



IT Audit Bootcamp

By the *Institute of Internal Auditors Belgium*



What we offer

IIA Belgium's IT Audit Bootcamp is a comprehensive training program designed for non IT audit professionals seeking to deepen their understanding of IT audit principles and practices. This program is structured into 10 distinct modules, spanning across various training sessions. Each module focuses on a specific area of IT audit, ensuring a thorough and well-rounded educational experience.

How it works

We recommend you to follow the complete IT Audit Bootcamp experience, which includes all the modules, ensuring you get a deep dive into the world of IT audit. Alternatively, you have the flexibility to register for individual modules that best fit your learning needs. Please consider to attend the [Introduction to IT audit: Understanding & Auditing Business Processes' risks related to IT](#) before registering for the [IT Audit Bootcamp](#) or any other individual module. [This course is designed to provide foundational knowledge and context that will be essential for all subsequent modules within the IT Audit Bootcamp.](#) Make sure to register separately for that course as it's not included in the ITAB . Abstain if you have some basic knowledge of IT General Controls and you exceed the prerequisites of that course.

Target Audience

The program is uniquely tailored for non-IT auditors or beginner/intermediate IT auditors. It assumes no prior IT audit experience, making it accessible to a broad range of professionals including auditors, who wish to gain IT audit competencies.

Location & Time

The introduction course will be delivered as a 2-day training. The other modules will be delivered as half-day sessions, with one session scheduled in the morning



and another in the afternoon. All modules will be conducted in person at our IIA Belgium offices.

Pricing

- Register for the entire IT Audit Bootcamp for **€ 2.250** (you benefit from a total discount of **-25%**). If you follow the trainings separately, fees vary according to the length of the training. Members always enjoy reduced prices. An early-bird discount is also applicable.

To register for the IT Audit Bootcamp, please click on the button below. If you have any questions or require further assistance, don't hesitate to [contact us](#). We look forward welcoming you to the IT Audit Bootcamp and supporting your professional growth. See you in class!

Register today!

Why attend the IT-Audit Bootcamp?

- **Broaden Knowledge:** Gain comprehensive insights into the various aspects of IT auditing.
- **Career Advancement:** Enhance your professional qualifications and career prospects in the field of IT auditing.
- **Practical Skills:** Acquire practical skills through case studies and real-world scenarios.
- **Networking Opportunities:** Connect with peers and experts in the field.
- **Stay Relevant:** Keep up-to-date with the latest trends and technologies in IT audit.
- **Professional Recognition:** Add value to your professional profile.



Meet our expert Trainers



Gauthier Brun is a Senior Manager in Information Systems Audit at Toyota Motor Europe with over 12 years' experience in IT auditing. Gauthier is an expert in SOX integration, operational audits (including cybersecurity, data protection, identity and access management, business continuity, etc.), and a leader in the adoption of the agile approach to internal auditing. In parallel, he is an official trainer for IFACI and IIA Belgium, bringing extensive expertise in IT auditing, risk management, SOX audits, and much more. Formerly with PwC for 9 years, with a solid experience in auditing IT systems and processes.



Francisco Ríos is an experienced internal audit manager with a Master's in Mathematics and over two decades of experience across telecom, finance, and IT. He combines deep technical expertise with critical thinking to deliver impactful audits and training. Certified in CIA, CISA, CRISC, Agile, MSP and ITIL amongst others, Francisco is passionate about using data analytics to enhance audit quality and organizational resilience.



Mark Dekeyser is an Audit professional involved at the Institute of Internal Auditors. Prior to that he was Audit Methodologist and IT Auditor at KBC Group. He obtained CISA and is also member of ISACA. At IIA he is involved as a coordinator and facilitator of the Master Classes. He's also teaching Risk Based Auditing, Auditing Cyber Security, Auditing Corporate Governance and several Data Analysis courses. He's involved in advocacy teaching at universities in Belgium, and he's also performing Audit Quality Assessments in various sectors and industries.

General Information

Description	
Title	Title of the event
Duration	Duration of the event
Price	Early bird/non-early member prices*
Facilitator	Name of the facilitator
Date	Date of the event

Level	Description
Beginner	IT Audit experience < 2Yr
Intermediate**	IT audit experience 2Yr - 5Yr
Expert	IT audit experience > 5Yr

*VAT is not included

**Providing that you have attended the Introduction to IT audit: Understanding & Auditing Business Processes' risks related to IT or exceed the prerequisites .



Overview of Training Events

Title	Duration	Price	CPE Points	Facilitator	Date	Level
Introduction to IT audit: Understanding & Auditing Business Processes' risks related to IT*	2 Days	€1200/1400	14 CPE	G. Brun	12-13/03/2026	Beginner
Module 1 - IT Governance and Compliance and IT regulatory framework	1/2 Day	€300/350	4 CPE	F. Ríos	20/03/2026	Intermediate
Module 2 - IT Risk Management Essentials	1/2 Day	€300/350	4 CPE	F. Ríos	20/03/2026	Intermediate
Module 3 - Fundamentals of IT Infrastructure: Hardware and Software Essentials	1/2 Day	€300/350	4 CPE	M. Dekeyser	27/03/2026	Beginner
Module 4 - Understanding IT Networks: Assessing Connectivity and Ensuring Security	1/2 Day	€300/350	4 CPE	M. Dekeyser	27/03/2026	Intermediate
Module 5 - Cybersecurity Fundamentals for Non-IT Auditors: A Practical Approach	1/2 Day	€300/350	4 CPE	M. Dekeyser	24/04/2026	Intermediate
Module 6 - Navigating Disruptive Technologies: A Guide for Business Auditors	1/2 Day	€300/350	4 CPE	M. Dekeyser	24/04/2026	Intermediate

*Please consider to attend this course before registering for the IT Audit Bootcamp or any other individual module. This course is designed to provide foundational knowledge and context that will be essential for all subsequent modules within the IT Audit Bootcamp. Make sure to register separately for that course as it's not included in the ITAB . Abstain if you have some basic knowledge of IT General Controls and you exceed the prerequisites of that course.

The Institute of Internal Auditors Belgium | 5

Overview of Training Events

Title	Duration	Price	CPE Points	Facilitator	Date	Level
Module 7 - Understanding the IT Environment and its core processes	1/2 Day	€300/350	4 CPE	F. Ríos	22/05/2026	Intermediate
Module 8 - Automated Business Processes and Application Controls	1/2 Day	€300/350	4 CPE	F. Ríos	22/05/2026	Intermediate
Module 9 - Data, Databases, Big Data, Encryption, Anonymization	1/2 Day	€300/350	4 CPE	M. Dekeyser	05/06/2026	Intermediate
Module 10 - Business Continuity Management (BCM) and Disaster Recovery Planning (DRP)	1/2 Day	€300/350	4 CPE	M. Dekeyser	05/06/2026	Intermediate

Introduction to IT audit: Understanding & Auditing Business Processes' risks related to IT*



G. Brun

€1200/1400

2 Days

12-13/03/2026

Beginner

14 CPE

Overview

This training is tailored for internal auditors, providing them with essential knowledge and practical skills to understand and assess IT General Controls (ITGC) within the context of business risks. The course focuses on presenting the major IT general controls, ensuring participants can detect and identify key controls even without any technical knowledge.

Target Audience

This program is designed for internal auditors (IT or non-IT), internal controllers, risk managers, IT staff, seeking a practical understanding of ITGCs within the broader context of business risk. No advanced technical IT knowledge is required.

Course Objectives

As internal auditors, you are required to understand basics of those risks, detect them and identify applicable key controls even if you aren't a technical IT specialist.

IT General Controls (ITGC) are controls that apply to all systems, components, processes, and data for a given organization.

This training aims to place these ITGCs in a business risk perspective, which requires internal auditors to develop an understanding of Information Technology, business insights and audit techniques.

Course Content

- **Information and technology:** introduction, IT governance and frameworks.
- **IT challenges and risks:** IT risks.
- **IT planning & organisation:** organisation structure, enterprise architecture, data management, third party management, innovation.
- **IT controls:**
 - IT general controls (access management, change management, etc.).
 - IT solution life cycle: project management and development life cycle.
 - IT operations: IT infrastructure, Network & client/server, ITIL service management: incident, business continuity, etc.
 - IT application controls,
 - Integrated audit.
- **IT frameworks:** ISO 27001 information security, COBIT, ITIL, etc.

Prerequisites

- None. Foundation course. No advanced technical IT knowledge is required. Participants are encouraged to actively engage in quizzes, discussions, and practical exercises to reinforce their understanding of ITGCs within the broader context of business risk.

Register

*Please consider to attend this course before registering for the IT Audit Bootcamp or any other individual module. This course is designed to provide foundational knowledge and context that will be essential for all subsequent modules within the IT Audit Bootcamp. Make sure to register separately for that course as it's not included in the ITAB. Abstain if you have some basic knowledge of IT General Controls and you exceed the prerequisites of that course.

IT Governance, Compliance, and Regulatory Framework

F. Ríos

€300/350

1/2 Day

20/03/2026

Intermediate

4 CPE



Overview

This training is strategically designed to seamlessly integrate the topics of IT Governance, Compliance, and the IT Regulatory Framework. Auditors will explore how IT operations align with strategic objectives while adhering to relevant regulations. The training empowers participants to evaluate the effectiveness of IT policies, procedures, and controls, measure compliance with industry standards, and navigate the complexities of the IT regulatory landscape.

Target Audience

This training is made for auditors, compliance professionals, and individuals responsible for ensuring IT governance and regulatory adherence. Participants should have a basic understanding of IT fundamentals and regulatory concepts.

Course Objectives

- **Strategic alignment of IT operations:**
 - Understand how IT operations align with the organization's strategic objectives.
- **Evaluation of IT policies, procedures, and controls:**
 - Learn techniques to assess the effectiveness of IT policies, procedures, and controls.
 - Understand the role of these components in ensuring governance and compliance.
- **Measuring compliance with industry standards:**
 - Explore methods for measuring compliance with industry standards.
 - Understand the implications of non-compliance and its impact on organizational risk.

- **Comprehensive understanding of IT regulatory framework:**
 - Gain insights into the IT regulatory landscape, including PSD2, DORA, NIS 2, GDPR and others.
 - Learn to interpret and apply these regulations to ensure compliance and data security.
- **Assessment and audit of IT systems within regulatory boundaries:**
 - Acquire skills for assessing and auditing IT systems within the boundaries of complex regulatory requirements.
 - Develop a systematic approach to evaluate compliance and governance effectiveness.

Course Content

- **Introduction to IT governance and compliance:**
 - Understanding the intersection of IT operations, strategic objectives, and compliance.
 - Overview of governance principles in IT operations.
- **Effectiveness of IT policies, procedures, and controls:**
 - Techniques for evaluating the effectiveness of IT policies, procedures, and controls.
- **Measuring compliance with industry standards:**
 - Methods for measuring and assessing compliance with industry standards.
 - Impact analysis of non-compliance on operational and legal aspects. [\(read more\)](#)

Prerequisites

Intermediate knowledge of IT fundamentals and basic familiarity with regulatory concepts is recommended. Participants should have a willingness to engage actively in discussions, case studies, and practical exercises to reinforce learning.

Register

IT Risk Management Essentials

F. Ríos

€300/350

1/2 Day

20/02/2026

Intermediate

4 CPE



Overview

This training program is tailored for non-IT auditors seeking to enhance their foundational knowledge and practical skills in IT Risk Management. The training delves into critical concepts related to safeguarding an organization's digital assets against IT risks, with a specific focus on cyber threats. Participants will learn to recognize common IT risks, understand security best practices, and assess the effectiveness of IT controls in preventing data breaches, cyber-attacks, and other digital threats.

Target Audience

This program is tailored for auditors seeking insights into IT risk management, with a focus on safeguarding digital assets against threats. Basic knowledge of IT fundamentals is recommended.

Course Objectives

- **Understanding IT risk management:**
 - Grasp the fundamental concepts of IT risk management.
 - Understand the importance of safeguarding digital assets against a spectrum of IT risks.
- **Management of IT risks:**
 - Develop the ability to identify common IT risks faced by organizations.
 - Risk assessment
 - Risk treatment
- **Security best practices:** Learn and understand security best practices for mitigating IT risks.

Course Content

- **Introduction to IT Risk Management:**
 - Definition and importance of IT risk management.
 - Overview of the key components of an effective IT risk management program.
- **Common IT Risks:**
 - Identification and categorization of common IT risks.
 - Understanding the impact and potential consequences of identified risks.
 - Understand risk treatments to be applied.
- **Cyber Threats:**
 - In-depth exploration of cyber threats facing organizations.
 - Strategies for recognizing and mitigating cyber threats.
- **Security Best Practices:**
 - Overview of security best practices for IT risk management.
 - Application of best practices in real-world scenarios.

Prerequisites

Basic knowledge of IT fundamentals, including an understanding of general IT components and risk awareness, is recommended. Active participation in discussions, case studies, and practical exercises will enhance the learning experience.

Register

Fundamentals of IT Infrastructure: Hardware and Software Essentials



M. Dekeyser

€300/350

1/2 Day

27/03/2026

Beginner

4 CPE

Overview

This training program is designed for non-IT auditors seeking to enhance their foundational knowledge and practical skills in Information and Communication Technology (ICT). The focus will be on essential components of IT infrastructure, distinguishing between hardware and software. Participants will gain insights into servers, workstations, peripherals, networks, operating systems, protocols, and applications.

Target Audience

This program is tailored for non-IT auditors and other individuals involved in reviewing business processes supported by IT and automation. It fits those who wish to develop a solid understanding of IT infrastructure components. No prior technical knowledge is required, making it accessible for participants with various backgrounds.

Course Objectives

- **Understand IT Infrastructure Components:**

Gain a comprehensive overview of hardware components such as servers, workstations, peripherals, and networks.

- **Differentiate Between Hardware and Software:**

- Develop the ability to distinguish between hardware elements and software components in IT systems.

- **Explore Operating Systems:**

- Understand the role and functions of operating systems in managing computer hardware and software resources.

- **Examine Network Protocols:**

- Learn about essential network protocols and their communication between devices.

[\(Read more\)](#)

Course Content

- **Introduction to IT Infrastructure:**

- Overview of IT components.
- Importance of IT infrastructure in organizational operations.

- **Hardware Essentials:**

- Servers and their roles.
- Workstations and peripherals.
- Networking basics.

- **Software Fundamentals:**

- Operating systems and their functions.
- Common applications and their uses.
- Introduction to protocols.

[\(Read more\)](#)

Prerequisites

No specific prerequisites are required for this training program. Basic familiarity with general computer usage is beneficial but not mandatory. Participants should come with a willingness to learn and engage in hands-on activities to enhance their understanding of IT fundamentals.

Register

significance in facilitating

Understanding IT Networks: Assessing Connectivity and Ensuring Security

M. Dekeyser

€300/350

1/2 Day

27/03/2026

Intermediate

4 CPE



Overview

This training program is designed for non-IT auditors aiming to enhance their foundational knowledge and practical skills in Information and Communication Technology (ICT), specifically focusing on networks and connectivity. Participants will delve into local and wide-area networks, understanding their impact on business operations. The training emphasizes the importance of assessing network architecture, configuration, and connectivity for vulnerabilities, as well as the potential risks associated with data transmission, access controls, and network security.

Target Audience

This program is tailored for non-IT auditors and other individuals involved in auditing business processes who seek a deeper understanding of IT networks, their configurations, and the associated security considerations. Prior basic knowledge of IT fundamentals is recommended but not mandatory.

Course Objectives

- **Comprehensive Network Understanding:**
 - Gain a thorough understanding of local and wide-area networks and their role in business operations.
- **Vulnerability Assessment:**
 - Learn to assess network architecture and configurations for potential vulnerabilities.
- **Risk Identification:**
 - Understand the risks associated with data transmission, access controls, and network security.

- **Security Best Practices:**
 - Explore best practices for securing networks and ensuring data integrity.

[\(Read more\)](#)

Course Content

- **Introduction to IT Networks:**
 - Overview of local and wide-area networks.
 - Importance in modern business operations.
- **Network Architecture and Configuration Assessment:**
 - Understanding network architecture.
 - Assessing network configurations for vulnerabilities.
- **Risk Factors in Data Transmission:**
 - Identifying potential risks in data transmission.
 - Impact on business continuity.
- **Access Controls and Network Security:**
 - Importance of access controls.
 - Network security protocols and best practices.

[\(Read more\)](#)

Prerequisites

Basic knowledge of IT fundamentals, including an understanding of hardware and software components, is recommended. Participants should have a familiarity with general computer usage and basic networking concepts. A willingness to engage in discussions and hands-on activities to reinforce learning is essential.

Register

Cybersecurity Fundamentals for Non-IT Auditors: A Practical Approach

M. Dekeyser

€300/350

1/2 Day

24/04/2026

Beginner

4 CPE



Overview

This training program is designed to empower non-IT auditors with essential knowledge and practical skills in cybersecurity. The program covers the basics of cybersecurity, major threats in the digital landscape, and practical protective measures. Participants will gain insights into the ever-evolving world of cybersecurity, enabling them to better assess and mitigate risks in their auditing processes.

Target Audience

This training aims at non-IT auditors and other individuals engaged in auditing functions who are seeking foundational knowledge in cybersecurity. No specific technical background is required, making the program accessible to participants with diverse professional experiences.

Course Objectives

- **Understanding Basics of Cybersecurity:**
 - Grasp fundamental concepts and terminology in cybersecurity.
- **Identification of Major Threats:**
 - Identify and comprehend major threats in the cybersecurity landscape.
- **Implementing Protective Measures:**
 - Learn practical protective measures and best practices to enhance cybersecurity.
- **Risk Mitigation Skills:**
 - Develop skills to assess and mitigate cybersecurity risks in auditing processes.

- **Awareness of Evolving Threats:**
 - Stay informed about emerging cybersecurity threats and trends.
- **Integration of Cybersecurity in Auditing:**
 - Understand how cybersecurity considerations integrate into the audit process.

Course Content

- **Introduction to Cybersecurity**
 - Definition and importance of cybersecurity.
 - Role of non-IT auditors in cybersecurity awareness.
- **Major Threats in Cybersecurity:**
 - Overview of common cybersecurity threats (e.g., malware, ransomware, supplier chain, ddos, ...).
 - Understanding social engineering attacks.
- **Protective Measures and Best Practices:**
 - Implementing strong passwords and multi-factor authentication.
 - Best practices for secure data handling and storage. [\(Read more\)](#)

Prerequisites

No specific prerequisites are required for this training program. Participants should come with a basic understanding of business processes and a willingness to engage in discussions and hands-on activities to reinforce their learning in the field of cybersecurity.

Register

Navigating Disruptive Technologies: A Guide for Business Auditors



M. Dekeyser

€300/350

1/2 Day

24/04/2026

Intermediate

4 CPE

Overview

This training program is designed to equip business auditors with comprehensive knowledge and practical skills in auditing and evaluating disruptive technologies. Participants will explore a wide spectrum, including cloud computing, virtualization, IoT (Internet of Things), blockchain, AI (Artificial Intelligence), cryptocurrency, quantum computing, and nanotechnology. The program delves into the fundamentals, risks, and compliance considerations for these technologies, providing auditors with the expertise to offer valuable assurance in the dynamic digital landscape.

Target Audience

Business auditors and other individuals engaged in auditing functions who are looking to enhance their understanding of disruptive technologies. This program is suitable for those with a foundational knowledge of IT and business processes, seeking to delve deeper into emerging technologies. Basic familiarity with IT concepts is recommended but not mandatory.

Course Objectives

- **Comprehensive Understanding of Disruptive Technologies:**
 - Gain in-depth knowledge of various disruptive technologies shaping the digital landscape.
- **Assessment of Risks and Opportunities:**
 - Learn to assess the risks and opportunities associated with disruptive technologies.
 -

- **Compliance Considerations:**
 - Understand compliance requirements for different disruptive technologies.
- **Practical Applications in Auditing:**
 - Apply auditing principles to evaluate the implementation of disruptive technologies.

[\(Read more\)](#)

Course Content

- **Introduction to Disruptive Technologies:**
 - Overview of cloud computing, virtualization, IoT, blockchain, AI, cryptocurrency, quantum computing, and nanotechnology.
- **Fundamentals of Each Technology:**
 - In-depth exploration of the fundamentals of each disruptive technology.
- **Risk Assessment and Management:**
 - Identifying and managing risks associated with disruptive technologies.

[\(Read more\)](#)

Prerequisites

Basic familiarity with IT concepts and business processes is recommended. Participants should have a keen interest in understanding emerging technologies and their impact on business operations. A willingness to engage in discussions and case studies is essential for optimal learning in this advanced-level training program.

[Register](#)

Understanding the IT Environment and its core processes

F. Ríos

€300/350

1/2 Day

22/05/2026

Intermediate

4 CPE



Overview

This training is designed to equip internal auditors with a comprehensive understanding of the key components of an IT environment. Participants will delve into the basics of IT infrastructure, common applications, and services, with a specific focus on identifying main risks efficiently. The training aims to provide auditors with the knowledge and tools to engage in a 2-hour meeting with an IT manager, eliciting critical information and posing targeted questions to assess the robustness of the IT environment.

Target Audience

This program is tailored for internal auditors seeking an overview of IT environments, including the fundamental components and associated risks. No prior IT knowledge is required, making this course suitable for those entering the field of IT auditing.

Course Objectives

- **Overview of IT environment:**
 - Understand the basics of IT applications and services management.
 - Gain insights into the interconnected nature of IT components.
- **Main risks identification:**
 - Develop the ability to identify main risks in an IT environment efficiently.
 - Understand the importance of risk awareness in the context of IT auditing.
- **Effective questioning techniques:**
 - Learn techniques for crafting and posing targeted questions in a limited timeframe.
 - Enhance communication skills for efficient information extraction from IT managers

Course Content

- **Introduction to IT environment:**
 - Understanding of the IT environment and core processes.
 - Introduction to COBIT (Control Objectives for Information and Related Technologies) framework.
 - Understanding the role of COBIT in IT governance and audit processes.
- **Risks in IT environment:**
 - Identification of main risks associated with IT environments.
 - Analysis of potential impacts and consequences of identified risks.
- **Key components of IT applications & data:**
 - Exploration of fundamental IT applications elements.
 - Common applications and services.
- **Time-efficient meeting strategies:**
 - Techniques for conducting efficient 2-hour meetings with IT managers.
 - Maximizing information extraction in a limited timeframe.
- **Practical questionnaire development:**
 - Guidelines for crafting a questionnaire to challenge IT managers.
 - Designing questions to elicit critical information about the IT environment.

Prerequisites

This course is designed for individuals with limited or no prior IT knowledge but participation in the IT audit introduction training is highly recommended. A willingness to engage actively in discussions, case studies, and practical exercises is essential for optimal learning.

[Register](#)

Automated Business Processes and Application Controls

F. Ríos

€300/350

1/2 Day

22/05/2026

Intermediate

4 CPE



Overview

This training is specifically designed to empower participants with the knowledge and skills to conduct effective audits of automated business processes, with a focus on application controls. Participants will gain a comprehensive understanding of automated business processes, learn to identify controls and vulnerabilities, and develop improvement recommendations. The training is structured to enhance participants' capabilities in ensuring control and efficiency within automated business processes.

Target Audience

This program is tailored for auditors and professionals involved in auditing automated business processes, with a particular interest in application controls. Prior knowledge of IT fundamentals and audit concepts is recommended.

Course Objectives

- Understanding Automated Business Processes:**
 - Gain a deep understanding of the nature and intricacies of automated business processes.
 - Explore the relationship between automation and operational efficiency.
- Identification of Controls and Vulnerabilities:**
 - Develop skills to identify and evaluate controls within automated business processes.
 - Recognize vulnerabilities that may impact the effectiveness of automation.

- Application Controls:**

- Delve into the concept of application controls and their significance in automated business processes.
- Understand how application controls contribute to overall risk management.

Course Content

- Introduction to Automated Business Processes:**

- Overview of automated business processes and their impact on organizational efficiency.
- Understanding the automation lifecycle.

- Identification and Evaluation of Controls:**

- Techniques for identifying and evaluating controls within automated processes.
- Case studies illustrating successful control implementations.

- Vulnerability Assessment:**

- Methods for recognizing vulnerabilities in automated business processes.
- Strategies for assessing the impact of vulnerabilities on process outcomes.

- Application Controls in Automated Processes:**

- In-depth exploration of application controls and their role in ensuring process integrity.
- Practical examples demonstrating the implementation of application controls.

Prerequisites

Basic knowledge of IT fundamentals, including an understanding of hardware and software components, is recommended. Participants should have a familiarity with general computer usage and basic networking concepts. A willingness to engage in discussions and hands-on activities to reinforce learning is essential.

[Register](#)

Data, Databases, Encryption, Anonymization

M. Dekeyser

€300/350

1/2 Day

05/06/2026

Intermediate

4 CPE



Overview

This training is designed to equip business auditors with comprehensive knowledge and practical skills in auditing and evaluating database systems, data access controls, data privacy regulations, and the risks associated with data breaches and unauthorized access. Emphasis is placed on ensuring the confidentiality, integrity, and availability of sensitive information.

Target Audience

This program is tailored for non-IT auditors and other individuals involved in auditing business processes who seek a deeper understanding of data, data management and the associated security considerations. Prior basic knowledge of IT fundamentals is recommended.

Course Objectives

- **Comprehensive Understanding of Data Management:**
 - Gain in-depth knowledge of data management, covering concepts from traditional databases to modern big data systems.
- **Auditing Database Systems:**
 - Develop practical auditing skills specific to database systems, including assessing data structures, query performance, and overall system security.
- **Data Access Controls:**
 - Learn about effective access control mechanisms for securing sensitive data, ensuring only authorized personnel can access and manipulate information.

- **Data Privacy Regulations:**

- Understand the landscape of data privacy regulations and compliance requirements, with a focus on how auditors can ensure organizations adhere to these standards.

- **Risks and Mitigation Strategies:**

- Identify and analyse risks associated with data breaches and unauthorized access.
- Develop strategies for mitigating and preventing potential data security threats.

Course Content

- **Comprehensive Understanding of Data Management:**

- Gain in-depth knowledge of data management, covering concepts from traditional databases to modern big data systems.

- **Auditing Database Systems:**

- Develop practical auditing skills specific to database systems, including assessing data structures, query performance, and overall system security.

- **Data Access Controls:**

- Learn about effective access control mechanisms for securing sensitive data, ensuring only authorized personnel can access and manipulate information.

[\(Read more\)](#)

Prerequisites

Basic knowledge of IT fundamentals, including an understanding of IT general components, data awareness and security awareness, is recommended. A willingness to engage in discussions and hands-on activities to reinforce learning is essential.

Register

Business Continuity Management (BCM) and Disaster Recovery Planning (DRP)



M. Dekeyser

€300/350

1/2 Day

05/06/2026

Intermediate

4 CPE

Overview

This training is crafted to provide non-IT auditors with a comprehensive understanding of Business Continuity Management (BCM) and Disaster Recovery Planning (DRP). Participants will gain practical skills to assess the robustness of business continuity and disaster recovery plans, ensuring swift recovery of critical IT systems in the face of unforeseen incidents such as natural disasters, cyberattacks, or system failures.

Target Audience

This program is designed for non-IT auditors and individuals involved in auditing business processes, seeking a deeper understanding of Business Continuity Management and Disaster Recovery Planning. Basic knowledge of IT fundamentals is recommended but not mandatory.

Course Objectives

- **Comprehensive Understanding of BCM and DRP:**
 - Gain in-depth knowledge of Business Continuity Management and Disaster Recovery Planning principles.
 - Understand the importance of these plans in ensuring the resilience of critical IT systems.
- **Assessment of Robustness:**
 - Develop practical skills to assess the robustness of business continuity and disaster recovery plans.
 - Learn to identify potential vulnerabilities and gaps in the plans.

- Risk Mitigation and Recovery Preparedness:
 - Understand the significance of risk mitigation in the context of IT systems.
 - Develop strategies for recovery preparedness in the face of unexpected incidents.

Course Content

- **Introduction to BCM and DRP:**
 - Overview of Business Continuity Management and Disaster Recovery Planning.
 - Importance of these plans in maintaining operational continuity.
- **Assessment Techniques:**
 - Practical methodologies for assessing the robustness of BCM and DRP.
 - Identifying key components and critical dependencies in recovery plans.
- **Risk Identification and Mitigation:**
 - Techniques for identifying and assessing risks associated with unexpected incidents.
 - Strategies for effective risk mitigation in BCM and DRP.
- **Incident Response:**
 - Developing incident response protocols for quick recovery.
 - Case studies illustrating effective responses to real-world incidents. [\(Read more\)](#)

Prerequisites

Basic knowledge of IT fundamentals is recommended. Familiarity with general IT components and an understanding of risk awareness will enhance the learning experience. Active participation in discussions and case studies is encouraged to reinforce practical learning.

[Register](#)