



Training Course Catalog 2026

PECB

Dr. Eric Lachapelle

Chairman at PECB

At PECB, our goal is to prepare professionals for the challenges of tomorrow. Through high-quality training and certifications, we equip individuals with the tools they need to protect data and privacy, and build trust in a digital-first world. We focus on practical knowledge and skills that apply directly to the workplace, ensuring professionals can not only achieve their goals but also go beyond them. Innovation and continuous growth are at the heart of everything we do, and that's how we help people succeed in an environment that is constantly evolving.



Dr. Faton Aliu

President at PECB

Excellence, to us, is where knowledge, innovation, and digital trust come together. These are more than guiding principles; they're the backbone of progress in a world that demands reliability and resilience. As security and trust become essential for every organization, PECB is here to equip professionals and teams with the skills and confidence they need to stay ahead.

Our purpose is simple: to help people grow. We want every learner, every partner, and every organization we support to feel empowered, armed with the right tools, clear insights, and a mindset built for the future. With PECB, training isn't just about acquiring credentials; it's about real transformation and meaningful steps toward stronger careers and stronger organizations.



This training catalog may be reproduced or transmitted to inform current or potential PECB Partners and Trainers, or interested trainees, of the current PECB training and certification opportunities, on the condition that the reproduction or transmission includes the following notice: "© Professional Evaluation and Certification Board 2026. All rights reserved." Reproductions or transmissions for any other purpose require prior written permission.

TABLE OF CONTENT

PECB Training Catalog 2026.....	8
PECB's Diverse Training Portfolio	9
Your PECB Certification is Your Credibility!.....	11
Registration, Enrollment, and Certification Process Pathway.....	12
Digital Trust: Securing Your Future	14
PECB Training Course.....	15
Delivery Formats.....	15
INFORMATION SECURITY & CYBERSECURITY	17
ISO/IEC 27001 Information Security Management Systems.....	18
ISO/IEC 27002 Information Security Controls	21
PECB Chief Information Security Officer (CISO).....	23
EBIOS	25
ISO/IEC 27005 Information Security Risk Management	27
ISO/IEC 27035 Information Security Incident Management	30
ISO/IEC 27034 Application Security	32
ISO/IEC 27400 IoT Security and Privacy	34
Why Choose a Career in Information Security?	36
Cybersecurity Management.....	38
Cloud Security	40
Penetration Testing.....	42
SCADA Security.....	44
ISO/IEC 27033 Networking Security.....	46
Cybersecurity Maturity Model Certification (CMMC)	49
NIS 2 DIRECTIVE.....	51
SOC 2.....	53
NIST Cybersecurity	55
ISA/IEC 62443	57
Canadian Program for Cybersecurity Certification	59
Why Choose a Career in Cybersecurity Management?.....	61
Certified Lead Ethical Hacker (CLEH).....	63
Certified Cyber Threat Analyst (CCTA).....	65
Certified Digital Forensics Examiner (CDFE).....	68
Certified Linux Foundations (CLF)	70
Certified Advanced Penetration Tester (CAPT)	72
Certified Artificial Intelligence Auditor (CAIA).....	74

Certified Cloud Security Analyst (CCSA).....	76
Certified SOC Analyst (CSOCA).....	78
Certified Elastic Stack Analyst (CESA).....	80
Certified Web Application Security Analyst (CWASA).....	82
Certified Splunk Analyst (CSA).....	84
Certified Cloud Incident Responder (CCIR).....	86
Why Choose a Career in Technical Cybersecurity?.....	88
CONTINUITY, RESILIENCE, AND RECOVERY	90
ISO 22301 Business Continuity Management System.....	91
Disaster Recovery.....	93
Digital Operational Resilience Act (DORA).....	96
Crisis Management.....	98
Operational Resilience Management.....	100
Why Choose a Career in Continuity, Resilience, and Recovery?.....	103
PRIVACY AND DATA PROTECTION.....	104
ISO/IEC 27701 Privacy Information Management System.....	105
GDPR – Certified Data Protection Officer (CDPO).....	108
Certified US Data Privacy.....	110
Why Choose a Career in Privacy and Data Protection?.....	112
AI AND DIGITAL TRANSFORMATION.....	114
ISO/IEC 42001 Artificial Intelligence Management System.....	115
Certified Artificial Intelligence Professional (CAIP).....	117
AI Risk Management.....	119
Certified AI Manager (CAIM).....	122
Why Choose a Career in Artificial Intelligence (AI)?.....	124
Certified Digital Transformation Officer (CDTO).....	125
Why Choose a Career in Digital Transformation?.....	127
GOVERNANCE, RISK, AND COMPLIANCE	129
ISO 31000 Risk Management.....	130
ISO/IEC 38500 IT Governance.....	132
ISO 37000 Corporate Governance.....	134

ISO 37001 Anti-Bribery Management System	136
ISO 37301 Compliance Management System.....	138
Management Systems Internal Auditor.....	141
Certified Management Systems Consultant (CMSC).....	144
ISO/TS 31050 Emerging Risks	146
Why Choose a Career in GRC?	148
QUALITY, HEALTH, SAFETY AND SUSTAINABILITY	150
ISO 9001 Quality Management System.....	151
ISO 21502 Project Management	153
ISO 28000 Supply Chain Security Management System.....	156
ISO 13485 Medical Devices Quality Management System.....	158
ISO/IEC 17025 Laboratory Management System.....	160
ISO/IEC 20000 IT Service Management System	163
Six Sigma Belts	166
ISO 21001 Educational Organizations Management System	168
ISO 55001 Asset Management System	170
Why Choose a Career in Quality & Management?	172
ISO 45001 Occupational Health and Safety Management System.....	174
ISO 22000 Food Safety Management System	176
ISO 18788 Security Operations Management System.....	178
Why Choose a Career in Health and Safety?	180
ISO 50001 Energy Management System.....	182
ISO 14001 Environmental Management System.....	184
ISO 26000 Social Responsibility Management System.....	187
ISO 20400 Guidelines for Sustainable Procurement.....	190
ISO 56001 Innovation Management System	192
Why Choose a Career in Sustainability?	194
<i>myPECB – Leading in a New Era of Personalized Digital Experiences</i>	<i>196</i>
A Redesigned Website for a Modern User Experience	197
PECB Skills	198
PECB Connect.....	199
Examination and Certification	201
PECB Certification Rules and Policies	203
AMF Discount	205
eLearning	206
Discover What’s Inside the PECB Store	207

PECB Training Catalog 2026

A training catalog is a structured collection of learning programs that helps professionals in selecting the right courses for their career goals.

Why it's Important

A training catalog is essential because it:

- Provides **clarity** by organizing diverse learning options in one place.
- Ensures **relevance** with up-to-date knowledge and recognized certifications.
- Builds **digital trust** by equipping professionals with skills that drive security, resilience, and sustainable growth.



About PECB

PECB is a global certification body and trusted partner in professional training.

We empower individuals and organizations to enhance expertise, strengthen competencies, and demonstrate credibility in digital security and beyond.

Our Principles



Agility

Adapting quickly fuels innovation.



Inclusivity

Diversity promotes value and connection.



Sustainability

Responsible practices ensure long-term success.

PECB's Diverse Training Portfolio

PECB offers a broad range of training courses across multiple portfolios. These training courses are designed to help professionals gain skills and knowledge in specific fields, providing them with a thorough understanding of relevant standards and frameworks. PECB's methods of education equip participants with the ability to effectively implement and manage these practices within their organizations, enhancing their expertise in their respective domains.

Take a glimpse at the training courses featured under each designated portfolio:

Cybersecurity

Training courses in this portfolio focus on safeguarding information systems, identifying and mitigating cyber threats, and building robust security strategies that ensure data protection and integrity.

Continuity, Resilience, and Recovery

Courses under this portfolio prepare professionals to develop and implement strategies that ensure business continuity, organizational resilience, and effective recovery in the face of disruptive events.

Privacy and Data Protection

This portfolio covers critical data protection laws and practices, including GDPR compliance and strategies for protecting personal and sensitive information in an increasingly data-driven world.



AI and Digital Transformation

This portfolio focuses on the intersection of artificial intelligence and digital innovation. These courses help organizations harness AI technologies and navigate the challenges and opportunities posed by digital transformation.

Governance, Risk, and Compliance

This portfolio emphasizes governance frameworks, risk management, and compliance strategies, equipping participants to align organizational objectives with regulatory and business requirements.

Quality, Health, Safety, and Sustainability

This portfolio focuses on quality management systems, occupational health and safety, and sustainable practices for long-term organizational success and environmental stewardship.

Professional Development Pathways: Training Course Levels And Durations

MANAGEMENT SYSTEM TRAINING COURSES	WHO SHOULD ATTEND	
FOUNDATION	Individuals who wish to learn the basics of implementing a management system and its processes	2 DAYS
LEAD IMPLEMENTER	Individuals responsible for the implementation and management of a management system within their organization	5 DAYS
LEAD AUDITOR	Individuals responsible for auditing and monitoring management systems	5 DAYS
MANAGER TRAINING COURSES		
FOUNDATION	Individuals who wish to study the fundamentals of the processes and procedures in the related field or standard	2 DAYS
MANAGER / OFFICER	Managers in the relevant field who wish to develop the skills and knowledge to carry out and implement processes, approaches, and techniques for different programs, plans, strategies, etc	3 DAYS
LEAD MANAGER / OFFICER	Managers in the relevant field who wish to assess, manage, or maintain plans, assessments, frameworks, programs, or the like, and develop their management expertise	5 DAYS
NON-ISO TRAINING COURSES		
FOUNDATION	Individuals who wish to study the foundations of the associated field and its related processes	2 DAYS
MANAGER / OFFICER	Managers in the relevant field who wish to gain knowledge on the fundamental principles and concepts of a management program	3 DAYS
LEAD MANAGER / OFFICER / PROFESSIONAL AND ANALYST	Managers in the relevant field who wish to develop their skills and knowledge in the associated field and improve their management expertise	5 DAYS
TECHNICAL CYBERSECURITY COURSES		
OFFENSIVE SECURITY	Professionals wishing to learn more about the tactics and techniques malicious hackers use and improve their capacity to protect their systems	5 DAYS
DEFENSIVE SECURITY	Individuals wishing to significantly improve their defensive capabilities and learn best practices for hardening systems and configuring security effectively	5 DAYS
FORENSICS	Professionals who wish to learn a wide range of skills and knowledge crucial for digital forensics	5 DAYS

Your PECB Certification is Your Credibility!

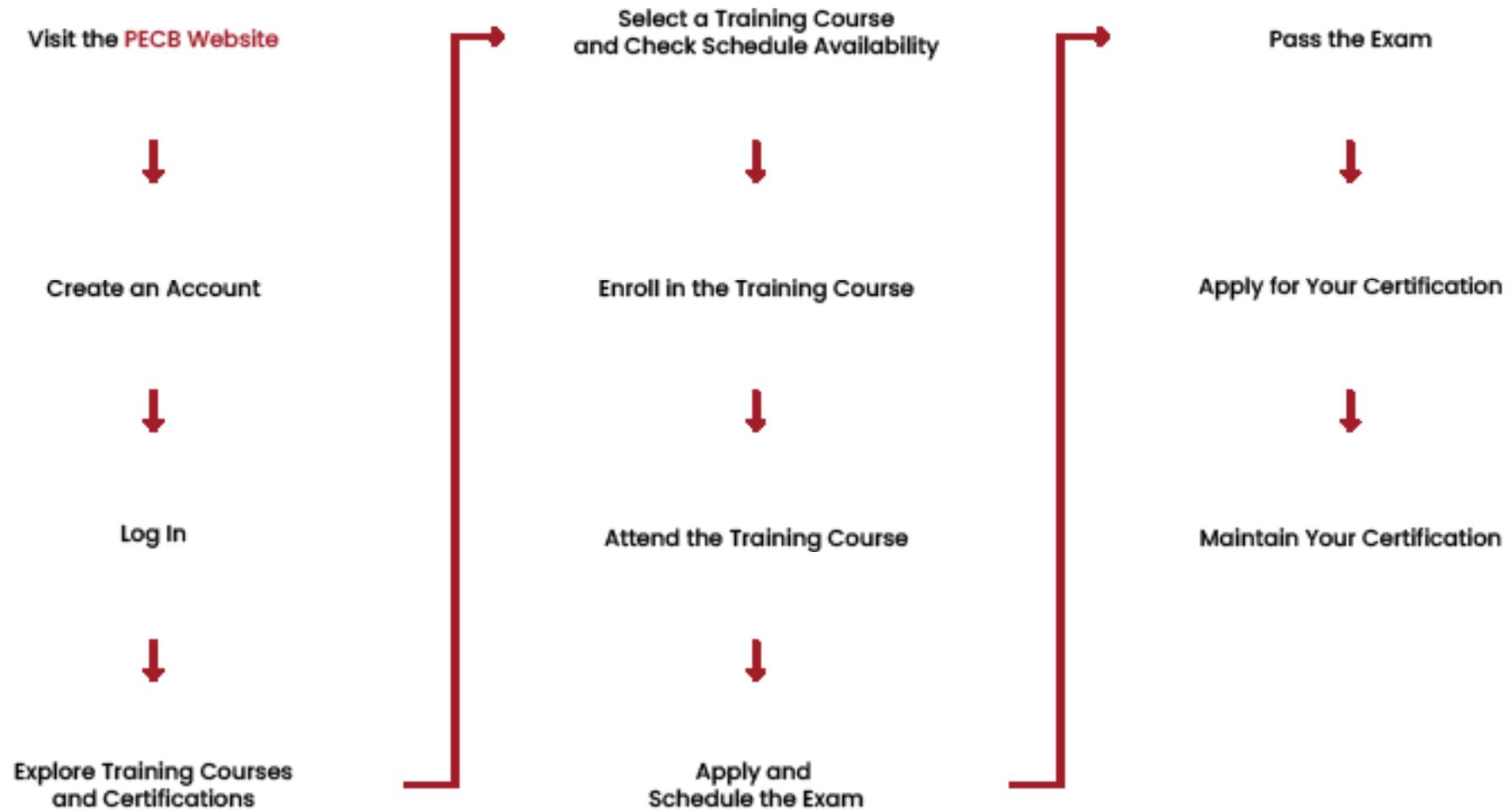
Professional certification serves as official proof of education, competence, and professional recognition. But more than that, certifications provided by PECB show that you are a driven individual who is committed to your professional growth. More importantly, it shows that you have gained validated skills and knowledge.

No matter if you are just beginning your journey or already have a successful career in the field of ISO standards and other regulatory frameworks, PECB certification heightens your career path and ensures greater success in your chosen profession.

Our certifications help you execute your tasks and serve as reliable evidence that you have met the minimum requirements for professional and ethical behavior while also aiding you to achieve and manage all aspects of your work more effectively.

An investment that is certainly a worthwhile investment of your time and resources — because a continuous thirst for knowledge translates into a thriving business and professional development.





Certification Criteria: Designation, Experience, and Project Requirements

EXAM	DESIGNATION	PROFESSIONAL EXPERIENCE	AUDIT EXPERIENCE	PROJECT EXPERIENCE
FOUNDATION	Foundation	-	-	-
	Provisional Manager	-	-	-
LEAD MANAGER	Manager	2 years (1 in the specialized field)	-	200 hours
	Lead Manager	5 years (2 in the specialized field)	-	300 hours
	Senior Lead Manager	10 years (7 in the specialized field)	-	1000 hours
	Provisional Auditor	-	-	-
LEAD AUDITOR	Auditor	2 years (1 in the specialized field)	200 hours	-
	Lead Auditor	5 years (2 in the specialized field)	300 hours	-
	Senior Lead Auditor	10 years (7 in the specialized field)	1000 hours	-
	Provisional Implementer	-	-	-
LEAD IMPLEMENTER	Implementer	2 years (1 in the specialized field)	-	200 hours
	Lead Implementer	5 years (2 in the specialized field)	-	300 hours
	Senior Lead Implementer	10 years (7 in the specialized field)	-	1000 hours
	Master	20 years (10 in a leadership role in the specialized field)	10,000 hours combination of auditing and project activities	

Note: For the ANAB Accredited Foundation Certificate Programs, attending the corresponding training course is a mandatory requirement.

Digital Trust: Securing Your Future

Customers want to know their data is safe, and businesses need to prove they can protect it. Digital Trust is the key to building strong relationships and staying competitive.

What is Digital Trust?

Digital Trust is the confidence that people and organizations have in your digital environment. It means your systems, data, and interactions are secure, reliable, and free from threats. Digital Transformation has enabled organizations across various industries to achieve sustained growth and improved productivity. An effective Digital Transformation strategy helps avoid problems during transition and after implementation. A successful Digital Transformation requires appropriate technology and competent people.

Why Does Digital Trust Matter?

When customers trust you, they stay loyal. Digital Trust builds confidence, boosts your brand, and keeps you ahead of competitors. It is not just about security—it is about growth and success.

PECB: Your Partner in Digital Trust

At PECB, we provide top-tier certification programs that help you build, maintain, and showcase Digital Trust. Our internationally recognized training courses cover everything from cybersecurity and data protection to ethical hacking and digital transformation.

Why Choose PECB?

With PECB, you gain the skills and certifications needed to lead in a digital-first world. We empower professionals to secure their organizations and build trust with customers.



PECB Training Course Delivery Formats

PECB's diverse learning delivery methods cater to a wide range of learners, ensuring accessibility, flexibility, and quality in the training and certification process.



Classroom

Engage in direct, interactive sessions with PECB Certified Trainers in a structured, face-to-face learning environment, ideal for hands-on knowledge application.



Virtual Classroom

Experience engaging, interactive training led by PECB Certified Trainers in a virtual classroom, accessible to all, including those with time constraints or travel limitations.



eLearning

Flexible, location-independent courses via pre-recorded videos. Offers quizzes and additional reading.



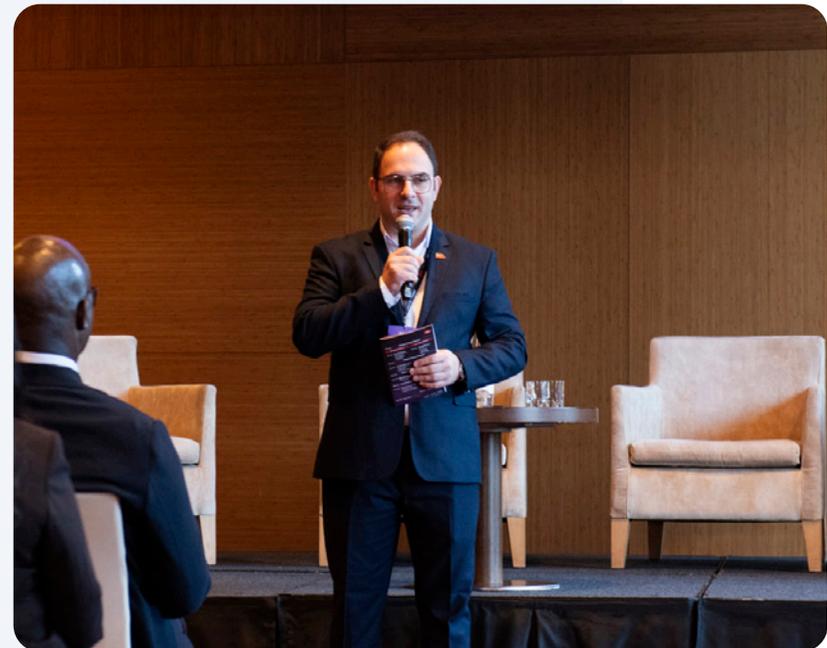
Self-Study

Self-paced learning with access to course materials. Best for those with prior knowledge and no need for guided teaching.

Tim Rama

Chief Executive Officer at PECB

Education is at the core of what we do at PECB. We aim to nurture talent, inspire excellence, and place Digital Trust at the center of every learning experience. As organizations and individuals increasingly rely on digital systems, we provide the skills necessary to protect information and create secure environments. Our work extends beyond certifications, encouraging continuous learning and personal growth. We believe that knowledge creates opportunities, and we want professionals to face the future with confidence, embracing change and building success on a foundation of trust.



INFORMATION SECURITY & CYBERSECURITY



Why Information Security?

Information security is important because it safeguards the core principles of data confidentiality, integrity, and availability. Without these protections, sensitive information is at risk, which can lead to consequences for individuals, organizations, and society as a whole.



Why Cybersecurity Management?

Cybersecurity management is needed because it offers the strategic guidance and control required to protect an organization's digital resources and ensure smooth operations.



Why Technical Cybersecurity?

Technical cybersecurity is critical because it includes the tools, technologies, and methods that actively protect systems and data from cyber threats.



ISO/IEC 27001 Information Security Management Systems

Overview of ISO/IEC 27001 and Its Certification Process

ISO/IEC 27001 provides the requirements for organizations aiming to establish, implement, maintain, and continually enhance an information security management system. The ISO/IEC 27001 certification represents a global benchmark in Information Security Management Systems (ISMS). This certification guides organizations in implementing a structured method for safeguarding sensitive information. It involves a comprehensive framework for pinpointing, evaluating, and addressing information security risks, crucial for maintaining the confidentiality, integrity, and availability of vital organizational data.

According to Gartner, Inc., worldwide end-user spending on information security is projected to reach U.S. \$213 billion in 2025, and further grow to approximately U.S. \$240 billion in 2026.



Benefits of ISO/IEC 27001 Certification



Improved
information
security



Better risk
management



Improved
organizational
competence



Access to a global
network of experts in
security standards

[Learn more](#)



Training Course and Learning Objectives	
ISO/IEC 27001 Foundation Gain knowledge on the fundamental components necessary to implement and manage an ISMS based on ISO/IEC 27001	2 DAYS
ISO/IEC 27001 Lead Implementer Develop the skills to support an organization in implementing and maintaining an ISMS based on ISO/IEC 27001	5 DAYS
ISO/IEC 27001 Lead Auditor Acquire the knowledge and skills to perform an ISMS audit by applying widely recognized audit principles, procedures, and techniques	5 DAYS
ISO/IEC 27001 Transition Understand the differences between ISO/IEC 27001:2013 and ISO/IEC 27001:2022 and help an organization plan and implement the necessary changes to an existing ISMS in accordance with ISO/IEC 27001:2022	2 DAYS



Since 2017, EduGroupe and PECB have combined their expertise to support organizations and professionals in acquiring high-value certification-based skills. Over the years, this partnership has established itself as a model of strong and forward-thinking cooperation, serving security, performance, and responsibility. The partnership between EduGroupe and PECB is rooted in a shared conviction: that skills are the driving force behind sustainable and secure business transformation. In an environment where regulatory compliance, data protection, and social responsibility have become essential, both entities are committed to promoting a culture of compliance and resilience.

Jérôme Belzacki
President of EduGroupe

ISO/IEC 27002 Information Security Controls

Overview of ISO/IEC 27002 and Its Certification Process

ISO/IEC 27002 is a globally recognized standard offering a robust guide for enhancing information security management in organizations. Adhering to ISO/IEC 27002 demonstrates expertise in information security and equips professionals to navigate evolving cyber threats with confidence. ISO/IEC 27002 plays a pivotal role in helping organizations protect their sensitive data, complying with legal and regulatory obligations, and cultivating a strong security culture.

According to Business Research Insights, the global "Information Security Management System (ISMS)" market was valued at about U.S. \$69.65 billion in 2024, projected to reach U.S. \$107.13 billion by 2033 (CAGR ~4.9%).



Benefits of ISO/IEC 27002 Certification



**Address Evolving
Cyber Threats**



**Strengthen Data
Assurance**



**Ensure Regulatory
Compliance**



**Protect Sensitive
Data**

[Learn more](#)



Training Course and Learning Objectives



ISO/IEC 27002 Foundation

Gain knowledge on information security management practices including the selection, implementation, and management of controls based on ISO/IEC 27002

2 DAYS

ISO/IEC 27002 Manager

Develop the skills necessary to implement, manage, and communicate information security controls based on ISO/IEC 27002

3 DAYS

ISO/IEC 27002 Lead Manager

Acquire the knowledge and skills to perform an ISMS audit by applying widely recognized audit principles, procedures, and techniques

5 DAYS

PECB Chief Information Security Officer (CISO)

Overview of PECB CISO and Its Certification Process

PECB CISO (Chief Information Security Officer) is a specialized accreditation for professionals aiming to assume senior-level executive positions in information security management. Embarking on the journey to obtain a CISO certification involves an in-depth exploration of the strategic and operational aspects of information security leadership. This certification process covers a comprehensive curriculum including cybersecurity policies, risk management, incident response, compliance, and stakeholder communication.



Benefits of CISO Certification



Career
Advancement



Enhanced Credibility
and Marketability



Comprehensive
Knowledge



Global
Recognition

[Learn more](#)



Training Course and Learning Objectives



PECB CISO

Gain necessary knowledge, skills, and strategies to lead information security programs effectively

5 DAYS

EBIOS

Overview of EBIOS and Its Certification Process

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) stands as a prominent risk assessment methodology predominantly utilized in France and other French-speaking regions. EBIOS certification is a recognition of an individual's expertise in the EBIOS risk assessment methodology. This certification demonstrates proficiency in evaluating and managing information security risks effectively through the structured approach provided by EBIOS.



Benefits of EBIOS Certification



Enhanced Career in
Information Security



Contributing to
Robust Security



Recognition of
Expertise



Commitment to High
Security Standards

[Learn more](#)



Training Course and Learning Objectives



EBIOS Risk Manager

Understand risk assessment elements and concepts related to information security and develop the skills to successfully carry out such assessments by using the EBIOS method

3 DAYS

ISO/IEC 27005 Information Security Risk Management

Overview of ISO/IEC 27005 and Its Certification Process

ISO/IEC 27005 sets the benchmark for guidelines in information security risk management. This standard facilitates a methodical approach for organizations to identify, assess, and manage risks associated with their information assets. ISO/IEC 27005 certification is very important for information security professionals. It equips professionals with the skills to identify threats, vulnerabilities, and their impacts, making informed risk mitigation decisions.

According to IBM the average cost of a data breach in 2025 was \$4.4 million.



Benefits of ISO/IEC 27005 Certification



Expertise in
Safeguarding
Information



Adaptability
in Security
Landscape



Informed Risk
Mitigation
Decisions



Threat and Vulnerability
Identification

[Learn more](#)



Training Course and Learning Objectives



ISO/IEC 27005 Foundation

Gain knowledge on interpreting the guidelines of ISO/IEC 27005 in order to identify, assess, and manage information security-related risks

2 DAYS

ISO/IEC 27005 Risk Manager

Develop the skills to carry out risk management processes related to information security assets by following the guidelines of ISO/IEC 27005

3 DAYS

ISO/IEC 27005 Lead Risk Manager

Acquire the expertise to support an organization in performing information security risk management processes by referring to the guidelines of ISO/IEC 27005

5 DAYS



As the person responsible for procurement at Global Knowledge, I have been working with PECB for over 12 years now. A flawless partnership over all these years thanks to their great professionalism and responsiveness. Their training courses are of high quality and aligned with market needs, and their certifications are recognized for their rigor and value in the market.

Selim Zeggai
Global Knowledge, France

ISO/IEC 27035 Information Security Incident Management

Overview of ISO/IEC 27035 and Its Certification Process

ISO/IEC 27035 is an international standard that provides guidelines for information security incident management. ISO/IEC 27035 certification is a crucial credential for professionals aiming to master the art of managing information security incidents. This certification is designed to validate and enhance your skills in effectively identifying, managing, and preventing security incidents in any organization.

According to Business Research Insights, the global Incident Response market size is valued at U.S. \$29.76 billion in 2025, and is expected to reach approximately U.S. \$148.61 billion by 2035, with a projected CAGR of about 17.3% over 2025–2035.



Benefits of ISO/IEC 27035 Certification



Effective Incident Response



Boosts Organizational Security



Global Recognition



Enhanced IT Skills and Knowledge

[Learn more](#)



Training Course and Learning Objectives



ISO/IEC 27035 Foundation

Gain knowledge on the main elements of implementing a Security Incident Management Plan and managing information security incidents

2 DAYS

ISO/IEC 27035 Lead Incident Manager

Gain the skills and knowledge to support an organization in implementing and managing an Information Security Incident Management Plan in accordance with the guidelines of ISO/IEC 27035

5 DAYS

ISO/IEC 27034 Application Security

Overview of ISO/IEC 27034 and Its Certification Process

The ISO/IEC 27034 Application Security certification equips professionals with advanced skills in managing the application security program based on the ISO/IEC 27034 standards.

Pursuing the ISO/IEC 27034 Application Security certification entails comprehensive training including legal compliance, risk management, and security integration throughout the application development lifecycle, up to deployment and maintenance. This certification process develops your ability to identify and mitigate security risks, preparing you for leadership roles in IT security.



Benefits of ISO/IEC 27034 Certification



Enhanced Expertise in
a Critical IT Security
Domain



Advanced Career
Opportunities in
Cybersecurity



Strategic
Leadership



Professional
Growth

[Learn more](#)



Training Course and Learning Objectives



ISO/IEC 27034 Foundation

Gain knowledge about the fundamental principles of application security based on ISO/IEC 27034

2 DAYS

ISO/IEC 27034 Lead Application Security Implementer

Acquire the skills to lead and implement an application security program in accordance with ISO/IEC 27034

5 DAYS

ISO/IEC 27034 Lead Application Security Auditor

Acquire the knowledge and skills to perform an application security audit by applying widely recognized audit principles, procedures, and techniques

5 DAYS

ISO/IEC 27400 IoT Security and Privacy

Overview of ISO/IEC 27400 and Its Certification Process

The ISO/IEC 27400 certification signifies expertise in managing the security and privacy of IoT systems and services. Achieving an ISO/IEC 27400 certification requires mastering the unique security challenges of IoT systems. This certification assesses your ability to safeguard organizations against threats, emphasizing user privacy and the distributed nature of IoT. It is increasingly vital for professionals in IoT system management to highlight a deep understanding of and capability to mitigate associated risks.



Benefits of ISO/IEC 27400 Certification



Expertise in IoT Security



Risk Mitigation Skills



Enhanced Professional Profile



Ability to Manage IoT Security Challenges

[Learn more](#)



Training Course and Learning Objectives



ISO/IEC 27400 Foundation

Gain knowledge on the basic principles of IoT security and privacy and ISO/IEC 27400

2 DAYS

ISO/IEC 27400 Lead Manager

Master the management of processes and controls for security and privacy of IoT systems based on ISO/IEC 27400

5 DAYS

Why Choose a Career in Information Security?

- Growing Demand
- Thriving Industry
- Advancement Opportunities



High-Paying Careers in Information Security

Chief Information Security Officer (CISO)

The CISO is a senior-level executive responsible for establishing and maintaining an organization's vision, strategy, and program to ensure information assets and technologies are adequately protected.

Annual Average Salary: **U.S. \$315,868**

Information Security Director

Oversees an organization's overall information security strategy, ensuring the confidentiality, integrity, and availability of data.

Annual Average Salary: **U.S. \$216,812**

Information Security Manager

This role focuses on managing and overseeing an organization's entire information security program.

Annual Average Salary: **U.S. \$187,221**

Security Architect

A Security Architect designs, builds, and oversees the implementation of network and computer security for an organization.

Annual Average Salary: **U.S. \$204,664**

Information Security Analyst

Protects an organization's computer systems and networks by identifying and solving potential and actual security problems.

Annual Average Salary: **U.S. \$160,292**

Note: The salary data presented here is sourced from [Glassdoor](#) and may be subject to change over time due to various factors.



We are pleased to contribute to PECB's 2026 Training Catalog. Our partnership with PECB is of exceptional quality, we particularly appreciate the responsiveness, availability, and constant attentiveness of the PECB teams. The feedback from our clients and candidates is excellent, both regarding the quality of the training courses and the follow-up and support provided. For us, this partnership represents real added value, built on trust and professionalism, with services and content perfectly tailored to the needs of the market and our clients—always driven by innovation and continuous improvement.

Carine de Freitas
Agency Director at M2i Formation

Cybersecurity Management

Overview of Cybersecurity Management and Its Certification Process

Cybersecurity management refers to the process of overseeing and coordinating efforts to protect an organization's computer systems, networks, and data from digital attacks, unauthorized access, or damage. Embarking on a Cybersecurity Management certification is a pivotal step towards becoming a proficient leader in the realm of digital security. This certification is tailored for professionals who aim to acquire a deep understanding and practical skills in overseeing and directing cybersecurity strategies within organizations.

According to Fortune Business Insights, the global cybersecurity market was valued at about U.S. \$193.73 billion in 2024, and is projected to grow to approximately U.S. \$218.98 billion in 2025 and reach around U.S. \$562.77 billion by 2032 (≈14.4 % CAGR)



Benefits of Cybersecurity Management Certification



Enhanced
Expertise in
Digital Security



Improved
Leadership Skills



Better
Decision-Making



Broadened
Understanding
of Risk Assessment

[Learn more](#)



Training Course and Learning Objectives



Cybersecurity Foundation

Gain knowledge on the main elements of cybersecurity principles and concepts aligned with industry best practices, such as ISO/IEC 27032 and NIST Cybersecurity Framework

2 DAYS

Lead Cybersecurity Manager

Gain the skills and knowledge to support an organization in implementing, managing, and continually improving cybersecurity programs

5 DAYS

Cloud Security

Overview of Cloud Security and Its Certification Process

Cloud Security Certification is a professional accreditation that validates expertise in designing, implementing, and managing secure cloud infrastructure and services. The journey to obtaining a Cloud Security certification involves mastering the complexities of cloud computing and its security challenges. This certification process educates you on various cloud service models (IaaS, PaaS, SaaS), cloud deployment types (public, private, hybrid), and the unique security considerations for each.



Benefits of Cloud Security Certification



Specialized Skills



Relevance in the Growing Field of Cloud Security



Enhanced Employability



Boosts Job Security

[Learn more](#)



Training Course and Learning Objectives



Lead Cloud Security Manager

Obtain the necessary competence to plan, implement, manage, and maintain a cloud security program based on ISO/IEC 27017 and ISO/IEC 27018

5 DAYS

Penetration Testing

Overview of Penetration Testing and Its Certification Process

Penetration Testing Certification is a professional accreditation that demonstrates expertise in assessing and exploiting vulnerabilities in computer systems and networks to enhance their security. The journey to obtaining a Penetration Testing Certification involves a comprehensive exploration of ethical hacking and security assessment techniques. This certification path teaches you to think like a hacker and use that knowledge to identify and fix security vulnerabilities.



Benefits of Penetration Testing Certification



Commitment to
Cybersecurity



Higher Earning
Potential



Professional
Growth



Demonstrated Skills in
Hacking and Identifying
Vulnerabilities

[Learn more](#)



Training Course and Learning Objectives



Lead Pen Test Professional

Gain the knowledge and skills to lead a professional Penetration Test using a mix of practical techniques and management skills to analyze the test results

5 DAYS

SCADA Security

Overview of SCADA and Its Certification Process

SCADA (Supervisory Control and Data Acquisition) is a system used for monitoring and controlling industrial processes and infrastructure remotely. This certification journey equips you with the specialized skills and knowledge essential for securing SCADA systems, which are pivotal in industrial control and critical infrastructure.

The certification covers areas such as understanding SCADA system architectures, identifying and mitigating vulnerabilities, implementing robust security protocols, and responding effectively to potential cyber threats.



Benefits of SCADA Certification



Improved Security
Implementation



Comprehensive
Professional
Approach to
Security



Enhanced SCADA
Security
Knowledge



Holistic Security
Approach

[Learn more](#)



Training Course and Learning Objectives



Lead SCADA Security Manager

Develop the skills to effectively implement a SCADA security program that protects systems from threats, vulnerabilities, and risks

5 DAYS

ISO/IEC 27033 Networking Security

Overview of ISO/IEC 27033 and Its Certification Process

Network security certification is a formal recognition of expertise in protecting the network infrastructure and data from various types of cyber threats and vulnerabilities and ensures confidentiality, integrity, and availability. Embarking on a network security certification journey involves diving deep into the realm of understanding the concepts, approaches, methods, and techniques of the implementation and effective management of network security, as well as the interpretation of guidelines in the ISO/ IEC 27033 series of standards. This certification path covers a comprehensive curriculum, including guidelines for the design and implementation of network security, as well as usage of gateways, VPNs, and wireless IP network access to secure the communication between networks.



Benefits of ISO/IEC 27033 Certification



Boosts Career in IT and Cybersecurity



Preparedness for Complex Challenges



Enhanced Professional Credibility



Improved Marketability

Learn more



Training Course and Learning Objectives



ISO/IEC 27033 Lead Network Security Manager

Obtain the necessary competence to plan, implement, manage, and maintain network security based on ISO/IEC 27033 series of standards

5 DAYS



Our collaboration with PECB has been truly exceptional. The support provided by the PECB team is highly responsive and professional, and their staff is always friendly and approachable. The PECB Conference in Barcelona was excellently organized – it offered valuable learning opportunities and outstanding networking experiences. Feedback from our training participants has been overwhelmingly positive, particularly regarding the quality of the training materials, the expertise of the instructors, as well as the examination and certification processes. We are proud to be a partner of PECB and look forward to continuing our successful cooperation in the years ahead.

Bojan Varga

Development Manager at SIQ Ljubljana

Cybersecurity Maturity Model Certification (CMMC)

Overview of CMMC and Its Certification Process

The Cybersecurity Maturity Model Certification (CMMC) is a unified cybersecurity standard incorporating best practices from various frameworks. It features five maturity levels tailored to organizations in the Defense Industrial Base (DIB) sector, with the required level dependent on the type of information handled. Embarking on the path to CMMC certification involves understanding and implementing a range of cybersecurity practices and processes aligned with the maturity level your organization is aiming to achieve. The certification process encompasses five maturity levels, ranging from basic to advanced cyber hygiene.

According to IBM, average breach costs in the United States reached a record \$10.22 million in 2025, a 9% increase year over year.



Benefits of CMMC Certification



Advanced
Cybersecurity
Knowledge



Compliance
Expertise



Industry
Recognition



Career Advancement in
Cybersecurity



Training Course and Learning Objectives



CMMC Foundations

Learn the fundamental concepts and principles of the CMMC model

2 DAYS

Certified CMMC Professional (CCP)

Gain the necessary knowledge and skills to interpret, implement, and manage the CMMC practices based on the CMMC model and assess CMMC level 1 practices

4 DAYS

Note: CMMC Foundations is a PECB training course, not approved by the Cyber-AB, therefore the PECB CMMC Foundations credential is not a CMMC credential. As such, this credential does not replace, complement, or lead toward a CMMC credential.

NIS 2 DIRECTIVE

Overview of NIS 2 Directive and Its Certification Process

The NIS 2 Directive Certification refers to compliance with the revised EU Directive on the security of Network and Information Systems, focusing on enhancing cybersecurity across various sectors. Achieving compliance with the NIS 2 Directive involves a comprehensive understanding of the updated regulations and standards for network and information systems security within the EU. This process includes identifying and implementing the necessary measures to protect critical infrastructure and services from cyber threats. The certification journey covers risk management, incident reporting, and the adoption of appropriate security protocols.



Benefits of NIS 2 Certification



Compliance with
EU Standards



Robust Commitment
to Cybersecurity



Enhanced
Credibility



Critical Sector Expertise

[Learn more](#)



Training Course and Learning Objectives



NIS 2 Directive Foundation

Understand the core concepts required to support organizations in the initial phases of planning, implementation, and management of cybersecurity programs

2 DAYS

NIS 2 Directive Lead Implementer

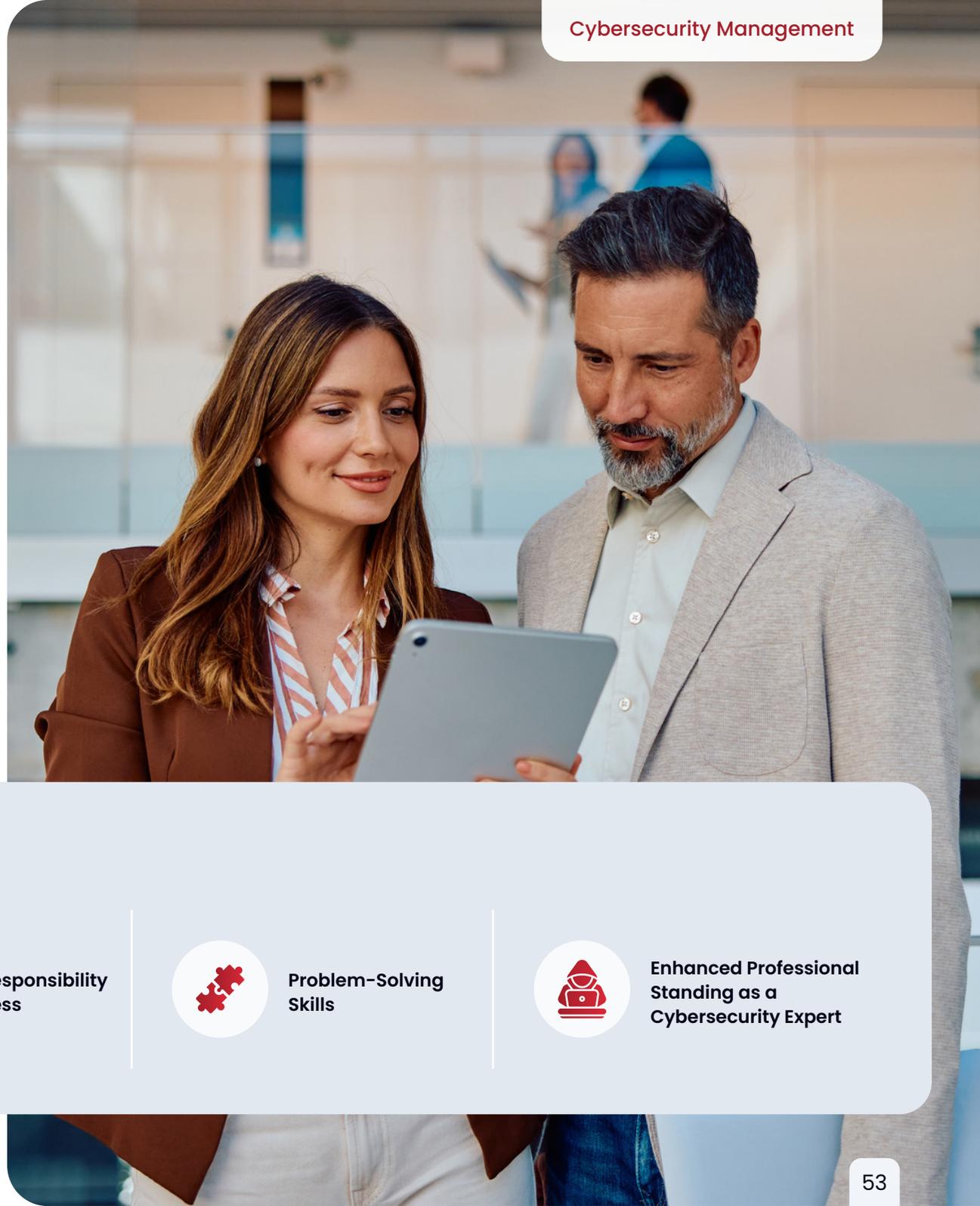
Acquire essential skills to help organizations effectively develop, implement, manage, and maintain a cybersecurity program compliant with the NIS 2 Directive requirements

5 DAYS

SOC 2

Overview of SOC 2 and Its Certification Process

The SOC 2 certification is a professional credential that recognizes expertise in cybersecurity, focusing on the five trust principles of security, availability, processing integrity, privacy, and confidentiality. Embarking on the journey to become a SOC 2 certified analyst is a significant step towards enhancing your role in the cybersecurity field. This certification journey entails gaining in-depth knowledge and understanding of the SOC's five trust principles, along with the expertise to protect customer data privacy using the SOC 2 specified measures to counter threats.



Benefits of SOC 2 Certification



Expertise
in Security
Assessment



High-Responsibility
Readiness



Problem-Solving
Skills



Enhanced Professional
Standing as a
Cybersecurity Expert

[Learn more](#)



Training Course and Learning Objectives



Lead SOC 2 Analyst

Master the implementation and management of SOC 2 framework to ensure organizational data privacy and security compliance

5 DAYS

NIST Cybersecurity

Overview of NIST Cybersecurity and Its Certification Process

The NIST Cybersecurity Certification provides professionals with the expertise to apply NIST's widely respected cybersecurity frameworks, guidelines, and best practices. It focuses on managing security risks, enhancing privacy protection, and aligning with the NIST Cybersecurity Framework (CSF). NIST's broader guidance, including key Special Publications such as SP 800-12 (security principles), SP 800-53 (security and privacy controls), SP 800-37 (risk management), and SP 800-171 (protection of controlled unclassified information), further strengthens an organization's ability to build a robust security posture. Mastery of these resources gives you a competitive advantage, enabling you to confidently navigate the cybersecurity landscape and support the development of resilient and secure digital environments.



Benefits of NIST Cybersecurity Certification



Tailored
Cybersecurity
Solutions



Expertise in Threat
Assessment



Comprehensive
Knowledge



Career Advancement as
Cybersecurity Expert

[Learn more](#)



Training Course and Learning Objectives



NIST Cybersecurity Foundation

Gain knowledge of the fundamental principles and core concepts of cybersecurity, grounded in NIST cybersecurity standards, needed to understand risk management concepts, and control mechanisms that support the protection of information systems and data.

2 DAYS

NIST Cybersecurity Professional

Master the application of NIST guidelines and management of cybersecurity controls and risks

5 DAYS

ISA/IEC 62443

Overview of ISA/IEC 62443 and Its Certification Process

The ISA/IEC 62443 certification validates expertise in industrial automation and control systems (IACS) cybersecurity, grounded in the only globally agreed-upon standards dedicated to securing operational technology environments. Pursuing this certification provides a structured exploration of the ISA/IEC 62443 framework, including its governance requirements, system and component security controls, risk assessment methods, and “secure by design” engineering principles. This certification journey equips participants with the skills needed to assess IACS risks, design secure architectures, manage life-cycle security practices, and align suppliers and integrators with industry expectations, enabling organizations to strengthen resilience across diverse industrial sectors.



Benefits of ISA/IEC 62443 Certification



Demonstrated Proficiency in Industrial Cybersecurity



Ability to Conduct IACS Risk Assessments



Competence in Designing Secure-by-Design Industrial Systems



Strengthened Capability to Maintain and Improve IACS Security



Enhanced Evaluation of Suppliers and Service Providers



Effective Adaptation of IT Security Principles to OT Environments



Improved Cross-Stakeholder Communication Using a Unified Standards Language



Globally Recognized Professional Credibility in IACS Security



Training Course and Learning Objectives



ISA/IEC 62443 Lead Implementer

Acquire the skills to lead and implement an industrial automation and control systems (IACS) cybersecurity program in accordance with ISA/IEC 62443

5 DAYS

Canadian Program for Cybersecurity Certification

Overview of CP-CSC and Its Certification Process

The Canadian Program for Cyber Security Certification (CP-CSC) helps professionals build solid, practical expertise in cybersecurity as it applies across Canadian industries and government-regulated environments. The program is designed to give participants a clear understanding of Canada's cybersecurity requirements, risk-management expectations, and security best practices. Through this certification, learners explore key Canadian frameworks, governance principles, assessment methods, and secure-by-design approaches.

The program equips professionals to identify and manage cyber risks, design and maintain secure environments, and ensure alignment with Canadian regulatory and industry standards. Completing CP-CSC supports individuals and organizations to strengthen their cybersecurity background and meet Canada's digital-security expectations.

Benefits of CP-CSC



Proven understanding of Canadian cybersecurity standards and requirements



Ability to carry out cybersecurity assessments within Canadian regulatory contexts



Skills to design and maintain secure systems aligned with Canadian best practices



Improved ability to manage and reduce cyber risks across an organization



Better evaluations of vendor and partner security readiness



Stronger alignment between IT/OT operations and Canadian compliance needs



Clearer communication and coordination between technical and non-technical teams



Recognition as a trusted cybersecurity professional within Canada



Training Course and Learning Objectives



Certified Canadian Program for Cyber Security Officer

5 DAYS

Equips future cyber officers with a clear understanding of Canadian standards, assessment methods, and operational security tasks essential for supporting organizational protection strategies

Why Choose a Career in Cybersecurity Management?

- Rapidly Evolving Field
- Vital Role in Protecting Digital Assets
- Diverse Career Paths



High-Paying Careers in Cybersecurity Management

Cybersecurity Consultant

Provides expert advice and guidance to organizations on how to protect their digital assets and infrastructure.

Annual Average Salary: **U.S. \$153,027**

Incident Response Manager

Leads the response to cyber-attacks and breaches, managing the process of containing and mitigating the damage.

Annual Average Salary: **U.S. \$120,000**

Cybersecurity Engineer

Develops and implements security measures to safeguard information against hackers, cyber-attacks, and other vulnerabilities.

Annual Average Salary: **U.S. \$158,002–\$160,836**

Network Security Engineer

Focuses on protecting an organization's networking infrastructure from threats and attacks.

Annual Average Salary: **U.S. \$161,521–\$162,531**

Penetration Tester

Penetration Testers are responsible for testing and securing computer systems, networks, and applications to prevent breaches.

Annual Average Salary: **U.S. \$152,323**

Note: The salary data presented here have been sourced from [Glassdoor](#) and may be subject to change over time due to various factors.



Working with PECB has been an excellent experience. Their training programs are exceptionally well-structured, practical, and aligned with real-world standards, making professional development both engaging and effective. The team's support and responsiveness throughout the collaboration have been outstanding, ensuring a smooth and rewarding experience from start to finish.

Radu Dănilă

Training Coordinator at Noble Prog, Romania

Certified Lead Ethical Hacker (CLEH)

Overview of CLEH and Its Certification Process

The Certified Lead Ethical Hacker (CLEH) certification provides comprehensive requirements for professionals aspiring to master, implement, and continuously refine ethical hacking methodologies. This certification is designed for individuals who seek to identify, exploit, and mitigate cybersecurity vulnerabilities effectively while adhering to ethical standards. It equips candidates with the advanced knowledge and practical skills to perform in-depth security assessments, understand emerging cyber threats, and develop proactive defense strategies. Furthermore, the CLEH certification emphasizes the importance of staying updated with the latest tools, techniques, and regulatory requirements, enabling professionals to address real-world cybersecurity challenges with confidence and precision. This certification serves as a benchmark for expertise in ethical hacking, ensuring that certified individuals can safeguard digital ecosystems across various industries.



Benefits of CLEH Certification



Enhanced
Offensive Security
Skills



Comprehensive
Ethical Hacking
Expertise



Master Advanced
Ethical Hacking
Techniques



Enhanced Problem
Solving Abilities

[Learn more](#)



Training Course and Learning Objectives



Certified Lead Ethical Hacker (CLEH)

Gain the knowledge and skills to manage a penetration testing project and team, as well as plan and perform internal and external penetration testing, following best practices

5 DAYS

Certified Cyber Threat Analyst (CCTA)

Overview of CCTA and Its Certification Process

The Certified Cyber Threat Analyst (CCTA) is developed for cybersecurity professionals seeking to build expertise in advanced threat detection, analysis, and mitigation. This training course equips candidates with comprehensive methodologies and frameworks to establish, implement, maintain, and continually enhance organizational capabilities in identifying, assessing, and neutralizing evolving cyber threats. The CCTA certification represents a global benchmark in cyber threat analysis and incident response. This certification guides professionals in implementing a structured approach to safeguarding organizational assets by integrating threat intelligence, proactive threat hunting, and incident management.



Benefits of CCTA Certification



Enhanced Threat
Detection and
Response



Proactive Threat
Hunting



Improved Incident
Management



Adoption of Advanced
Frameworks

[Learn more](#)



Training Course and Learning Objectives



Certified Cyber Threat Analyst (CCTA)

Develop the expertise to proactively hunt for cyber threats using threat intelligence and behavioral analysis techniques. Gain hands-on skills to assess attack patterns, track threat actors, and enhance security operations with proactive defense strategies

5 DAYS



It is an honor to be a partner with PECB, a global leader in ISO training. Thanks to this alliance, we have trained dozens of professionals in Ecuador through high-level training courses delivered by instructors with over 20 years of experience. We have witnessed how, through this learning, students have developed practical skills they can immediately apply within their organizations, allowing them to exceed objectives and create a positive and sustainable impact. One particularly valuable aspect of PECB is the continuous updating of its materials, ensuring that the content is always aligned with changes in standards and current industry best practices. We are proud to be part of this global alliance of excellence alongside PECB.

Ramiro Pulgar

CEO at Blue Hat Corporation, Ecuador

Certified Digital Forensics Examiner (CDFE)

Overview of Certified Digital Forensics Examiner and Its Certification Process

The Certified Digital Forensics Examiner (CDFE) training course is specifically designed to equip professionals with the expertise needed to perform comprehensive and reliable digital forensic investigations. Offered by PECB, this training course fosters digital trust by teaching participants the methodologies and best practices for executing computer forensics processes to extract, preserve, and analyze digital evidence with precision and accuracy. Recognized as a global benchmark in digital forensics, the CDFE certification provides a structured framework for investigating cybercrimes and digital incidents. This certification ensures professionals are well-prepared to safeguard the integrity, confidentiality, and availability of digital evidence—an essential capability in today's rapidly evolving digital landscape.



Benefits of CDFE Certification



Access to
Advanced
Forensic Tools and
Techniques



Staying Ahead of
Emerging Threats



Improved Incident
Response
Capabilities



Hands-on Knowledge of
Forensic Tools

[Learn more](#)



Training Course and Learning Objectives



Certified Digital Forensic Examiner (CDFE)

Gain hand-on experience through technical labs designed to teach you how to collect, analyze, and process digital evidence. Learn industry-standard forensic investigation techniques and legal compliance to support cybersecurity

5 DAYS

Certified Linux Foundations (CLF)

Overview of CLF and Its Certification Process

The Certified Linux Foundations (CLF) training course is designed for professionals who want to build a solid, practical understanding of Linux as a modern operating system for IT, cybersecurity, and cloud environments. This course provides a structured journey from core Linux concepts and command-line interaction to user, process, and system management, remote administration, and security-focused operations. Participants will explore how the Linux kernel, shell, and user space interact, learn to navigate the filesystem, manage users and groups, control processes and services, and interpret system logs for operational and security purposes.

Through extensive hands-on labs, they will practice real-world tasks such as file management, scripting, authentication, scheduling, SSH hardening, and basic system hardening. Completing this certification demonstrates your ability to operate Linux confidently, troubleshoot common issues, and support secure, reliable Linux-based systems in production environments.



Benefits of CLF Certification



Build a Strong Practical Foundation in Linux and Command-Line Proficiency



Understand Core Concepts of Users, Processes, Services, and System Resources



Strengthen Skills in Secure Remote Administration and Log-Based Monitoring



Improve Readiness for Advanced Cybersecurity, DevOps, and Cloud Training



Validate Your Capability to Maintain, Harden, and Troubleshoot Linux Systems



Training Course and Learning Objectives



Certified Linux Foundations (CLF)

CLF provides a practical foundation in Linux by teaching command-line navigation, file and user management, software and process control, and basic networking

Participants also learn core security, logging, and troubleshooting practices needed to operate and maintain Linux systems in modern IT environments

5 DAYS

Certified Advanced Penetration Tester (CAPT)

Overview of Certified Advanced Penetration Tester and Its Certification Process

The Certified Advanced Penetration Tester (CAPT) is a professional-level certification designed for cybersecurity professionals who want to take their ethical hacking and penetration testing skills to the next level. The program equips participants with the technical expertise and practical experience to simulate real-world attacks and secure critical assets. This training course provides an in-depth understanding of cutting-edge techniques and tools used to simulate real-world cyber-attacks across networks, applications, mobile platforms, and cloud infrastructures. Through comprehensive, instructor-led sessions and hands-on labs, PECB ensures participants gain practical experience and confidence in performing complex penetration tests.



Benefits of CAPT Certification



Improved Incident Response Planning



Comprehensive Exploitation Techniques



Proficiency with Advanced Pen Testing tools like Metasploit, Burp Suite Pro, and Wireshark



Deep Understanding of Security Weaknesses



Training Course and Learning Objectives



Certified Advanced Pen Test (CAPT)

Gain the expertise to perform advanced penetration testing techniques, assess complex network infrastructures, and exploit vulnerabilities. Develop hands-on skills in post-exploitation, lateral movement, and evasion techniques to strengthen cybersecurity defenses

5 DAYS

Certified Artificial Intelligence Auditor (CAIA)

Overview of CAIA and Its Certification Process

The Certified Artificial Intelligence Auditor (CAIA) training course provides a comprehensive exploration of artificial intelligence assurance by guiding you through essential auditing principles, compliance frameworks, and governance models. You will learn how to assess AI systems from ethical, technical, operational, and regulatory perspectives to ensure transparency, accountability, fairness, and security throughout the AI lifecycle.

This certification emphasizes evaluating data quality, model integrity, bias mitigation controls, documentation practices, and explainability requirements. Completing this certification demonstrates your ability to plan, execute, and report AI audits that support safe, compliant, trustworthy, and responsible AI adoption within organizations.



Benefits of CAIA Certification



Strengthen Oversight of
AI Governance and Risk



Ensure Compliance with
Global AI Regulations and
Standards



Validate Fairness,
Explainability, and
Transparency Controls



Improve Audit Assurance for
Ethical and Responsible AI



Enhance Career Competitiveness
as AI Regulations Expand



Training Course and Learning Objectives



Certified Artificial Intelligence Auditor (CAIA)

5 DAYS

Prepares professionals to evaluate and audit AI systems by reviewing governance controls, data and model risks, and compliance with ethical and regulatory requirements

Participants learn practical assurance and reporting techniques that help ensure AI solutions are transparent, reliable, and responsibly implemented

Certified Cloud Security Analyst (CCSA)

Overview of Certified Cloud Security Analyst and Its Certification Process

Certified Cloud Security Analyst (CCSA) training course is designed for cybersecurity professionals who secure workloads, data, and identities across modern cloud environments. This course provides a structured journey from core cloud security concepts to advanced defensive techniques, combining theory with practical exercises. You will learn how to evaluate shared responsibility models, harden cloud configurations, secure identities and access, protect data in transit and at rest, and monitor cloud-native infrastructure for threats and misconfigurations.

Through guided hands-on labs, you will apply these skills across leading cloud platforms and containerized environments. Completing this certification demonstrates your ability to analyze, detect, and respond to cloud security risks while helping organizations maintain resilient and compliant cloud architectures.



Benefits of CCSA Certification



Build Practical Expertise in Securing Multi-Cloud and Hybrid Environments



Strengthen Identity, Access, and Data Protection in the Cloud



Enhance Threat Detection and Response Using Cloud-Native Monitoring Tools



Validate Skills in Hardening Containers, Kubernetes, and Cloud Services



Increase Career Opportunities as Cloud Adoption and Security Needs Grow



Training Course and Learning Objectives



Certified Cloud Security Analyst (CCSA)

Equips cloud security professionals to secure and monitor workloads across cloud and containerized environments using IAM, data protection controls, and hardened configurations

Participants practice leveraging cloud-native logging, monitoring, and investigation tools to detect, analyze, and mitigate threats in real-world cloud infrastructures

5 DAYS

Certified SOC Analyst (CSOCA)

Overview of CSOCA and Its Certification Process

The Certified SOC Analyst (CSOCA) training course is designed for professionals responsible for monitoring, detecting, and responding to security events within a Security Operations Center (SOC). The course takes you from foundational SOC concepts and threat landscapes to advanced alert triage, investigation, and incident response practices. You will learn how to work effectively with SIEM platforms, analyze logs and network traffic, investigate phishing and malware incidents, and coordinate response activities with other stakeholders.

Through guided hands-on labs and case-based scenarios, you will practice end-to-end investigations, from initial alert to containment and recovery. Completing this certification demonstrates your ability to operate as a SOC analyst who can recognize, prioritize, and remediate real-world cyber threats in a structured and repeatable way.



Benefits of CCSA Certification



Build Practical Skills in SOC Monitoring, Alert Triage, and Escalation



Strengthen Detection and Investigation of Phishing, Malware, and Ransomware



Enhance Proficiency in Using SIEM, Log Analysis, and Network Forensics Tools



Improve Coordination of Incident Response and Reporting within the SOC



Increase Career Opportunities in Security Operations and Threat Detection

Coming Soon



Training Course and Learning Objectives



Certified SOC Analyst (CSOCA)

Prepares analysts to perform core SOC duties by monitoring alerts, analyzing logs and endpoint data, and investigating phishing, ransomware, and other security incidents

Participants gain practical experience in alert triage, correlation, basic forensics, and incident reporting to support effective, end-to-end security operations

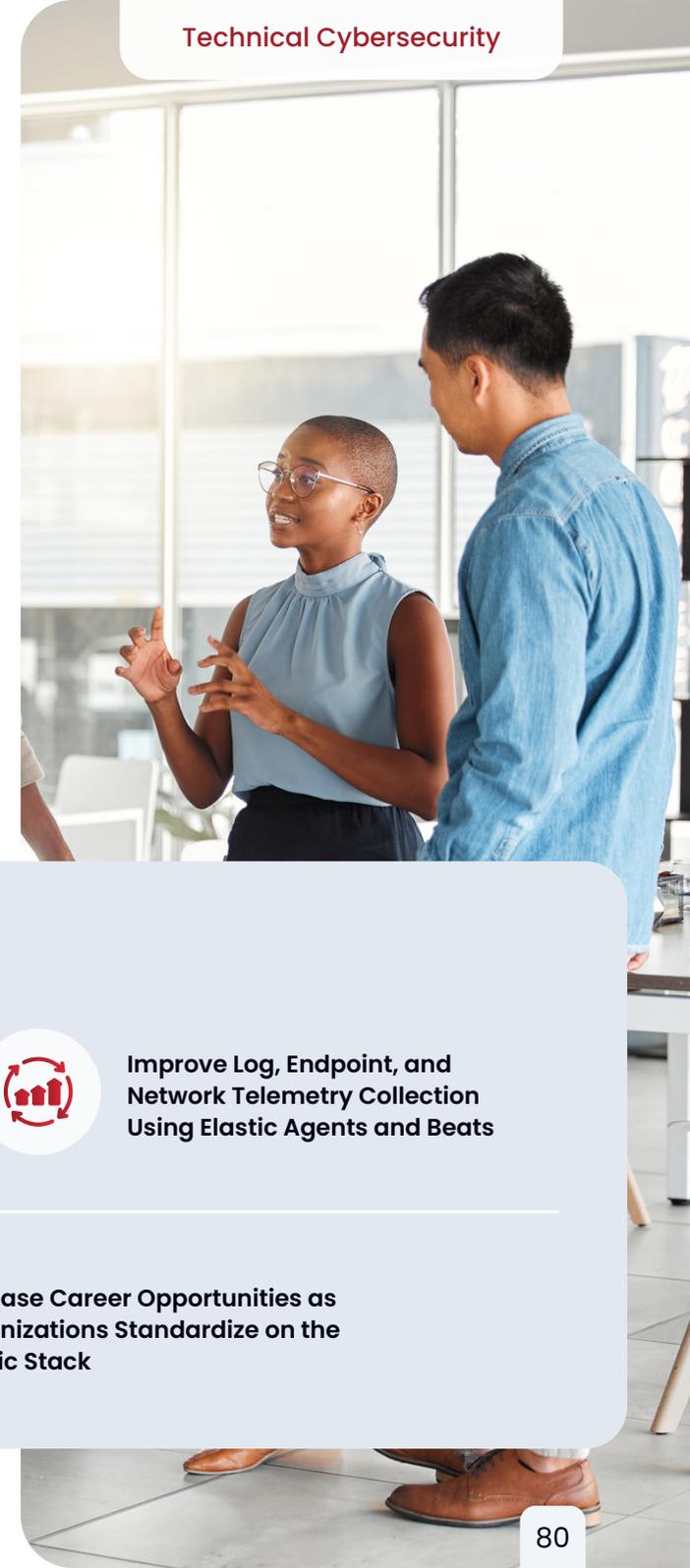
5 DAYS

Certified Elastic Stack Analyst (CESA)

Overview of CESA and Its Certification Process

The Certified Elastic Stack Analyst (CESA) training course is designed for security professionals who use the Elastic Stack to detect, investigate, and respond to threats. This course takes you from navigating Elasticsearch and Kibana to building security-focused visualizations, searches, and alerts that support day-to-day SOC operations. You will learn how to deploy and manage Elastic Agents and Beats, collect and normalize logs and endpoint telemetry, leverage Elastic Security, and apply EQL and analytics for threat hunting.

Through hands-on labs, you will configure detection rules, investigate incidents with timelines and cases, and integrate endpoint protection capabilities. Completing this certification validates your ability to operate Elastic as a security analytics platform and to turn raw data into actionable security insights.



Benefits of CESA Certification



Develop Practical Skills in Using Elastic and Kibana for Security Operations



Enhance Threat Hunting and Detection with EQL, Analytics, and Detection Rules



Improve Log, Endpoint, and Network Telemetry Collection Using Elastic Agents and Beats



Strengthen Incident Investigation and Case Management Workflows in Elastic Security



Increase Career Opportunities as Organizations Standardize on the Elastic Stack

Coming Soon



Training Course and Learning Objectives



Certified Elastic Stack Analyst (CESA)

Enables security professionals to use the Elastic Stack as a security analytics platform by onboarding data, building dashboards, and configuring searches and alerts for key use cases

Participants gain practical experience with Elastic Security, detection rules, EQL-based threat hunting, and investigation workflows to detect, analyze, and respond to threats efficiently

5 DAYS

Certified Web Application Security Analyst (CWASA)

Overview of CWASA and Its Certification Process

The Certified Web Application Security Analyst (CWASA) training course is designed for professionals who assess, secure, and monitor modern web applications and APIs. This course takes you from core HTTP and application architecture concepts to advanced analysis of common and emerging web vulnerabilities. You will learn how to identify, exploit, and validate issues such as injection, broken authentication, sensitive data exposure, access control failures, security misconfiguration, XSS, insecure deserialization, and vulnerable components.

Throughout the course, you will perform guided hands-on labs that simulate real-world attack and defense scenarios, including secure configuration and remediation guidance. Completing this certification demonstrates your ability to analyze web applications, communicate technical findings to development teams, and support secure software development practices across the lifecycle.



Benefits of CWASA Certification



Master Practical Techniques for Identifying and Exploiting Web Application Vulnerabilities



Strengthen Skills in Testing Authentication, Authorization, and Session Management



Improve Ability to Secure APIs, Data Handling, and Application Configuration



Provide Actionable Remediation Guidance to Developers and DevOps Teams



Enhance Career Prospects in Application Security, Penetration Testing, and Secure Development



Training Course and Learning Objectives



Certified Web Application Security Analyst (CWASA)

5 DAYS

Equips security professionals to evaluate the security of web applications and APIs by analyzing architecture, mapping attack surfaces, and testing for common vulnerabilities such as injection, XSS, and broken access control

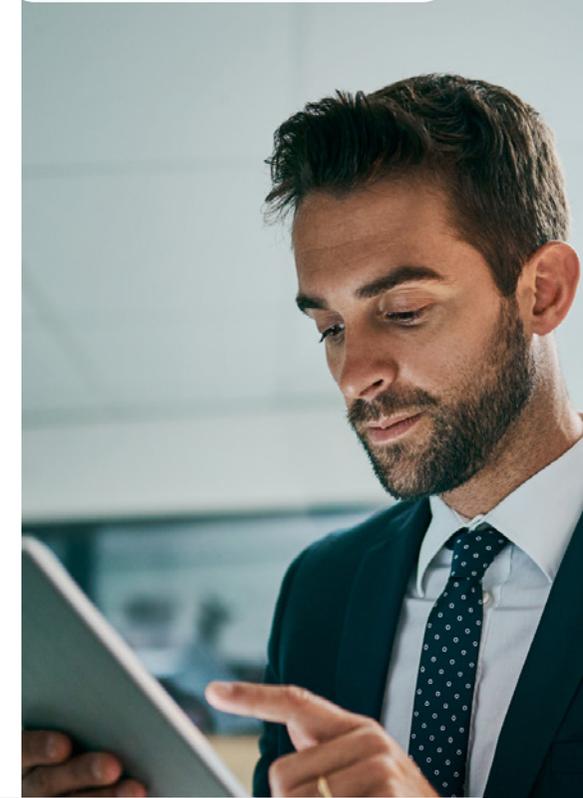
Participants practice exploiting and validating findings, prioritizing risks, and recommending secure coding and configuration improvements to support secure development and protect critical web assets

Certified Splunk Analyst (CSA)

Overview of CSA and Its Certification Process

The Certified Splunk Analyst (CSA) training course is designed for security and operations professionals who use Splunk to collect, analyze, and act on machine data. This course takes you from foundational Splunk concepts and configuration to advanced search, correlation, and incident-response workflows. You will learn how to onboard data, build efficient searches and dashboards, create alerts, and leverage Splunk apps and add-ons to support security operations.

Through hands-on labs and realistic incident exercises, you will investigate events, pivot across logs, and collaborate on response activities using Splunk as a central investigation hub. Completing this certification demonstrates your ability to operate Splunk as a powerful analytics and incident-response platform that supports timely detection and remediation of security threats.



Benefits of CSA Certification



Develop Practical Skills in Searching, Visualizing, and Correlating Data in Splunk



Improve Detection and Investigation of Security Incidents Using Dashboards and Alerts



Strengthen Ability to Onboard and Normalize Logs from Diverse Data Sources



Enhance Incident-Response Efficiency with Playbooks, Workflows, and Case Evidence in Splunk



Increase Career Opportunities in SOC, Threat Detection, and Security Engineering Roles



Training Course and Learning Objectives



Certified Splunk Analyst

Enables security professionals to use Splunk for security monitoring and incident response by configuring data inputs, building SPL searches, dashboards, and alerts for key use cases

Participants gain practical experience performing end-to-end investigations, correlating events across multiple data sources, and turning machine data into actionable insights that support rapid detection, triage, and response

5 DAYS

Certified Cloud Incident Responder (CCIR)

Overview of CCIR and Its Certification Process

The Certified Cloud Incident Responder (CCIR) training course is designed for professionals responsible for detecting, analyzing, and resolving security incidents across cloud environments. This course provides a structured journey from core cloud incident-response principles to platform-specific playbooks for AWS, Azure, Google Cloud, Microsoft 365, and Google Workspace. You will learn how to prepare cloud environments for incident handling, triage alerts, investigate compromised identities and workloads, and coordinate containment and recovery activities.

Through hands-on labs, you will work with native cloud security tools, logs, and telemetry to investigate real-world attack scenarios and apply standardized response procedures. Completing this certification demonstrates your ability to lead and execute cloud-focused incident response operations that restore services quickly while preserving evidence and supporting compliance requirements.



Benefits of CCIR Certification



Develop Practical Skills in Responding to Incidents Across Major Cloud Platforms



Strengthen Detection, Triage, and Investigation of Cloud-Based Threats



Improve Use of Native Cloud Security Tools, Logs, and Telemetry for Forensics



Enhance Ability to Contain, Eradicate, and Recover from Cloud Compromises



Increase Career Opportunities in Cloud Security Operations and Incident Response

Coming Soon



Training Course and Learning Objectives



Certified Cloud Incident Responder

Prepares professionals to handle the full incident-response lifecycle in cloud environments by readying accounts and tenants, analyzing logs, and investigating threats across identities, workloads, data, and SaaS services

Participants gain practical experience executing playbooks in AWS, Azure, Google Cloud, Microsoft 365, and Google Workspace, documenting findings, coordinating with stakeholders, and implementing corrective actions to strengthen resilience against future incidents

5 DAYS

Why Choose a Career in Technical Cybersecurity?

- Critical for Digital Trust and Business Protection
- High Demand Across All Industries
- Lucrative and Future-Proof Career Paths

Technical cybersecurity professionals play a critical role in protecting systems, applications, data, and emerging technologies from increasingly sophisticated cyber threats. As organizations accelerate digital transformation, the demand for skilled security specialists continues to rise globally.



High-Paying Careers in Technical Cybersecurity

Certified Advanced Penetration Tester (CAPT)

Conducts advanced penetration testing and red team exercises to simulate real-world cyber-attacks. This role focuses on exploiting complex vulnerabilities and strengthening organizational defenses.

Annual Average Salary: **U.S. \$132,900**

Certified Cloud Incident Responder (CCIR)

Responds to and manages security incidents in cloud based environments, including data breaches, unauthorized access, malware infections, and misconfigurations.

Annual Average Salary: **U.S. \$116,000**

Certified Cloud Security Analyst (CCSA)

Focuses on securing cloud-based infrastructures, platforms, and applications. This role ensures compliance, risk management, and security controls across cloud service providers, such as AWS, Azure, and Google Cloud.

Annual Average Salary: **U.S. \$121,700**

Certified Elastic Stack Analyst (CESA)

Specializes in using Elastic Stack (ELK) for threat detection, log analysis, and security monitoring. Elastic Analysts support incident detection, investigation, and response through advanced data analytics.

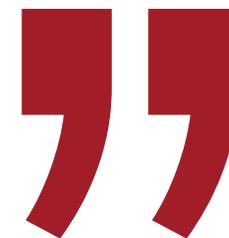
Annual Average Salary: **U.S. \$118,500**

Certified Web Application Security Analyst (CWASA)

Responsible for identifying, analyzing, and mitigating security vulnerabilities in web applications. This role focuses on secure coding practices, application testing, and protecting against attacks, such as SQL injection, XSS, and CSRF.

Annual Average Salary: **U.S. \$115,000**

Note: The salary data presented here have been sourced from [Glassdoor](#) and may be subject to change over time due to various factors.



Partnering with PECB has strengthened my credibility as a consultant, trainer, and training provider. Their accredited certifications assure my clients that I have the training, experience, and recognized qualifications to guide them effectively. Whether I'm delivering consulting services or delivering courses, clients know they're receiving trusted, high-quality support backed by a globally respected certification body. With PECB's flexible training course formats, I'm able to meet diverse learning needs while maintaining a high standard of excellence. PECB stands out for its global recognition, accredited certifications, practical course design, diversity in delivery methods, and commitment to excellence. If you're looking to empower professionals and elevate your brand, PECB is the partner to choose.

Michael Gross

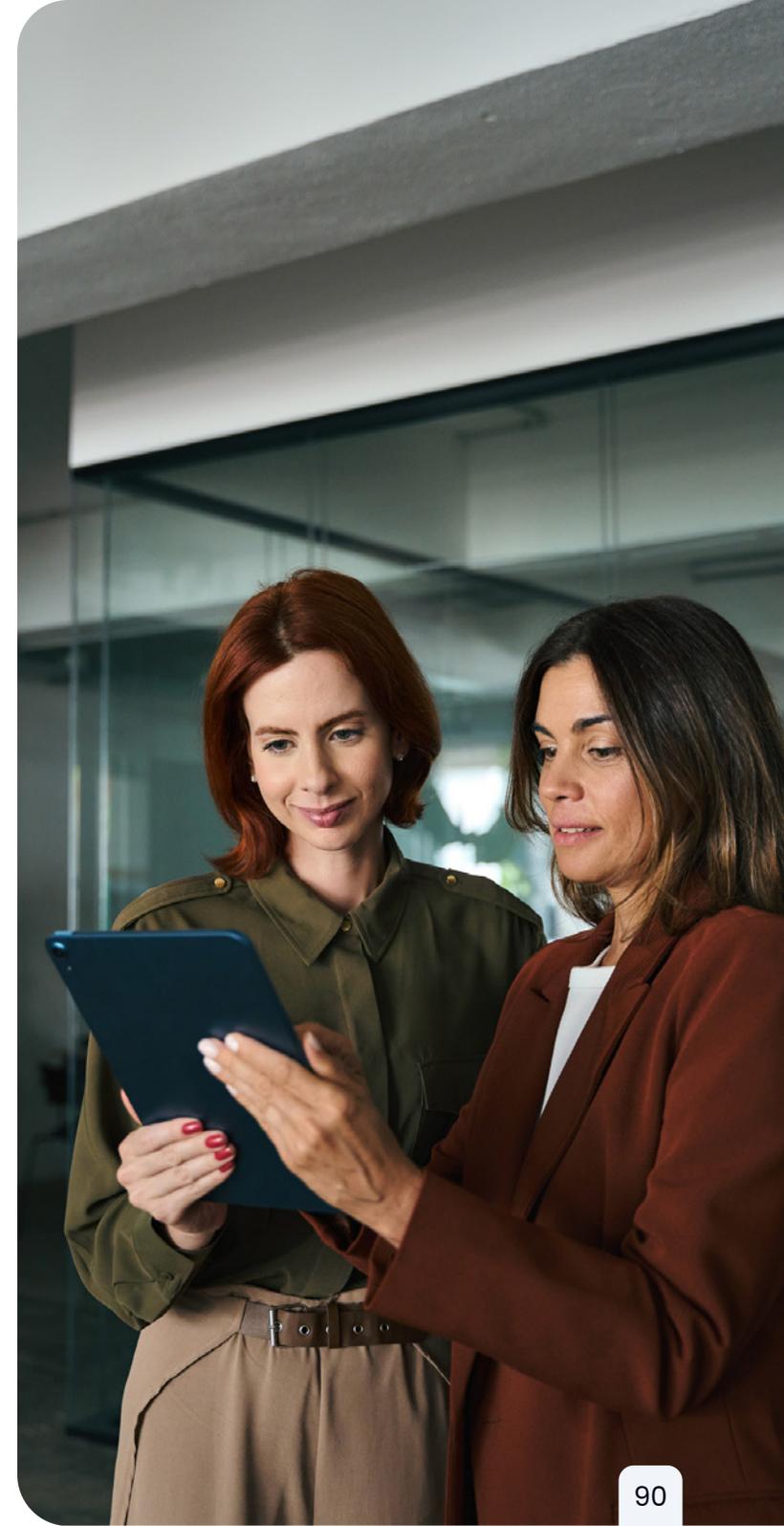
Management System Certification Training Solutions - USA

CONTINUITY, RESILIENCE, AND RECOVERY



Why Continuity, Resilience, and Recovery?

Continuity, resilience, and recovery are important for organizations to maintain operations during disruptions, protect critical assets, and reduce financial and reputational risks. These strategies build adaptability, ensure quick recovery, and foster stakeholder trust, positioning organizations for continued success in a competitive and unpredictable environment.

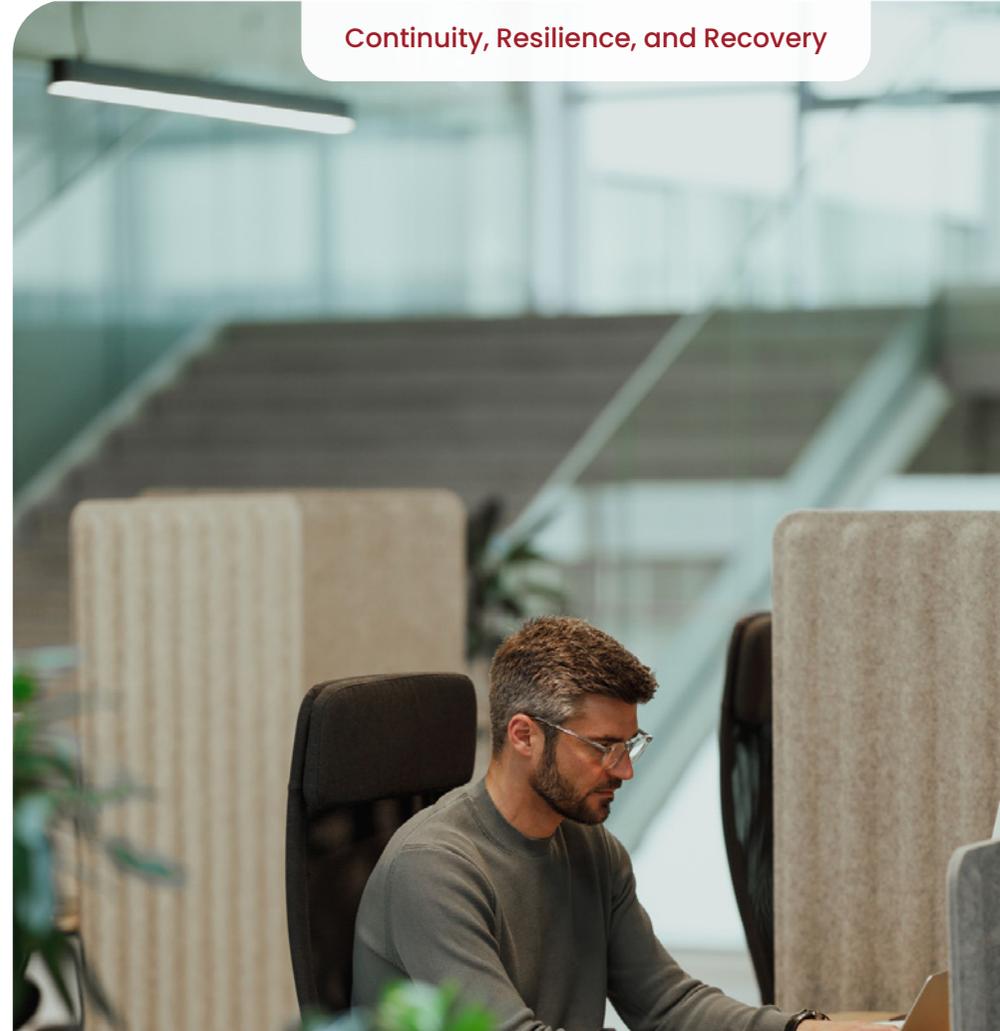


ISO 22301 Business Continuity Management System

Overview of ISO 22301 and Its Certification Process

ISO 22301 is a globally recognized standard for business continuity management, ensuring organizations are prepared to continue operations during and after a disruptive incident. Embarking on the ISO 22301 certification journey entails mastering the art of business continuity and resilience. This certification process involves understanding and implementing the best practices for developing, maintaining, and improving a Business Continuity Management System (BCMS). It covers critical areas such as risk assessment, incident response planning, business impact analysis, and recovery strategies.

According to VynZ Research, the global Business Continuity Management (BCM) Market was valued at U.S. \$1.62 billion in 2025 and is estimated to reach U.S. \$3.82 billion by 2035 with a CAGR of 13.7%.



Benefits of ISO 22301 Certification



Professional Expertise
in Business Continuity
and Resilience Planning



Career
Opportunities



Validates
Organizational
Preparedness
Ability



Enhanced Credibility in
Business Continuity and
Planning

Learn more



Training Course and Learning Objectives	
ISO 22301 Foundation Understand the essential principles, concepts, and techniques of a BCMS and the requirements of ISO 22301	2 DAYS
ISO 22301 Lead Implementer Gain a comprehensive understanding of the BCMS implementation techniques and learn how to lead a team in implementing a BCSM based on ISO 22301	5 DAYS
ISO 22301 Lead Auditor Obtain knowledge and become competent to audit an organization's BCMS against the requirements of ISO 22301	5 DAYS

Disaster Recovery

Overview of Disaster Recovery and Its Certification Process

Disaster Recovery Certification is a professional accreditation that signifies expertise in planning, implementing, and managing strategies to restore ICT infrastructure and services following a disaster. Pursuing a Disaster Recovery certification involves a comprehensive exploration of the methodologies and best practices for ICT service restoration after disruptive events. This certification path covers critical areas such as risk assessment, business impact analysis, recovery strategy development, and the implementation of disaster recovery plans.

According to Precedence Research, the global disaster recovery as a service market is projected to grow from U.S. \$22.40 billion in 2025 to U.S. \$195.71 billion by 2034, expanding at a CAGR of 27.23% during the forecast period.



Benefits of Disaster Recovery Certification



Critical Skills Development



Validates Expertise in Disaster Recovery Strategy Implementation



Safeguarded Infrastructure



Career Opportunities

Learn more



Training Course and Learning Objectives



Disaster Recovery Foundation

Gain knowledge on the main concepts of an ICT disaster recovery planning process

2 DAYS

Lead Disaster Recovery Manager

Master the skills required to help organizations plan, develop, implement, and test an ICT disaster recovery planning process

5 DAYS



PECB stands as a premier benchmark for professional development within the IT GRC landscape, consistently delivering high-caliber training that bridges the gap between complex standards and practical application. Their commitment to global accessibility is unmatched, offering a versatile range of delivery modes—from self-study to interactive live sessions—alongside course materials in multiple languages to cater to diverse learning styles. As a dedicated partner, we are immensely grateful for the collaborative ecosystem PECB has cultivated. Their unwavering support extends far beyond accreditation, offering the resources and responsiveness necessary to help us grow and serve our local market effectively. We wholeheartedly recommend a partnership with PECB to any organization seeking a relationship built on mutual success, operational excellence, and a shared vision for elevating global industry standards.

Mostafa AlShamy
Egybyte

Digital Operational Resilience Act (DORA)

Overview of DORA and Its Certification Process

The Digital Operational Resilience Act (DORA) certification demonstrates your expertise in leading and overseeing the implementation of digital operational resilience strategies within financial entities to help them ensure compliance with the European Union's Digital Operational Resilience Act (DORA). This certification validates your proficiency in areas such as ICT risk management, incident management, digital operational resilience testing, third-party risk management, and information and intelligence sharing. It affirms your ability to meet the technical standards set by DORA and positions you as a trusted professional who can contribute to the operational resilience of financial entities.



Benefits of DORA Certification



Enhanced Career Prospects



Ability to Navigate Complex Regulations



Competitive Advantage



Career Growth

[Learn more](#)



Training Course and Learning Objectives



DORA Foundation

Understand the fundamental elements of the Digital Operational Resilience Act

2 DAYS

Lead DORA Manager

Master the implementation and management of the operational resilience framework as outlined by the Digital Operational Resilience Act

5 DAYS

Crisis Management

Overview of Crisis Management and Its Certification Process

Crisis Management certification is a professional credential that validates expertise in planning, managing, and responding effectively to organizational crises. Pursuing a Crisis Management certification involves a deep dive into the strategies and skills required for effectively handling unexpected and high-pressure situations within organizations.

This certification covers critical aspects of crisis management, including risk assessment, crisis communication, decision-making under pressure, and recovery strategies.



Benefits of Crisis Management Certification



Crisis Mitigation Skills



Crisis Communication Expertise



Improved Leadership and Decision-Making



Enhanced Career Prospects

[Learn more](#)



Training Course and Learning Objectives



Lead Crisis Manager

Develop competencies in planning, establishing, and continually improving strategic crisis management capabilities

5 DAYS

Operational Resilience Management

Overview of Operational Resilience Management and Its Certification Process

The Operational Resilience Manager certification validates your expertise in building, managing, and improving operational resilience frameworks aligned with global best practices. This certification demonstrates your ability to identify, assess, and mitigate risks to ensure business continuity and operational resilience. It reflects your proficiency in designing resilient strategies that address the complex challenges organizations face, safeguarding critical operations and promoting long-term resilience.



Benefits of Operational Resilience Certification



Proficiency
in Resilience
Measures



Increased
Professional
Credibility



Valuable Skill
Set



Enhances
Organizational Security

[Learn more](#)



Training Course and Learning Objectives



Lead Operational Resilience Manager

Master the skills to drive operational resilience within your organization, ensuring robust systems and processes that withstand and adapt to disruptions

5 DAYS



Working with PECB has been a highly valuable and enriching experience. Their professionalism, responsiveness, and commitment to quality have greatly supported our mission at Aswar Akka Consultancy. Through our partnership, we've been able to elevate our training offerings, expand our market presence, and provide our clients with internationally recognized certification programs that truly make a difference. One of the most notable outcomes of our collaboration has been the increased credibility and visibility we've gained in the region. The seamless coordination with the PECB team—especially in content delivery and partner support—has allowed us to serve our clients more efficiently and with greater confidence. We look forward to continuing this strong partnership and achieving even greater milestones together.

Eng. Noor Diab, MBA, Head of Strategic Advisory & Excellence Services
Aswar Akka Consultancy

Why Choose a Career in Continuity, Resilience, and Recovery?

- Essential for Business Stability
- Growing Importance Across Industries
- Rewarding and Impactful Career Paths



High-Paying Careers in Continuity, Resilience, and Recovery

Director of Crisis Management

Responsible for leading and coordinating the organization's response to emergencies and critical situations, ensuring effective planning, preparedness, and recovery efforts.

Annual Average Salary: **U.S. \$161,850**

Disaster Recovery Manager

Specializes in preparing strategies and plans to recover IT systems, data, and operations effectively after a disaster.

Annual Average Salary: **U.S. \$124,920**

Business Continuity Manager

This role involves planning and managing programs to maintain business functions or quickly resume them in the event of a major disruption.

Annual Average Salary: **U.S. \$167,985**

Chief Resilience Officer (CRO)

The CRO is a top executive who leads the development and implementation of strategies to manage risks, recover from disruptions, and ensure organizational resilience.

Annual Average Salary: **U.S. \$117,139**

Resilience Analyst/Consultant

Focuses on analyzing potential threats and developing strategies to ensure organizational resilience against various disruptions.

Annual Average Salary: **U.S. \$71,825**

Note: The salary data presented here have been sourced from [Glassdoor](#) and may be subject to change over time due to various factors.

PRIVACY AND DATA PROTECTION



Why Privacy and Data Protection?

Privacy and data protection are essential for securing sensitive information, ensuring compliance with laws, and building customer trust. They help mitigate risks of breaches and financial losses, support business continuity, and enhance resilience against continual cyber threats. In today's digital world, they are critical for maintaining security, trust, and legal compliance.



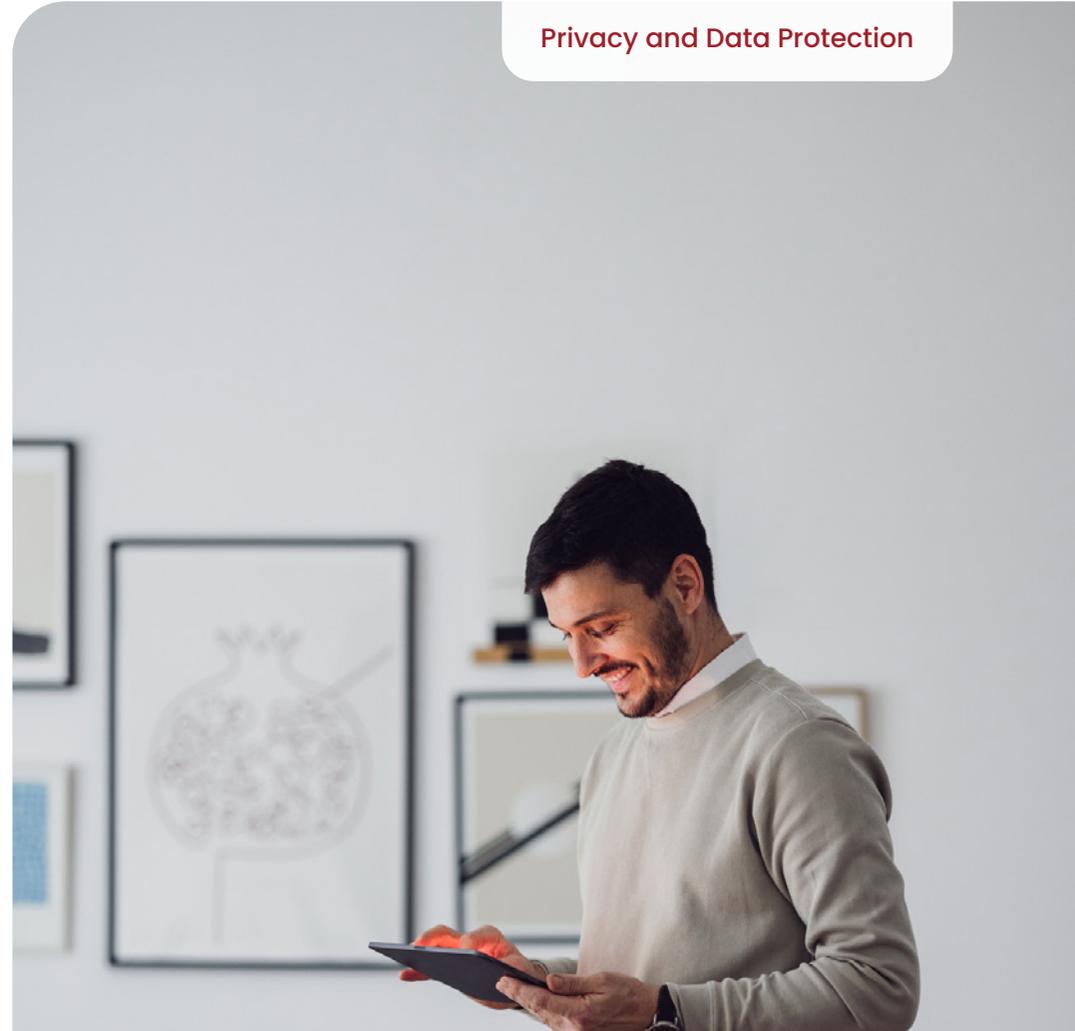
ISO/IEC 27701 Privacy Information Management System

Overview of ISO/IEC 27701 and Its Certification Process

ISO/IEC 27701 is a global standard for privacy information management, providing guidelines for managing and protecting personal data. The journey to achieve the ISO/IEC 27701 certification involves a deep dive into privacy information management systems (PIMS).

This certification process encompasses learning how to establish, maintain, and continuously improve a PIMS, aligned with data protection regulations such as GDPR.

According to Global Growth Insight, the global data privacy service market size was U.S. \$3.78 billion in 2024 and is projected to reach U.S. \$5.33 billion in 2025, rising to U.S. \$74.1 billion by 2034 while exhibiting a CAGR of 36.08% during the forecast period [2025-2034].



Benefits of ISO/IEC 27701 Certification



Enhanced
Professional
Standing



Validates Expertise
in Managing and
Safeguarding
Personal Data



Global
Relevance



Career Advancement
Opportunities

[Learn more](#)



Training Course and Learning Objectives



ISO/IEC 27701 Foundation

Understand the fundamental concepts, principles, methods, and techniques used for the implementation and management of a PIMS

2 DAYS

ISO/IEC 27701 Lead Implementer

Acquire the ability to support an organization in planning, implementing, managing, monitoring, and maintaining a PIMS based on ISO/IEC 27701

5 DAYS

ISO/IEC 27701 Lead Auditor

Develop the knowledge and skills to perform a PIMS audit based on audit best practices

5 DAYS

ISO/IEC 27701 Transition

Understand the significant updates in ISO/IEC 27701:2025 by learning how the clauses on understanding, planning, and implementing a privacy information management system (PIMS) are now independent and not tied to ISO/IEC 27001

2 DAYS



I am very pleased to express my appreciation for our partnership with PECB. We particularly value the quality of our collaboration and the responsiveness of PECB's teams. The training programs offered are also of an excellent standard, allowing us to ensure a high-quality offering to our own clients. Our clients are very satisfied with these training courses, and we are delighted to continue this fruitful collaboration with PECB.

Eli KUDJIE

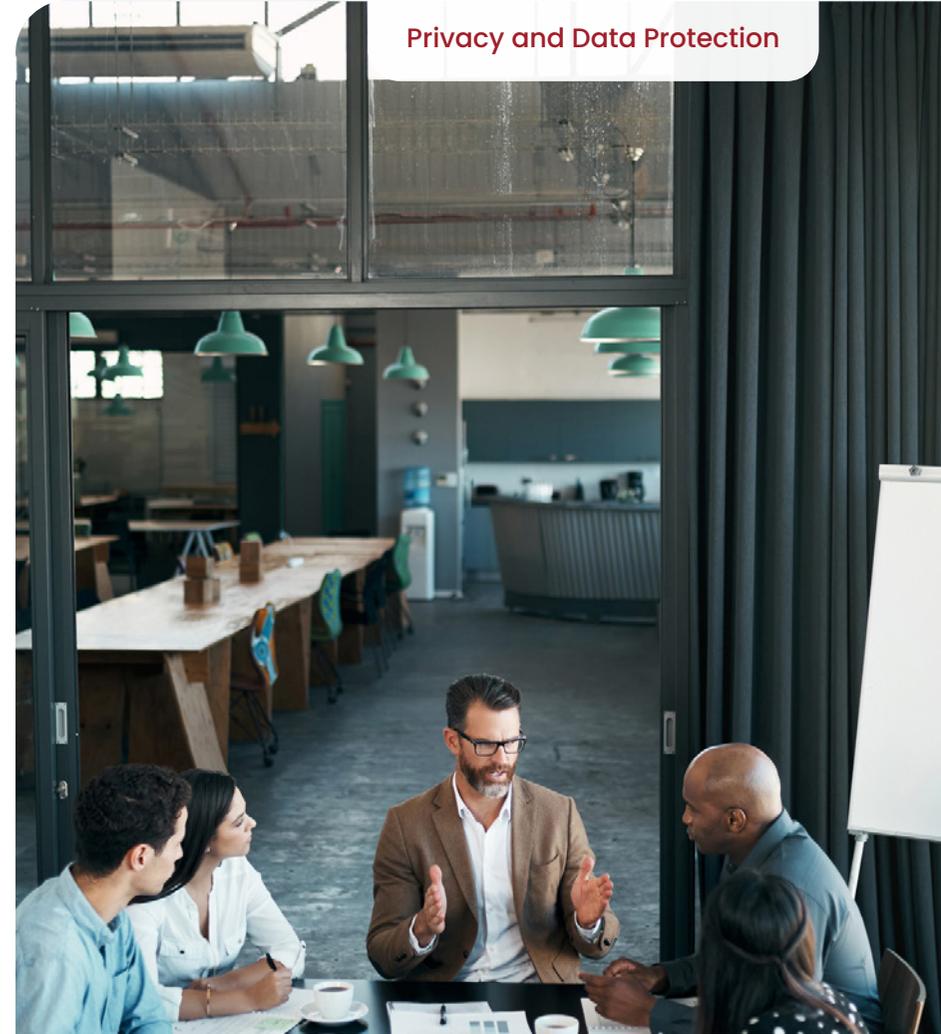
Founder of KEKELI ACADEMY

GDPR – Certified Data Protection Officer (CDPO)

Overview of CDPO and Its Certification Process

The GDPR – Certified Data Protection Officer (CDPO) certification validates expertise in data protection laws and practices under the EU General Data Protection Regulation (GDPR). Pursuing the GDPR – CDPO certification involves a thorough exploration of GDPR's requirements and the skills necessary to effectively manage data protection within an organization. This certification journey includes understanding the legal framework of GDPR, the rights of data subjects, the obligations of data controllers and processors, data protection impact assessments, and data breach response protocols.

According to CMS, as of 2025, GDPR enforcement remains active and intensified, with over EUR 5.65 billion in fines issued up to March 2025 for violations like insufficient legal basis for data processing and lack of transparency. The number of fines recorded is around 2,245, with an average fine of approximately EUR 2.36 million.



Benefits of CDPO Certification



Demonstrated Proficiency in GDPR



Critical Role in Data Protection



Increased Marketability



Career Enhancement



Training Course and Learning Objectives



GDPR Foundation

Learn the basic elements to implement and manage a compliance framework with regard to the protection of personal data

2 DAYS

GDPR – Certified Data Protection Officer

Obtain the skills and knowledge necessary to lead all the processes for implementing a GDPR compliance program in an organization

5 DAYS



Certified US Data Privacy

Overview of USDPO and Its Certification Process

The Certified US Data Privacy certification validates advanced proficiency in the regulatory landscape and governance practices shaping data privacy compliance in the United States. As state-level legislation rapidly expands, organizations need professionals who can interpret and implement requirements across major laws such as the CCPA/CPRA, VCDPA, CPA, CTDPA, and other emerging state statutes.

The US Data Privacy certification equips candidates with the skills to design and manage privacy programs that comply with federal guidance and diverse state regulations. It covers core areas of U.S. privacy compliance, including consumer rights, organizational obligations, data subject request handling, notice and transparency requirements, and the operational aspects of breach notification and incident response.

The program also builds strategic capabilities in privacy governance, program development, risk assessments, vendor management, and cross-functional coordination, competencies essential for strengthening privacy maturity across an organization.

Benefits of USDPO Certification



Strengthened Organizational Compliance Posture



Improved Readiness for Emerging State Privacy Laws



Enhanced Ability to Lead Privacy-by-Design Initiatives



Greater Credibility in Regulatory and Legal Interactions



Stronger Alignment Between Privacy, Security, and Risk Functions



Increased Capacity to Oversee Third-Party Privacy Risks



Improved Competence in Managing Data Subject Requests at Scale



Expanded Leadership Opportunities in Privacy Governance



Enhanced Trust from Customers, Partners, and Stakeholders

Coming Soon



Training Course and Learning Objectives



Certified US Data Privacy Officer

Build the expertise needed to confidently manage US privacy requirements, drive organizational compliance, and support effective data protection practices across the enterprise

5 DAYS

Why Choose a Career in Privacy and Data Protection?

- Critical in Safeguarding Personal and Sensitive Information
- Rapidly Expanding Field Due to Technological Advancements
- Highly Rewarding with Significant Impact on Business and Society



High-Paying Careers in Privacy and Data Protection

Chief Privacy Officer (CPO)

A senior executive role responsible for developing and implementing privacy policies and practices, ensuring compliance with data protection laws, and managing data privacy risks.

Annual Average Salary: **U.S. \$250,000**

Privacy Counsel

Provides legal expertise in privacy and data protection matters, advises on compliance with privacy laws, and handles privacy-related legal issues.

Annual Average Salary: **U.S. \$215,000**

Privacy Program Manager

Manages the development and execution of privacy programs, including policies, training, and compliance initiatives.

Annual Average Salary: **U.S. \$180,000**

Data Protection Officer (DPO)

Specializes in overseeing the data protection strategy and implementation to ensure compliance with GDPR and other data protection laws.

Annual Average Salary: **U.S. \$145,000**

Privacy Engineer

Develops and implements technical solutions and controls to ensure the privacy of personal data within IT systems and applications.

Annual Average Salary: **U.S. \$119,062**

Note: The salary data presented here have been sourced from [Glassdoor](#) and may be subject to change over time due to various factors.



At Cynthus, we value PECB as a strategic partner for advancing talent development across Latin America. Its portfolio of certifications, continuous content updates, and academic-commercial support enable us to design rigorous, relevant learning experiences for multiple industries. Thanks to PECB, our clients strengthen their management systems, make progress on compliance, and adopt internationally recognized best practices. I would also highlight the consistency of the assessments and the clarity of the guidelines for training centers, which ensure end-to-end quality. We are excited to embrace the new learning pathways in the 2026 PECB Training Catalog to continue delivering value to the region.

Cynthus
Mexico

AI AND DIGITAL TRANSFORMATION



Why Artificial Intelligence?

Artificial Intelligence (AI) is transforming industries by improving efficiency and automating tasks. It helps businesses make better decisions, reduce costs, and gain a competitive advantage. AI improves customer experiences and is driving change in sectors like healthcare, finance, and manufacturing. By solving complex problems and optimizing operations, AI is a key tool for success today.



Why Digital Transformation?

Digital transformation is essential for businesses to remain competitive. It uses technology to optimize processes, improve customer experiences, and drive innovation. By adopting digital tools, organizations can increase efficiency, adapt to market changes, and unlock new revenue opportunities.



ISO/IEC 42001 Artificial Intelligence Management System

Overview of ISO/IEC 42001 and Its Certification Process

The ISO/IEC 42001 certification equips professionals with the expertise to implement and maintain an artificial intelligence (AI) management system in line with international best practices. Pursuing an ISO/IEC 42001 certification immerses you in the complexities of AI management, where you will gain the ability to effectively plan, implement, manage, monitor, maintain, and continually improve an artificial intelligence management system (AIMS). This certification also focuses on the ethical, legal, and efficient application of AI, preparing you to play a pivotal role in the evolving landscape of AI technology.



Benefits of ISO/IEC 42001 Certification



Effective
AI Management



Enhanced
Credentials



Specialized
Expertise



Career
Advancement

[Learn more](#)



Training Course and Learning Objectives



ISO/IEC 42001 Foundation

Gain knowledge about the fundamental principles and concepts necessary to implement and manage an AIMS based on ISO/IEC 42001

2 DAYS

ISO/IEC 42001 Lead Implementer

Obtain the competencies needed to support an organization in implementing and maintaining an AIMS based on ISO/IEC 42001

5 DAYS

ISO/IEC 42001 Lead Auditor

Acquire the knowledge and skills to perform an AIMS audit by applying widely recognized audit principles, procedures, and techniques

5 DAYS

Certified Artificial Intelligence Professional (CAIP)[®]

Overview of CAIP and Its Certification Process

The Certified Artificial Intelligence Professional (CAIP) training course offers a thorough exploration of artificial intelligence by guiding you from its foundational ideas to cutting-edge methods and applications. You will learn how to gather and analyze data, build and refine machine learning models, and get into more advanced areas like deep learning, natural language processing, and even robotics. Completing this certification not only demonstrates your technical expertise but also highlights your commitment to shaping AI initiatives that are safe, compliant, and valuable for both businesses and society.



Benefits of Certified Artificial Intelligence Professional (CAIP) Certification



Master AI Fundamentals for Innovative Solutions



Improve Data Analysis and Machine Learning for Smarter Decisions



Advance in Deep Learning and NLP for Adaptability



Address Ethics and Compliance for Responsible AI Use

Learn more



Training Course and Learning Objectives



Certified Artificial Intelligence Professional (CAIP)

5 DAYS

Gain the knowledge and skills to explore foundational AI concepts, perform data analysis and visualization, build and evaluate machine learning models, and explore natural language processing (NLP) and deep learning techniques

In this training course, you will learn to apply ethical and regulatory frameworks, manage AI risk, and form governance strategies to ensure responsible and effective AI deployments

AI Risk Management

Overview of AI Risk Management and Its Certification Process

The AI Risk Management certification equips professionals with the capabilities required to oversee how AI systems are assessed, controlled, and monitored throughout the organization. It emphasizes the practical dimensions of managing AI-related exposure, from fairness and transparency considerations to security risks and operational integrity. Participants engage in structured applied components that reinforce how to identify risks, evaluate potential impacts, and establish measures that keep AI initiatives aligned with internal policies and external requirements. This certification builds proficiency in applying recognized frameworks, including the NIST AI Risk Management Framework and the EU AI Act, within day-to-day oversight.

The WEF Global Risks Report flags AI-driven misinformation and misuse among the most severe global risks in the short term, underscoring the increasing need for structured AI oversight and governance expertise.



Benefits of Lead AI Risk Manager Certification



Verified competence in AI risk assessment and oversight



Increased organizational confidence in responsible and compliant AI



Enhances the organization's ability to adopt AI solutions



Improved reliability of AI model performance



Stronger oversight across the full AI lifecycle



Training Course and Learning Objectives



Lead AI Risk Manager

Gain essential knowledge to identify, assess, and manage AI-related risks, with guidance from the NIST AI RMF, the EU AI Act, and the MIT AI Risk Repository

5 DAYS



As a trusted PECB partner, our collaboration is a cornerstone of our strategy to deliver top-tier information security training in the Nordic region. PECB's rigorous, standards-based training courses provide the technical and scientific depth we require, enabling us to equip professionals with actionable skills to build resilient ISMS and manage risk effectively. This partnership translates into direct business value for our clients: achieving compliance, building stakeholder trust, and securing a competitive edge. We eagerly anticipate integrating new offerings from the 2026 PECB catalog to continue empowering organizations with future-proof security expertise.

Dr. Gabriel Silva
Digital2me, Costa Rica

Certified AI Manager (CAIM)[®]

Overview of CAIM and Its Certification Process

The Certified AI Manager (CAIM) training course is designed for leaders, managers, and decision-makers who are responsible for shaping AI strategy, governance, and implementation within their organizations. This course provides a comprehensive journey from core AI concepts and global trends to practical frameworks for use-case identification, data readiness, risk management, and automation. Participants will examine real-world case studies, learn how to align AI initiatives with business objectives, and understand emerging regulatory requirements and ethical considerations.

They will also develop skills in data-driven decision-making using Power BI and explore how to design, govern, and deliver AI-powered automations with tools such as n8n. Completing this certification demonstrates your ability to lead AI programs responsibly, translate technical capabilities into business value, and manage AI projects across their full lifecycle, from idea to impact.



Benefits of CAIM Certification



Translate AI Concepts into Clear Business Value and Strategic Roadmaps



Strengthen AI Governance, Policy Development, and Regulatory Readiness



Improve Data-Driven Decision-Making Using Structured Analytics and Power BI



Enhance Ability to Identify, Prioritize, and Manage High-Impact AI Use Cases



Lead Responsible AI Automation Initiatives that Balance Innovation and Risk



Training Course and Learning Objectives



Certified AI Manager

CAIM equips managers to design and lead AI initiatives by aligning use cases with business strategy, establishing governance and risk controls, and promoting responsible data-driven decision-making

Participants also gain practical exposure to analytics and automation tools such as Power BI and n8n to translate AI capabilities into measurable organizational value

5 DAYS

Why Choose a Career in Artificial Intelligence (AI)?

- At the Core of Innovation and Automation
- Driving Competitive Advantage Across Industries
- High Demand and Excellent Earning Potential

Artificial Intelligence is transforming how organizations operate, make decisions, and deliver value. AI professionals are at the forefront of developing intelligent systems that enhance efficiency, accuracy, and innovation across sectors such as finance, healthcare, manufacturing, insurance, and cybersecurity.



High-Paying Careers in Artificial Intelligence

Machine Learning Engineer

Builds, trains, and optimizes machine learning models at scale, ensuring performance, reliability, and scalability in production environments.

Annual Average Salary: **U.S. \$170,000**

AI Engineer

Designs, develops, and deploys AI and machine learning models to solve complex business problems. This role requires strong skills in data science, algorithms, and system integration.

Annual Average Salary: **U.S. \$164,000**

AI Security Engineer

Focuses on securing AI and machine learning systems against adversarial attacks, data poisoning, model theft, and misuse of AI technologies.

Annual Average Salary: **U.S. \$145,000 – \$170,000**

Data Scientist (AI-Focused)

Analyzes large datasets to build predictive and prescriptive models that support AI-driven decision-making.

Annual Average Salary: **U.S. \$140,000**

Certified AI Auditor / AI Governance Specialist

Assesses AI systems for compliance, ethics, transparency, risk, and alignment with governance and regulatory requirements.

Annual Average Salary: **U.S. \$126,000**

Note: The salary data presented here have been sourced from [Glassdoor](#) and may be subject to change over time due to various factors.

Certified Digital Transformation Officer (CDTO)

Overview of CDTO and Its Certification Process

The Certified Digital Transformation Officer (CDTO) certification is a professional accreditation that focuses on equipping individuals with the skills and knowledge needed to lead and manage digital transformation initiatives in organizations.

Embarking on the CDTO certification path involves mastering a comprehensive set of skills critical for driving digital change in modern businesses. This certification covers strategic planning, the adoption of digital technologies, change management, digital culture cultivation, and innovation leadership.



Benefits of CDTO Certification



Networking
Opportunities



Leadership in
Digital Strategy



Enhanced
Career Profile



Future-Ready
Skills

[Learn more](#)



Training Course and Learning Objectives



Certified Digital Transformation Officer (CDTO)

Obtain the necessary skills and knowledge to lead and maintain digital transformation strategies in organizations

5 DAYS

Why Choose a Career in Digital Transformation?

- Enabling Organization-Wide Change
- Aligning Technology with Business Strategy
- Strong Demand at Leadership and Senior Levels

Digital transformation professionals lead the integration of digital technologies across business functions, reshaping operating models, customer experiences, and organizational culture. These roles combine strategic leadership with a strong understanding of technology, change management, and innovation.



High-Paying Careers in Digital Transformation

Chief Digital Officer (CDO)

A senior executive responsible for defining and executing the organization's digital strategy, driving innovation, and ensuring alignment between technology and business goals.

Annual Average Salary: **U.S. \$240,000**

Digital Transformation Director

Leads digital transformation initiatives across departments, overseeing technology adoption, process optimization, and organizational change.

Annual Average Salary: **U.S. \$185,000**

Enterprise Digital Architect

Designs enterprise-wide digital and technology architectures to support long-term transformation objectives.

Annual Average Salary: **U.S. \$155,000**

Digital Transformation Officer

Oversees the integration of digital technologies into business operations, improving efficiency, agility, and customer value delivery.

Annual Average Salary: **U.S. \$150,000**

Certified AI Auditor / AI Governance Specialist

Digital Transformation Consultant Advises organizations on digital strategy, technology implementation, and change management to support sustainable transformation.

Annual Average Salary: **U.S. \$140,000**

Note: The salary data presented here have been sourced from [Glassdoor](#) and may be subject to change over time due to various factors.



At Risk, Governance & Compliance Consulting, we believe that PECB training goes beyond the classroom, driving professional excellence. The quality and depth of the materials provided, along with the robustness of their certification process, ensures that each participant acquires real competencies applicable to today's challenges. Over the years, as both a partner and instructor, I have witnessed how PECB certifications transform participants' practice and perspective, while strengthening their confidence in their professional development.

Raúl Gonzáles

Risk, Governance & Compliance Consulting, Ecuador

GOVERNANCE, RISK, AND COMPLIANCE



Why Governance, Risk, and Compliance?

Governance, Risk, and Compliance (GRC) helps organizations achieve their goals while following ethical, legal, and regulatory standards.

It ensures accountability, manages risks continually, and fosters a culture of compliance, reducing legal issues and building stakeholder trust. GRC enables efficient, responsible, and maintainable operations in a complex business environment.



ISO 31000 Risk Management

Overview of ISO 31000 and Its Certification Process

The ISO 31000 certification is a globally recognized standard that signifies expertise in risk management principles and guidelines. The ISO 31000 certification process involves mastering a framework for effective risk management, suitable for all types of organizations. This certification journey encompasses understanding the principles, framework, and process of risk management, as outlined in the ISO 31000 standard.

According to Coherent Market Insights, the global Risk Management Market is estimated to be valued at U.S. \$14.93 billion in 2025 and is expected to reach U.S. \$40.20 billion by 2032, exhibiting a compound annual growth rate (CAGR) of 15.2% from 2025 to 2032.



Benefits of ISO 31000 Certification



Enhanced Professional Capabilities



Strategic Value



Enhanced Skills in Risk Management



Career Advancement

[Learn more](#)



Training Course and Learning Objectives



ISO 31000 Foundation

Gain knowledge on the main components of ISO 31000, its principles, and approaches to managing risks

2 DAYS

ISO 31000 Risk Manager

Acquire the skills and knowledge to implement risk management process and framework in an organization in accordance with the guidelines set out in ISO 31000

3 DAYS

ISO 31000 Lead Risk Manager

Develop the competence to successfully implement a risk management process and framework based on ISO 31000 and apply risk management principles aligned with the standard

5 DAYS

ISO/IEC 38500 IT Governance

Overview of ISO/IEC 38500 and Its Certification Process

The ISO/IEC 38500 certification is a credential that signifies expertise in corporate governance of information technology, providing guidelines for effective IT management and usage within organizations. Embarking on the ISO/IEC 38500 certification process involves gaining an in-depth understanding of the principles and best practices for IT governance. This certification journey covers key areas such as establishing a framework for effective IT governance, aligning IT with organizational goals, ensuring IT investments are wise and deliver value, and managing IT-related risks and compliance.



Benefits of ISO/IEC 38500 Certification



Effective
IT Governance



Increased
Influence in
Organizational IT
Strategy



Professional
Development



Commitment to
Standards
of IT Governance

[Learn more](#)



Training Course and Learning Objectives



ISO/IEC 38500 Foundation

Gain knowledge on the best industry practices of IT governance and its key principles

2 DAYS

ISO/IEC 38500 IT Corporate Governance Manager

Gain a thorough understanding of the core principles for good IT governance based on ISO/IEC 38500 and the implementation of an effective framework

3 DAYS

ISO/IEC 38500 Lead IT Corporate Governance Manager

Develop the skills and knowledge to successfully evaluate, implement, and monitor an IT governance model by following the guidelines of ISO/IEC 38500

5 DAYS

Note: The update of the training courses has been discontinued for the time being.

ISO 37000 Corporate Governance

Overview of ISO 37000 and Its Certification Process

The ISO 37000 standard provides guidance on corporate governance, enabling organizations to establish, develop, evaluate, and maintain effective governance practices. The ISO 37000 certification is a professional credential that validates your expertise in applying governance principles aligned with this international standard. It equips you with the knowledge to promote ethical leadership, ensure accountability, and drive sustainable performance.

By achieving this certification, you demonstrate your capacity to support organizations in integrating good governance practices into their operations, decision-making processes, and overall strategy, fostering transparency and stakeholder trust.



Benefits of ISO 37000 Certification



Proficiency in
Governance
Practices



Ethical
Decision-Making



Strengthened
Stakeholder Trust



Leadership
Opportunities

[Learn more](#)



Training Course and Learning Objectives



ISO 37000 Corporate Governance Manager

Obtain the necessary competencies to assist organizations in establishing, maintaining, and improving good governance based on ISO 37000

4 DAYS

ISO 37000 Lead Corporate Governance Manager

Obtain the necessary competence to establish, maintain, and improve good governance in organizations based on ISO 37000

5 DAYS

Note: The update of the training courses has been discontinued for the time being.

ISO 37001 Anti-Bribery Management System

Overview of ISO 37001 and Its Certification Process

ISO 37001 is a globally recognized standard that demonstrates an organization's commitment to implementing an effective anti-bribery management system (ABMS). Achieving ISO 37001 certification involves a comprehensive process of understanding and applying the standard for establishing, maintaining, and improving an ABMS. This certification journey includes learning about the principles and practices of bribery risk assessment, due diligence procedures, financial and non-financial controls, and implementing policies and procedures to combat bribery.



Benefits of ISO 37001 Certification



Validated
Competence
in Anti-Bribery
Management



Enhanced
Credibility



Improved
Job Opportunities



Increased
Marketability

[Learn more](#)



Training Course and Learning Objectives



ISO 37001 Foundation

Gain knowledge on the concepts and principles of an ABMS based on ISO 37001 and the structure and components of the standard

2 DAYS

ISO 37001 Lead Implementer

Become competent in successfully implementing and managing an ABMS based on ISO 37001

5 DAYS

ISO 37001 Lead Auditor

Develop the skills and expertise to audit an ABMS against the requirements of ISO 37001 and other audit best practices

5 DAYS

ISO 37001:2025 Transition

Understand the differences between ISO 37001:2016 and ISO 37001:2025 and acquire knowledge needed to align an ABMS with the updated standard

2 DAYS

ISO 37301 Compliance Management System

Overview of ISO 37301 and Its Certification Process

ISO 37301 is a certification for compliance management systems, providing guidelines to help organizations establish, develop, evaluate, and maintain an effective compliance management system. Achieving an ISO 37301 certification involves a systematic approach to understand and implement compliance standards within your organization. It begins with a thorough assessment of your existing compliance processes, identifying areas that need alignment with the ISO 37301 standard.



Benefits of ISO 37301 Certification



Commitment to Compliance



Increases Risk Mitigation Abilities



Culture of Integrity



Encourages Proactive Compliance

[Learn more](#)



Training Course and Learning Objectives



ISO 37301 Foundation

Understand the basic concepts of compliance and the requirements of ISO 37301 for a compliance management system (CMS)

2 DAYS

ISO 37301 Lead Implementer

Develop the competence necessary for the establishment, implementation, maintenance, and continual improvement of a compliance management system based on ISO 37301

5 DAYS

ISO 37301 Lead Auditor

Acquire the skills and knowledge necessary to conduct audits of compliance management systems based on ISO 37301 and the guidelines for auditing management systems provided in ISO 19011 and the certification process presented in ISO/IEC 17021-1

5 DAYS



My company became a partner with PECB in 2014. That year was a watershed year for me personally as it marked the beginning of a remarkable journey of unprecedented professional growth and development. Through my association with PECB as a partner I have gained credentials in a wide range of management system disciplines. As a PECB Certified Trainer, I have trained many persons who have gone on to become Certified Trainers themselves. Partnering with PECB has been the best opportunity for my company. We are recognized as having the capacity to offer cutting-edge knowledge and to enable employees at various levels to gain competencies that facilitate professional development and the capacity to add value to their organizations. I recommend partnering with PECB as the best choice for any organization that desires to be associated with a truly global company that is guided by ethical standards and believes in mutual development.

Jacob McLean

Principal Consultant and Lead Trainer at Kaizen Training and Management Consultants Limited (KTMC) – Jamaica

Management Systems Internal Auditor

Overview of Management Systems Internal Auditor and Its Certification Process

The CMSIA (Certified Management Systems Internal Auditor) certification is a professional accreditation that validates expertise in managing and conducting internal audits within organizations. Embarking on the CMSIA certification journey involves gaining a comprehensive understanding of the principles and practices of internal auditing. This certification process covers key areas such as audit planning and execution, risk assessment, compliance checks, report writing, and communication skills.



Benefits of Management Systems Certification



Expertise in
Internal Audits



Operational
Efficiency



Enhanced Auditing
Skills



Leadership
Opportunities in Audit
and Governance Sectors

[Learn more](#)



Training Course and Learning Objectives



Certified Management Systems Internal Auditor

Develop the necessary skills to plan and conduct management systems internal audits

3 DAYS



As an official partner of PECB, Deming Training Center is proud to collaborate with one of the most recognized certification bodies in the world in the fields of ISO management systems, information security, sustainability, and professional development. Through this partnership, we have been able to offer our learners and corporate clients internationally recognized certifications that strengthen their expertise, credibility, and employability in an increasingly demanding global market. The support, professionalism, and responsiveness of the PECB team are exemplary. The quality of the training materials, the rigor of the examinations, and the integrity of the certification process perfectly align with our values. We look forward to continuing this fruitful collaboration with PECB and contributing together to the development of world-class competencies.

Omar Ait Ouakha

PECB Certified Trainer and Director at Deming Training Center

Certified Management Systems Consultant (CMSC)

Overview of CMSC and Its Certification Process

The Management Systems Consultant Certification (CMSC) validates your expertise in consulting and supporting organizations to establish, optimize, and sustain effective management systems. Rooted in proven principles, this certification demonstrates your mastery of industry-leading methodologies and your commitment to elevating the quality of consultancy services. It proves that you possess the necessary expertise to guide organizations through the complexities of implementing and maintaining management systems, highlighting your proficiency to deliver strategic and effective solutions tailored to organizational needs.



Benefits of CMSC Certification



Enhanced
Consulting
Skills



Expertise in
Management
Systems



Improved
Client Value
Delivery



Better Networking
Opportunities

Coming Soon



Training Course and Learning Objectives	
Management Systems Consultant Foundation Become familiar with and gain an understanding of the basic theoretical and practical concepts of management systems consultancy	2 DAYS
Certified Management Systems Consultant Develop the skills and gain the necessary knowledge to interpret and implement management system consultancy practices	5 DAYS

ISO/TS 31050 Emerging Risks

Overview of ISO/TS 31050 and Its Certification Process

ISO/TS 31050 is a forward-looking guidance standard focused on the identification, assessment, and management of emerging risks in a rapidly evolving global environment. The ISO/TS 31050 certification process equips professionals with the knowledge and competencies needed to anticipate future threats, evaluate complex and interconnected risks, and support organizations in building resilience. This certification involves learning how to apply emerging risk principles, develop structured risk-forecasting approaches, and integrate these practices into organizational decision-making to ensure preparedness in uncertain and dynamic contexts.



Benefits of ISO/TS 31050 Certification



Advanced
Emerging-Risk
Competence



Enhanced
Future-Threat
Anticipation



Improved
Organizational
Resilience



Recognition in
Emerging-Risk
Management



Training Course and Learning Objectives



ISO/TS 31050 Emerging Risk Manager

Obtain the necessary competencies to support organizations in identifying, analyzing, and understanding emerging risks based on ISO/TS 31050

2 DAYS

Why Choose a Career in GRC?

- Rapidly Evolving Field
- Essential Roles in Modern Business
- Diverse and Impactful Career Paths



High-Paying Careers in GRC

Chief Risk Officer (CRO)

Responsible for overseeing the organization's risk management strategies, identifying potential risks, and ensuring compliance with laws and regulations.

Annual Average Salary: **U.S. \$260,000**

Risk Management Director

Directs risk management policies and programs, identifying and analyzing risks that could impact the organization.

Annual Average Salary: **U.S. \$170,000**

GRC Program Manager

Manages the overall governance, risk, and compliance program, coordinating across different departments to ensure alignment with strategic goals.

Annual Average Salary: **U.S. \$150,000**

IT Governance, Risk, and Compliance Manager

Specializes in managing GRC issues related to information technology, including cybersecurity risks and IT governance frameworks.

Annual Average Salary: **U.S. \$155,000**

Compliance Officer

Oversees the compliance function, ensuring the organization adheres to legal standards and internal policies.

Annual Average Salary: **U.S. \$125,000**

Note: The salary data presented here have been sourced from [Glassdoor](#) and may be subject to change over time due to various factors.



The Quality Institute of the Bureau of Standards Jamaica (QI BSJ) has proudly partnered with PECB for several years. This collaboration has significantly enhanced the credibility and visibility of our training institute, providing a competitive edge through a comprehensive range of ISO-related training programs. This partnership has expanded our capacity to serve professionals across Jamaica's business sectors, thereby strengthening our role in promoting a culture of quality, operational efficiency, and continuous improvement. Through PECB's support and resources QI BSJ is able to deliver high-quality, internationally aligned training that consistently meets global standards. This relationship has been instrumental in strengthening our reputation and expanding our reach both locally and regionally through their globally recognized certifications. The Quality Institute at the Bureau of Standards Jamaica (QI BSJ) would strongly recommend partnering with PECB, as their trusted support and vast resources will help strengthen clients' confidence and satisfaction. Partnering with PECB enables organizations to expand their market reach and offer training courses that meet internationally recognized benchmarks.

Bureau of Standards Jamaica (BSJ)
Jamaica

QUALITY, HEALTH, SAFETY AND SUSTAINABILITY



Why Quality and Management?

Quality and management are essential for organizations to keep consistency, satisfy customers, and improve operations. Effective management ensures efficient resource use and goal achievement, while a focus on quality ensures high standards. Combining both of them helps improve processes, drive innovation, and foster continuous improvement, leading to a competitive edge, improved reputation, and enduring success aligned with business goals and customer needs.



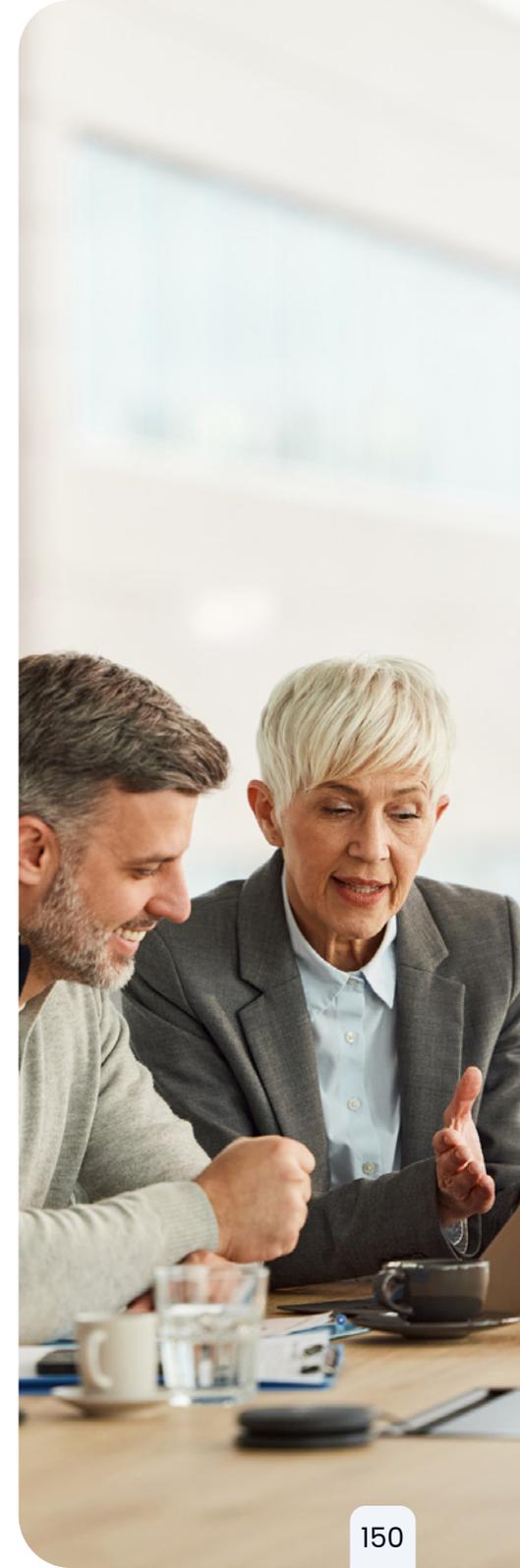
Why Health and Safety?

Health and safety are important for protecting employees, reducing risks, and ensuring legal compliance. A strong safety culture prevents accidents, increases productivity, and employee morale. By prioritizing health and safety, organizations minimize legal and financial risks while improving their reputation for responsible and ethical practices.



Why Sustainability?

Sustainability is fundamental to long-term environmental, social, and economic health. It helps reduce resource consumption, minimize waste, and address climate challenges, while improving efficiency and reputation. Sustainable practices drive innovation and ensure a better future equally for businesses and communities.



ISO 9001 Quality Management System

Overview of ISO 9001 and Its Certification Process

ISO 9001 is an internationally recognized standard that specifies requirements for a quality management system (QMS), focusing on consistent performance and customer satisfaction. Embarking on the ISO 9001 certification journey means diving into the principles of quality management that are universally applicable to any organization, regardless of size or industry. This certification process involves understanding and applying the ISO 9001 standards' requirements, which include establishing a strong customer focus, the commitment of top management, the process approach, and continual improvement.



Benefits of ISO 9001 Certification



Demonstrates Expertise in Quality Management



Career Advancement in Management and Leadership Roles



Increased Credibility



Career Flexibility

Learn more



Training Course and Learning Objectives



ISO 9001 Foundation

Gain knowledge on the basic elements to implement and manage a QMS as specified in ISO 9001, as well as the requirements of the standard

2 DAYS

ISO 9001 Lead Implementer

Develop the skills and competence to support an organization in implementing, managing, and maintaining a QMS based on ISO 9001

5 DAYS

ISO 9001 Lead Auditor

Develop the skills and competence to perform an ISO 9001 audit of an organization's QMS by applying widely recognized audit principles, procedures, and techniques

5 DAYS

ISO 21502 Project Management

Overview of ISO 21502 and Its Certification Process

ISO 21502 is a standard that provides guidelines for effective project management, enhancing the efficiency and success rate of projects in various industries. Embarking on the journey to achieve the ISO 21502 certification involves mastering the comprehensive principles and practices of project management as outlined in the standard. This process covers a range of key areas including project planning, execution, monitoring, control, and closure. It emphasizes the importance of effective communication, stakeholder engagement, risk management, and resource allocation in managing projects successfully. The certification process also highlights the need for adaptability and responsiveness to changes in the project scope or objectives.



Benefits of ISO 21502 Certification



Successful Project Delivery



Demonstrates Expertise in Project Management



Increased Competitiveness



Equips You with the Latest Project Management

[Learn more](#)



Training Course and Learning Objectives



ISO 21502 Foundation

Learn the best practices for the management of projects, as well as the key concepts and processes related to it

2 DAYS

ISO 21502 Lead Project Manager

Acquire the expertise to lead an organization and its team to implement, manage, and maintain projects based on ISO 21502

5 DAYS



Since 2010, Behaviour Brasil has proudly served as the pioneering representative of PECB in Brazil. Over the years, we have certified a vast number of professionals who have become benchmarks in their respective industries, contributing to the advancement of excellence in organizational management across the country. Our partnership with PECB is built on trust, ethics, and a shared commitment to quality. Behaviour Brasil has positioned itself as the leading PECB partner in Brazil, offering the most extensive portfolio of ISO training courses. This achievement is a direct result of PECB's outstanding ability to maintain a comprehensive and up-to-date repository of ISO management system standards. PECB stands out as an ethical, responsible, and dedicated organization, deeply committed to its partners, certified professionals, and the organizations it serves. Professionals and companies holding PECB certifications are highly regarded in the market, benefiting from the credibility of an internationally recognized and accredited certification body. We are confident that our partnership with PECB will continue to generate meaningful and lasting impact on professional and organizational development throughout Latin America.

Fábio Anjos and Luciane Oliveira

CEO and Training and Development at Behaviour Brasil

ISO 28000 Supply Chain Security Management System

Overview of ISO 28000 and Its Certification Process

ISO 28000 is a global standard for supply chain security management systems, designed to enhance security processes and mitigate risks in supply chains. Embarking on the ISO 28000 certification journey entails gaining a comprehensive understanding of supply chain security management principles. This certification process involves learning how to implement and manage a security system that addresses potential security threats at various stages of the supply chain. Key components of the certification include risk assessment, development of security policies, planning and implementing security measures, and emergency response protocols.



Benefits of ISO 28000 Certification



Industry
Recognition in
Supply Chain
Security and Risk
Management



Operational
Efficiency in Supply
Chain



Global
Opportunities



Increased Potential for
Leadership Roles

[Learn more](#)



Training Course and Learning Objectives



ISO 28000 Foundation

Learn the best practices that contribute to the implementation of a supply chain security management system as required by ISO 28000

2 DAYS

ISO 28000 Lead Implementer

Gain the knowledge and skills to support an organization in establishing, implementing, and managing a supply chain security management system

5 DAYS

ISO 28000 Lead Auditor

Develop the skills and knowledge to perform SCSMS audits against the requirements of ISO 28000

5 DAYS

ISO 28000:2022 Transition

Understand the differences between ISO 28000:2007 and ISO 28000:2022 and acquire knowledge on the new concepts, requirements, and recommendations

5 DAYS

Note: The update of the training courses has been discontinued for the time being.

ISO 13485 Medical Devices Quality Management System

Overview of ISO 13485 and Its Certification Process

The ISO 13485 certification is a specialized standard that demonstrates compliance with quality management systems for the design and manufacture of medical devices. The journey to achieving an ISO 13485 certification involves gaining an in-depth understanding of the requirements for a comprehensive quality management system specific to the medical device industry. This certification process includes learning about the standards for designing, developing, producing, and delivering medical devices that consistently meet both customer and regulatory requirements.



Benefits of ISO 13485 Certification



Job Market Advantage



Increased Credibility in Medical Device Design



Validates Expertise for Medical Device Industry



Career Advancement

[Learn more](#)



Training Course and Learning Objectives



ISO 13485 Foundation

Acquire knowledge on the best industry practices for implementing an MDQMS based on ISO 13485

2 DAYS

ISO 13485 Lead Implementer

Develop the skills necessary to support an organization in implementing, managing, and maintaining an MDQMS based on ISO 13485

5 DAYS

ISO 13485 Lead Auditor

Develop the necessary skills to perform an MDQMS audit by applying widely recognized audit principles, procedures, and techniques

5 DAYS

Note: The update of the training courses has been discontinued for the time being.

ISO/IEC 17025 Laboratory Management System

Overview of ISO/IEC 17025 and Its Certification Process

ISO/IEC 17025 is an international standard that specifies the general requirements for the competence, impartiality, and consistent operation of laboratories. Embarking on the ISO/IEC 17025 certification process involves a deep understanding of laboratory operations and the ability to implement a quality management system. This certification covers critical areas such as technical competence, equipment calibration, testing methodologies, quality control, and reporting accuracy.

According to Imarc, the global calibration services market is expected to grow from U.S. \$6.2 billion in 2024 to U.S. \$9.2 billion by 2033 – underscoring the growing importance of accredited testing and calibration laboratories.



Benefits of ISO/IEC 17025 Certification



Business Opportunities



Enhanced Expertise in Managing a Laboratory



Increased Trust



Enhanced Credibility

Learn more



Training Course and Learning Objectives



ISO/IEC 17025 Foundation

Gain knowledge on the main components to implement an LMS as specified in ISO/IEC 17025

2 DAYS

ISO/IEC 17025 Lead Implementer

Develop the skills and knowledge to assist a laboratory in successfully implementing, managing, and maintaining an LMS based on the requirements of ISO/IEC 17025

5 DAYS

ISO/IEC 17025 Lead Assessor

Become skilled in assessment techniques and lead an ISO/IEC 17025 certification audit

5 DAYS

Note: The update of the training courses has been discontinued for the time being.



Alcodefi is very satisfied with the partnership established with PECB. The certified training courses we offer through this collaboration fully meet our clients' expectations and enhance the quality of our offerings. They bring real added value in terms of international recognition, professional development, and the upskilling of participants. We look forward to continuing this fruitful collaboration.

Salem Tigzrine
Managing Director at ALCODEFI

ISO/IEC 20000 IT Service Management System

Overview of ISO/IEC 20000 and Its Certification Process

ISO/IEC 20000 is an international standard that demonstrates excellence and proves best practices in IT service management. Achieving ISO/IEC 20000 certification involves a deep understanding and compliance with the standards of IT service management (ITSM). This journey includes mastering the principles of designing, implementing, operating, monitoring, and improving an ITSM system. You will learn about aligning IT services with business needs, managing and delivering services effectively, and improving service quality continuously.

According Grand View Research, the global IT services market size was estimated at U.S. \$1.50 trillion in 2024 and is projected to reach U.S. \$2.59 trillion by 2030, growing at a CAGR of 9.4% from 2025 to 2030.



Benefits of ISO/IEC 20000 Certification



Aligns IT Services
with Business
Goals



Validates the
Ability to Manage
IT services



Operational
Improvements



Higher Earning
Potential

[Learn more](#)



Training Course and Learning Objectives



ISO/IEC 20000 Foundation

Gain knowledge on the principles and processes of IT SMS implementation

2 DAYS

ISO/IEC 20000 Lead Implementer

Develop the skills and competence to implement and manage an IT SMS based on ISO/IEC 20000

5 DAYS

ISO/IEC 20000 Lead Auditor

Develop the skills and acquire the knowledge to plan and conduct IT SMS audits against the ISO/IEC 20000 requirements

5 DAYS



Partnering with PECB has strengthened our credibility and expanded our global footprint in ISO management and information security auditing. Through this collaboration, we've gained access to world-class certification programs, consistent audit methodologies, and a trusted framework that elevates the quality of our services. PECB's expertise has helped us deliver globally recognized, value-driven compliance and governance solutions. We highly recommend PECB for their integrity, professionalism, and commitment to excellence. Their globally recognized certification ecosystem empowers organizations to grow with confidence and credibility. Partnering with PECB means joining a community that truly defines and advances best practices in auditing, risk management, and compliance.

ISMPP
USA

Six Sigma Belts

Overview of Six Sigma Belts and Its Certification Process

The Six Sigma certification is a quality management certification that validates expertise in identifying and eliminating defects or inefficiencies in business processes using statistical methods. Embarking on a Six Sigma certification journey means delving into a systematic approach to process improvement through problem-solving and statistical analysis. The certification typically includes different belt levels – Yellow, Green, Black, and Master Black – each representing a deeper level of understanding and practical application of the Six Sigma methodology.



Benefits of Six Sigma Certification



Improves
Professional
Skills



Enhances Job
Market Appeal



Demonstrates
Expertise in Process
Improvement



Increases Cross-
Industry Value

[Learn more](#)



Training Course and Learning Objectives



Six SIGMA Green Belt

Develop the technical knowledge and skills to improve processes in an organizational setting

5 DAYS

ISO 21001 Educational Organizations Management System

Overview of ISO 21001 and Its Certification Process

ISO 21001 is a global standard focused on educational organizations management systems (EOMS), providing requirements and guidelines for delivering and improving educational services. Achieving ISO 21001 certification involves a deep understanding of the EOMS by encompassing learning on how to effectively apply the standard's requirements to enhance the quality of education and align educational services with learners' needs. It covers areas such as curriculum development, teaching methods, assessment processes, and learning resource management.



Benefits of ISO 21001 Certification



Improved Educational Quality



Increased Student Satisfaction



Leadership Opportunities in Educational Management



Reputation Boost for Educators and Institutions

Learn more



Training Course and Learning Objectives



ISO 21001 Foundation

Learn the main concepts and principles of an EOMS based on ISO 21001

2 DAYS

ISO 21001 Lead Implementer

Develop the necessary skills to support an organization in implementing and managing an EOMS based on ISO 21001

5 DAYS

ISO 21001 Lead Auditor

Gain the skills and knowledge to perform an ISO 21001 audit by applying widely recognized audit principles, procedures, and techniques

5 DAYS

ISO 55001 Asset Management System

Overview of ISO 55001 and Its Certification Process

ISO 55001 is an international standard for asset management systems, specifying requirements for the effective management of assets throughout their lifecycle. Pursuing an ISO 55001 certification involves gaining a thorough understanding of the principles and practices of asset management. This certification process includes learning how to develop, implement, maintain, and improve an asset management system (AMS), ensuring that assets are managed and utilized as effectively as possible.



Benefits of ISO 55001 Certification



Expertise Validation
in Effective Asset
Management



Career
Advancement
Opportunities



Enhanced
Asset Utilization
Capabilities



Global Recognition
of ISO 55001
Competencies

[Learn more](#)



Training Course and Learning Objectives	
ISO 55001 Foundation Understand the main concepts and elements needed to implement and manage an asset management system in accordance with ISO 55001	2 DAYS
ISO 55001 Lead Implementer Develop the skills and knowledge required to support an organization in implementing, managing, and improving an asset management system (AMS) based on ISO 55001 requirements	5 DAYS
ISO 55001 Lead Auditor Become competent to perform audits of an AMS against the requirements of ISO 55001 and to manage a team of auditors	5 DAYS
ISO 55001:2024 Transition Understand the differences between ISO 55001:2014 and ISO 55001:2024 and acquire knowledge of the updated concepts, requirements, and recommendations	2 DAYS

Why Choose a Career in Quality & Management?

- Essential for Ensuring High Standards and Efficiency
- Key to Continuous Improvement in Organizations
- Career Path with Diverse Opportunities and Financial Rewards



High-Paying Careers in Quality and Management

Quality Management Director

Oversees quality management systems, policies, and procedures, ensuring compliance with industry standards and regulations.

Annual Average Salary: **U.S. \$174,824**

Data Quality Manager

Ensures data is accurate, consistent, and reliable across the organization by implementing data quality standards and governance practices that support compliance and informed decision-making.

Annual Average Salary: **U.S. \$139,122**

Quality Assurance Manager

Manages and coordinates quality assurance efforts, focusing on maintaining product or service quality.

Annual Average Salary: **U.S. \$132,294**

Quality Manager

Responsible for developing, implementing, and overseeing quality systems and continuous improvement initiatives.

Annual Average Salary: **U.S. \$125,434**

Quality Control Manager

Leads quality control inspections, testing, and procedures to ensure products meet required specifications.

Annual Average Salary: **U.S. \$107,132**

Note: The salary data presented here have been sourced from [Glassdoor](#) and may be subject to change over time due to various factors.



Partnering with PECB has been an extremely positive and rewarding experience for Nash Partner Training Ltd. The PECB team is consistently supportive, responsive, and professional, making collaboration both smooth and productive. PECB's extensive catalog of globally recognized training courses has allowed us to offer our clients training that is highly relevant to today's business environment and individual professional development needs. These programs have strengthened our capacity to deliver high-quality, internationally accredited training across the Caribbean and Latin America. We highly recommend partnering with PECB to any organization seeking a trusted provider of high-quality training solutions that embody quality, integrity, and continuous improvement.

Nash Partner Training Ltd
Jamaica

ISO 45001 Occupational Health and Safety Management System

Overview of ISO 45001 and Its Certification Process

ISO 45001 is an international standard that provides a framework work for an effective occupational health and safety management system. Embarking on the ISO 45001 certification journey involves mastering the principles of occupational health and safety management. This process covers comprehensively assessing workplace hazards, implementing effective risk mitigation strategies, and promoting a safe and healthy work environment. The certification focuses on the proactive management of health and safety risks, employee training, and the continuous improvement of safety practices.

According to International Labour Organization, U.S. \$361 billion could be saved globally by implementing improved safety and health measures to prevent injuries from excessive heat in the workplace.



Benefits of ISO 45001 Certification



**Increases
Professional Value**



**Increases the
Capability to
Manage an HSMS**



**Opens up Career
Advancement
Opportunities**



Validates Expertise

[Learn more](#)



Training Course and Learning Objectives



ISO 45001 Foundation

Learn the main steps and elements to implement and manage an OH&S MS based on ISO 45001

2 DAYS

ISO 45001 Lead Implementer

Develop the skills and knowledge necessary to implement, manage, and maintain an OH&S MS based on ISO 45001

5 DAYS

ISO 45001 Lead Auditor

Develop the necessary skillset to perform OH&S MS audits by applying widely recognized audit principles, procedures, and methods

5 DAYS

ISO 22000 Food Safety Management System

Overview of ISO 22000 and Its Certification Process

ISO 22000 is an international standard that specifies the requirements for a food safety management system (FSMS), ensuring safe food production and supply chains. Embarking on ISO 22000 certification involves a comprehensive journey through the principles of food safety management. This certification process includes understanding and implementing critical elements such as hazard analysis, operational prerequisite programs (OPRPs), critical control points (HACCP), and effective food safety policies.



Benefits of ISO 22000 Certification



Demonstrated Proficiency in Managing Food Safety Risks



Strengthened Professional Reputation



Commitment to Quality



Employer Appeal

[Learn more](#)



Training Course and Learning Objectives



ISO 22000 Foundation

Gain knowledge on the main elements and key industry practices for implementing an FSMS based on ISO 22000

2 DAYS

ISO 22000 Lead Implementer

Develop the skills and knowledge to successfully implement, manage, and maintain an FSMS based on the requirements of ISO 22000

5 DAYS

ISO 22000 Lead Auditor

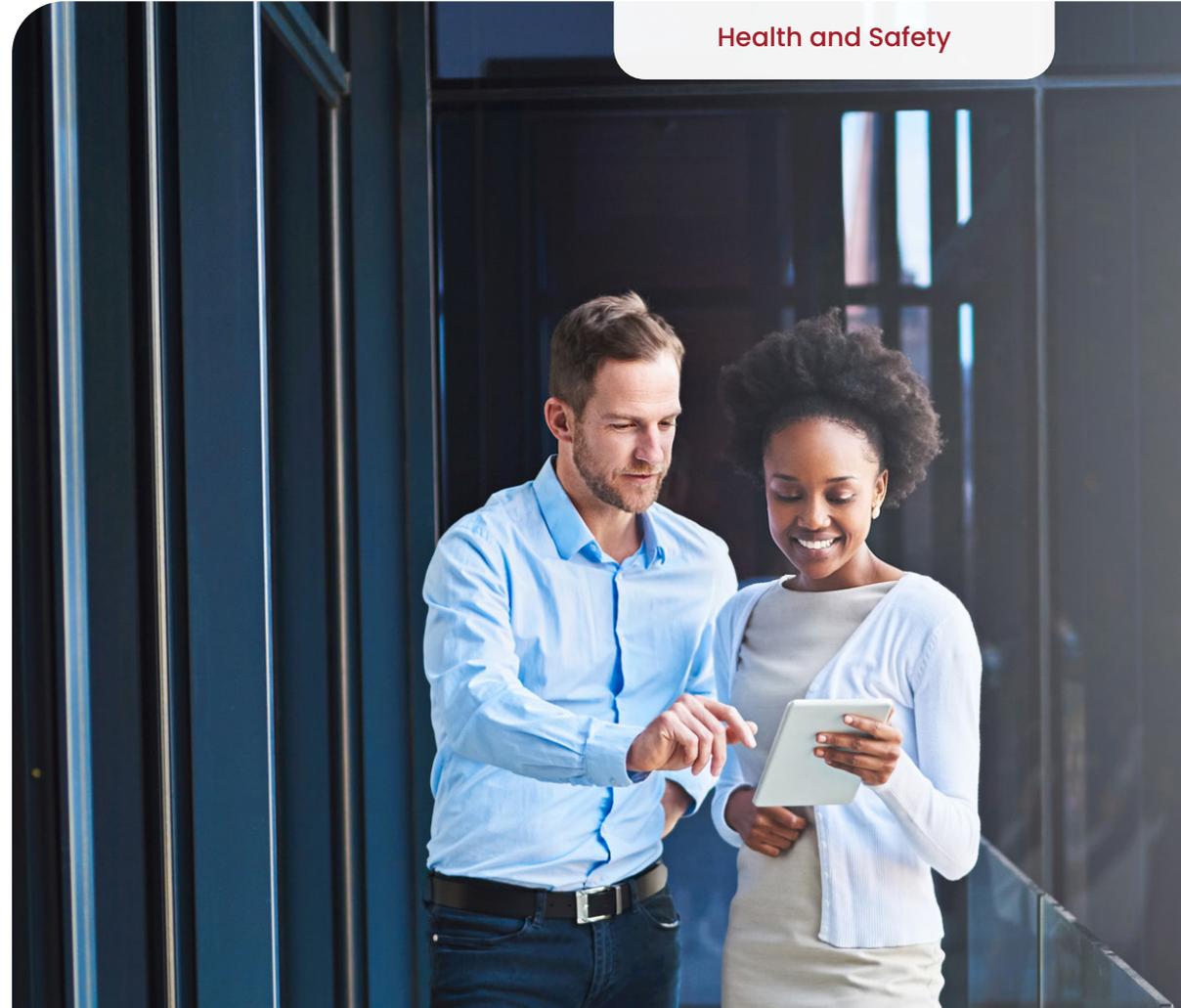
Master the audit techniques to successfully conduct FSMS audits in accordance with ISO 22000 requirements

5 DAYS

ISO 18788 Security Operations Management System

Overview of ISO 18788 and Its Certification Process

The ISO 18788 certification provides a framework for establishing, implementing, operating, monitoring, reviewing, and improving the management of security operations. Embarking on the ISO 18788 certification journey entails acquiring a comprehensive understanding of the management system for private security operations. This certification process involves learning how to develop and implement policies and procedures that align with the protection of human rights, ensure quality and ethical business practices, and support security operations consistency.



Benefits of ISO 18788 Certification



Enhanced Knowledge for Private Security Operations



Professional Credibility



Adherence to Standards



Validates Ability to Manage Security Operation

[Learn more](#)



Training Course and Learning Objectives



ISO 18788 Foundation

Become acquainted with the fundamentals of a SOMS and best practices to implement and manage one, based on ISO 18788

2 DAYS

ISO 18788 Lead Implementer

Develop the skills and knowledge to support an organization in implementing, managing, and maintaining a SOMS based on ISO 18788

5 DAYS

ISO 18788 Lead Auditor

Develop the necessary skills to perform a SOMS audit by applying widely recognized audit principles, procedures, and techniques

5 DAYS

Note: The update of the training courses has been discontinued for the time being.

Why Choose a Career in Health and Safety?

- Crucial for Ensuring Workplace Safety and Health Standards
- Vital in Preventing Injuries and Occupational Hazards
- Profession with Rewarding Impact and Financial Benefits



High-Paying Careers in Health and Safety

Environmental, Health, and Safety Director

Leads the strategic planning and implementation of health and safety policies to ensure a safe working environment.

Annual Average Salary: **U.S. \$140,000**

Chief Safety Officer (CSO)

Responsible for overseeing comprehensive safety policies and programs across an organization.

Annual Average Salary: **U.S. \$150,000**

Health and Safety Manager

Manages and coordinates health and safety programs, ensuring compliance with laws and regulations.

Annual Average Salary: **U.S. \$100,000**

Environmental Health and Safety Manager (EHS Manager)

Oversees programs to ensure environmental, health, and safety compliance in the workplace.

Annual Average Salary: **U.S. \$108,000**

Occupational Health and Safety Specialist

Focuses on identifying and mitigating workplace hazards, conducting safety training, and ensuring regulatory compliance.

Annual Average Salary: **U.S. \$85,000**

Note: The salary data presented here have been sourced from [Glassdoor](#) and may be subject to change over time due to various factors.



Partnering with PECB has been a great relationship. The PECB/Arrakis partnership has expanded our company footprint in new international directions, as well as bringing in new training students into the PECB fold. Additionally, as Arrakis is primarily a consulting firm with a training division and numerous managed services, the ability to directly reference PECB training and valid ISO documentation as underlying reference material greatly supports our consultation process. In a nutshell, partnering with PECB is well worth the effort, you won't regret the professionalism and support they provide.

Arrakis Consulting
USA

ISO 5001 Energy Management System

Overview of ISO 5001 and Its Certification Process

ISO 5001 is an international standard that specifies requirements for establishing, implementing, maintaining, and improving an energy management system. Embarking on the ISO 5001 certification journey entails mastering a framework for efficient energy management within organizations. This process involves understanding the principles of energy management, including the development of an energy policy, setting achievable energy targets, and designing action plans to reach these goals.



Benefits of ISO 5001 Certification



Improved Energy Efficiency



Enhanced Professional Value



Compliance Assurance



Cost Savings

[Learn more](#)



Training Course and Learning Objectives



ISO 50001 Foundation

Learn the main elements to implement and manage an EnMS

2 DAYS

ISO 50001 Lead Implementer

Gain the skills and knowledge to support an organization in establishing, implementing, managing, and maintaining an EnMS

5 DAYS

ISO 50001 Lead Auditor

Acquire the knowledge and skills to plan and conduct EnMS audits by applying widely recognized audit principles, procedures, and techniques

5 DAYS

Note: The update of the training courses has been discontinued for the time being.

ISO 14001 Environmental Management System

Overview of ISO 14001 and Its Certification Process

ISO 14001 is an internationally recognized standard for environmental management systems (EMS), focusing on sustainable practices and reducing environmental impact. Embarking on the ISO 14001 certification journey involves a comprehensive understanding of environmental management systems and their implementation. This process includes learning how to develop, maintain, and continually improve an EMS, ensuring it effectively manages environmental aspects and impacts associated with organizational activities.



Benefits of ISO 14001 Certification



Sustainability
Commitment



Professional
Credibility in
Environmental
Stewardship



Competitive
Advantage



Demonstrated Ability to
Manage Environmental
Performance

[Learn more](#)



Training Course and Learning Objectives



ISO 14001 Foundation

Gain knowledge on the main elements to implement and manage an EMS as specified in ISO 14001

2 DAYS

ISO 14001 Lead Implementer

Acquire the necessary knowledge for supporting an organization in implementing, managing, and maintaining an EMS as specified in ISO 14001

5 DAYS

ISO 14001 Lead Auditor

Develop the necessary skills to perform a SOMS audit by applying widely recognized audit principles, procedures, and techniques

5 DAYS



IGP Perú and PECB: United for Global Excellence. At IGP Perú, we are committed to driving our clients' growth through high-impact training that strengthens their professional and organizational development. Our partnership with PECB reinforces this mission by combining their internationally recognized certification expertise with our training experience to deliver programs that enhance talent, competitiveness, and management standards. Together, we work to provide world-class education that inspires, transforms, and contributes to the sustainable progress of organizations.

IGP
Perú

ISO 26000 Social Responsibility Management System

Overview of ISO 26000 and Its Certification Process

The ISO 26000 standard is a guideline on social responsibility that helps organizations operate ethically and transparently which contributes to the health and welfare of society. Embarking on the ISO 26000 certification journey involves understanding and integrating social responsibility into an organization's values and practices. This process includes learning about the principles of social responsibility, such as ethical behavior, transparency, respect for stakeholder interests, and environmental sustainability.



Benefits of ISO 26000 Certification



Strengthens CSR Expertise



Supports Sustainability Goals



Stakeholder Engagement



Enhanced Ability in Ethical Practice Guidance

[Learn more](#)



Training Course and Learning Objectives



ISO 26000 Foundation

Learn the best practices for guiding organizations to operate in a socially responsible way

2 DAYS

ISO 26000 Lead Manager

Gain comprehensive knowledge and skills in the field of Social Responsibility, as outlined in the ISO 26000 standard

5 DAYS



With PECB's partnership, SMATICA has been able to provide world-class training and certification with global recognition for our clients. PECB is now a leading name among personal certification bodies, trusted by both government and private sector clients when they need their employees certified in ISO standards and the latest trending technologies. PECB has a rewarding reseller program, with a pathway to success recognition for training providers.

SMATICA LLC
USA

ISO 20400 Guidelines for Sustainable Procurement

Overview of ISO 20400 and Its Certification Process

ISO 20400 is a standard for sustainable procurement, guiding organizations in making procurement processes socially, economically, and environmentally sustainable. Embarking on the ISO 20400 certification journey involves gaining a comprehensive understanding of sustainable procurement principles and practices. This process covers strategies for integrating sustainability into procurement policies, decision-making processes, and throughout the supply chain.



Benefits of ISO 20400 Certification



Expertise in Sustainable Procurement



Decision-Making Power



Professional Credibility



Contributes to Organizational Sustainability

[Learn more](#)



Training Course and Learning Objectives



ISO 20400 Lead Manager

Help organizations integrate sustainability into their procurement policies and practices

5 DAYS

Note: The update of the training courses has been discontinued for the time being.

ISO 56001 Innovation Management System

Overview of ISO 56001 and Its Certification Process

ISO 56001 is an international standard that provides requirements and guidance for establishing, implementing, maintaining, and continually improving an innovation management system (IMS). The certification process equips professionals with the knowledge and competencies needed to drive structured innovation, support organizational creativity, and ensure sustainable value creation. This certification involves learning how to apply innovation management principles, develop innovation processes, and integrate innovation practices into strategic and operational activities across an organization.



Benefits of ISO 56001 Certification



Structured
Innovation
Capability



Enhanced
Organizational
Creativity



Improved
Innovation
Governance



Strengthened
Value-Creation
Processes



Training Course and Learning Objectives



ISO 56001 Foundation

Understand the fundamental concepts, principles, methods, and techniques used for the implementation and management of an innovation management system (IMS)

2 DAYS

ISO 56001 Lead Implementer

Acquire the ability to support an organization in planning, implementing, managing, monitoring, and maintaining an innovation management system (IMS) based on ISO 56001

5 DAYS

ISO 56001 Lead Auditor

Develop the knowledge and skills needed to perform an ISO 56001 certification audit based on audit best practices and methodologies

5 DAYS

Why Choose a Career in Sustainability?

- Critical to Addressing Environmental Challenges
- Growing Demand in Various Industries
- Offers Opportunities to Make a Positive Impact on the Planet and Society



High-Paying Careers in Sustainability

Chief Sustainability Officer (CSO)

Top executive role responsible for incorporating eco-friendly practices into an organization's strategy and operations.

Annual Average Salary: **U.S. \$170,000**

Director of Sustainability

Oversees and implements sustainability initiatives and programs across an organization.

Annual Average Salary: **U.S. \$150,000**

Environmental Program Manager

Manages environmental programs, focusing on sustainability goals and environmental impact.

Annual Average Salary: **U.S. \$115,000**

Sustainability Consultant

Advises businesses on developing and executing strategies for sustainable practices.

Annual Average Salary: **U.S. \$92,000**

Sustainability Analyst

Analyzes and reports on an organization's sustainability performance and develops strategies to improve it.

Annual Average Salary: **U.S. \$70,000**

Note: The salary data presented here have been sourced from [Glassdoor](#) and may be subject to change over time due to various factors.



The new training and certification services catalog clearly reflects an understanding of market trends and the evolving needs of organizations. Its focus on competency development and skill accreditation adds significant value, ensuring professionals who are highly qualified, competent, and aligned with today's workplace demands.

César Augusto Duque
CEO at CIRECOM, Dominican Republic

myPECB – Leading in a New Era of Personalized Digital Experiences

In its commitment to innovation and excellence, PECB has launched **myPECB**, a personalized, centralized platform designed to elevate user experience and streamline access to PECB's services.

This advancement provides an intuitive, efficient, and engaging digital journey for our global community, ensuring that every interaction with PECB is simple, seamless, and user-centric.

Introducing **myPECB** – Your All-in-One Digital Hub

- Access **personalized dashboards** tailored to their specific role
- Manage **training records, course materials, certificates, and exam results** with ease
- Stay informed through **real-time updates** on course availability and upcoming events

Access **myPECB**

The image displays two overlapping screenshots of the myPECB platform. The top screenshot shows a user dashboard for 'Johni' with three summary cards: '12 Courses Available', '12 Renewals', and '4 Certificate Applications'. Below these is a grid of course cards, each with a status indicator and a 'View' button. The bottom screenshot shows the 'Certificate Applications' page, which includes a search bar and a table of application records.

COURSE	SUB LEVEL	STATUS
GDPR - Certified Data Protection Officer	Provisional Officer	Rejected
ISO 20400 Lead Manager	Lead Manager	Revoked
ISO/IEC 27001 Lead Auditor	Provisional Auditor	Rejected
GDPR - Certified Data Protection Officer	Provisional Officer	Revoked
ISO 20400 Lead Manager	Lead Manager	Rejected
ISO/IEC 27001 Lead Auditor	Provisional Auditor	Revoked

A Redesigned Website for a Modern User Experience

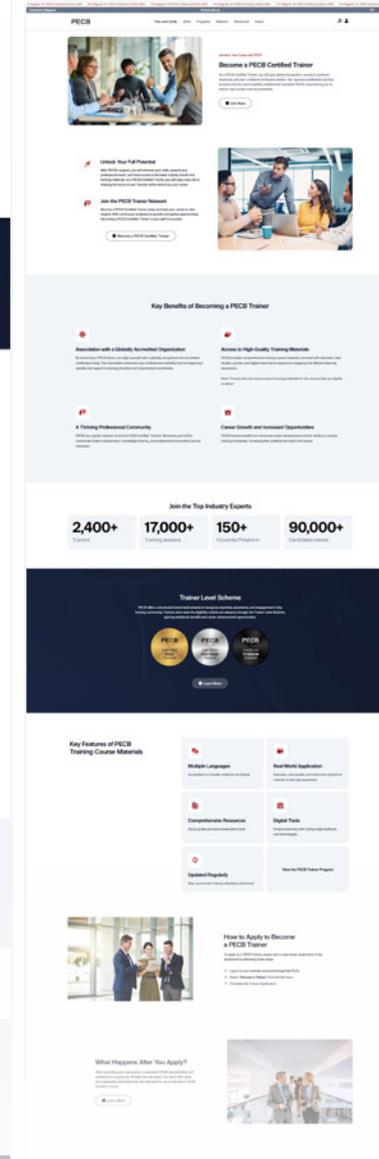
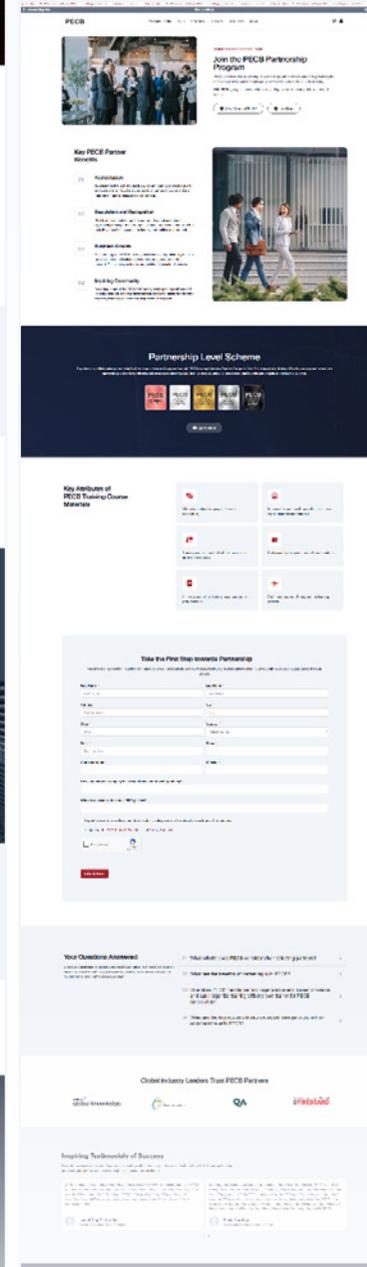
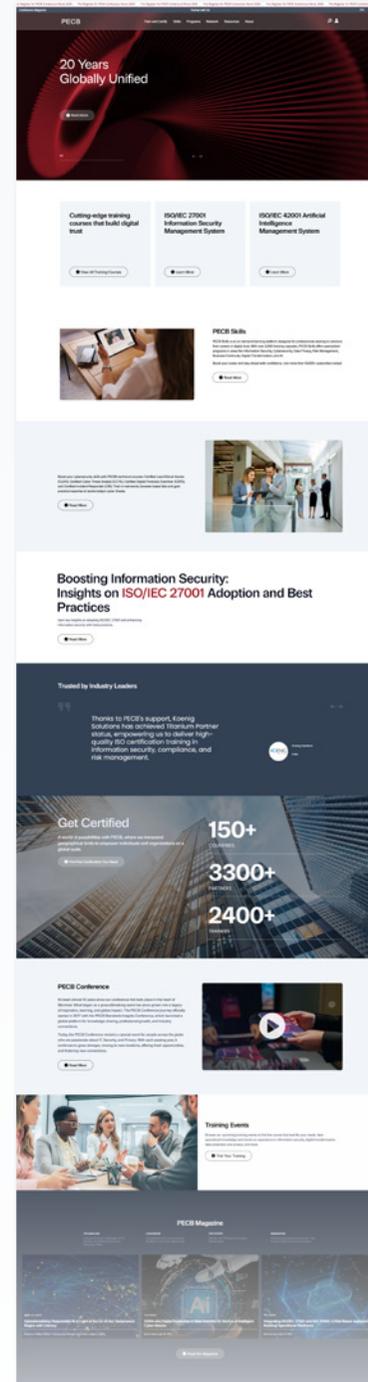
Complementing the launch of *myPECB* is our fully revamped PECB website, offering a faster, cleaner, and more intuitive browsing experience. The updated design ensures:

- Enhanced navigation for quick and easy access to information
- Improved structure and speed for an uninterrupted experience
- A modernized look and feel that reflects our forward-thinking vision

A Commitment to Continuous Innovation

Whether managing certifications, enrolling in training, or discovering more about PECB's services, the redesigned website is made to simplify and enhance the experience every step of the way.

Explore the new website



PECB Skills

Advancing digital trust competence, one skill at a time.

PECB Skills is a dynamic micro-learning platform designed for auditors, implementers, and managers in Information Security, AI, Privacy, and Data Governance who need fast and practical, standards-based training.

Why Choose PECB Skills?

Expert-Led Learning:

Access a comprehensive library of 4,000+ interactive video capsules delivered by leading industry experts.

Accredited Certification:

Gain certificates with selected ANAB-accredited competency programs to showcase your expertise.

Interactive Experience:

Engage with dynamic lessons, quizzes, and practical activities.

Flexible Learning:

Tailored for industry professionals, business leaders, educators, and teams.

Comprehensive Topics:

Explore a broad spectrum of subjects, including Information Security, Risk Management, GDPR, AI, Cybersecurity, CMMC compliance, and more.

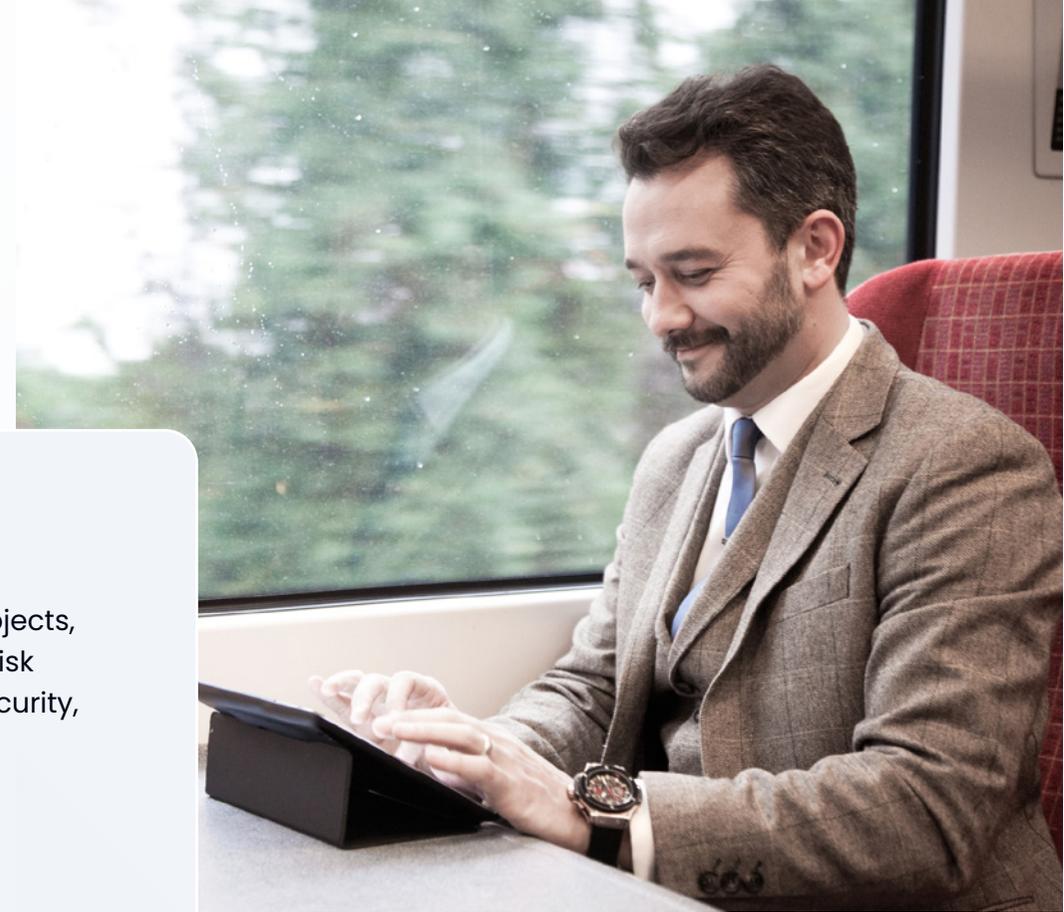
Structured Roadmap:

Follow a clear path from capsules to modules and competency certificates.

CPD Credits: Master essential skills in a 4-hour program, earn 4 CPD credits.

Progress Tracking:

Monitor your learning journey with intuitive analytics.

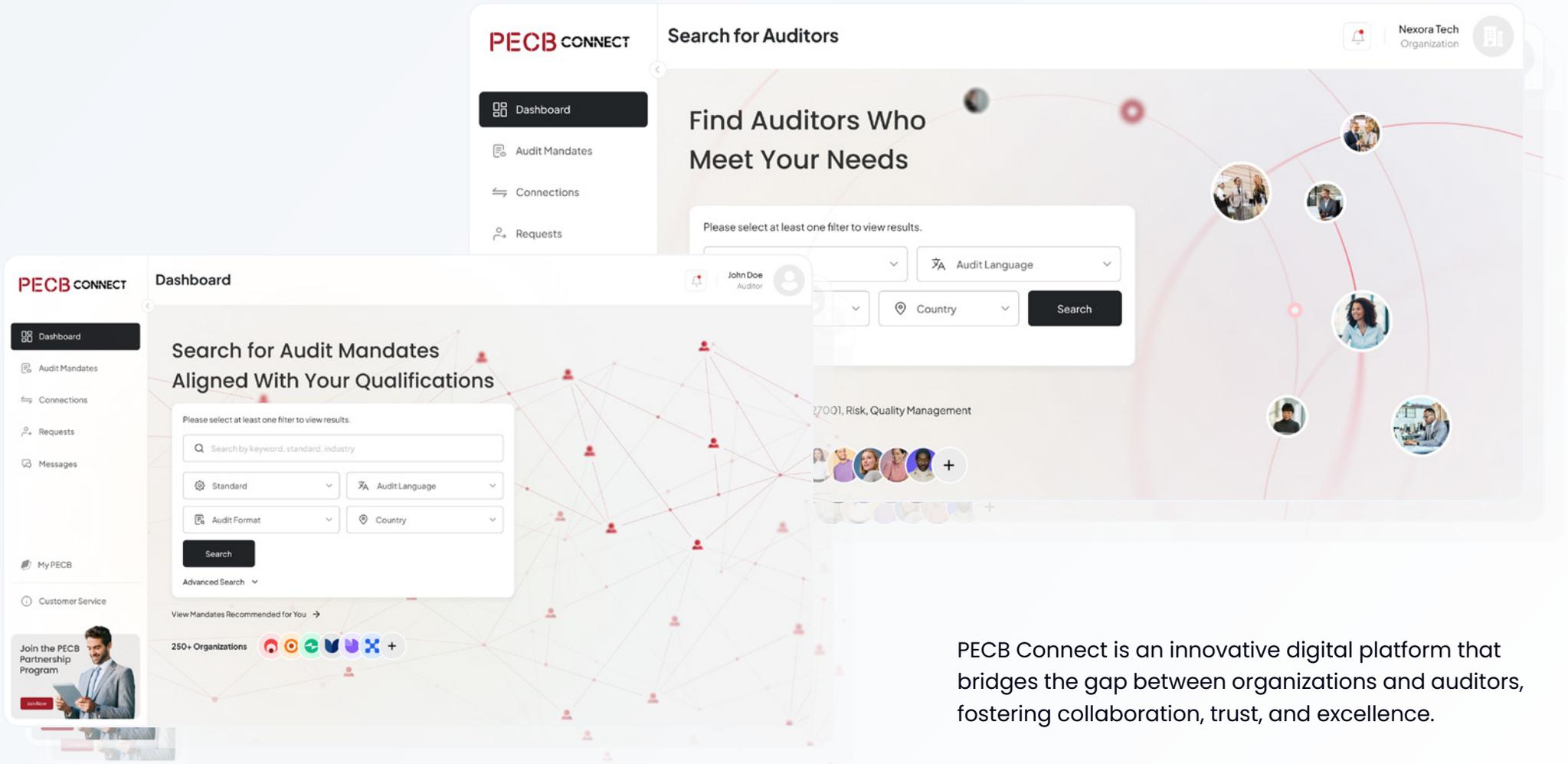


PECB Skills combines cutting-edge content with a user-friendly platform to offer a seamless learning experience. Whether you're advancing your career, gaining certifications, earning CPDs, or deepening your expertise, PECB Skills is your partner in professional development.

[Explore Now](#)

PECB Connect

Bridging Auditors and Organizations



PECB Connect is an innovative digital platform that bridges the gap between organizations and auditors, fostering collaboration, trust, and excellence.

Built on the Certified Management Systems Auditor (CMSA) framework, PECB Connect provides a transparent, efficient way to connect, collaborate, and complete audits globally.

Why Join PECB Connect?

FOR ORGANIZATIONS

Easily find and connect with qualified auditors who meet your organization's needs. Join PECB Connect to simplify the process of finding professionals for certification, compliance, or internal audits.

Here's what you can expect:

- Access to Auditors: Connect with auditors who are trained, certified, and vetted, ensuring the highest level of competence and professionalism.
- Simplified Auditor Search: Use advanced filters to identify auditors based on standards, experience, region, or industry, ensuring a perfect fit for each audit mandate.
- Support for Accreditation & Compliance: PECB Connect helps organizations in the accreditation process by providing easier access to auditor documentation for compliance purposes. This simplifies record-keeping and facilitates regulatory reporting.
- Centralized Platform: Manage all auditor connections, communications, and audit mandates in one place. Find relevant and qualified auditors easily for each mandate.

To join as an Organization, click [here](#).

FOR AUDITORS

PECB Connect is a platform designed to help auditors connect with organizations that need auditing services.

Whether you are an experienced auditor or just starting your career, this platform provides access to available auditing projects and to organizations seeking professionals to conduct audits.

Here's how you benefit:

- Increased Visibility: Auditors gain exposure to a wider network of organizations seeking auditing services.
- Access to a Global Network: PECB Connect connects auditors with organizations worldwide, enabling them to expand their reach and collaborate on a global scale.
- Targeted Opportunities: Auditors receive tailored opportunities based on their expertise, location, language, and other criteria, making it easier to find relevant audit mandates.
- Simplified Process for Job Matching: The platform's structured system streamlines the matching of auditors with organizations seeking specific expertise, saving time for both parties.

PECB Connect offers both organizations and auditors a trusted, efficient, and collaborative environment to enhance the certification ecosystem and drive continuous professional excellence.

To join as an auditor, click [here](#).

Examination and Certification

Examination is the pivotal step in the PECB certification journey, and our exams are crafted to evaluate your critical thinking and problem-solving skills.

Available worldwide through esteemed partners and distributors, we offer two convenient formats to cater to your needs:

- Online
- Paper-based



PECB Exam Types

a) Multiple-choice, closed-book, where the candidates are not allowed to use any reference materials. Usually, Foundation and Transition exams are of this type.

b) Essay-type, open-book, where candidates are allowed to use the following reference materials:

- A hard copy of the main standard
- Training course materials (printed)
- Any personal notes taken during the training course (printed)
- A hard copy dictionary

c) Multiple-choice, open-book, where candidates are allowed to use the following reference materials:

- A hard copy of the main standard
- Training course materials (printed)
- Any personal notes taken during the training course (printed)
- A hard copy dictionary

Exams are provided electronically via the PECB Exams application. The use of secondary electronic devices, such as tablets and phones, is not allowed during the exam. The exam session is supervised remotely by a PECB Invigilator via the PECB Exams application and an external/integrated camera.

Note: Essay-type open-book exams are being phased out in favor of multiple-choice open-book exams. Open-book exams feature scenario-based questions that evaluate candidates' ability to apply, analyze, and evaluate information effectively.

Depending on the type of examination scheme, the duration of the exam varies:

Foundation Exams	1 hour
Manager Exams	2 hours
Lead Exams	3 hours
Technical Cybersecurity Exams	6 hours

Note: Both online and paper-based exams have the same duration as noted above

To begin the process and attend our training courses, you can:

- Find a training course provider in your region by checking our [Partners List](#).
- Sign up for a PECB training course and exam from our [Event Schedule](#).
- Check the list of [PECB Exams](#).

IMPORTANT: When preparing for the exam, please refer only to our official website for candidate handbooks and exam information. Please avoid using unofficial exam dumpsites or any unauthorized third-party sources. Using such materials can result in severe consequences, including, but not limited to, not accepting the exam as valid or revoking certifications.

PECB Certification Rules and Policies

Each PECB certification has a set of requirements.

Candidates are required to complete the online Certification Application Form and all other online forms, including the contact details of references who will be contacted to validate the candidates' professional experience.

For more information, please visit the [Certification Rules and Policies](#) page.



PECB Certification Maintenance Policy

PECB Certifications are valid for three-year.

To maintain a certification, PECB certified professionals must comply with the following requirements:

- Submit Continuing Professional Development (CPD) credits
- Pay Annual Maintenance Fees (AMFs)
- Adhere to the PECB Code of Ethics

To be able to renew a certification, PECB certified professionals will need to demonstrate that they are maintaining their certifications by submitting CPDs and AMFs throughout the three-year certification cycle.

Upon meeting these requirements, your certification will be renewed at the end of the third year.

Note: *The CNIL certification has different renewal requirements. The following credentials do not require maintenance: Foundation, Provisional, and Transition.*

For more information, please visit [Certification Maintenance Policy](#).



AMF Discount

To make AMF payments easier and more manageable, we offer the following benefits:

10% Discount for Early Payment

You can choose to pay for three years of AMFs in advance and receive a 10% discount. This way, you'll avoid annual payments for the next three years.

AMF Cap

Regardless of how many certifications you hold, you will only be required to pay AMFs for a maximum of **five certificates per year.**



eLearning

A Custom-Made Exclusive Platform to Fit Your Learning Style

PECB's eLearning platform offers customized online training courses designed to accommodate various learning styles and lifestyles. This digitalized teaching method enhances efficiency and quality of learning, catering to different preferences. It provides access to comprehensive training course materials developed with input from professionals and experienced trainers across various fields.



Why Choose PECB's eLearning?

24/7 Access to Training Courses

Learn at your own pace, anytime, anywhere—no more worries about schedules, travel, or work commitments.

Expert-Curated Content

Benefit from materials developed by professionals with real-world experience in their fields.

Concise 20-Minute Video Lessons

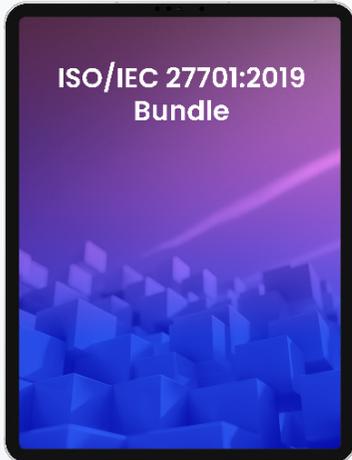
Short, focused modules designed to make learning easier and improve retention.

Unlimited Training Course Materials

Access comprehensive learning resources, available whenever you need them for reference or revision.

Entirely Online

Train, study, and even take examinations without leaving the comfort of your home.



ISO/IEC 27701:2019 Bundle

The ISO/IEC 27701 Bundle includes a toolkit, standard, and introductory training course by PECB.

[Shop Now](#)

\$665

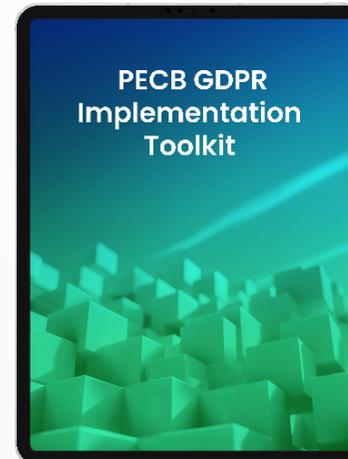


ISO/IEC 27001:2022 Standard

Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

[Shop Now](#)

\$143



PECB GDPR Implementation Toolkit

This Toolkit offers effective strategies for assigning roles and meeting data privacy requirements efficiently.

[Shop Now](#)

\$495

Discover What's Inside the PECB Store

Explore and purchase top-quality resources, from toolkits and eBooks to thousands of ISO and IEC standards, to support your training and professional growth.

Access everything instantly, right from your *myPECB* dashboard.

- One login
- One central hub
- One seamless journey

[myPECB](#)



 +1-844-426-7322

 support@pecb.com

 www.pecb.com