ACPM

Audit Consulting Project Management

BUDAPEST • DUBAI • GABORONE • KIGALI
KUALA LUMPUR • NAIROBI • PRETORIA • SHANGHAI

2022 Training Courses

Our Offices

Budapest
Dubai
Kigali
Kuala lumpur
Nairobi
Pretoria
Shanghai
Wien

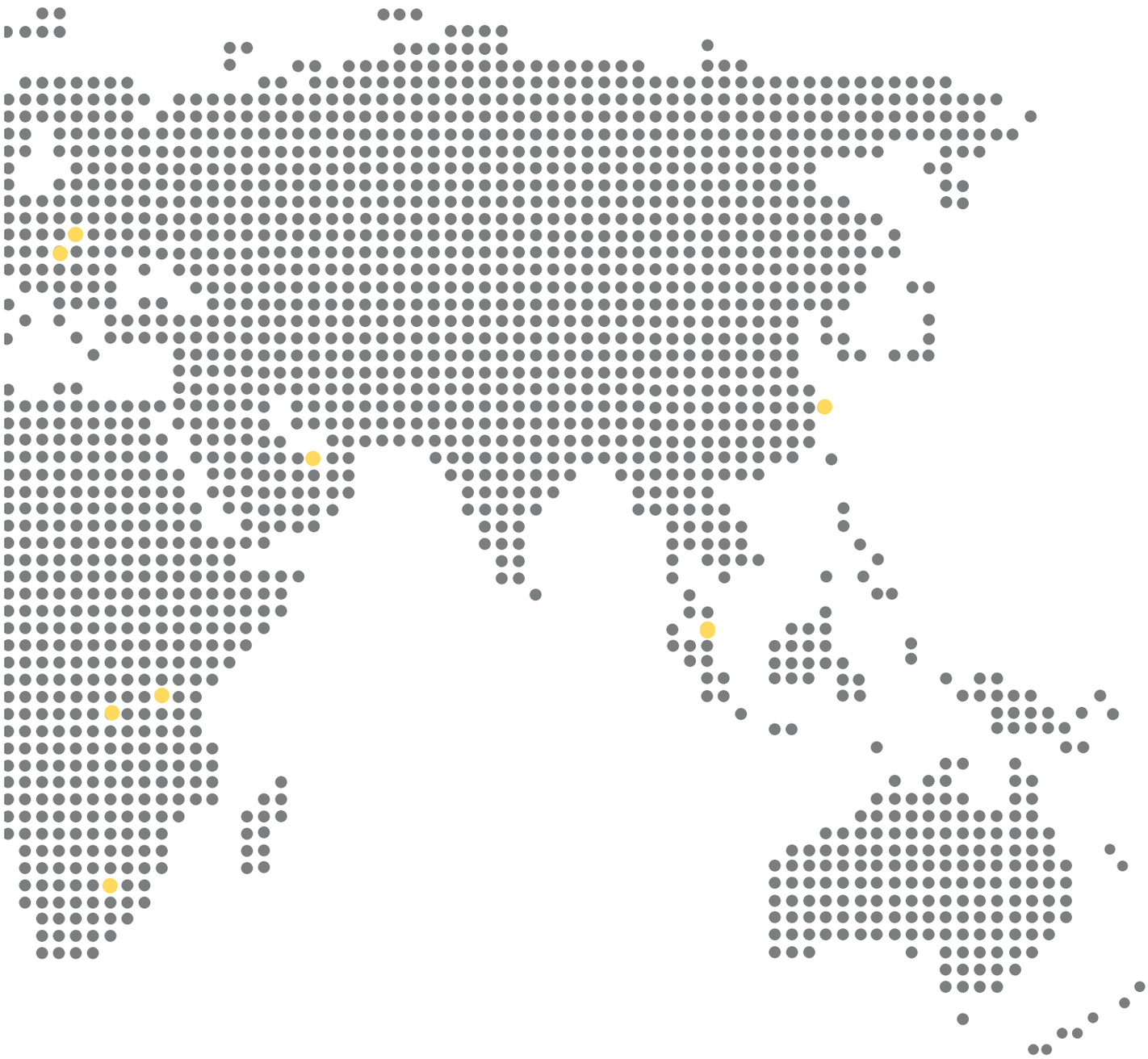


Table of Contents

ACPM Training Courses

ACPM is an internatinal provider of consulting services in IT security, IT audit and IT project management.

A compilation of trainings provided by ACPM IT Consulting Ltd.

We have over 20 years of experience in these fields and are among the leading providers of IT consulting in Hungary. Our company also provides an extensive range of IT related training courses for various audiences.

Our trainings give introductory or advanced knowledge into various fields of IT security and related topics. Our trainers have experience of 10-20 years in these areas as consultants, developers and operators; most of them back this experience with internationally acclaimed certificates. Besides being experienced in the specific areas, our trainers also have decorated experience in teaching these topics; most of them teach regularly on different prominent universities in Hungary.

Our goals for the provided trainings are to give a comprehensive and structured knowledge to our students, that can help their development and expertise in the coming years. It is important to clarify that by taking part in our trainings, students will not immediately become IT security experts or top hackers. Practice, commitment, live experience and continuous hard work cannot be replaced by anything. But our trainings certainly make development in these fields easier and quicker, by our materials summing up our 10-20 years of related knowledge, and by the virtual laboratories that we use to simulate real-life situations and to explain certain practices. We continuously help our students with materials, suggested reads on the topics and instructions throughout the courses. Training programs described in the following sections of this document include eight 45-minute long classes per day with on-site trainers and virtual laboratory demonstrations provided.

Our training programs are highly customizable and we can adapt them to our clients' specific needs. In case the client wants to change the curriculum, combine training courses, have shorter or more in-depth versions of the existing training programs, we are always ready to customize our materials and curriculum in order to meet the requirements.

Becoming an IT security expert is like practicing martial arts: it takes lifelong learning, where the goal is the progress itself.

If you are interested in a customized version of our training programs, please contact our experts with your ideas or special requirements.

1 Management Security Awareness Trainings

5-Day Bank Manager IT Security Training

An introduction into IT security for managers of financial institutions.

This training course is designed for those in managerial positions at financial institutions who want to have a deeper understanding of their operation's IT background and about how to keep it secure.
Our five-day training course for bank and financial institution managers covers all necessary topics for establishing a solid basis of IT security knowledge. Topics include an introduction into IT security standards, as well as defensive and offensive IT security technologies.

The curriculum of the course is as follows:

1. **Introduction – Day 1**
- IT Security Standards
- ISO 27000 Standards
- COBIT (Control Objectives for Information and Related Technologies) standards

2. **Defensive Technologies – Day 2-3**
- Introduction to Firewalls
- VPN Basics
- Monitoring
- Intrusion Detection / Prevention Systems
- Log Collecting and Log Analysis

3. **Offensive Technologies – Day 4-5**

- OWASP Top10
- Phases of System Analysis Reconnaissance
- Web Server and Web Application Security
- Password Cracking
- Cryptography, Public Key Infrastructure
- Wireless Security
- Social Engineering
- Phishing
- Email Account Security

1 Management Security Awareness Trainings

IT Security Awareness Training

1.5-day manager-level training on IT security knowledge and awareness

Course material

This up-to-date, comprehensive training course by ACPM IT Consulting Ltd. is designed to equip managers of government institutions and large organizations in the ASEAN region with the essential knowledge, mindset and toolkit to understand and tackle the cybersecurity-related challenges their respected organizations are facing.

This training follows the success of the joint training of ACPM and the Indonesian Banking Development Institute in cybersecurity for bank managers in Jakarta in November 2017, as well as a successful training conducted for Companies Commission of Malaysia (SSM) in Budapest in 2018.

Key benefits

• Learn how to identify main cybersecurity threats that your organization is facing. Master the mindset to equip your teams the necessary knowledge to defend your infrastructure against cyberattacks.

• Develop a mindset that is focused on security throughout the whole operation in order to create a safe environment from development to implementation.

• Create an environment in your organization which is focused on the risks and threats from a cyber standpoint and is quick and capable to respond properly to take the necessary measures against any attack.

Recommended for the following audience

Information technology and information security are both rapidly rising to become the most important building blocks of government entities', and large corporations' operation.

Our training course is designed for those in managerial positions at government institutions and large organizations who want to have a deeper understanding of their operation's IT background and about how to keep it secure.

Curriculum

This 1,5-day training course covers the most necessary topics for establishing a solid basis of IT security awareness and mindset. Topics include an introduction into IT security standards, as well as defensive and offensive IT security technologies.

Day 1 (morning and afternoon, including lunch and coffee breaks)

• Most important IT security standards: The way to develop a security-focused mindset IT Security
• Threat identification: How to spot flaws and potential threats in the system
• Physical and cyber security
• Defensive technologies: An introduction
• Offensive technologies: An introduction

Day 2 (morning)

• Open discussion on cybersecurity
• Networking brunch

According to client requirements, the training program can take place on-premise or at ACPM HQ training facility.

2-Day Cybersecurity Training Course for Bank Managers

A comprehensive IT security training for managers of financial institutions

Course material

This interactive and comprehensive training course will use small-classroom methodology to create a relaxed and innovative learning environment. ACPM provides its own virtual learning environment including security training exercises, case studies and more. At the end of the training, attendees can take part in our exam covering the topics mentioned during the course. Completion of the training and passing the exam provides attendees with a certificate issued by ACPM and recognized by our international network. We also provide participants of the training with a toolkit including lessons learned during the training.

1 Management Security Awareness Trainings

Key benefits

• Learn how to identify main cybersecurity threats that your organization is facing. Master the knowledge to equip your teams the necessary knowledge to defend your infrastructure against cyberattacks.

• Develop a mindset that is focused on security throughout the whole operation in order to create a safe environment from development to implementation.

• Create an environment in your organization which is focused on the risks and threats from a cyber standpoint and is quick and capable to respond properly to take the necessary measures against any attack.

Recommended for the following audience

Information technology and information security are both rapidly rising to become the most important building blocks of financial institutions' operations. Our training course is designed for those in managerial positions at financial institutions who want to have a deeper understanding of their operation's IT background and about how to keep it secure.

Curriculum

Our two-day training course for bank and financial institution managers covers all necessary topics for establishing a solid basis of IT security knowledge. Topics include an introduction into IT security standards, as well as defensive and offensive IT security technologies.

Each day of training includes morning and afternoon coffee breaks, and a longer lunch break.

Day 1: Introduction, Defensive Technologies

Information Security Standards

International standards briefly covered in this part of the training offer an introduction into how an organization can put security into the focus of its operations, as well as the less technical side of information security, which involves policies and internal regulations of an organization.

• IT Security Standards

• ISO 27000 Standards

• COBIT (Control Objectives for Information and Related Technologies) standards

Defensive Technologies

On the afternoon of the first day, we start our introduction into defensive (i.e. passive) cybersecurity technologies managers should be familiar with. These are techniques required for monitoring and preventing possible attacks. Live training using ACPM's virtual platform is included.

• Introduction to Firewalls
• VPN Basics
• Monitoring
• Intrusion Detection / Prevention Systems
• Log Collecting and Log Analysis

Day 2: Offensive Technologies

Offensive Technologies

Introduction into the most important offensive (i.e. proactive) security technologies. Offensive technologies are related to the attacks themselves: how to implement them, how to defend a structure against them. Live training sessions included.

• OWASP Top10
• Phases of System Analysis Reconnaissance
• Web Server and Web Application Security
• Password Cracking
• Cryptography, Public Key Infrastructure
• Wireless Security
• Social Engineering
• Phishing
• Email Account Security

2. Offensive Security Topics

12 Week Ethical Hacking Training

This is a very intense 12 weeks long seminar that includes all the topics required by the CEH certification.

The curriculum of the course is as follows:

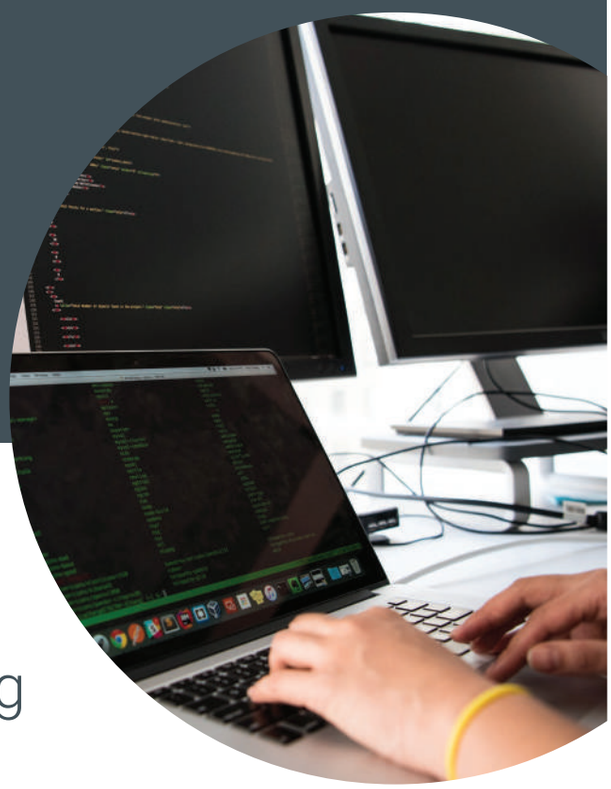
- Introduction to Ethical Hacking (Ethics and Legality)
- Footprinting
- Scanning
- Enumeration
- System Hacking
- What is a Trojan?
- Sniffers
- Denial of Service
- Social Engineering
- Session Hijacking
- Hacking Web Servers
- Web Application Vulnerabilities
- Web-Based Password Cracking Techniques
- SQL Injection
- Command Injection

Pre-requisites for participation on this seminar:

- Must be a computer systems expert who is very knowledgeable about computer programming, networking, and operating systems
- In-depth knowledge about highly targeted platforms (such as Windows,Unix, and Linux)
- Networking, web programming, and database skills are all useful in performing ethical hacking and vulnerability testing
- Prior to enrolling in this training course all applicants must pass a short test designed to assess the level of their relevant knowledge.

Technical details of the course:

- 12 weeks long
- 5 days a week
- On-site trainer
- Virtual lab access and exercises



Web Application Hacking

Min. course length (days): 3
Max. course length (days): 15
Dependency on other knowledge or training: Knowledge in web development
Min. level of difficulty: ++
Max. level of difficulty: +++
Min. achievement: Students will learn the basics of web application hacking, tools to use and methodology of application hacking.
Max. achievement: Students will learn the basics of web application hacking, will be able to use the related tools and will be able to conduct basic web application penetration testing without senior help.
Topics covered: Introduction, Definitions, Methodology, Reconnaissance, SQLi, XSS, Directory Traversal, Slowloris, Authentication, Session Management, Passwords, HTTPS Certificates.

Crypto Analysis

Min. course length (days): 3
Max. course length (days): 10
Dependency on other knowledge or training: Mathematical knowledge, Cryptography Basics
Min. level of difficulty: ++
Max. level of difficulty: +++
Min. achievement: Students will learn the basics of crypto-analysis, most common methods and techniques.
Max. achievement: Students will learn the basics of crypto-analysis, most common methods and techniques. Students learn the modern mathematical basics of cryptography. Applications of the techniques are shown using practical examples.

2. Offensive Security Topics

Reverse Engineering

Min. course length (days): 1
Max. course length (days): 10
Dependency on other knowledge or training: Advanced knowledge in development
Min. level of difficulty: ++
Max. level of difficulty: +++
Min. achievement: Students get to know the basics of reverse engineering and related tools, and their basic use.
Max. achievement: Students get to know the basics of reverse engineering and related tools, and their advanced use.

Exploiting

Min. course length (days): 1
Max. course length (days): 10
Dependency on other knowledge or training: Advanced knowledge in development
Min. level of difficulty: ++
Max. level of difficulty: +++
Min. achievement: Students get to know the basics of exploiting and its related tools, and their basic use.
Max. achievement: Students get to know the basics of exploiting and its related tools, and their advanced use.

Wi-Fi Attacks

Min. course length (days): 1
Max. course length (days): 3
Dependency on other knowledge or training: Networks Basics
Level of difficulty: ++
Min. achievement: Students get to know the basics of Wi-Fi security and its related tools, and their basic use.
Max. achievement: Students get to know the basics of Wi-Fi security and its related tools, and their basic use. Students learn to use analysis tools and techniques with practical examples.
Topics covered: Technologies, Standards, Topology, Wi-Fi Encrypt Algorithms, Tools and Technics of Wi-Fi Attacking

3. Banking Technical Trainings

ACPM's technical training courses are designed for banking and non-banking technical IT staff members to deepen their knowledge in IT security and its related topics, such as secure coding, code review, and others.
Technical trainings vary from shorter, introductory-level courses in both offensive and defensive security all the way to completely in-depth courses that provide a very deep understanding of IT security for technical employees.

5-Day Defensive Banking Security Training

This training course provides a technical introduction into the most important topics of defensive security. It is mostly recommended to general banking IT staff members who need a basic understanding of IT security-related matters but do not require high-level knowledge on it.

Curriculum of this course is as follows:

- Day 1 – Introduction
- Day 1-2 – Firewall Technologies
- Day 2 – VPN Basics
- Day 3-4 – Monitoring
- Day 4 – Intrusion Detection / Prevention Systems
- Day 4-5 – Log Collection and Log Analysis

5-Day Offensive Banking Security Training

This training course provides a technical introduction into the most important topics of offensive security. It is mostly recommended to general banking IT staff members who need a basic understanding of IT security-related matters but do not require high-level knowledge on it.

Curriculum of this training is as follows:

1. **Application Security – Day 1**
   - Patch Management
   - Viruses, Worms and Trojans
2. **Phases of System Analysis Reconnaissance – Day 1**
   - Foot-printing
   - Scanning
   - Enumeration
   - Sniffing Techniques
3. **OWASP Top10 – Day 2**
4. **Web Server and Web Application Security – Day 2-3**
5. **Password Cracking – Day 4**
   - Cryptography
   - Public Key Infrastructure
6. **Other Offensive Topics – Day 5**
   - Wireless Security
   - Social Engineering
   - Phishing
   - Email Account Security

4. Secure Coding

Secure Web Coding Methodology

Course length (days): 3
Dependency on other knowledge or training: Knowledge in development
Level: ++
Achievement: Students will learn the most common web vulnerabilities, their causes and common methods of avoiding them.

Secure Coding in C#

Course length (days): 5
Dependency on other knowledge or training: Knowledge in development
Level of difficulty: +++
Achievement: Students will learn the most common web vulnerabilities and their causes. Through various examples, students will learn the most common C# coding mistakes, as well as best practices and technical methodology in order to avoid mistakes.

Secure Coding in Java

Course length (days): 5
Dependency on other knowledge or training: Knowledge in development
Level of difficulty: +++
Achievement: Students will learn the most common web vulnerabilities and their causes. Through various examples, students will learn the most common Java coding mistakes, as well as best practices and technical methodology in order to avoid mistakes.

5. Introductory topics

Linux Basics

This course introduces enrolled students into the basics of Linux.
Min. course length (days): 5
Max. course length (days): 10
Dependency on other knowledge or training: None
Level of difficulty: +
Min. achievement: Students will learn the basics of Linux and by completing the course, will be know the basic Linux commands.
Max. achievement: Students will learn the basics of Linux and by completing the course, will be able to use basic Linux commands confidently.

Shell Programming

This course introduces students into the basics of shell programming.
The course requires knowledge on basics of Linux.
Min. course length (days): 5
Max. course length (days): 10
Dependency on other knowledge or training: Linux Basics
Level of difficulty: +
Min. achievement: Students will be able to write basic shell scripts, will know the basic commands and the basics of programming elements.
Max. achievement: Students will be able to write basic shell scripts, know the basic commands and the basics of programming elements, as well as confidently using them.

Networks Basics

This course gives students an introduction into IT networks.
Min. course length (days): 5
Max. course length (days): 10
Dependency on other knowledge or training: Linux Basics
Level of difficulty: +

SQL Basics

This course gives an introduction into the basics of SQL.
Min. course length (days): 5
Max. course length (days): 10
Dependency on other knowledge or training: None
Level of difficulty: +

Min. achievement: Students will be able to write basic SQL queries.
Max. achievement: Students will be able to write more advanced SQL queries, and use basic SQL language elements confidently.

Web Development Basics

This course is an introduction into the basics of web development. Suggested coding languages of learning are Java and C#.
Min. course length (days): 5
Max. course length (days): 10
Dependency on other knowledge or training: None
Level of difficulty: +
Min. achievement: Students will learn the basics of web development.
Max. achievement: Students will be able to develop more simple types of webpages and web applications.

6. Defensive Security Topics

Monitoring

Min. course length (days): 3
Max. course length (days): 10
Dependency on other knowledge or training: Networks Basics, operating system knowledge, knowledge in network services
Min. level of difficulty: ++
Max. level of difficulty: +++
Min. achievement: Students will learn the basics of Monitoring techniques, its applications, and possibilities of its use in action through various examples.
Max. achievement: Students will learn the basics of Monitoring techniques and its applications. Possibilities of monitoring and software supporting are taught through various practical examples.

Log Collecting and Analysis

Min. course length (days): 3
Max. course length (days): 15
Dependency on other knowledge or training: Networks Basics, operating system knowledge, knowledge in network services
Min. level of difficulty: ++
Max. level of difficulty: +++
Min. achievement: Students will learn the topics of log collecting and log analysis, their requirements and applications, and its ways of use through various examples.
Max. achievement: Students will learn the topics of log collecting and log analysis, their requirements and applications. Log analysis' possibilities and software support are shown with practical examples.

Firewalls

Min. course length (days): 3
Max. course length (days): 15
Dependency on other knowledge or training: Networks Basics
Min. level of difficulty: ++
Max. level of difficulty: +++
Min. achievement: Students will learn the basics of firewalls, their types and applications, their use through various examples.
Max. achievement: Students will learn the basics of firewalls, their types and applications. Basic configurations and rules of firewalls are shown through practical examples.

VPN

Min. course length (days): 3
Max. course length (days): 10
Dependency on other knowledge or training: Networks Basics
Min. level of difficulty: ++
Max. level of difficulty: +++
Min. achievement: Students will learn the basics of VPNs, their types and applications, their use through examples.
Max. achievement: Students will learn the basics of VPNs, their types and applications. Basic configurations and use of various VPNs are shown with practical examples.

6. Defensive Security Topics

IPS / IDS

Min. course length (days): 3
Max. course length (days): 10
Dependency on other knowledge or training: Networks Basics, operating system knowledge, knowledge in network services
Min. level of difficulty: ++
Max. level of difficulty: +++
Min. achievement: Students will learn the basics of the IDS/IPS topic, their types and applications, their use through examples.
Max. achievement: Students will learn the basics of IDS/IPS, their types and applications. Basic configurations and use of various IDS/IPS tools are shown with practical examples.

Cryptography

Min. course length (days): 3
Max. course length (days): 10
Dependency on other knowledge or training: None
Min. level of difficulty: +
Max. level of difficulty: ++
Min. achievement: Students will learn the history of cryptography, its basics, most common algorithm types and algorithms.
Max. achievement: Students will learn the history of cryptography, its basics, most common algorithm types and algorithms. Students will learn the modern underlying mathematics basics of cryptography. Students will get to know the basics of crypto-analysis.

Public Key Infrastructure – PKI

Min. course length (days): 1
Max. course length (days): 3
Dependency on other knowledge or training: None
Min. level of difficulty: +
Max. level of difficulty: ++
Min. achievement: Students will get to know the basics of PKI technology.
Max. achievement: Students will learn the basics of PKI technology, its mathematical background and its applications.

Forensic

Min. course length (days): 5
Max. course length (days): 20
Dependency on other knowledge or training: Strong IT basics, Networks Basics, operating system knowledge, knowledge about network services.
Min. achievement: Students will learn the basics of Forensic, basic techniques and using a couple of tools.
Max. achievement: Students will learn Forensics techniques, use of multiple tools, and analysis of various platforms (Linux, Windows, database, network border protection, etc.).

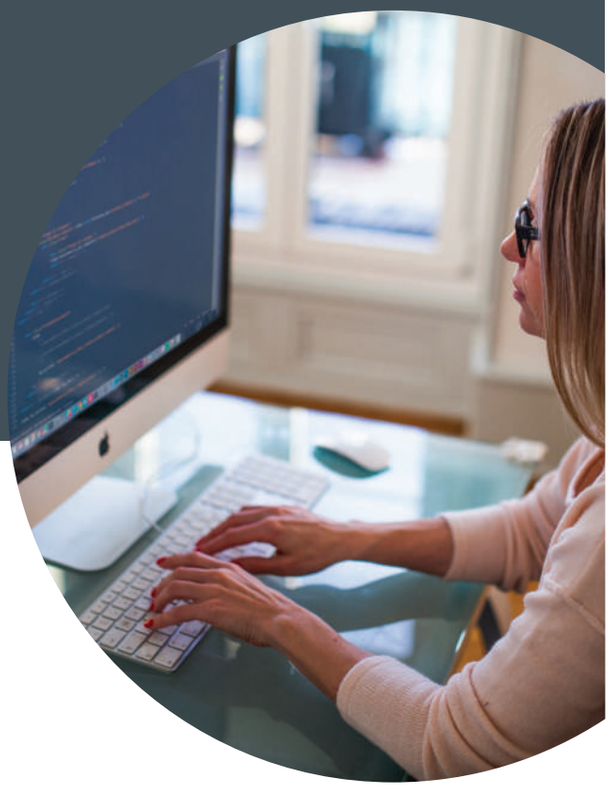
7. IT Security Standards Trainings

ISO/IEC 27000 Family

Min. course length (days): 3
Max. course length (days): 10
Dependency on other knowledge or training: Basic knowledge in IT
Min. level of difficulty: +
Max. level of difficulty: ++
Min. achievement: Students will learn the basics of the mentioned standard family, its structure, application and its basic requirements.
Max. achievement: Students will learn the basics of the mentioned standard family, its structure, application and its basic requirements. Requirements and operations laid down by the standards, and corresponding to them are shown in practical examples.

Common Criteria for Information Technology Security Evaluation (CC)

Min. course length (days): 3
Max. course length (days): 10
Dependency on other knowledge or training: Developer or administrator-level knowledge
Min. level of difficulty: +
Max. level of difficulty: ++
Min. achievement: Students will learn the basics of the mentioned standard, its structure, application and its basic requirements.
Max. achievement: Students will learn the basics of the mentioned standard, its structure, application and its basic requirements. Requirements and operations laid down by the standards, and corresponding to them are shown in practical examples.



COBIT

(Control Objectives for Information and Related Technologies)

Min. course length (days): 3
Max. course length (days): 10
Dependency on other knowledge or training: Basic knowledge in IT
Min. level of difficulty: +
Max. level of difficulty: ++
Min. achievement: Students will learn the basics of the mentioned standard, its structure, application and its basic requirements.
Max. achievement: Students will learn the basics of the mentioned standard, its structure, application and its basic requirements. Requirements and operations laid down by the standards, and corresponding to them are shown in practical examples.

NIST Special Publication 800-53 Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

Min. course length (days): 3
Max. course length (days): 10
Dependency on other knowledge or training: Basic knowledge in IT
Min. level of difficulty: +
Max. level of difficulty: ++
Min. achievement: Students will learn the basics of the mentioned standard, its structure, application and its basic requirements.
Max. achievement: Students will learn the basics of the mentioned standard, its structure, application and its basic requirements. Requirements and operations laid down by the standards, and corresponding to them are shown in practical examples.

ACPM

Audit Consulting Project Management

BUDAPEST • DUBAI • GABORONE • KIGALI
KUALA LUMPUR • NAIROBI • PRETORIA • SHANGHAI

TO US, YOUR SECURITY COMES FIRST

ACPM IT Consulting Ltd.
Széchenyi István tér 7-8.
Budapest, Hungary
1051

info@acpmit.com