ICBC

Capacity Building Center of the
Institute for Security and Safety

Training courses

Trainings can be held as:

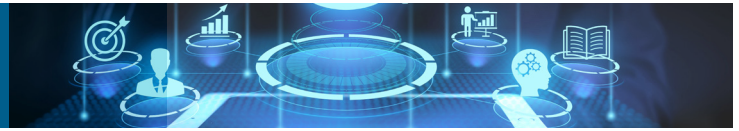
- E-learning/self-study (with interactive workshops)
- Web-seminars of Face-to-Face training
- Presence training incl. laboratory exercises (in-house or external)

Please contact us to find out if the training courses can be delivered in your preferred training format.

ICBC
Capacity Building Center of the
Institute for Security and Safety

Management Courses	Target Group	Contents	Learning Goals
Introduction to IT Security DE/EN	Non-professionals, ordinary workforce with no direct IT security responsibilities who require IT security knowledge as part of a holistic cybersecurity approach.	Introduction to basic principles of IT security such as threats, vulnerabilities, protection measures and dynamics on networks and PCs.	Understanding of basic principles that determine the security of the IT infrastructure in either the private or corporate environment.
Awareness and Compliance for Cybersecurity DE/EN	Professionals at all employment levels.	IT vulnerabilities in corporate environment, passwords/ authorization and verification processes, legal framework/requirements, protection through awareness (human factor).	Awareness of IT and information security vulnerabilities in the work environment, understanding of the use of protective measures against cyber incidents, understanding of the role of each individual in cybersecurity, understanding of the implementation of (basic) compliance requirements for information security.
Introduction to Information Security Management Systems (ISMS) DE/EN	Corporate users interested or required in establishing an Information Security Management System (ISMS) framework at their own organization.	Introduction to the conceptual structure of an ISMS, benefits and requirements, first-steps guide to establish an ISMS in corporate structures. Familiarization with the requirements for certification.	Understanding of benefits and requirements as well as steps for practical implementation of an ISMS. Basic understanding of what is needed for a certification audit.
Risk Management DE/EN	Professionals with information security esponsibilities, managers, ISOs, CISOs.	Risk assessment and risk management as a core process for an ISMS, risk handling and mitigation strategies. General introduction to emergency operation planning, crisis management, and cyber-insurance.	Understanding of risk management processes according to ISO 27000 and ISO 31000.
Incident Response EN	Professionals at management or employment level with any information security responsibility or supporting roles.	Introduction to cyber incidents and subsequent response measures, structure of response plans, roles and responsibilities of staff in incident response.	Understanding of the importance of cyber incident response, consequences of inadequately handled incidents, guide to the preparation of cyber response plans, understanding of the main phases of the response process, main techniques for incident response, knowledge of the desired behavior, of roles, and responsibilities during incidents.
Security culture DE/EN	Employees in leadership positions and all responsible for implementing data protection, information security, and cyber security in a company.	From organizational culture to security culture - more than awareness: steps to be taken to assess the status, define roles and start implementing a security culture. Dealing with mistakes and how to establish trustful communication.	Participants can assess the status and define steps to improve security culture in their company.

Specific training courses are available for different industries such as energy, automotive and industrial/mechanical engineering.



ISS Capacity Building Center Ettlingen (ICBC) · Ottostraße 1 · 76275 Ettlingen · Germany · info@uniss.org · www.icbc.uniss.org

ICBC

Capacity Building Center of the
Institute for Security and Safety

Technical Courses	Target Group	Contents	Learning Goals
IT Security Techniques DE/EN	Managers, engineers, employees from all fields (public & private) with the desire or need for extending their expertise in cyber-security.	Computer security elements fundamentals, Computer Access Control, Security Architecture, technical measures for network and host security, network management best practices, the role of physical protection in computer security.	Understanding of basic techniquesof cyber-security on a technical level, knowledge of best practices in cyber-security.
OT-Security for Industry 4.0 DE/EN	OT specialists wanting to extend their knowledge in OT security for future developments related to interconnected industrial infrastructure (4IR).	Industrial IoT concepts, challenges of interconnected systems, best practices for a secure IoT implementation, non-technical aspects of Industry 4.0.	Understanding of challenges and opportunities of smart systems, implemtation of security relevant processes in building up inter-connected industrial systems.
OT-Security for SCADA/ICS DE/EN	ICS engineers, technical employees in digitalization, security architects, ISOs, CISOs.	Introduction to the world of ICS, main differences between office computer systems and industrial control systems, challenges in ICS protection, best practices in ICS security.	Understanding of peculiarities of ICS security in comparison to classical security control, protection of critical assets without compromising their availability, understanding of conflict potentials between IT and OT security.
Protection of Physical Security Systems against Cyber Attacks DE/EN	Professionals with security responsibilities in IT or building technology, integrators, engineers, ISOs, CISOs.	Threats overview, physical vulnerabilities (attack vectors), protection measures, security system performance testing and assessment techniques, connection between physical and cyber security.	Understanding of physical threats and vulnerabilities and related threat mitigation techniques, understanding of the effects of cybersecurity on physical security and the other way round.
Penetration Testing DE/EN	Network administrators, Red-Team members, security officers, CISOs, ISOs.	Differences between vulnerability analysis and penetration testing, comparison of penetration testing methodologies and real attacker techniques, presentation of the most prominent tools for penetration testing, writing of good penetration testing protocols.	Learners can expose cyber vulnerabilities in their company, eliminate them, and write penetration testing protocols.
Forensics DE/EN	Experienced employees with responsibility in computer security and Cyber Incident Response.	Building on participant's existing knowledge of computer technology and network communication, typical techniques and methods for computer forensic procedures and network forensics will be trained hands-on.	Understanding of main application areas, principles, techniques and limitations of computer forensics.

Specific training courses are available for different industries such as energy, automotive and industrial/mechanical engineering.