

ISO/IEC 27001 – Information Security Management Systems (ISMS)



24 - 26 February 2010

Bucharest, Romania



International
Organization for
Standardization



Introduction

THIS SEMINAR WILL HELP YOU TO:

- ✓ Understand the requirements of the well known international standard ISO/IEC 27001
- ✓ Understand how to implement the ISO/IEC 27001 and ISO/IEC 27002 standards and the route to certification
- ✓ Gain insight into how to carry out ISMS (Information Security Management Systems) risk assessments and selection of controls
- ✓ Discuss important issues in risk management and gain hands-on experience in performing risk assessments

LEARN ALL ABOUT THE LATEST DEVELOPMENTS OF STANDARDS

- The new "27000 Family of Standards" (ISO/IEC 27000 – ISO/IEC 27007)
- ISO/IEC 27001:2005
- ISO/IEC 27002:2005
- ISO/IEC 27005:2008
- ISO/IEC 18044

MEET YOUR TRAINER: DR. ANGELIKA PLATE

Dr. Angelika Plate is editor of the revised version of ISO/IEC 27002 (former ISO/IEC 17799), of the accreditation standard ISO/IEC 27006, and currently edits the new standard ISO/IEC 27007.

She also supported and contributed to the development of ISO/IEC 27001, the international version of BS 7799-2.

WHO SHOULD ATTEND

IT and information security professionals who, through their involvement in managing or directing their organisation's IT infrastructure, are responsible for establishing and maintaining information security policies, practices and procedures. Additionally: System Administrators, Telecommunications Managers, Corporate Security Managers and Safety and Continuity Planning Managers will also benefit.

This seminar will also be of value to financial and operational audit professionals as well as non-IT professionals tasked with the responsibility of assessing their organisation's IT operations, infrastructure and security.

ACKNOWLEDGEMENTS

The workshop is hosted by the Asociatia de Standardizare din România (ASRO) and co-financed by the Swedish International Development Cooperation Agency (Sida).



Programme

24 February 2010

The 27000 Family of Standards and ISO/IEC 27001:2005

- Introduction
- MCSI Initiatives In Information Security Area by **Maria Bădilă**
- The “27000 Family of Standards” – an overview
- History of the standards
- What is in ISO/IEC 27001?
 - PCDA process
 - Management system requirements
- Information about the revisions
- Certification process
 - ISO/IEC 27006 requirements for the accreditation of bodies providing certification of ISMS
- Principles of ISMS auditing
- How an organisation can address certification

25 February 2010

ISO/IEC 27001 – Risk Assessment and Management

- Introduction to risk assessment
 - ISO/IEC 27005 ISMS risk management
- Identifying security requirements
- Identifying and evaluating assets
- Identifying threats and vulnerabilities and the risk of exposure
- Calculating risks
- Selecting the right risk treatment option(s)
- Selecting the best set of controls and producing a statement of applicability
- Case Study

26 February 2010

The 27000 Family of Standards

- Other related standards in the 27000 family, including:
 - ISO/IEC 27000 principles and vocabulary
 - ISO/IEC 27002 Code of practice for information security management
 - ISO/IEC 27003 implementation guidance
 - ISO/IEC 27004 information security management metrics and measurement
 - Examples of useful measurements
 - ISO/IEC 27007 ISMS auditor guidelines
 - ISO/IEC 2701x Sector-specific ISMS standards
 - ISO/IEC 18044 information security incident management
 - In-depth discussion of information security incident handling
 - Setting up an incident management process
 - ISO/IEC 2701x Sector-specific standards
 - ISO/IEC 20000 IT service management
 - BS 25999 Business continuity management
- Summary of the course

Discussion, questions and answers





International
Organization for
Standardization

1, chemin de la Voie-Creuse
Case postale 56
CH -1211 Genève 20
Switzerland

Tel. + 41 22 749 01 11
Fax + 41 22 733 34 30
E-mail central@iso.org
Web www.iso.org