources for AI systems /Assessing impacts on AI systems /AI system life cycle /DATA for AI systems /Information for interested parties of AI systems /Use of AI systems /Third party relationships

4. Introduction to Audit

Auditing based on ISO 19011 /Types of Audit /Audit Principles /Auditor Behavior and Performance /Auditor Roles and Responsibilities

5. Audit Program Management

Creating an Audit Programme / Establishing Audit Programme / Audit Programme Implementation / Audit Programme Monitoring and Reviewing

6. The Audit Process

Audit Initiation /Audit Planning /Execution /Reporting /Follow-Up Auditing

LEARNING OBJECTIVES

Know and understand artificial intelligence management fundamental concepts, standards, best practices and laws/regulations.

Know and understand ISO/IEC 42001 requirements, and describe their function and operation.

Know and understand ISO/IEC 42001 – Annex A controls, and describe their purposes and auditing methods.

Know, understand and be able to participate in AIMS auditing projects and related activities.

Know, understand and be able to audit AIMS projects and related activities.

TARGET AUDIENCE

The ISO/IEC 42001 Lead Auditor training course is developed for professionals responsible for the audit and maintenance of the AIMS, for example: Information Security Specialists, Cybersecurity Specialists, Compliance Officers, External and/or Internal Auditors, Security Analysts.

Business Continuity

ISO/IEC 22301 Foundation (2 Days)

The BCMS Foundation training course is an entry-level course developed based on the ISO/IEC 22301 requirements. In this two-day course, participants are provided with a fundamental understanding of the Business Continuity Management System (BCMS). Individuals will have the opportunity to gain a basic understanding of ISO/IEC 22301 requirements, controls, and associated terminology and concepts.

Educational Objectives

-Become familiar with the vocabulary of the ISO/IEC 22301.

-Understand the structure of the ISO/IEC 22301, the components and the operation of a BCMS based on ISO/IEC 22301 and its principal processes

-Become familiar with the mandatory clauses of the ISO/IEC 22301.

-Acknowledge the correlation between ISO/IEC 22301 and other standards and regulatory frameworks.

Targeted Audience

For individual interested in joining a BCMS team and personnel involved in BCMS intending to complement their on-the-job training related to business continuity.

Examination and Certification

Candidates interested to obtain Certified ISO/IEC 27001 foundation credential are required to successfully pass the exam. The ISO/IEC 27001 Foundation exam consists of 40 multiple choices questions, including the stem and four alternatives (only one correct answer).

ISO/IEC 22301 Lead Implementer (4 Days)

TRECCERT ISO 22301 Lead Implementer is an expert-level course to equip trainees with a practical understanding of the Business Continuity Management system (BCMS) implementation approach based on the ISO 22301 Standard.

Educational Objectives

-Know and understand business continuity, including principles, fundamental concepts, and standards, best practices and laws/regulations.

-Know and understand ISO 22301 requirements and describe their function and operation.

-Know and understand how a business continuity management system can be implemented in an organization.

-Know, understand and be able to initiate and establish the implementation of a BCMS.

-Know, understand and be able to operate, monitor and maintain the implementation of a BCMS.

Targeted Audience

For individual responsible for the implementation and maintenance of a BCMS for example:

-Head of Technology, Compliance or Risk

-Business Continuity Analyst, Consultant, Manager or Officer

-Disaster Recovery Analyst or Consultant

Course Outline

Chapter 1 – Introduction to BCMS

Introduction to business continuity
BCMS overview
Incident Management and Disaster Recovery

Chapter 2 – ISO 22301 Requirements

- Context of the organization
- Leadership
- Planning
- Support
- Operation
- Performance Evaluation

Chapter 3 – BCMS Initiation

- Develop the BCMS Project Charter
- Ensure Management Commitment
- Identify the Interested Parties
- Conduct a Gap Analysis

Chapter 4 – Establishment Phase

- Establish the Context of the Organization
- Define the BCMS Scope
- Establish the Objectives, Processes, and Procedures
- Establish the BCMS Policy
- Define the Risk Assessment Approach
- Create the BCMS Implementation Plan
- Management Authorization

Chapter 5- Implementation and Operation Phase

- Business Impact Analysis and Risk Assessment
- Business Continuity Strategies and Solutions
- Business Continuity Plans and Procedures
- Implementation of Exercise Programs
- Manage Operations and Resources

Chapter 6 – Monitor and Review Phase

- Monitor the BCMS
- Conduct Internal Audits
- Review the BCMS

Chapter 7. Maintenance and Improvement Phase

- Implement the Identified Improvements
- Corrective and Preventive Actions
- Communicate the Actions and Improvements
- Ensure Continual Improvement of the BCMS

Examination 150 MCQ online - 180 minutes (60% to pass)

ISO/IEC 22301 Lead Auditor (4 Days)

TRECCERT ISO 22301 Lead Auditor is an expert-level course to equip trainees with a practical understanding of the Business Continuity Management system (BCMS) audit approach based on the ISO 22301 and ISO 19011 standards.

Educational Objectives

-Know and understand business continuity, including principles, fundamental concepts, and standards, best practices and laws/regulations.

-Know and understand ISO 22301 requirements and describe their function and operation.

-Know and understand the audit process essentials and the principles based on which an auditor must carry out an audit.

-Know, understand and be able to participate in the management of an audit programme.

-Know, understand and be able to participate in a BCMS audit process

Targeted Audience

For individual responsible for the audit and maintenance of a BCMS for example:

-Head of Technology, Compliance or Risk

-Business Continuity Analyst, Consultant, Manager or Officer

-External and/or Internal Auditor

-Disaster Recovery Analyst or Consultant

Course Outline

Chapter 1 – Introduction to BCMS

Introduction to business continuity
Business Continuity Statutory and Regulatory Requirements
Business Continuity Best Practices

Chapter 2 – ISO 22301 Requirements

- Context of the organization
- Leadership
- Planning
- Support
- Operation
- Performance Evaluation

Chapter 3 – Introduction to Audit

- Auditing based on 19011
- Types of Audit
- Audit Principles
- Auditor Behavior and Performance
- Auditor Roles and Responsibilities

Chapter 4 – Audit Programme Management

- Creating an Audit Programme
- Establishing Audit Programme
- Audit Programme Implementation
- Audit Programme Monitoring and Reviewing

Chapter 5- The Audit Process

- Audit Initiation
- Audit Planning
- Audit Execution
- Reporting
- Follow-Up Auditing

Examination 150 MCQ online - 180 minutes (60% to pass)

Compliance

ISO 37301 Foundation (2 Days)

Course Overview

TRECCERT ISO 37301 Foundation is an entry-level course developed to provide trainees with fundamental knowledge of ISO 37301 requirements. The training course provides a complete introduction to the Compliance Management System (CMS) based on the ISO 37301 standard.

Course Outline

1. CMS Establishment Requirements

Overview of ISO 37301 /Context of the organization /Leadership /Planning /Support

2. CMS Operation Requirements

Operation

3. CMS Evaluation and maintenance

Performance Evaluation / Improvement

Learning Objectives

Understand the purpose and benefits of a compliance management system (CMS) and how it aligns with an organization's overall risk management strategy.

Familiarize yourself with the structure and requirements of the ISO 37301 standard, including the role of top management, the CMS process approach, and the use of documented information.

Understand the importance of establishing and maintaining a compliance culture and function following the requirements of ISO 37301 standard.

Understand how to continuously improve the CMS through the use of corrective and preventive actions, management review, and other process improvement techniques.

Target Audience

The ISO 37301 Foundation training course is developed for individuals interested in building a career or contributing to compliance management systems, for example:

Compliance Officer /Risk Manager /Internal Auditor /Other Management Personnel

Examination and Certification

Individuals interested in ISO/IEC 37301 Foundation certification will have the opportunity to undergo TRECCERT examination and pursue certification. Candidates can take TRECCERT certification exam as part of our training sessions, which are provided by TRECCERT partners, including Nitroxis.

The CMS Foundation exam consists of 40 multiple-choice questions. Candidates have 1 hour to complete the exam.

The CMS Foundation certification demonstrates that an individual comprehends the structure and approach of an Compliance Management System (CMS) based on the requirements of the ISO/IEC 37301. Being TRECCERT CMS Foundation Certified provides you with the opportunity to advance further your credentials or certification level within the TRECCERT Certification Path.

ISO 37301 Lead Implementer (4 Days)

TRECCERT MS Lead Implementer is an advanced-level course developed to provide trainees with a solid knowledge of the ISO 37301 guidelines. The training course provides an in-depth explanation of guidelines and controls mandated to establish, manage and improve a compliance management system.

TARGET AUDIENCE

The ISO 37301 Lead Implementer training course is developed for individuals responsible for the implementation and maintenance of a CMS, for example:

Compliance Expert, Consultant, Manager, or Officer

Quality manager

Risk manager

Regulatory affairs professional

LEARNING OBJECTIVES

Develop the skills necessary to effectively lead the implementation and maintenance of a compliance management system (CMS) in accordance with the ISO 27301 standard.

Learn how to continuously improve the CMS through the use of corrective and preventive actions, management review, and other process improvement techniques.

Develop the skills necessary to effectively train and mentor others on the implementation and maintenance of a CMS.

Understand the role of a lead implementer in managing the CMS implementation project, including risk assessment and stakeholder engagement.

COURSE OUTLINE

1. Introduction to CMS

Introduction to Compliance Management System / CMS Overview /Importance of CMS /The Need for a CMS

2. ISO 37301 Requirements

Context of the Organization Leadership / Planning/ Support /Operation Performance Evaluation /Improvement

3. CMS Initiation

Develop the CMS Project Charter / Ensure Management Commitment /Identify the Interested Parties / Conduct a Gap Analysis

4. Establishment Phase

Establish the Context of Organization /Define the CMS Scope /Establish the Objectives, Processes, and Procedures /Establish the CMS Policy /Define the Risk Assessment Approach /Create the CMS Implementation /Plan Management Authorization

5. Implementation and Operation Phase

Compliance Culture and Governance /Implement Operational Controls / Implement Technical Controls / Compliance Risk Assessment /Manage Operations and Resources

6. Monitor and Review Phase

Monitor the CMS / Conduct Internal Audits / Review the CMS

7. Maintenance and Improvement Phase

Implement the Identified Improvements /Corrective and Preventive Actions /Communicate the Actions and Improvements /Ensure Continual /Improvement of the CMS.

Examination Details

150 MCQ Questions - 180 minutes

Online

ISO 37301 Lead Auditor (4 Days)

TRECCERT ISO 37301 Lead Auditor is an expert-level course developed to equip trainees with a practical understanding of the Compliance Management System (CMS) auditing approach based on the ISO 37301 and ISO 19011 standards.

COURSE OUTLINE

1. Introduction to CMS

Introduction to Compliance Management System /CMS overview /Importance of CMS /The Need for a CMS

2. ISO 37301 Requirements

Context of the Organization /Leadership /Planning /Support /Operation /Performance Evaluation /Improvement

3. Introduction to Audit

Auditing based on ISO 19011 /Types of Audit /Audit Principles /Auditor Behavior and Performance /Auditor Roles and Responsibilities

4. Audit Programme Management

Creating an Audit Programme /Establishing Audit Programme /Audit Programme Implementation /Audit Programme Monitoring and Reviewing

5. The Audit Process

Audit Initiation /Audit Planning Audit /Execution /Reporting / Follow-Up Auditing

LEARNING OBJECTIVES

Develop the skills necessary to effectively plan and conduct audits of compliance management systems (CMS) in accordance with the ISO 37301 standard and ISO 19011.

Understand the process for identifying and addressing non-conformities during an audit.

Learn how to communicate audit findings and report on the results of an audit.

Understand the requirements for certification and the role of the lead auditor in the certification process.

Understand the role of the lead auditor in managing the audit process, including risk assessment and stakeholder engagement.

TARGET AUDIENCE

The ISO 37301 Lead Auditor training course is developed for individuals responsible for the audit and maintenance of a CMS, for example:

Compliance Expert, Consultant, Manager, or Officer /Internal or external auditor / Legal professional with a focus on compliance /Regulatory affairs professional

EXAMINATION DETAILS

150 MCQ Questions - 180 minutes

Online

Data Protection

GDPR Essentials (1 day)

TRECCERT GDPR Essentials is an introductory-level course developed to provide individuals with fundamentals knowledge in data protection. The training course introduces key associated terminology, concepts, practices and frameworks.

Course Outline

Chapter 1- Introduction to Data Protection

- Data Protection Essentials
- Data Protection Trends
- Data Protection Development

Chapter 2- Data Protection Framework

- Regulation
- Technical
- Organizational

Chapter 3- Spotlight on GDPR

- Introduction to GDPR
- GDPR Scope
- Processing Principles
- Rights of Data Subjects
- Cross-Border Processing
- Data Breaches

Audience

The GDPR Essentials training course is developed for individuals interested in gaining basic competency in data protection, for example:

Data or Privacy Manager ; DPO ; Data Processor ; Data Controller

Learning objectives

Know and understand the core elements of data protection, data protection laws, regulations and acts.

Know and understand the TRECCERT data protection framework and its domains.

Know and understand data protection form a legal point of view and get familiar with data protection acts and legislations outside the EU.

Know and understand the technical aspects of data protection.

Know and understand the governance and management aspects of data protection in an organization.

Exam – 20 MCQ online (60% to pass)

GDPR Professional (3 days)

TRECCERT GDPR Professional is an advanced-level course developed to provide trainees with a solid knowledge of the GDPR 2016/679 requirements and controls. The training course provides an in-depth understanding of the applicability, principles, requirements and obligations of GDPR.

Course Outline

Chapter 1- Introduction to GDPR
- Introduction to Data Protection
- GDPR Overview
- Personal Data

Chapter 2- GDPR Core Elements
- Principles of Data Processing
- Data Subjects
- Data Controller and Data Processor
- Data Protection Officer
- Cross-Border Transfers of Personal Data
- Personal Data Breaches

Chapter 3- Implementing a Data Protection Framework
- Building a GDPR Implementation Plan
- Define and Implement Data Protection Measures
- Managing Risks
- Data Breach Preparedness and Response

Chapter 4- GDPR Compliance Assessment
- Data Protection Assessment
- Compliance Assessment Process

Audience

The GDPR Professional training course is developed for individuals responsible for the implementation and maintenance of a GDPR program, for example:

DPO ; Data Processing Assessment Manager ; Privacy Assessment Manager ; Information Security Risk Manager

Learning objectives

Know and understand the core elements of the GDPR, including its status, scope, impact and responsibilities of the parties involved.

Know and understand the importance of processing personal data based on data protection principles and compliance with GDPR requirements.

Know and understand and be able to establish a data protection implementation plan, implement data protection measures and maintain a data protection framework.

Know and understand the basics methods used to manage information security risk and data breach programs.

Know, understand and be able to assess compliance of the implemented data protection frameworks with the GDPR requirements.

Exam – 100 MCQ online – 120 minutes (60% to pass)

Data Protection Impact Analysis Specialist (1 day)

Data Protection Impact Specialist (DPIAS) is a course developed to provide trainees with a solid knowledge of data protection risk identification and minimization applications. The training course provide an in-depth explanation of personal data processing activities and their related risk levels, which can be managed by initiating the integration of appropriate safeguards.

Course Outline

Chapter 1- Introduction to Data Protection

Defining Data Protection
Personal Data
Data Protection Regulation

Chapter 2- Data Protection Framework

Introduction to DPIA
Standards and Laws that Support the DPIA

Chapter 3- Inputs of conducting the DPIA

Roles and Responsibilities
DPIA Pre-Assessment
Business Processes
Processing Purposes and Types of Data
Data Protection Policies and International Transfers

Chapter 4 – 6 steps Model to conduct DPIA

Identify whether DPIA is required
Define Project Characteristics
Identify Data Protection Related Risks
Identify Solutions
Sign-off the DPIA Outcomes
Integrate DPIA Solutions into Projects

Chapter 5 – DPIA Template

DPIA Template Examples for Candidates

Audience

The DPIAS training course is developed for Data Protection Specialist and any professional who aims to enhance skills in managing and minimizing data protection risk through a DPIA framework.

Learning objectives

Know and understand the data protection essentials and get introduced to data protection laws and regulations

Know and understand the importance of processing personal data based on data protection principles and compliance with data protection requirements

Know and understand and be able to establish a data protection impact analysis framework.

Know and understand the basics methods used to integrate the DPIA framework into organizations and manage it effectively.

Know, understand and be able to assess compliance of the implemented DPIA framework.

Exam – 40 MCQ online – 60 Minutes (60% to pass)

Digital Operational Resilience ACT (DORA)

DORA Essentials (2 Days)

Course Overview

The TRECCERT DORA Essentials course is an entry-level program designed to provide trainees with fundamentals knowledge of the Digital Operational Resilience Act (DORA) requirements. This training offers a comprehensive introduction to the core components of DORA, focusing on how financial institutions can establish and maintain operational resilience in the face of digital and ICT-related risks.

Course Outline

Chapter 1- Introduction to DORA

Introduction to Digital Operational Resilience
DORA Overview
Importance of Digital Resilience in Finance
How does ISO Standards align with DORA?

Chapter 2- Risk Management Requirements

Risk identification
Risk Protection and Prevention
Risk Detection
Response and Recovery
Backup Policies and Procedures, Restoration and Recovery Procedures and Methods

Chapter 3- Incident Reporting Process

ICT-Related Incident Management Process
ICT-Related Incidents and Cyber threats

Chapter 4- Digital Operational Resilience Testing Requirements

Testing of ICT Tools and Systems
Advanced Testing of ICT Tools, Systems and Processes for TLPT (*)
Requirements for testers for the carrying out of TLPT

(*) Thread-Lead Penetration Testing

Chapter 5- ICT Third Party Management Requirements

Management of ICT Third Party Principles
Due Diligence Process for ICT Service Providers
Exit Strategies

Learning Objectives

Understand the Core Principles of DORA:

Grasp the fundamental concepts of the Digital Operational Resilience Act (DORA) and its significance within the financial sector.

Learn the Regulatory Requirements:

Gain a comprehensive understanding of the regulatory landscape DORA introduces, including the specific requirements for ICT risk management, incident reporting, and third-party management.

Implement Digital Resilience Strategies:

Develop the ability to implement effective digital operational resilience strategies that align with DORA's requirements, ensuring financial institutions are prepared to manage ICT-related risks.

Enhance Operational Resilience:

Learn how to enhance the operational resilience of your organization by applying best practices in ICT risk management and conducting regular resilience testing.

Prepare for Compliance:

Equip yourself with the knowledge needed to prepare your organization for compliance with DORA, including how to maintain and continuously improve operational resilience practices.

Foster a Culture of Resilience:

Understand the importance of fostering a culture of digital resilience within your organization, ensuring that all levels of the organization are aligned with DORA's objectives.

Target Audience

The DORA Essentials training course is designed for individuals who are interested in building a career or contributing to the implementation of digital operational resilience frameworks within financial institutions, such as:

Compliance Officers – Risk Managers – IT Security Professionals – Internal Auditors – Others Management Personnel involved in ICT and risk management

Examination and Certification

Individuals interested in DORA certification will have the opportunity to undergo TRECCERT examination and pursue certification. Candidates can take TRECCERT certification exam as part of our training sessions, which are provided by TRECCERT partners, including NITROXIS.

The DORA Essential exam consist of 20 multiple-choice questions. Candidates have 1 hour to complete the exam.

The DORA Essential certification demonstrates that an individual comprehends the structure and approach of DORA based on the requirements of DORA. Being TRECCERT DORA Essentials Certified provides you with the opportunity to advance further your credentials or certification level within the TRECCERT Certification Path.

Environmental Social Governance (ESG)

ESG Essentials (1 Day)

The Environmental, Social, and Governance (ESG) Essentials training is an introductory course that aims to equip participants with a basic understanding of ESG principles and practices. This course provides an overview of the key concepts related to ESG and its Pillars and provides information on the ISO Standards that support each Pillar of the ESG integration of appropriate safeguards.

Course Outline

Chapter 1- Introduction to Corporate sustainability and ESG fundamentals

- Defining Corporate Sustainability
- Defining ESG
- ESG Regulations Landscape
- Introduction to ISO and Relevant Standards for ESG

Chapter 2- ESG Pillars Risk Management Requirements

- Environmental Pillars
- Social Pillars
- Governance Pillars

Audience

The ESG Essentials training course is ideal for individuals looking to grasp the fundamental aspects of ESG in the context of business and sustainability.

This course is suitable for a wide range of professionals, including:

Entry-level employees
Small business owners
Students
Environmental enthusiasts

Learning objectives

Know and understand the fundamental concepts of Corporate Sustainability, its importance, and its pillars.

Know and understand the fundamental concepts of the Environmental, Social, and Governance (ESG) movement, its factors, and its impact on organizations.

Know and understand the ESG Pillars and how ISO Standards support the management of each pillar.

Get familiar with the ESG evolution and regulations such as the Global Reporting Initiative (GRI), UN Global Compact, UN Sustainable Development Goals (SDGs).

Exam – 20 MCQ online (60% to pass)

Information Security

ISO/IEC 27001 Foundation (2 Days)

The ISMS Foundation training course is an entry-level course developed based on the ISO/IEC 27001 requirements. In this two-day course, participants are provided with a fundamental understanding of the Information Security Management System (ISMS). Individuals will have the opportunity to gain a basic understanding of ISO/IEC 27001 requirements, controls, and associated terminology and concepts.

Educational Objectives

-Become familiar with the vocabulary of the ISO/IEC 27001.

-Understand the structure of the ISO/IEC 27001.

-Become familiar with the mandatory clauses of the ISO/IEC 27001.

-Become familiar with the controls of the ISO/IEC 27001.

Training Approach

-Trainer Slides

-Quizzes

Targeted Audience

-Entry-level professionals of an information security team.

-Personnel of organizations intending to complement their on-the-job training related to information security.

-New ICT professionals wanting to increase their competency in information security.

Training Course Outline
Day One
Introduction to ISMS concepts as required by ISO/IEC 27001:2022
Day Two
Introduction to Annex A Controls

Examination 40 MCQ online - 60 minutes (60% to pass)

ISO/IEC 27001 Lead Implementer (4 Days)

Fast Track for ISMS Professional (ISO/IEC 27001) and Lead Implementer (ISO 19600). TRECCERT offers the ISO/IEC 27001 Lead Implementer fast track course for candidates that want to learn intensively to achieve their goals. The ISO/IEC 27001 Lead Implementer consists of two TRECCERT training courses, the ISMS Professional (ISO/IEC 27001) and Lead Implementer (ISO 19600). These training courses are professional-level courses developed based on the pertinent ISO standards' requirements or guidelines. In this four-day course, participants are provided with a practical understanding of ISO/IEC 27001 requirements and controls, and how to establish, implement, manage and improve an information security management system (ISMS) based on ISO/IEC 27001 and ISO 19600. Participants will also gain a thorough understanding of best practices used to implement information security controls based on ISO/IEC 27002.

Educational Objectives

Understand the basic concepts of information security.
Become familiar with information security frameworks.
Understand the mandatory requirements of ISO/IEC 27001.
Understand the information security controls of ISO/IEC 27001: Annex A.
Learn how to implement an information security management system (ISMS).
Learn how to audit an information security management system (ISMS).
Become familiar with management systems (MSs).
Become familiar with integrated management systems (IMSs).
Understand the processes of the initiation phase.
Understand the processes of the establishment phase.
Understand the processes of the implementation and operation phase.
Understand the processes of the maintaining and improving phase.

Training Approach

Trainer Slides
Quizzes

Targeted Audience

Members of an information security management system (ISMS) team.
Personnel involved in information security management system (ISMS) implementation
Professionals wanting to increase their competency in implementing an information security management system (ISMS).

Prerequisites

None. However, it is recommended to have a basic knowledge of the ISO/IEC 27001 standard and guidelines or to have read the standard once prior the course.

Day 1: Introduction to ISO/IEC 27001 and initiation of an ISMS
Day 2: Planning the implementation of an ISMS
Day 3: Implementation of an ISMS
Day 4: ISMS monitoring, continual improvement, and preparation for the certification audit

Examination 150 MCQ online - 180 minutes (60% to pass)

ISO/IEC 27001 Lead Auditor (4 Days)

Fast Track for ISMS Professional (ISO/IEC 27001) and Lead Auditor (ISO 19011).

TRECCERT offers the ISO/IEC 27001 Lead Auditor fast track course for candidates that want to learn intensively to achieve their goals. The ISO/IEC 27001 Auditor consists of two TRECCERT training courses, the ISMS Professional (ISO/IEC 27001) and Lead Auditor (ISO 19011). These training courses are professional-level courses developed based on the pertinent ISO standards' requirements or guidelines. In this four-day course, participants are provided with a practical understanding of ISO/IEC 27001 requirements and controls, and how to establish and manage an audit program, and conduct an information security management system (ISMS) audit.

Educational Objectives

Understand the basic concepts of information security.
Become familiar with information security frameworks.
Understand the mandatory requirements of ISO/IEC 27001.
Understand the information security controls of ISO/IEC 27001: Annex A.
Learn how to implement an information security management system (ISMS).
Learn how to audit an information security management system (ISMS).
Become familiar with management systems (MSs).
Become familiar with management system auditing based on ISO 19011.
Understand the types of audit and auditing principles.
Become familiar with the auditor behavior and performance.
Understand how to establish, implement and manage a management system (MS) audit program.
Understand how to initiate, plan, execute, report and complete a management system (MS) audit.

Training Approach

Trainer Slides
Quizzes

Targeted Audience

Members of an information security management system (ISMS) team.
Personnel involved in information security management system (ISMS) and auditing.
Professionals wanting to increase their competency in auditing an information security management system (ISMS).

Prerequisites

None. However, it is recommended to have a sound knowledge of the ISO/IEC 27001 standard and guidelines.

Introduction to ISMS

Introduction to Information Security / ISMS Overview / IS Frameworks and Best practices

ISMS Requirements

Context of the organization / Leadership / Planning / Support / Operation Performance Evaluation /Improvement

Organizational and People Controls

Information Security Policies and Management / Asset Management and Access Control / Supplier Relationships and Incident Management /Legal and Compliance / HR Security

Physical and Technological Controls

Physical / Technical / Network / Application Security

Introduction to audit

MS Audit and Audit Types / Audit Principles / Auditor Competence and Evaluation/ Code of Ethics and Conflict of Interest

Managing and Audit Programme

Creating an Audit Programme / Establishing an Audit Programme / Audit Programme Implementation / Audit Programme Monitoring and Reviewing

Conducting an ISMS Audit

Initiation of Audit / Audit Planning / Audit Execution /Audit Report / Follow-up auditing

Examination 150 MCQ online - 180 minutes (60% to pass)

ISO 27005 Risk Professional (3 Days)

TRECCERT ISO/IEC 27005 Professional is an advanced-level course developed to provide trainees with a solid knowledge of the ISO/IEC 27005 guidelines and controls. The training course provides an in-depth explanation of guidelines and controls mandated to establish, implement, manage, improve and assess an Information Security Risk Management (ISRM).

Target Audience

The ISO/IEC 27005 Specialist training course is developed for professionals seeking to expand their professional skills on the assessment and management of an information security risk management process, for example:
Information Security Risk Manager, Team Leader or Technician, Business Owner, COO, CIO, CISO, Risk Analyst, Model Risk Specialist, Risk Manager

Learning Objectives

Know and understand the purpose of an information security risk management process, including basic concepts, principles and other risk management frameworks.
Know and understand the whole information security risk management process steps and activities.
Know, understand and be able to identify, assess and treat the information security risks and perform other related activities.
Know and understand the basic analysis and methods used to establish a risk management context, assess and manage information security risks and implement security controls.
Know, understand and be able to support the information security risk manager perform risk management activities.

Course Outline
Chapter 1. Information Security Risk Management
Information Security Background
Risk Management Background
Information Security Risk
Information Security Risk Management Process based on ISO 27005 Standard
Statement of Applicability and Risk Management Risk Heat Maps

Chapter 2. Establishing the Context of the Information Security Risk Management Process

Context Establishment
Information Security Risk Management Process Basic Criteria

Information Security Risk Management Scope and Boundaries
Defining the Organization's Structure

Chapter 3. Information Security Risk Assessment
Information Security Risk Assessment
Approaches Identification of Information Security
Risks Information Security Risk Analysis
Evaluation of Information Security Risks

Chapter 4. Information Security Risk Treatment
Risk Treatment Options and Techniques for Selecting such Options
Risk Treatment Plan Development and Residual Risk Evaluation
Acceptance of Information Security Risks Risk Recording and Reporting

Chapter 5. Risk Communication and Consultation
Overview of Risk Communication and Consultation
Risk Communication and Consultation Phases and Plan Risk Communication and Consultation Techniques

Chapter 6. Risk Monitoring and Review
Overview of the Risk Monitoring and Review Process
Monitoring, Reviewing and Improving the Information Security Risk Management Process

Exam – 100 MCQ online in 120 minutes (60% to pass)

ISO 31000 Risk Practitioner (2 Days)

TRECCERT ISO/IEC 31000 Practitioner is an advanced-level course developed to provide trainees with a solid knowledge of the ISO/IEC 31000 guidelines and controls. The training course provides an in-depth explanation of guidelines and controls mandated to establish, implement, manage, improve and assess Risk Management.

Risk management is an essential aspect of modern business, influencing decisions, strategy, and organizational resilience. The ISO 31000 Risk Practitioner certification equips participants with the tools and knowledge to implement effective risk management frameworks based on the internationally recognized ISO 31000 standard.

Who should attend?

Risk Practitioners: Individuals responsible for designing and implementing risk management systems in their organizations.

Management Professionals: Leaders and decision-makers seeking to align organizational goals with effective risk management strategies.

Auditors and Assessors: Professionals responsible for evaluating risk frameworks and compliance.

Project and Operations Managers: Those dealing with significant operational or strategic risks in their roles.

Consultants: Advisors supporting organizations in building and improving risk management frameworks.

Compliance Officers: in Supporting regulated organizations facing different types of risks

Individuals: Seeking to gain knowledge about the risk management principles, framework, and process. Responsible for the creation and protection of value in their organizations. Interested in pursuing a career in risk management

Course Agenda

Day 1: Introduction to ISO 31000 and risk management and establishing the risk management framework

Day 2: Initiation of the risk management process and risk assessment based on ISO 31000. Risk treatment, recording and reporting, monitoring and review, and communication and consultation according to ISO 31000

Learning objectives

Gain a comprehensive understanding of ISO 31000 principles and risk management frameworks.

Establish, maintain, and continually improve a risk management framework, in accordance with ISO 31000 guidelines.

Apply the risk management process, in accordance with ISO 31000 guidelines.

Develop the ability to identify, assess, and prioritize risks effectively.

Learn to apply risk management techniques in diverse organizational contexts.

Demonstrate the ability to contribute to organizational resilience and sustainability.

Educational approach

The training course is based on theory and best practices used in risk management. Lecture sessions are illustrated with practical examples.

The participants are encouraged to communicate and engage in discussions and exercises.

The exercises are similar in structure with the certification exam questions.

Prerequisites
A fundamental understanding of ISO 31000 and comprehensive knowledge of risk management

Exam

50 MCQ online - 1hour (60% to pass)

Nitroxis Trainings

Introduction Training

Cybersecurity Training

NIST CSF 2.0 – (3 Days)

Course Introduction

The digital age has ushered in a wave of innovation, but it has also opened the door to a growing landscape of cyber threats. Malicious actors are constantly evolving their tactics, targeting critical infrastructure, sensitive data, and operational systems of organizations of all sizes – from large enterprises to small businesses and startups.

These cyberattacks can cause significant financial losses, disrupt operations, and damage an organization's reputation.

The National Institute of Standards and Technology (NIST) addresses this challenge with the Cybersecurity Framework (CSF). This voluntary, non-regulatory framework by NIST provides a structured approach for managing cyber risks. This workshop dives into NIST CSF 2.0.

Through lectures, exercises, and case studies, you'll gain a deep understanding of the framework and how to effectively implement and continuously improve the cybersecurity program, strengthening their organization's cybersecurity posture.

Course Objectives

Gain a thorough understanding of the NIST Cybersecurity Framework (CSF) 2.0 structure and key components (i.e., Core, Tiers, and Profiles).

Learn how to leverage the CSF 2.0 framework within your organization.

Develop an adequate approach for cyber risk governance and management.

Understand how to tailor the CSF 2.0 to meet your organization's specific security needs.

Identify valuable resources and tools to support continuous improvement of your cybersecurity program.

Intended Audience

This training workshop is designed for a broad audience, including:

IT professionals

Security managers

Risk management professionals

IT auditors and compliance officers

Business leaders

Anyone interested in strengthening their organization's cybersecurity posture.

Prerequisites

While no prior cybersecurity experience is mandatory, a basic understanding of IT and security terminology is beneficial. Participants who have completed foundational IT security courses will gain the most from this workshop.

Training Agenda

Day 1: Setting the Stage

Overview of Cyber Risks and Cybersecurity Governance

- Top Business Risks
- The Evolving Threat Landscape
- Importance of Effective Governance for Cybersecurity

NIST CSF Journey:

- Brief History and Role of NIST in Technology Cybersecurity
- Overview of the NIST Cybersecurity Framework (CSF)
- Evolution of the CSF since 2013
- CSF by the Numbers (key statistics about CSF and its adoption)

Understanding the NIST CSF Components:

Core

Deep dive into the framework's Core functions

Explore the categories and subcategories within each function, providing a granular understanding of cybersecurity outcomes.

Tiers

Demystify the CSF Tiers (Partial, Risk-Informed, Repeatable, Adaptive).

Learn how these tiers represent different levels of cybersecurity maturity.

Explore how to select the appropriate tier for your organization.

Profiles

Organizational Profiles

Understand the purpose of Current and Target Profiles in assessing your cybersecurity posture.

Learn how to develop these profiles to identify gaps and set improvement goals.

Community Profiles:

Explore the structure and lifecycle of Community Profiles

Discover how these profiles can provide valuable benchmarks and best practices.

Day 1 Q&A Session and Course Review

Day 2: Implementing and Managing Cybersecurity Program.

Continuous Improvement of Cybersecurity Program:

for Scoping an Organizational Profile

Gathering Information for Profile Development

Building the Current and Target Profiles

Identifying Gaps and Creating Action Plans

Implementing Action Plans and Measuring Progress

Risk Management Integration:

Enterprise Risk Management (ERM) and its Connection to Cybersecurity

Information and Communications Technology (ICT) Risk Management

Understanding Cybersecurity Risk Management (CSRM)

Integrating and Coordinating Risk Management Activities

Using the Cybersecurity Risk Register (CSRR) for Effective Risk Management

Cybersecurity Supply Chain Risk Management (C-SCRM):

Overview of Information and Communications Technology (ICT) Supply Chain Risks

Establishing a C-SCRM Capability

Setting C-SCRM Requirements and Processes

Day 2 Q&A Session and Course Review

Day 3: Deep Dive and the Future

NIST Online Resources:

Examining CSF Resources such as Quick Start Guides, Informative References, CSF Resource Tool, Cybersecurity & Privacy Reference Tool (CPRT), and CSF Implementation Examples

Methods for submitting new resources to NIST

Cybersecurity Maturity Assessment:

Benefits of conducting cybersecurity maturity assessments

Using NIST CSF for cybersecurity assessments

Leveraging CSF with Other Standards and Frameworks:

NIST CSF vs ISO 27001 vs CIS Controls vs NIST SP 800-53 (highlighting similarities and differences)

CSF Relationship with ISO Standards and other NIST publications

Leveraging the CSF for Effective Compliance Management

Exploring the Value of the CSF:

Use Cases and Success Stories (real-world examples of CSF implementation)

Applying the CSF to Address Specific Challenges

What's Coming Next for the NIST CSF?

Additional Informative References

Additional Quick Start Guides

Future Community Profiles

Resources Translations

Use Cases and Success Stories

Online Training Materials

Wrap-Up:

Importance of continuous improvement in cybersecurity

Key takeaways and actionable steps for implementing the CSF in your organization.

Training Methodology

This workshop employs a variety of engaging and interactive learning methods to ensure a comprehensive understanding of the NIST CSF 2.0. Here's what you can expect:

Experienced instructors will guide you through the concepts and practical applications.

Interactive discussions to share experiences, ask questions, and gain insights from participants.

Analyzing real-world scenarios where organizations have successfully implemented the NIST CSF.

Applying your knowledge through practical exercises, such as conducting risk and maturity assessments, and building sample profiles.

Quizzes and poll questions will help you gauge your understanding throughout the workshop.

You'll receive a comprehensive course material with all the key concepts, resources, and references covered during the training.

CIS Critical Security controls (v8) (3 Days)

Introduction

This comprehensive training workshop equips participants with the knowledge and skills necessary to understand and implement the Center for Internet Security (CIS) Critical Security Controls version 8 (CIS Controls v8). Through a blend of interactive lectures, group discussions, practical exercises, and case studies, participants will gain a thorough understanding of the 18 CIS Controls and their associated Safeguards.

The training delves into the core principles and objectives of CIS Controls v8, highlighting their significance in mitigating modern cyber threats. Participants will learn how to prioritize and select relevant controls for their specific organization, integrate them seamlessly into existing security practices, and maintain ongoing monitoring and improvement.

Course Objectives

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

-Gain a deep understanding of the CIS Controls framework.
-Identify and explain the 18 CIS Controls and their associated Safeguards.
-Recognize the importance of implementing CIS Controls in your organization.
-Develop strategies for integrating CIS Controls into existing security practices based on your organization's size and resources.

-Learn best practices for managing and maintaining CIS Controls implementation.

-Identify valuable resources for further exploration of CIS Controls.

-Understand how CIS Controls map to other security frameworks like ISO and NIST.

Intended Audience

This training is designed for a broad audience, including:

-IT professionals (system administrators, network security specialists, security analysts)

-Developers and programmers

-Business managers and executives

-Anyone involved in protecting their organization's data and systems

Prerequisites

Basic understanding of cybersecurity concepts like firewalls, malware, and user access control.

Training Agenda

Module 1: Introduction to CIS Controls v8

-Overview of the CIS Controls and its history.

-The importance of CIS Controls in a modern threat landscape.

-Benefits of implementing CIS Controls.

-Understanding the structure of CIS Controls v8 with a focus on Safeguards.

-Introduction to CIS Critical Security Controls Implementation Groups (IGs) and their purpose.

-Module 1 Q&A Session and Course Review

Module 2: Breakdown of the 18 CIS Controls

-This section will cover each of the 18 CIS Controls in detail, including:

-A clear explanation of the control's objective.

-The associated Safeguards and their implementation recommendations.

-Examples of how the control can be implemented in different IT environments.

-Real-world scenarios where the control can prevent cyberattacks.

-Module 2 Q&A Session and Course Review

Module 3: Implementing CIS Controls in Your Organization

-Introduction to the CIS Risk Assessment Method (CIS RAM) and its role in prioritizing CIS Controls implementation.

-Prioritization and selection of relevant CIS Controls based on organizational needs, risk profile, and Implementation Group (IG) membership.

-Strategies for integrating CIS Controls into existing security policies and procedures.

-Considerations for implementing CIS Controls in Cloud and hybrid environments.

-Resources and tools available to assist with CIS Controls implementation (e.g., CIS CSAT).

-Module 3 Q&A Session and Course Review

Module 4: Best Practices and Ongoing Management

-Importance of continuous monitoring and improvement of CIS Controls implementation.

-Best practices for user awareness training and promoting a culture of security.

-Maintaining compliance with CIS Controls and adapting them to evolving threats.

-Mapping CIS Controls to other security frameworks such as ISO 27001 and NIST CSF.

-Module 4 Q&A Session and Course Review

Training Methodology

This CIS Controls v8 training workshop utilizes a variety of engaging and interactive learning methods to ensure a comprehensive understanding and practical application of the controls. Here's what you can expect:

-Experienced instructors with real-world experience will guide you through the core principles, objectives, and implementation strategies of CIS Controls v8.
-Interactive discussions to share experiences, ask questions, and gain valuable insights from fellow participants.
-Analyzing case studies exploring successful implementations of CIS Controls.
-Hands-on exercises such as prioritizing and selecting CIS Controls for your organization, developing sample implementation plans based on your IG, and mapping CIS Controls to other frameworks (optional, depending on time).
-Quizzes and poll questions will help you gauge your understanding throughout the workshop.
-You'll receive a comprehensive course material with all the key concepts, resources, and references covered during the training.

Preparation for certifications (Bootcamps)

Over the years and building our experience, we have created and written our own ISACA and (ISC)2 courses. We thus keep control and control of the content as well as the updating of it to follow the evolution of the certifications and the various examination contents.

This allows us to seek training that seems interesting to today's information security practitioner without having to spend astronomical sums at the start of the year, no longer pay for content accreditations, no longer pay to have each trainer audited and accredited and all this, without knowing whether a course will be given or not.

You benefit directly because we do not pass on this hidden cost to you by the big publishers.

For the same reasons, and because we want to maintain our independence, we cannot register you for the ISACA and (ISC)2 exams.

It is therefore in full transparency that we are communicating this to you.

If you also fell like the soul of a trainer with a minimum of commercial flair and you don't have the time to write the content yourself, this product is also a good compromise because we can sell it to you under license. You teach the course yourself and manage everything from A to Z.

ISACA

CISA® (Certified Information Systems Auditor) (5 Days)

This 5-day course prepares the CISA® Certified Information Systems Auditor exam by covering the entire Common Body of Knowledge (CBK) course, a common core of knowledge in security defined by the ISACA® Information Systems Audit and Control Association.

CISA® certification is recognized around the world. It is aligned with the 28th Edition of the CBK, updated for 2024 Job Practice.

Educational Objective:

-Know the five major areas covered by CISA® certification
-Understand the concepts of IT audit and IT governance
-Preparing the CISA® Certification Exam, ISACA Certified Security Auditor

Certification:

A 5-Year experience is required to obtain CISA® certification after passing the exam. You can still take the exam first, and must register on the ISACA website.

Participants:

Information System Directors /Auditors /Responsible for Business Continuity / CISO / people for which the control of Information Security is fundamental in achieving their goals

Prerequisites:

Basic Knowledge in the Information System

Chapter 1: Information System Auditing Process

Part A: Planning

-IS Audit Standards, Guidelines, Functions and Code of Ethics
-Types of Audits, Assessments and Reviews
-Risk-Based Audit Planning
-Type of Controls and Considerations

Part B: Execution

-Audit Project Management
-Audit Testing and Sampling Methodology
-Audit Evidence Collection Techniques
-Audit Data Analytics

-Reporting and Communication Techniques
-Quality Assurance and Improvement of the Audit Process

Exercises: Multiple Choices Questions from previous CISA sessions (or comparable exams)

Chapter 2: Governance and Management of IT

Part A: IT Governance

-Laws, Regulations and Industry Standards
-Organizational Structure, IT governance and IT Strategy
-IT Policies, Standards, Procedures and Guidelines
-Enterprise Architecture Consideration
-Enterprise Risk Management
-Data Privacy Program and Principles
-Data Governance and Classification

Part B: IT Management

-IT Resource Management
-IT Vendor Management
-IT Performance Monitoring and Reporting
-Quality Assurance and Quality Management of IT

Exercises: Multiple Choices Questions from previous CISA sessions (or comparable exams)

Chapter 3: Information Systems Acquisition, Development and Implementation

Part A: Information Systems Acquisition and Development

-Project Governance and Management
-Business Case and Feasibility Analysis
-System Development Methodologies
-Control Identification and Design

Part B: Information System Implementation

-System Readiness and Implementation Testing
-Implementation Configuration and Release Management
-System Migration, Infrastructure Deployment and Data Conversion
-Post-implementation Review

Exercises: Multiple Choices Questions from previous CISA sessions (or comparable exams)

Chapter 4: Information Systems Operations and Business Resilience

Part A: Information Systems Operations

-IT Components
-IT Asset Management
-Job Scheduling and Production Process Automation
-System interfaces
-End-User Computing and Shadow IT
-Systems Availability and Capacity Management
-Problem and Incident Management
-IT Change, Configuration, and Patch Management
-Operational Log Management
-IT Service Level Management
-Database Management

Part B: Business Resilience

-Business Impact Analysis
-System and Operational Resilience
-Data Backup, Storage and Restoration
-Business Continuity Plan
-Disaster Recovery Plan

Exercise: Multiple Choices Questions from previous CISA sessions (or comparable exams)

Chapter 5: Protection of Information Assets

Part A: Information Asset Security and Control

-Information Asset Security Policies, Frameworks, Standard and Guideline
-Physical and Environmental Controls
-Identity and Access Management
-Network and Endpoint Security
-Data Loss Prevention
-Data Encryption
-Public Key Infrastructure
-Cloud and Virtualized Environment
-Mobile, Wireless and Internet-of-things

Part B: Security Event Management

-Security Awareness Training and Programs
-Information System Attack Methods and Techniques
-Security Testing Tools and Techniques
-Security Monitoring Logs, Tools and Techniques
-Security Incident Response Management
-Evidence Collection and Forensics

Exercices Multiple Choices Questions from previous CISA sessions (or comparable exams)

Preparation to the Exam

Blank Exam - Partial simulation of the examination carried out at the end of the training.

Registration to be made on the site www.isaca.org.

Presentation of the event: 3 hours of multiple choices questions with 150 questions to be chosen beforehand in French or in English.

CISM® 16th Edition (Certified Information Security Manager) (4 Days)

This 4-day course will prepare for the CISM® exam Certified Information Security Manager, covering the entire CBK (Common Body of Knowledge) common core of knowledge in security defined ISACA®, Information Systems Audit and Control Association. The CISM certification is recognized worldwide.

The training is aligned on the 16th Edition of the CBK updated in 2022 for the professional practice.

Content
Domain 1: Information Security Governance
Domain 2: Information Security Risk Management
Domain 3: Information Security Program
Domain 4: Incident Management
Preparation and Certification

Participants
Information System (IS) Directors, auditors, responsible for business continuity or security, or for which the control of IS is fundamental in achieving their goals.

Prerequisites
Basic knowledge in Information Systems. Understanding English is necessary because the documentation is in English (the training is in French or English).

Program
Domain 1: Information Security Governance

Part A: Enterprise Governance
-Importance of Information Security Governance
-Organizational culture
-Legal, regulatory and Contractual Requirements
-Organizational Structures, Roles and Responsibilities

Part B: Information Security Strategy
-Information Security Strategy Development
-Information Governance Frameworks and Standards
-Strategic Planning

-Questions from previous sessions (CISM or comparable examinations).

Domain 2: Information Risk Management

Part A: Information Risk Assessment

-Emerging Risk and Threat Landscape

-Vulnerability and Control Deficiency Analysis
-Risk Analysis, Evaluation and Assessment

Part B: Information Risk Response

-Risk Treatment/ Risk Response Options
-Risk and Control Ownership
-Risk Monitoring and Reporting

-Questions from previous sessions (CISM or comparable examinations).

Domain 3: Information Security Program

Part A: Information Security Program Development

-Information Security Program Overview
-Information Security Program Resources
-Information Asset Identification and Classification
-Industry Standards and Frameworks for Information Security
-Information Security Policies, Procedures and Guidelines
-Defining an Information Security Program Road Map
-Information Security Program Metrics

Part B: Information Security Program Management

-Information Security Control Design and Selection
-Information Security Control Implementation and Integration
-Information Security Control Testing and Evaluation
-Information Security Awareness and Training
-Integration of the Security Program with IT Operations
-Management of External Services and Relationships
-Information Security Program Communications and Reporting

-Questions from previous sessions (CISM or comparable examinations).

Domain 4: Incident Management

Part A: Incident Management Readiness

-Incident Management and Incident Response Overview
-Incident Management and Incident Response Plan
-Business Impact Analysis
-Business Continuity Plan
-Disaster Recovery Plan
-Incident Classification/Categorization
-Incident Management Training, Testing and Evaluation

Part B: Incident Management Operations

-Incident Management Tools and Technologies
-Incident Investigation and Evaluation
-Incident Containment Methods
-Incident Response Communications
-Incident Eradication and Recovery
-Post-Incident Review Practice

-Questions from previous sessions (CISM or comparable examinations).

Preparation and Certification

Partial simulation of the exam conducted at the end of training.
Subscribe to the www.isaca.org site.
Duration and conduct of the exam: 3 hours with 150 questions (review available only in English).

CRISC® 7th Edition (Certified in Risk and Information System Control) (4 Days)

This 4-Day training prepares the professionals who want to pass the ISACA's Certified in Risk and Information System Control CRISC® exam.

The program covers the four key areas covered in the exam: Governance, IT Risk Assessment, Risk Response and Reporting, Information Technology and Security

The program is aligned on the latest Edition (7th) of the CBK (Common Body of Knowledge) from the ISACA®

CRISC® certification is recognised around the world.

Educational objectives

Master the risk management approach according the CRISC®
Apply the best responses strategies to the risks weighing on the information system
Use best risk monitoring practices
Define information system controls
Use best practices to monitor and maintain these controls

Certification

-Candidates must apply for certification within 5 years of having passed the exam.

-A minimum of 3-year experience of cumulative work experience performing the tasks of a CRISC® professional across at least two of the four CRISC® domains is required for the certification.
Of these two domains, one must be in either domain 1 or 2.

-Adhere to the ISACA® code of Professional Ethics
-Agree to comply with the CRISC® continuing education policy.

Audience

- Job roles that can benefit from CRISC® training include, but are not limited to:
- CISO
- Information Security consultants
- Governance Consultants
- Cybersecurity Consultants
- IT professionals

- Risk professionals
- Control professionals
- Project managers
- Business analysts
- Compliance professionals
- Auditors
- CRISC®(R) exam candidates and anyone keen to improve their knowledge in the field of risk management and IS control.
- Participants who have completed an ISO 27005 or ISO 31000 course
- People working with an ERM (Enterprise Risk Management) framework

Prerequisite

There is no prerequisite to take the CRISC® exam; however, in order to apply for CRISC® certification you must meet the necessary experience requirements as determined by ISACA.
Participants should have a basic knowledge of the areas to be covered. The course consists of intense preparation for the certification exam.

English required for the exam.

Course Schedule

Day One
Introduction

Chapter 1: Governance

-Organizational Strategy, Goals and Objectives
-Organization structure, Roles and Responsibilities
-Organizational Structure
-Policies and Standards
-Business Process Review
-Organization assets
-Enterprise Risk Management and Risk Management Frameworks
-Three Lines of Defence
-Risk Profile
-Risk Appetite, Tolerance and Capacity
-Legal, Regulatory and Contractual Requirements
-Exercises - Multiple Choice questions in between chapters and at the end of each chapter

Day Two

Chapter 2: IT Risk Assessment

-Risk Events
-Threat Modelling and Threat landscape

-Vulnerability and Control Deficiency Analysis
-Risk Scenario Development
-Risk Assessment Concepts, Standards and Frameworks
-Risk Register
-Risk Analysis Methodologies
-Business Impact Analysis
-Inherent, Residual and Current risk
-Exercises - Multiple Choice questions in between chapters and at the end of each chapter

Day Three

Chapter 3: Risk Response and Reporting

-Risk and Control Ownership
-Risk Treatment/Risk Response Options
-Third-party Risk Management
-Issues, Finding and Exception Management
-Management of Emerging risk
-Control Types, Standards and Frameworks
-Control Design, Selection and Analysis
-Control Implementation
-Control Testing and Effectiveness Evaluation
-Risk Treatment Plans
-Data Collection, Aggregation, Analysis and Validation
-Risk and Control Monitoring Techniques
-Risk and Control Reporting Techniques
-Key Performances Indicators
-Key Risk Indicators
-Key Control Indicators
-Exercises - Multiple Choice questions in between chapters and at the end of each chapter

Day Four

Chapter 4: Information Technology and Security

-Enterprise Architecture
-IT Operations Management
-Project Management
-Enterprise Resiliency
-Data Life Cycle Management
-System Development Life Cycle
-Emerging Trends in Technology
-Information Security Concepts, Frameworks and Standards
-Information Security Awareness Training

-Data Privacy and Principles of Data Protection
-Exercises - Multiple Choice questions in between chapters and at the end of each chapter

Preparation to the exam

Multiple Choice Questions (MCQ) like the exam and correction performed together
Discussion and exchanges, hints, and tips to pass the exam.
Blank Exam.

Registration to be made on the site www.isaca.org,

The exam consists of 150 MCQ that cover the CRISC® job practice domains.

(ISC)2

CISSP (Certified Information Systems Security Professional) (5 Days)

This 5-day course will prepare for the CISSP exam Certified Information Systems Security Professional, covering the entire CBK (Common Body of Knowledge) as defined by (ISC)2.

The Certified Information Systems Security Professional (CISSP) is the most globally recognized certification in the information security market. CISSP validated an information security professional's deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization

Learning Objectives

The broad spectrum of topics included in the CISSP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following 8 domains:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

Who should attend

- Security (Consultant, Manager, Auditor, Architect, Analyst, System Engineer)
- IT Director/Manager
- CISO
- Director of Security
- Network Architect

Prerequisites
Basic knowledge of the Information System is recommended.
Strong English is necessary because the documentation is in English

Description

This training provides a comprehensive review of information security concepts and industry best practices, covering the 8 domains of CISSP CBK (Common Body of

Knowledge).
Several types of activities are used throughout the course to reinforce topics and increase knowledge retention. These activities include open ended questions from the instructor to the students, matching and poll questions, group activities, open/closed questions, and group discussions. the interactive learning technique is based on sound adult learning theories.
This training course will help candidates review and refresh their information security knowledge and help identify areas they need to study for the CISSP exam and features

Course Agenda

Domain 1: Security and Risk Management

- Understand and apply concepts of confidentiality, integrity and availability
- Evaluate and apply security governance principles
- Determine compliance requirements
- Understand legal and regulatory issues that pertain to information security in a global context
- Understand, adhere to, and promote professional ethic
- Develop, document, and implement security policy, standards, procedures, and guidelines
- Identify, analyze, and prioritize Business Continuity (BC) requirements
- Contribute to and enforce personnel security policies and procedures
- Understand and apply risk management concepts
- Understand and apply threat modeling concepts and methodologies
- Apply risk-based management concepts to the supply chain
- Establish and maintain a security awareness, education, and training program

Domain 2: Asset Security

- Identify and classify information and assets
- Determine and maintain information and asset ownership
- Protect privacy
- Ensure appropriate asset retention
- Determine data security controls
- Establish information and asset handling requirements

Domain 3: Security Engineering

- Implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models
- Select controls based upon systems security requirements
- Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module, encryption/Decryption)
- Assess and mitigate the vulnerabilities of security architectures, designs and solution elements
- Assess and mitigate vulnerabilities in Web-based systems

- Assess and mitigate vulnerabilities in mobile systems
- Assess and mitigate vulnerabilities in embedded devices
- Apply cryptography
- Apply security principles to site and facility design
- Implement site and facility security controls

Domain 4: Communications and Network Security

- Implement secure design principle in network architectures
- Secure network components
- Implement secure communication channels according to design

Domain 5: Identity and Access Management

- Control physical and logical access to assets
- Manage identification and authentication of people, devices, and services
- Integrate identity as a third-party service
- Implement and manage authorization mechanisms
- Manage the identity and access provisioning lifecycle

Domain 6: Security Assessment and Testing

- Design and validate assessment, test, and audit strategies
- Conduct security control testing
- Collect security process data (e.g., technical and administrative)
- Analyze test output and generate report
- Conduct or facilitate security audits

Domain 7: Security Operations

- Understand and support investigations
- Understand requirements for investigation types
- Conduct logging and monitoring activities
- Securely provisioning resources
- Understand and apply foundational security operations concepts
- Apply resources protection techniques
- Conduct incident management
- Operate and maintain detective and preventive measures
- Implement and support patch and vulnerability management
- Understand and participate in change management processes
- Implement recovery strategies
- Implement Disaster Recovery (DR) processes
- Test Disaster Recovery Plans (DRP)
- Participate in Business Continuity (BC) planning and exercises
- Implement and manage physical security
- Address personnel safety and security concerns

Domain 8: Software Development Security

- Understand and integrate security in the Software Development Life Cycle (SDLC)
- Identify and apply security controls in development environments
- Assess the effectiveness of software security
- Assess security impact of acquired software
- Define and apply secure coding guidelines and standards

Preparation to the Exam

The online CISSP exam (CAT: computerized adaptive testing) is available for all the exams in English. In the other languages, the exam is linearly managed.

You will have more information on the online exam on the link below:
https://www.isc2.org/certifications/CISSP/CISSP-CAT

Duration of the exam: 3 hours
Number of questions: 100 – 150
Types of questions: Multiple Choice and Innovative Advanced questions
Pass Mark: 700 out of1000 points
Available Language: English
Exam Center: PPC and PVTC, Pearson View Authorized Testing Centers (ISC)2

The linear CISSP exam:

Duration of the exam: 6 hours
Number of questions: 250
Types of questions: Multiple Choice and Innovative Advanced questions
Pass Mark: 700 out of 1000 points
Available Language: French, German, Brazilian Portuguese, Spanish, Japanese, Simplified Chinese, Korean
Exam Center: PPC and PVTC, Pearson View Authorized Testing Centers (ISC)2

CCSP (Certified Cloud Security Professional) (5 Days)

This 5-day course will prepare you for the CCSP Certified Cloud Security Professional Exam, which covers the entire (ISC)2 CCSP CBK - Common Body of Knowledge.

(ISC)2 developed the CCSP credential to ensure that cloud security professionals have the required knowledge, skills and abilities in cloud security design, implementation, architecture, operations, controls, and compliance with regulated frameworks.

Learning Objectives

The topics included in the CCSP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of cloud security. Successful candidates are competent in the following 6 domains:

- Cloud concepts, Architecture and Design
- Cloud Data Security
- Cloud Platform & Infrastructure Security
- Cloud Application Security
- Cloud Security Operations
- Legal, Risk and Compliance

Who should attend?

Responsible for the security of the information systems.
Responsible for the management system according to ISO 27001.
CIO, CISO
Director of Security
Information Security Officer
IT Director/Manager
Business security manager
Enterprise Architect, Network Architect, Security Administrator, Security Analyst, Security Architect.
Security Auditor, Security Consultant, Security Engineer, Security Manager, Security Systems Engineer, Systems Architect, Systems Engineer.

Prerequisites

Good knowledge of English since it is advisable to take the certification exam in English.

At least five years of professional experience in information security and a minimum of one year in one of the six CCSP domains mentioned above.

You can meet one year of professional experience in one of six CCSP domains if you have CSA CCSK certification.

You can meet all the prerequisites of professional experience if you have the CISSP certification.

A candidate who does not have the required experience to become a CCSP can become an ISC2 Associate by passing the CCSP exam. The (ISC)2 Associate will then have six years to acquire the five years of required experience.

Course Agenda

Domain 1: Cloud concept, Architecture and Design

- Understand cloud Computing Concepts
- Describe Cloud Reference Architecture
- Understand Security Concepts Relevant to Cloud Computing
- Understand the Design Principles of Secure Cloud Computing
- Evaluate Cloud Service Providers

Domain 2: Cloud Data Security

- Articulate Legal requirements and Unique Risks within the Cloud Environment
- Support Digital Forensics
- Understand Privacy Issues
- Understand Audit Process, Methodologies, and Required Adaptations for a Cloud Environment
- Understand Implications of Cloud to Enterprise Risk Management
- Understand Outsourcing and Cloud Contract Design

Domain 3: Cloud Platforms and Infrastructure Security

- Cloud Data Security Concepts
- Design and Implement Cloud Data Storage Architectures
- Design and Apply Data Security Technologies and Strategies
- Cryptography
- Understand and Implement Data Discovery and Classification Technologies
- Design and Implement Information Rights Management (IRM)
- Plan and Implement Data Retention, Deletion, and Archival Policies

- Design and Implement Auditability, Traceability, and Accountability of Data Events

Domain 4: Cloud Application Security

- Comprehend Cloud Infrastructure Components
- Secure Cloud Data Center Design
- Analyze Risks Associated with Cloud Infrastructure
- Design and Plan Security controls for Physical and Logical Cloud Infrastructure
- Design Appropriate Identity and Access Management (IAM) solutions
- Plan Disaster Recovery (DR) and Business Continuity (BC)

Domain 5: Cloud Security Operations

- Discuss Training and Awareness for Application Security
- Describe the Secure Software Development Lifecycle (SDLC) process
- Apply the Secure Software Development Lifecycle (SDLC)
- Apply Cloud Software Assurance and Validation
- Use Verified Source Software
- Explain the Specifics of a Cloud Application Architecture

Domain 6: Legal, Risk and Compliance

- Operate and Manage Physical and Logical Infrastructure for Cloud Environment
- Implement Operational Controls and Standards
- Manage Communication with Relevant Parties
- Manage Security Operations

Preparation to the Exam

Duration of the exam: 3 hours
Number of questions: 125
Types of questions: Multiple Choice
Pass Mark: 700 out of 1000 points
Available Language: English
Exam Center: Pearson View Testing Center

PCI-DSS

The PCI-DSS program

The bank card data, which are the card number, the expiry date and the three digits on the back of the card, have become sensitive because they allow payment to be made on the internet without the physical presence of the card. Fraudsters seek to capture these numbers by attacking the information systems of the players who store this data. The PCI-DSS program aims to improve the physical and logical security of information systems by requiring players to comply with good security practices.

The PCI-DSS standard (6 control objectives and 12 requirements)

The PCI DSS standard lists a set of control points relating to information systems that capture, transport, store and process bank card data. The control points relate to computer techniques but also to procedures and organizational controls on these systems.

PCI-DSS compliance

PCI-DSS compliance helps ensure that checkpoints are in place and effective for protecting credit card data. This compliance is required for banks and merchants (depending on their size) by an audit carried out by an approved auditor or by a self-assessment questionnaire to be completed and sent to their bank.
Compliance shall be checked annually.

Training objectives

• Understand the basic notions of electronic banking (Electronic payment system)
• Master the challenges of security in electronic banking
• Understand the Payment Card Industry Data Security Standard (PCI-DSS) and its compliance process

Impact objectives

At the end of this course, participants will be able to participate in a PCI-DSS project, they will have had an overview of:

-Electronic banking, its actor roles, risks
-The PCI-DSS standard ecosystem,
-Security issues in an electronic payment system
-The six domains, and the requirements of the standard
-Understand the security measures to put in place (do's and don'ts)
-Trace a certification path

Target audience

• Managers or employees involved in electronic payment security or compliance with the PCI DSS standard.
• Any person involved in an electronic payment system (bank, service provider, etc.). Or wishing to conform to the standard.
• CISO (or member of a CISO team – security engineer, security architect)
• Consultants wanting to work on the PCI DSS standard, security project manager (MOE, MOA)

Course content

• Context of compliance
• The benefits of compliance
• Roles and players in electronic banking
• The payment circuit and electronic banking process
• Fraud and payment risks
• What is PCI-SSC
• What is PCI-DSS
• History and objectives of the PCI committee
• Security
• What is confidential data and what is sensitive data?
• Applicability of the standard
• The perimeter
• Exercise
• Course of the six domains and the twelve requirements
• Overview of the Appendices
• The PCI-DSS project
• Action plans the path to certification
• Quiz

Prerequisites

Good knowledge of ISMS (Information Security Management Systems)

PCI-DSS v4 (2 days)

Day 1

- Context of compliance
- The benefits of compliance
- Roles and players in electronic banking
- The payment circuit and electronic banking process
- Fraud and payment risks
- What is PCI-SSC
- View of the other standards published by the council (PCI PTS, PCI P2PE)
- What is PCI-DSS
- History and objectives of the PCI committee
- Security (Confidentiality, Integrity and Availability)
- PCI DSS and other standards (ISO 27001, ISO 27002)
- The different types of merchants and questionnaires (SAQ)
- Certificates (AOC and ROC)
- Credit card data
- What is confidential data and what is sensitive data?
- Relationship between PCI DSS and PCI SSC
- Applicability of the standard
- The scope (organizational, technical, etc.)
- Exercise
- Overview of the six domains and the twelve requirements
    - Create and Maintain Secure Network and Systems
        1. Install and Maintain Network Security Security Measures.
        2. Apply Secure Configurations to All System Components
    - Protect Card Data
        3. Protect card data while in storage
        4. Protect Cardholder Data With Strong Cryptography When Transmitted Over Open Public Networks.
    - Maintain a Vulnerability Management Program
        5. Protect All Systems and Networks Against Malicious Software.
        6. Develop and Maintain Secure Systems and Software.

Day 2

- Implement Robust Access Control Measures
    7. Limit Access to System Components and Cardholder Data Based on Business Needs.
    8. Identify Users and Authenticate Access to System Components.
    9. Limit Physical Access to Cardholder Data.
- Regularly Monitor and Test Networks
    10. Log and Monitor All Access to System Components and Cardholder Data.
    11. Regularly Test System and Network Security.

- Maintain an Information Security Policy
    12. Strengthen Information Security through Organizational Policies and Programs.

- Overview of the Appendices
- The PCI-DSS project (Nature, challenges, governance, roles and responsibilities, success factors, plan, scope, technologies and required documentation)
- Actions 'to avoid'
- Action plans 'the path to certification' and practical advice
- Feedback on new features of PCI DSS v4 and comparison with v3.2.1
- Presentation of standard documents (gap analysis, Information Security Policy, Incident Response Plan, Flowchart, etc.)
- Quiz

PCI-DSS v4 (4 days)

Day 1

- Context of compliance
- The benefits of compliance
- Roles and players in electronic banking
- The payment circuit and electronic banking process
- Fraud and payment risks
- What is PCI-SSC
- View of the other standards published by the council (PCI PTS, PCI P2PE)
- What is PCI-DSS
- History and objectives of the PCI committee
- Security (Confidentiality, Integrity and Availability)
- PCI DSS and other standards (ISO 27001, ISO27002)
- The different types of merchants and questionnaires (SAQ)
- Certificates (AOC and ROC)
- Credit card data
- What is confidential data and what is sensitive data?
- Relationship between PCI DSS and PCI SSC
- Applicability of the standard
- The scope (organizational, technical, etc.)
- Exercise
- Implementation approaches
- Detailed course of the six domains and the twelve requirements
    - Create and Maintain Secure Network and Systems
        1. Install and Maintain Network Security Security Measures.
        2. Apply Secure Configurations to All System Components
- Quiz

Day 2-3: requirements walkthrough

- Protect Card Data
    3. Protect card data while in storage
    4. Protect Cardholder Data With Strong Cryptography When Transmitted Over Open Public Networks.
- Maintain a Vulnerability Management Program
    5. Protect All Systems and Networks Against Malicious Software.
    6. Develop and Maintain Secure Systems and Software.
- Implement Robust Access Control Measures
    7. Limit Access to System Components and Cardholder Data Based on Business Needs.
    8. Identify Users and Authenticate Access to System Components.
    9. Limit Physical Access to Cardholder Data.
- Regularly Monitor and Test Networks
    10. Log and Monitor All Access to System Components and Cardholder Data.
    11. Regularly Test System and Network Security.

• Quiz

Day 4 : requirements walkthrough

- Maintain an Information Security Policy
  12. Strengthen Information Security through Organizational Policies and Programs.

• Overview of the Appendices
• The PCI-DSS project (Nature, challenges, governance, roles and responsibilities, success factors, plan, scope, technologies and required documentation)
• Actions 'to avoid'
• Action plans 'the path to certification' and practical advice
• Feedback on new features of PCI DSS v4 and comparison with v3.2.1
• Presentation of standard documents (gap analysis, Information Security Policy, Incident Response Plan, Flowchart, etc.)
• Quiz