

Course:**Best Practice in IT Security Management
with ISO 27001 (Introduction)**

Duration: 3 Days (9:00 – 16:00)

Course Description:

The international standard ISO/IEC27001 provides a framework for organizations to implement 'best practices' in Information Security Management. The ISO standard is quite high level and generic and in most cases does not provide practical solutions. This course will fill up this gap by providing more examples in real life cases.

Course Objectives:

This course is a practical approach to the implementation of Security to ISO17799 and ISO 27001 standard

Who should attend:

- This course provides comprehensive first-level training for personal who would like to comply with ISO27001 or anyone involved in provision, support, and delivery of organization's computer IT Security to comply with the new Thai Computer Security Law that will start enforced estimated in year 2008. Potential attendants may includes:
 - IT Head / IT Manager / EDP Manager / CIO
 - Consultants / System Integrators
 - Regulators / Business Owners
 - IT Security and Control Professionals

Course Benefits:

- You will learn a world class framework for resolving security issues
- Enhancement of client confidence & perception of your organization
- Enhancement of business partners' confidence & perception of your organization
- Provides confidence that you have managed risk in your own security implementation
- Enhancement of security awareness within an organization
- Assists in the development of best practice
- Can often be a deciding differentiator between competing organization

Course outline:

- Background of ISO17799/27001
- Security policy
- Security organization
- Asset classification & control
- Personnel security
 - Personnel screening
 - Confidentiality agreements
- Physical & environmental security
- Communication & operation management
 - Change control
 - Segregation of duties

- Housekeeping (Back-ups, operator logs)
- Access control
 - User Registration
 - Privilege management
 - Password management (including quality/strong passwords)
- System Development & maintenance
- Information security incident management
- Business continuity management
- Business Impact analysis
- Compliance
- ISO Implementation Risks and Success Factors

What is ISO 27001?

ISO 27001 was published by the International Organization for Standardization (ISO) on 15 October 2005. Essentially, ISO/IEC 27001 defines an Information Security Management System (ISMS) and complements the ISO/IEC 17799 'code of practice' standard, itself first published as BS 7799-1. The two standards are closely aligned and related, but perform distinctive roles.

ISO/IEC 27001 is a standard setting out the requirements for an information security management system (ISMS). The standard is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties including an organization's customers. ISO 27001 is a risk based approach for assessing, evaluating, treating and managing Information and Asset security risks, a review process for re-assessing the risks and the effectiveness of this system and to have an internal ISMS audit process for checking compliance.

Benefits of ISO 27001

- A world class framework for resolving security issues
- Enhancement of client confidence & perception of your organization
- Enhancement of business partners' confidence & perception of your organization
- Provides confidence that you have managed risk in your own security implementation
- Enhancement of security awareness within an organization
- Assists in the development of best practice
- Can often be a deciding differentiator between competing organization

For more information please visit:

http://en.wikipedia.org/wiki/ISO_27001

http://en.wikipedia.org/wiki/International_Organization_for_Standardization

http://www.iso.org/iso/catalogue_detail?csnumber=42103