Cyber Resilience and ISO 27032 Cybersecurity Guidelines Training Course

21 - 25 Dec 2026

Munich

5100 € (Per Person)

Ref: #ISO4522_115614

Course Introduction / Overview:

This comprehensive training course provides an in-depth exploration of building and maintaining organizational cyber resilience, anchored by the internationally recognized ISO/IEC 27032 standard for cybersecurity. In today's hyper-connected digital landscape, a reactive approach to security is no longer sufficient. Organizations must develop the capacity to anticipate, withstand, recover from, and adapt to adverse cyber events. This course moves beyond traditional information security to a more holistic, strategic framework for resilience. As noted by cybersecurity expert Eugene H. Spafford, security is not a product, but a process. This principle is at the core of our curriculum, which is designed to equip participants with the knowledge to implement a continuous, process-oriented cybersecurity program. We will delve into the key components of the ISO/IEC 27032 guidelines, covering stakeholder collaboration, information sharing, and incident response coordination. Participants will gain practical insights inspired by foundational texts like "Cybersecurity and Cyberwar: What Everyone Needs to Know" by P.W. Singer and Allan Friedman, learning to apply these concepts within their own operational contexts. BIG BEN Training Center has meticulously designed this program to bridge the gap between theoretical knowledge and practical application, ensuring attendees can build a robust defense and a resilient operational posture against sophisticated cyber threats.

Target Audience / This training course is suitable for:

- Chief Information Security Officers (CISOs).
- Cybersecurity Managers and Analysts.
- IT Directors and Senior IT Staff.
- Information Security Consultants.
- Risk and Compliance Managers.
- Incident Response Team Members.
- IT Auditors and Governance Professionals.
- Security Architects and Engineers.
- Business Continuity and Disaster Recovery Planners.
- Professionals seeking to implement ISO/IEC 27032.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Information Technology and Telecommunications.
- Energy, Oil, and Gas Utilities.
- Retail and E-commerce.
- Manufacturing and Industrial Control Systems.
- Government Agencies and Public Sector Bodies.
- Transportation and Logistics.
- Education and Research Institutions.
- Consulting and Professional Services.

Target Organizations Departments:

- Information Technology (IT) Department.
- Information Security and Cybersecurity Department.
- Risk Management Department.
- Internal Audit and Compliance Department.
- Legal and Regulatory Affairs Department.
- Operations and Business Continuity Planning.
- Corporate Governance and Strategy.
- Research and Development.
- Human Resources (for security awareness programs).
- Procurement and Supply Chain Management.

Course Offerings:

By the end of this course, the participants will have able to:

- Develop a comprehensive cyber resilience strategy aligned with business objectives.
- Interpret and apply the ISO/IEC 27032 framework for enhancing cybersecurity.
- Establish effective mechanisms for information sharing and collaboration.
- Strengthen incident response and recovery plans to minimize operational impact.
- Conduct thorough cybersecurity risk assessments and vulnerability analyses.
- Integrate cyber resilience principles into the organizational culture and processes.
- Manage and coordinate responses to complex, multi-stage cyber-attacks.
- Ensure compliance with relevant cybersecurity regulations and standards.
- Improve the security of the digital supply chain and third-party relationships.
- Lead continuous improvement initiatives for the cybersecurity program.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to foster a dynamic and engaging learning environment that maximizes knowledge retention and practical application. This course employs a blended learning approach, combining expert-led instruction with interactive, participant-centered activities. Theoretical sessions will introduce core concepts, frameworks, and the intricacies of the ISO/IEC 27032 standard, providing a solid foundation of knowledge. These sessions are complemented by in-depth case study analyses of real-world cyber incidents, allowing participants to explore the strategic decisions and technical failures that led to them. A significant portion of the course is dedicated to hands-on workshops and group exercises where participants will collaborate to develop resilience strategies, draft incident response playbooks, and conduct simulated risk assessments. This collaborative approach encourages peer-to-peer learning and the sharing of diverse industry experiences. Our instructors facilitate interactive discussions, Q&A sessions, and provide continuous, constructive feedback to ensure all participants can confidently apply the learned skills in their professional roles. The focus is on moving beyond theory to build tangible capabilities for enhancing organizational cyber resilience.

Course Agenda (Course Units):

Unit One: Foundations of Cyber Resilience and the ISO/IEC 27032 Framework

- Defining cyber resilience versus traditional cybersecurity.
- The importance of a proactive and adaptive security posture.
- Introduction to the ISO/IEC 27000 family of standards.
- Detailed overview of ISO/IEC 27032 as a guideline for cybersecurity.
- Key principles and objectives of the ISO/IEC 27032 standard.
- Understanding the roles of stakeholders in the cybersecurity ecosystem.
- Establishing a framework for policy and governance.

Unit Two: Cybersecurity Risk Management and Threat Intelligence

- Identifying critical assets and business processes.
- Conducting comprehensive cybersecurity risk assessments.
- Methodologies for threat modeling and vulnerability analysis.
- The role of threat intelligence in a resilience strategy.
- Sources and types of cyber threat intelligence.
- Integrating threat intelligence into security operations.
- Developing a risk treatment plan and mitigation strategies.

Unit Three: Implementing Technical and Procedural Controls

- Mapping ISO/IEC 27032 controls to organizational needs.
- Implementing network security and endpoint protection measures.
- Application security and secure coding practices.
- Identity and access management (IAM) strategies.
- Data protection, encryption, and data loss prevention (DLP).
- Establishing security awareness and training programs for all employees.
- Managing third-party and supply chain security risks.

Unit Four: Incident Response, Management, and Recovery

- Developing a robust incident response plan (IRP).
- The incident response lifecycle: preparation, detection, analysis, containment, eradication, and recovery.
- Forming and training a Computer Security Incident Response Team (CSIRT).
- Techniques for digital forensics and evidence collection.
- Crisis communication and stakeholder management during an incident.
- Business continuity and disaster recovery planning for cyber events.
- Post-incident analysis and lessons learned for continuous improvement.

Unit Five: Building a Resilient Culture and Continuous Improvement

- Fostering a security-first culture throughout the organization.
- The role of leadership and executive sponsorship in cyber resilience.
- Metrics and Key Performance Indicators (KPIs) for measuring resilience.
- Conducting cybersecurity drills, tabletop exercises, and simulations.
- Auditing and assessing the effectiveness of the cybersecurity program.
- Adapting the resilience strategy to emerging threats and technologies.
- The future of cyber resilience and preparing for next-generation attacks.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

In an era of state-sponsored cyber-attacks and AI-driven threats, how can the principles of ISO/IEC 27032 evolve to address not just technical resilience but also geopolitical and ethical complexities?

What unique qualities does this course offer compared to other courses?

This training course distinguishes itself by uniquely integrating the strategic, high-level concept of cyber resilience with the practical, actionable framework of the ISO/IEC 27032 guidelines. While many courses focus either on broad resilience theory or narrow technical controls, this program bridges that critical gap. It provides a holistic perspective that treats cybersecurity not as an IT problem, but as a core business function essential for organizational survival and growth. The curriculum is meticulously structured to build a deep understanding of how to anticipate and adapt to threats, rather than merely reacting to them. We emphasize the interconnectedness of people, processes, and technology, dedicating significant time to building a security-aware culture and managing supply chain risks, which are often overlooked. The course content is enriched with contemporary case studies that go beyond typical examples, exploring complex, multi-faceted attacks and the strategic decisions that determined their outcomes. Participants will leave not just with knowledge of a standard, but with a strategic mindset and a practical roadmap for building a truly resilient organization capable of withstanding the sophisticated cyber challenges of today and tomorrow.