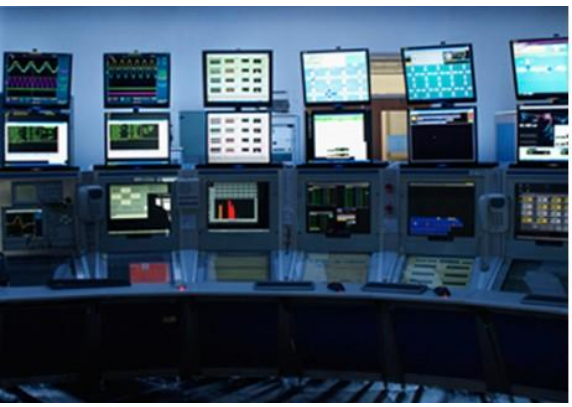
Deloitte.

Course Overview
Cyber Security



Deloitte Academy
2015-2016

This overview contains the following training courses:

Management Courses

- CISA Certification
- CISM Certification
- CISSP Certification
- Security Incident Management

Privacy Courses

- Prepare for Privacy
- CIPP-E Certification

Hacking Courses

- HackLab: Hands-on Hacking
- HackLab: Malware Analysis
- HackLab: Covert Operations
- HackLab: SAP
- ISC/SCADA Security
- Introduction to Cryptography
- Key Management & Payment Security

CyberLympics 2011, 2012, 2013 and 2015.
Deloitte has extensive experience in the field of advising and assessing the information security within governments and business. Our team consists of more than 30 specialists that describe "ethical hacking" as their great passion. The knowledge, experience and passion are reaffirmed in the recent finals of the Global CyberLympics. The team of Deloitte Netherlands did win, for the fourth time in 5 years, a contest which consisted of both offensive and defensive security challenges.

Management Courses

- CISA Certification
- CISM Certification
- CISSP Certification
- Security Incident Management

CISA Certification

CISA, Certified Information System Auditor, is a worldwide acknowledged certification for specialists in the area of audit, assurance and security of information systems. Being CISA certified showcases that participants have the necessary experience, skills and knowledge. It demonstrates that participants are capable to manage vulnerabilities, ensure compliance and institute controls within

Course objectives

The Deloitte CISA certification course is a three-day course, which aims to prepare participants for successfully passing the CISA exam.

During the CISA course participants will be trained to become a broad educated IT auditor. Upon completion of the course participants will have a thorough knowledge of the CISA domains which participants can apply in practice. The rapid IT developments makes it more difficult to unambiguously ensure that systems satisfy requirements. CISAs possess the knowledge, background and support to give assurance worldwide.

- ready for exam in three days
- participants will be trained to become a broad educated IT auditor
- exam preparation will be a significant part of the course

Target audience

- Security managers
- Risk managers
- IT auditors
- IT security professionals
- Security officers
- Compliance managers
- Administrators
- Privacy officers.

Course date and location

This three-day course will be held on 8−10 December 2015 in Rotterdam, the Netherlands. **The data for 2016 will be posted on the site when their confirmed.**

Day 1

- Introduction & Basics to CISA/ISACA
- Governance and Management of IT
- Protection of Information Assets
- Exercises

Day 2

- Recap & Information Systems Acquisition, Development, and Implementation
- Information Systems Acquisition, Development, and Implementation Continued
- Information Systems Operations, Maintenance and Support
- Exercises

Day 3

- Recap & The Process of Auditing Information Systems Summary
- The Process of Auditing Information Systems Summary Continued
- Exam preparation
- Exercises

Exam information

ISACA examinations are held two or three times per year at a fixed date and at a fixed locations. It is advisable to take the exam right after completing the training. Participants must register themselves in time for the CISA examination via the ISACA website. The deadline for the registration is typically 8 weeks before the date of the exam. After the deadline, it is not possible to register anymore, and the participant will not be allowed to take the exam. The deadlines are subject to a change, and are published on the **ISACA website**. It is recommended to register for the English version of the examination.

CISM Certification

CISM, Certified Information Security Manager, is a globally acknowledged information security management certification. This certification demonstrates you can connect information security to your organization's business goals, understand the security aspects of new and current technologies, and possess the knowledge and skills to manage information security within your organization.

Course objectives

The Deloitte CISM Certification course is a 3-day program that prepares you for the CISM exam.

The CISM certification demonstrates that the holder understands a common framework of information security management concepts and principles. These can be applied in differing situations in order for information security to optimally support the business. Topics covered during the course include risk management, handling security incidents, compliance issues, defining and managing information security programs and integrating information security into the business. The course emphasizes stakeholder management, reporting lines and governance.

- High passing rate
- Ready for the exam in three days
- Proven methodology

Target audience

- Information security managers
- IT security professionals
- Business managers with interest in IT

Course date and location

This three-day course will be held on 8 - 10 December 2015 in Rotterdam, the Netherlands. **The data for 2016 will be posted on the site when their confirmed.**

Day 1

- Introduction & Basics to CISM/ISACA
- Information Security Govenance
- Information Security Govenance Continued
- Excercises

Day 2

- Recap & Information Risk & Compliance
- Information Risk and Compliance Continued
- Information security Incident Management
- Excercises

Day 3

- Recap & Information security program development and management
- Information security program development and management continued
- Summary
- Exam preparation

CISSP Certification

The Certified Information Systems Security Professional (CISSP) certification is a globally recognized credential: the first of its kind and accredited by the American National Standards Institute (ANSI).

Course objectives

The Deloitte (ISC)2 CISSP Certification course is an intensive, five-day course with the goal to prepare participants for the CISSP exam.

The course covers the most comprehensive compendium of information security best practices – the Common Body of Knowledge (CBK). The CISSP CBK establishes a common framework of information security terms and principles that allow information security professionals worldwide to discuss, debate and resolve matters pertaining to the profession, with a common understanding.

The CISSP CBK consists of the following 10 domains:

1. Access Control;
2. Application Security;
3. Business Continuity and Disaster Recovery Planning;
4. Cryptography;
5. Information Security and Risk Management;
6. Legal, Regulations, Compliance and Investigations;
7. Operations Security;
8. Physical (Environmental) Security;
9. Security Architecture and Design;
10. Telecommunications and Network Security

The Deloitte CISSP certification course has a passing rate of over 90% as opposed to the average CISSP success rate of around 60%.

Target audience

- Security managers
- Risk managers
- IT auditors
- IT security professionals
- Security officers.

Course date and location

This five-day course will be held on 9 - 13 November 2015 in Rotterdam | 29 February - 4 March 2016 | 4 - 8 July | 24 - 28 October in the Netherlands. Participants will be notified 4 weeks in advance of the definitive location.

Day 1

- Information Security Governance and Risk Management
- Security Architecture and Design
- Excercises

Day 2

- Recap
- Access Control
- Application Security
- Operations Security
- Excercises

Day 3

- Recap
- Cryptography
- Cryptography continued
- Physical Security
- Excercises

Day 4

- Recap
- Networking
- Networking contintued
- Business Continuity Planning
- Excercises

Day 5

- Recap
- Business Continuity Planning Continued
- Legal and Regulatory
- Sample exam (50 questions)

Security Incident Management

Security Incident Management aims to solve security incidents as soon as possible and therefore limit the impact on the business and its processes. During this one-day training course we discuss the basic Incident Management process and more specifically security incidents.

Course objectives

Many organizations are equipped with a servicedesk where incidents can be reported, procedures for high priority incidents and a contact list for escalations. It is often thought that this is enough to provide the organization with an Incident Management process. However, these components are only part of a strong Security Incident Management process. Security Incident Management encompasses everything needed to manage your incidents. Are you in control?

- Insight in the differences between 'normal' and security incidents, roles and responsibilities
- one-day course
- necessary tips and tricks based on our experiences

- Importance of (Security) Incident Management
- The Incident Management process, standards, challenges and areas of concern & Procedure for high priority incidents
- Incident Management tools and requirements
- Managing the Incident Management process

Target audience

Everyone who has something to do with (Security) Incident Management in their daily work and/or wants to know more about it.

Information

For more information, please contact us: nlacademy@deloitte.nl

Privacy Courses

- Prepare for Privacy
- CIPP-E Certification

Prepare for Privacy

Are you prepared for privacy? Rules and regulations about privacy and protection of personal data are developing fast, but you still need to process the personal data. In 1 day you will gain new insights and practices that you need to create a private environment for your personal data.

Course objectives

This course will teach you the most important SAP security features and will allow you to understand their implications. It will enable you to tailor the security settings and procedures to best fit your organization without losing sight of best practices.

- In-depth and hands-on five-day course
- Tailor the security settings and procedures to best fit your organization
- Most important SAP security options

Target audience

- Data officers
- HR Managers
- Chief Information Officers
- Security managers
- Other persons who are responsible for protecting data or who work with personal data every day

The participants will not need a thorough knowledge of privacy legislation in order to participate in this course.

The course will discuss the notification and information requirement, the requirements for international transfers and the security measures to be implemented. The cookie legislation, the rules on direct marketing, emails and internet monitoring and privacy aspects of “the Cloud will be dealt with too.

Finally, the course goes into the various risks of processing personal data, unnecessary or otherwise, preventing data leakage, and the upcoming European Privacy Regulation.

- Introduction to Privacy, notification and information requirements
- Requirements for international transfers of personal data and security measures
- Cookie legislation, direct marketing, monitoring
- Process of personal data, preventing data leakage and European Privacy Regulation

Information

For more information, please contact us: nlacademy@deloitte.nl

CIPP-E Certification

Privacy and data protection today has the full attention of the general public, due to emerging technology generating every more personal data and due to incidents with that personal data in recent years. For a growing group of professionals this means they need to acquire in-depth knowledge in this field. For them we offer our “Privacy Advanced” training: a 4-day course focusing on all aspects of privacy from rules and regulations up to and including implementation and compliance. This will prepare participants for the exam needed to acquire their CIPP/E certification.

Course objectives

The Deloitte Privacy Advanced course is a four-day course, which aims to provide participants with all knowledge required for successfully passing both the CIPP/Europe exam. These Certified Information Privacy Professional certifications are given out by the International Association of Privacy Professionals.

- Four-day course
- In-depth knowledge, covering all aspects of privacy

The course takes four days as it is meant not just as exam training, but first and foremost as an advanced privacy course, with the objective to provide participants a more in-depth understanding of privacy in Europe and worldwide. By acquiring this knowledge, certifying becomes straightforward.

Target audience

- Data protection officersPrivacy officersSecurity officersLegal counselsCompliance officersOthers responsible for protecting personal data or working with personal data every day

This course requires some basic knowledge in the field of privacy and data protection, e.g. as thought in the Prepare for Privacy course, or through work experience.

Course date and location

This Four-day course will be held on 15 – 18 February 2016, 20 – 23 June 2016 and 7 – 10 November in Rotterdam or Utrecht, the Netherlands. Participants will be notified 4 weeks in advance of the definitive location. This course starts at 9.00 a.m. and ends at 5.00 p.m.

Day 1

- Introduction
- Common principles and approaches to privacy
- Jurisdiction and industry specific rules and regulations
- Exercises throughout the day

Day 2

- Recap
- Information security and privacy
- Privacy in online environments
- Exercises throughout the day

Day 3

- Recap
- Introduction to European data protection
- European data protection law and regulations
- Exercises throughout the day

Day 4

- The future of data protection in Europe
- Data protection compliance in practice
- Exercises throughout the day
- About the CIPP exam

Exam information
Participants will receive a voucher for a CIPP/Europe exam with which they can book an examination at a desired date and time at a KRYTERION Testing Network (KTN) test centre of their choice.

Hacking Courses

- HackLab: Malware Analysis
- HackLab: Hands-on Hacking
- HackLab: Covert Operations
- HackLab: SAP
- ISC/SCADA Security
- Introduction to Cryptography
- Key Management & Payment Security
- SAP Security

HackLab: Malware Analysis

Malware on your systems sounds like a nightmare to any organization. It is something that you wish to prevent. Having theoretical knowledge on this matter is not enough anymore. You need hands-on experience on how to discover, analyse and fight malware. This experience can be obtained by attending the 3-day Hacklab: Malware Analysis course.

Course objectives

This hands-on course enables participants to make their first steps towards malware analysis up to the full reverse engineering of the more advanced types of malware.

We will deal with different methods of malware analysis, such as behavioral, static analysis and reverse engineering. Topics addressed in this course include: the different properties and actions of malware, forensic traces, network traffic, code analysis, obfuscation and encryption. Various malware files, specifically written for this course, will be analyzed prior to analyzing existing malware. A major element of this course is hands-on reverse engineering, giving maximum experience to participants during the three days.

Following this course enables participants to perform their first analysis on encountered malware, correctly estimate the behavior of malware, and understand how it can be countered.

- Hands-on experience with the analysis of malware
- Different methods of malware analysis
- Major element of this course is hands-on reverse engineering

Target audience

- Incident response employees
- Digital forensic researchers
- IT system & network administrators
- IT professionals interested in malware analysis

Participants should have fundamental insight into network protocols, IP network services, and operating systems. Experience with malware is not required, but a solid technical background is desired.

Course date and location

This three-day course will be held on 25 – 27 April and 10 – 12 October 2016 in the Hague or Utrecht, the Netherlands.

Day 1

- General malware overview and history
- How victims are infected & Introduction to malware analysis
- Malware identification, botnets, Malware packers and unpacking
- Behavioural analysis & Malware debugging

Day 2

- Recap & Introduction to malware encryption
- Anti-Virus products and file recovery, Statical analysis, Banking malware
- Malware scripts analysis & Malware network traffic analysis
- Exploit analysis & Malware anti-Forensics bypassing

Day 3

- Recap & Hands-on excercises
- Hands-on excercises
- Hands-on excercises
- Summary

On Day 3, the knowledge gained is further put into practice. In different assignments, including the analysis of advanced malware specimens and Capture The Flag (CTF) exercises, insight will be provided into the inner working of malware analysis and reverse engineering in practice.

HackLab: Hands-on Hacking

Computer hacking is the practice of influencing computer hardware and software to accomplish a goal outside of their original purpose. A computer hacker is a person who identifies weaknesses and exploits them. Hacking is considered a complex activity. This course will explore the world of hacking and shed a light on how hackers work.

Course objectives

The practical five-day course equips participants with hands-on black box, white box and grey box vulnerability testing. We will address testing of web applications, mobile applications, mobile devices, wireless security, host based and network based infrastructure.

The course takes the participants through the different stages of our proven methodology of information gathering, target selection and vulnerability identification and exploitation. Besides the methodology we will also discuss the different leading practises, such as OWASP and go into the different tools for vulnerability testing.

- Practical five-day course
- Proven methodology of information gathering, target selection and vulnerability identification and exploitation
- Discuss the different leading practices and go into the different tools for vulnerability testing

Target audience

- Security managers
- Application developers
- IT professionals
- IT auditors who have an interest in ‘Vulnerability Assessment’ and ’hacking’.

Participants of the course are expected to have a basic understanding of network, TCP/IP and Operating Systems (Windows and Linux).

Course date and location

This five-day course will be held on 11 – 15 April 2016, 26 – 30 September 2016 in The Hague or Utrecht.

Day 1

- Introduction & Security Trends
- Penetration testing methodology & External Infrastructure penetration test
- Firewall security / Prevention systems
- Physical security assessments and social engineering

Day 2

- Recap & Infrastructure security tests
- Infrastructure security tests continued
- Host-based security test & Wireless security test
- Wireless security test continued

Day 3

- Recap & Security Architecture
- Code review
- OWASP top 10
- Executing of a web application vulnerability assessment

Day 4

- Recap & Mobile Applications and security
- Security Operating Centres
- Malware analysis / Incident response
- Hacking game

Day 5

- Recap & Interview the client
- Vulnerability assessment execution
- Reporting and presentation of the results
- Evaluation and closing

HackLab: Covert Operations

Hacking is not exclusive to cyberspace, but can also be done in the physical world. How are these attacks performed? From gaining physical access to digitally exploiting systems without being noticed once you are in.

Course objectives

Information security is more than securing your IT systems. Attackers do not limit themselves to only abusing computer security weaknesses. Instead, they will use the path of least resistance. They might observe your physical location or they may try and blend in amongst your employees. They might send phishing emails and they might even trick your employees in order to gain access to your organization. Once an attacker has gained access to your systems, they will use lateral movements to break or bypass your digital defenses. Without appropriate monitoring and response they may even be gone before you even had a chance to notice what happened.

This practical three-day course provides participants with a solid foundation for performing covert operations. We will address both the theory and practical sides of covert operations, allowing participants to directly apply what they have learned directly in real-life scenarios.

Target audience

- Security managers
- Application developers
- IT professionals
- IT auditors with interest in vulnerability assessment and hacking

A condition for participation in covert ops is that participants allready followed Hacklab : hands on hacking.

Course date and location

This three-day course will be held on 4 - 6 November 2015 in Amsterdam or Rotterdam area and 14 - 16 March 2016 in The Hague or Utrecht.

Day 1

- Introduction to covert operations, backgrounds & trends
- Legal background of covert operations & planning the engagement
- Social engineering introduction & gaining physical entry
- Hands-on: role play/assignment

Day 2

- Recap & Offensive hacking
- Exploitation theory
- Capture the Flag (CTF) challenge
- Hands-on: Reconnaissance for day 3

Day 3

- Recap & Post-reconnaissance/planning
- Maintaining your foothold & actions once inside
- Detection avoidance
- Advanced exploitation techniques (escalation/pivoting/tunneling)

HackLab: SAP

Prevent leakage of your companies' administration! SAP application is the heart of your organization which makes it vulnerable. Arm yourself against vulnerabilities and secure your system against them by attending this one-day course HackLab: SAP.

Course objectives

This one-day course provides insight into the vulnerabilities of a SAP application and the associated infrastructure. After a brief introduction on SAP security and penetration testing in general, we will discuss a selection of known SAP vulnerabilities, showing you how easy it can be to access critical functions and data. We will also discuss how you can detect these vulnerabilities and properly secure your system against them.

- One-day course
- Hhow to detect vulnerabilities and secure against them
- Discuss known SAP vulnerabilities

Target audience

- (SAP) Security professionals.
- IT Managers.
- Risk managers.
- IT Professionals having an interest in SAP security and ethical hacking.

Information

For more information, please contact us: nlacademy@deloitte.nl

- Introduction & pentesting methodology
- Overview SAP components & Risks in a SAP landscape
- Sample vulnerabilities for the different SAP components
- Possible countermeasures

An average SAP landscape comprises a large number of technical components. It is impossible to discuss all possible vulnerabilities for all these components in a single day. Hence we have selected a number of relevant vulnerabilities, applicable for different components. This enables us to clearly outline the security possibilities in a SAP landscape.

ICS/SCADA Security

Securing control systems is a challenge. Off the-shelve software and hardware as well as remote access possibilities in industrial environments increases continuously. The broader threat landscape and increased sophistication of attacks indicate the need to improve ICS security capabilities. But where to begin?

Course objectives

The Deloitte ICS/SCADA Security Training is an intensive, three day program that covers a number of topics to better understand the ICS environment and improve the security of ICS systems. The course follows a storyline that links all the exercises to a fictive company called ACMEA.

During this training we will provide insight into threats, best practices, vulnerabilities and the controls to mitigate them. We will take the participant through the complete ICS security cycle: Know, Prevent, Detect, Respond and Recover.

- Provide insight in threats, best practices, vulnerabilities and mitigating controls
- Discover the complete ICS security cycle: Know, Prevent, Detect, Respond and Recover
- Hands-on experience with SCADA exploitation

Target audience

- IT Professionals
- Penetration testers
- Managers who wish to increase their knowledge of the SCADA environment and SCADA security assessments.

Information

For more information, please contact us: nlacademy@deloitte.nl

Day 1: General Knowledge & ICS framework

- Security basics
- ICS basics
- Developing governance and ICS framework
- Threat Management
- Incident Management

Day 2: Workshop and challanges

- Hands-on SCADA exploitation workshop (CTF)
- Network segmentatio
- Monitoring
- Remote access
- Client talk

Day 3: Solutions and practical approach

- Patching and Antivirus strategies
- Portable media
- Client talk
- Active and passive security assessments

Introduction to Cryptography

Every day people share information. Much of this information is confidential However, few of these exchanges are secured proportionally to their importance/sensitivity. This hands-on course covers techniques for correctly encrypting and exchanging messages and technical pitfalls related to them. Participants learn how to use cryptography in practice through several exercises and hands-on scenarios.

Course objectives

Most of the exchanged information needs to remain secret or unaltered. For as long as mankind exists, one has been interested in a technique that make this possible: 'the art of cryptography' (Greek: writing hidden).

In this three-day course we start our journey in the antiquity and go past various interesting cryptographic algorithms towards current times. The goal of this course is to give the participants a basic understanding of the cryptographic concepts and the involved risks.

- Practice through several exercises and hands-on scenarios
- Apply various cryptographic techniques

Target audience

- Security managers
- Risk managers
- IT security professionals
- IT auditors
- Security officers

Information

For more information, please contact us: nlacademy@deloitte.nl

Day 1

- Introduction to cryptography & terminology
- Cryptanalysis
- Basic Cryptography: Caesar, Vigenère, Enigma, One-time-pad, Kerckhoff's Principle
- Symmetric Cryptography
  Stream ciphers: LFSR, RC4
  Block ciphers: DES, AES

Day 2

- Recap & Asymmetric Cryptography: Diffie-Hellman, ElGamal, RSA, DSA, Elliptic Curve
- Asymmetric Cryptography: Diffie-Hellman, ElGamal, RSA, DSA, Elliptic Curve Continued
- One-way functions
- One-way functions continued

Day 3

- Recap & Applied Cryptography: SSL, PGP, SSH, IPSec
- Applied Cryptography: SSL, PGP, SSH, IPSec Continued
- Hands-on scenario's
- Hands-on scenario's continued

Key Management & Payment Security

Organizations heavily rely on the use of cryptography in order to secure their systems. Secure cryptographic solutions depend on the correct application of key management. This hands-on training covers the entire key management process from the creation of procedures up to the execution of key management ceremonies. The focus of this training is on cryptography used within payment environments.

Course objectives

This two-day course provides insight into key management practices and the security aspects of payment environments. Participants will gain practical experience with various aspects of the key management process, including the design of key ceremony scripts and execution of key management activities using hardware security module (HSM) devices.

The course starts with an introduction to key management, covering the various phases of the key management lifecycle: key creation, key storage, key exchange, key renewal and key destruction. After the introduction we will cover the procedures and techniques applicable to these various aspects of key management.

- Insight into key management practices and the security aspects of payment environments
- Develop practical skills through simulated activities
- Hands-on two-day cours

Day 1

- Introduction to key management
- Key management lifecycle, Key ceremonies & HSM (hardware security module)
- Designing scripts of key ceremonies & Storage of key materials
- Hands-on key ceremony script design

Day 2

- Recap & Introduction to HSM usage
- Hands-on HSM exercises
- Payment standards and protocols & Encryption of PINs in payment environments
- Hands-on exercises payment security

Target audience

- Key management employees

Also suitable for:

- Security managers
- Risk managers
- IT auditors
- IT security professionals
- Security officers who deal with key management or payment security during their day to day activities

Information

For more information, please contact us: nlacademy@deloitte.nl

SAP Security

During this five-day course, we will facilitate an in-depth view of SAP security. Starting from the basic concepts, the most important SAP security options will be discussed. Since we believe in 'doing is learning', the course not only provides technical background: it includes plenty of opportunity to discuss practical use, benefits, constraints and real-life examples. More importantly, many hands-on exercises are included, challenging participants to put the theory into practise. Deloitte uses its own sandbox environments to this end.

Course objectives

If you have ever been involved with SAP and its security concept, you are most likely familiar with the term SAP_ALL. Developers say they can't work without it, auditors say nobody should have it assigned.

This course will teach you the most important SAP security features and will allow you to understand their implications. It will enable you to tailor the security settings and procedures to best fit your organization without losing sight of best practices.

- In-depth and hands-on five-day course
- Tailor the security settings and procedures to best fit your organization
- Most important SAP security options

Target audience

- Security managers
- SAP application managers
- SAP security professionals
- IT auditors regularly dealing with SAP related security challenges and such.

Information

For more information, please contact us: nlacademy@deloitte.nl

The SAP Security course will cover the most important security settings for an SAP ERP system. You will be introduced to SAP basis security features, their implications and constraints, where they are implemented, and how they can be audited. The course will also address topics such as 'hacking' vulnerabilities, tooling and best practises. Although the course will focus on SAP ERP (commonly also referred to as R/3 and ECC), these concepts likewise apply to all other ABAP based systems, such as CRM, SRM and BI.

The following topics will be addressed:

- The SAP Landscape
- Access Path
- Introduction to Security
- Navigation
- User Management
- Authorization concept
- Profile Generator
- Logging
- System Parameters
- Transaction Security
- Program Security
- Table Security
- Job Scheduling
- Change Management
- Interfaces
- Use of tooling such as GRC.

In-house training, custom training and learning programmes

Deloitte offers more than just the trainings referred to before. We provide in-house trainings too: anything from standard trainings to trainings tailored to your organization. We can even set up a full learning programme uniquely geared to your organization.

In-house training

In-house or in-company training distinguishes itself because it specifically focuses on your organization. The training can thus be adapted to your wishes.

Standard training

Apart from our offerings discussed in this flyer, we have a great choice of standard trainings available. We can consult with you to include specific priority aspects you consider to be important.

Custom training

A careful analysis of your learning needs and an extensive intake will enable us to prepare a custom training. This will allow you to train and educate your professionals very effectively. Since the course materials and examples will be geared to your own organization, your professionals will be able to immediately use what they have learned in their daily practice.

Learning programme

In addition to offering in-house trainings, we also offer you the option to prepare a full, tailored learning programme, entirely geared to your organization, the business objectives, and the employees' learning needs.

Costs

Feel free to contact us for more information on pricing or to get a quote. Even a relatively low number of participants can make an in-house training more economical than a regular external training.

Further information

If the training you need is not stated here, or if you want further information on our training and learning offering, please contact us. Contact details can be found in the back of this brochure.

Topics

Deloitte provides a great deal of trainings all across the world, so we have a large number of standard trainings and topics readily available. These are just some of the trainings we have on offer:

- Security & Risk Management (Governance, Frameworks, Architecture, Transformation)
- Business Continuity & Disaster Recovery
- Identity & Access Management
- Security Architecture
- Cyber Security
- Infrastructure Protection
- Application Protection
- Secure Software Development
- End User security (Awareness, Social media, Mobile devices)
- Vendor control (Cloud computing, Assurance)
- Privacy
- Hacking and Vulnerability Assessments

Specific systems & certifications

In addition, we offer security trainings on specific systems, such as SAP and Oracle. We can arrange trainings for most of the security certifications (CISSP, CISM, CISA, CEH, etc.) as well.

Training forms

We are able to provide various training forms such as: classroom based, e-learnings, webinars, workshops and game-based.

Your facilitators

Our professionals are your facilitators − sharing with you their practical knowledge. Our course offerings distinguish themselves by being topical and effective. The limited number of participants per course offers plenty of space for interaction between facilitator and participants in a stimulating and pleasant atmosphere. The following professionals facilitate the courses mentioned in this brochure:

Marko van Zwam

Partner Deloitte Security & Privacy

Marko is a partner within Deloitte Risk Services and leads the Security & Privacy team, which consists of more than 100 professionals. He has over 18 years of experience in IT, IT Security, IT Audit and IT Risk Management.

Gijs Hollestelle

Facilitator CISSP Certification

Gijs is a senior manager in the Security & Privacy team. Gijs has over 8 years of experience in security issues, from security awareness to IT infrastructure security and Ethical Hacking. Gijs was part of the winning team at the Global CyberLympics 2013.

Coen Steenbeek

Facilitator HackLab – Hands-on Hacking

Coen is a manager in the Security & Privacy team. Coen specializes in both technical engagements like vulnerability assessments and in performing security management related tasks (ISO27001 / 2). During his career at Deloitte Coen has earned the RE, CEH, CISSP, CISM and CGEIT certifications and he was part of the winning team at the Global CyberLympics 2013.

Trajce Dimkov

Facilitator ICS/SCADA

Trajce is a manager within the Security & Privacy team and has over 7 years of experience in ICT infrastructure and security. Trajce specializes in both security management of industrial control systems and vulnerability assessment. Previous to his work at Deloitte, Trajce did a PhD at the University of Twente on social engineering and physical penetration testing and is currently involved in many vulnerability assessments that include these two ingredients.

Frank Hakkennes

Facilitator SAP Security & HackLab: SAP

Frank is a manager in the Deloitte Security & Privacy Risk Services team. Frank specializes in security management, particularly for SAP environments. Frank is a certified SAP Security Consultant and has been responsible for audit, implementation and advisory services in respect of (SAP) security and configuration management.

Ivo Noppen

Facilitator CISSP Certification

Ivo is a junior manager at Deloitte Cyber Risk Services. With a strong background in telematics and software development he obtained in-depth knowledge of security in web applications, infrastructure and source code. Ivo was part of the winning team at the Global CyberLympics 2013.

Henk Marsman

Facilitator CISM Certification

Henk is a senior manager in the Security & Privacy team and has over 13 years of experience in IT Security and risk management. Henk focusses on security management and identity & access management. He also has a background in public key infrastructure and network security. Currently Henk co-leads the Security management practice within the Security & Privacy team.

Wieger van der Meulen

Facilitator CISM Certification

Wieger is a junior manager at Deloitte Cyber Risk Services with over 4 years of experience in IT-security. With a background in business administration, Wieger is focused on governance and process assignments, which include identity and access management assessments, ISO 2700X implementations and general IT-security management work.

Vojtech Brtnik

Facilitator CISA Certification

PJ has over ten years of experience in information security, and since 2011 works for the Deloitte Cyber Security team. PJ specializes in technical topics such as hacking, vulnerability management and risk assessments. He has been teaching various topics for the last three years. PJ holds all ISACA certifications.

Michiel de Jager

Facilitator CISA Certification

Michiel is a manager at Deloitte Risk Services and has over 6 years of experience within the fields of assurance. He worked on engagements related to IT audit, IT security, Data Analytics and risk management and holds several certifications in the area of security and controls such as CISA, CISSP and CISM.

Ruud Schellekens

Facilitator CISSP Certification, Key management & Payment Security

Ruud is a manager in the Security & Privacy team. With a strong IT background, Ruud started as an IT auditor. In this role he obtained a broad knowledge of the security of ERP applications and IT infrastructures. In addition, Ruud has been involved in developing various Deloitte security auditing tools. Ruud is a certified CISM, EDP auditor, CISSP and GRAPA professional.

Rob Muris

Facilitator Hands-on Hacking

Rob Muris is a senior consultant within the Cyber Risk Services team of Deloitte Netherlands. He has over 6 years of experience in IT from various medium to large companies with more than 3 years in IT security. Rob specializes in technical infrastructure related engagements like vulnerability assessments. During his career at Deloitte Rob has earned the CEH certification and he was part of the Deloitte team at the Global CyberLympics 2013.

Hugo van den Toorn

Facilitator HackLab: Covert Operations

Hugo is a Consultant at Deloitte Cyber Risk Services. Hugo graduated cum laude in Informatics, with focus on management and security. He passed his CISM examination and is ISO/IEC 27001:2005 Foundation certified. He has gained experience in penetrations tests and specializes in covert operations, covering aspects such as: social engineering, phishing and physical penetration testing. Beside security assessments, Hugo also provides hacking demonstrations and awareness trainings.

Arjan de Mooij

Facilitator CISM Certification & Security Incident Management

Arjan is a Junior Manager at Deloitte Cyber Risk Services. Arjan has more than 8 years of experience in the areas of process management, Incident Management and Crisis Management. From 2011 t/m 2013, Arjan fulfilled the position of National IT Incident Manager at the Dutch Ministry of Infrastructure and the Environment. He works at Deloitte since 2014.

Ari Davies

Facilitator HackLab: Covert Operations and Hands-on Hacking

Ari is Senior Manager at Deloitte Cyber Risk Services and has over 12 years of information security and ethical hacking experience. Ari is an experienced penetration testing consultant and engagement manager with notable experience in extensive and complex multi-tiered security engagements as well as an extensive background in security operations. Ari's big interest is with the more "covert" side of ethical hacking, such as red teaming, social engineering, phishing and physical penetration testing. Ari has experience with multiple government and private sector organizations both in the UK as well as overseas.

Jan-Jan Lowijs

Facilitator Prepare for Privacy & CIPP-E Certification

Jan-Jan is a manager in Deloitte's Dutch Privacy Team, part of Cyber Risk Services. He has a background in information security, but his focus today is on the subject of privacy and data protection. He has 8 years of experience in the privacy and data protection field, as an advisor regarding specific privacy rules and regulations and as an auditor of personal data processing environments. Besides a CIPP/E, Jan-Jan has also earned the CISSP certification for security professionals.

Marlous Theunissen

Facilitator HackLab: Malware Analysis & Introduction to Cryptography

Marlous is a consultant in the Security and Privacy team of Deloitte Risk Services. Marlous graduated cum laude in Computer Science and Engineering with focus on both security and algorithms. She has gained experience in penetrations tests and malware analysis, and passed both the CISM and CISSP examinations this year.

Joost Kremer

Facilitator HackLab: Malware Analysis & Introduction to Cryptography

Joost is a security consultant in the Cyber Risk Services team of Deloitte Risk Services. Joost has a background in Information Security Technology. During his study he obtained technical knowledge on various topics, including RFID, Mobile and Cryptography.
His analytical skills allow him to break down complex problems into manageable chunks. He furthermore has the ability to translate his knowledge in understandable presentations and trainings for any level.

Jan Wijma

Facilitator CISA Certification

Pieter Westein

Facilitator Hands-on Hacking

Martijn Roeling

Facilitator SAP Security

Martijn is a Senior Consultant within Deloitte Risk Services. Martijn has over 3 years of experience in IT, of which more than 2 years in the SAP area. He is a certified SAP HR (HCM module) consultant obtained at the SAP Academy. Martijn has experience with integrated audits, IT audits and is specialized in risks and controls for SAP and Human Capital Management.

Dima van der Wouw

Facilitator ICS/SCADA

Dima graduated at the Technical University of Eindhoven for the master Information Security Technology. In his thesis he determined the prior system knowledge needed for an attacker to develop malware for ICS. Recently, Dima created a small S7-based ICS used for educational, demo and CTF purposes. Dima is currently researching about patching and antivirus update methodologies and solutions for ICS.

Spase Stojanovski

Facilitator ICS/SCADA

Spase is a junior manager at Deloitte Cyber Risk Services and has over 6 years of experience in IT. He specializes in security management combined with deep understanding of industrial control systems. His main focus is security monitoring and automated vulnerability assessments of ICS systems.

Inez Gasman

Facilitator Prepare for Privacy and CIPP-E

Additional course information

Number of participants

Depending on the nature of the course and the level of interaction we have a maximum number of participants per course.

Course hours

9:00 to 17:30 hours, including lunch.

Location

Our courses are being facilitated at our office in Amsterdam. Approximately one month before the course date you will receive more information about the exact location of the course.

Language

The courses will be given in English or Dutch, depending on the participants' preferred language. The course material is in English.

Cancellation policy

Please refer to our website for our Terms and Conditions and cancellation policy.

Deloitte Academy reserves the right to cancel the course in the event of insufficient registrations. You will be informed about this on time.

Permanent Education

Deloitte Academy is a NBA (The Netherlands Institute of Chartered Accountants) acknowledged institution. These courses will earn you PE points.

Registration

You can register for this course throughwww.deloitte.nl/

More information

For more information about these courses contact:

Deloitte Academy
Postbus 2031
3000 CA Rotterdam
Phone: 088 − 288 9333
Fax: 088 − 288 9844
E-mail: **nlacademy@deloitte.nl**
Internet: **www.deloitte.nl/academy**