

## Course Content

This course will provide information on the following topics:

- Introduction to Management System Principles and Concepts
- Detailed introduction to ISO/IEC 27001:2005 (ISO 27001) and the related series of standards
- ISMS Requirements Definition, Scope Estimation, Design, and Implementation (using Requirements Specifications, Best Practices and Guidelines, Example Deliverables, Mindmaps, and Project Planning Documentation)
- Legal, Regulatory, Self-Imposed, and Contractual Requirements Definition and Documentation
- Information Security Risk Assessment, Governance, and Business Continuity Management
- ISO and ISMS Audit Perspective and Approach

Also included as part of the course are:

- Authorized printed **copies of the ISO 27001 and ISO 27002 standards**
- Practical exercises and feedback
- Tools and Examples

The course uses a mixture of tutored sessions, interactive group discussions, group and personal exercises, and functional workshops to achieve its objectives. The practical exercises are designed to directly address operational issues typically encountered in an ISMS implementation project. Examples and tools are provided which are immediately useable. Courseware has been designed to address issues that arise during Information Security Management System implementation projects and Registration audits. Course delivery will include Lecture (Slides and Examples), Facilitated Discussion (Instructor-/Delegate-Led), Tactical Exercises and Feedback and tools and examples. Participants are expected to use their own laptops during the course.

## Benefits

This course will provide successful delegates with the following benefits:

- Advanced knowledge of the requirements of ISO 27001 and related standards and guidelines
- A basic knowledge of Management Systems, focusing on Information Security Management Systems (ISMS)
- Detailed understanding of the processes necessary to design, document, and implement an Information Security Management System (ISMS) conforming to the requirements of ISO 27001
- A basic knowledge of U.S.-specific Security, Privacy, and Ethics Legislation

*Course Overview continued on next page...*

- An understanding of validated concepts and methodologies for assessing and managing Information Security Risk and performing adjudicated Gap Analyses
- An understanding of auditor expectations and the process approach to auditing of Information Security Management systems (from Consultant/Auditee perspectives)
- An understanding of the documentation and evidence necessary to state conformity to and/or pursue certification to the requirements and specifications of ISO 27001

## Prerequisites

It is recommended that delegates attending this course have moderate level working knowledge and understanding of Information Security (examples: CISSP, CSM, Previous ISO 27001 Certification and/or 5 Years Experience) and Management Systems (ISO Management Systems, Lead Auditor Courseware, IRCA/RAB-QSA Certification and/or 5 Years Experience) concepts. Delegates will work individually and in teams, and a laptop is required (Windows or Macintosh with Microsoft-compatible Word Processing, Spreadsheet, and Presentation software).

## Instructor

This class will be lead by **Robert A. Aanerud - CISSP, CISA, CPP, CHSP**, a leading expert in Information Security, Privacy and International Law. He is an internationally respected Security and Privacy consultant and speaker, with over 41 years experience in technology, security, privacy, risk assessment, project management, training, and business continuity planning.

Robert is a Principal Trainer, Auditor, and Consultant at JBW Group International. He previously held positions as Principal in a "Big 4" Audit and Management Consulting firm, Senior Executive Service positions in the Intelligence Community, and Management positions in multiple organizations. He has served on numerous Advisory, Internet, Electronic Commerce, Security, and Technology boards, and as chairman of multiple security and communications task forces.

Robert has consulted with over 120 of the Global Fortune 500 on major technology, security, and privacy projects, and currently specializes in support to clients in Healthcare, Insurance, Telecommunications, Transportation, Logistics, Manufacturing, Energy, Oil and Gas, Internet/Electronic Commerce, and Financial Services industries.

Mr. Aanerud is a Certified Information Systems Security Professional (CISSP), and an IRCA- and Registrar-Certified BS25999, ISO 9001, ISO 20000, ISO 27001, and ISO 28000 Lead Instructor and Principal Auditor.

Robert holds a PhD in International Law and Regulation, a BA in Business and Marketing Management, an LLB in U.S. Constitutional Law, and a British Computing Society ISEB Certificate in IT Law.

## Outcome

A JBW Group International "*Certificate of Demonstrated Competence*" will be issued to those delegates deemed to have achieved a satisfactory standard of learning and competence. An appraisal of delegates' knowledge and performance will be made through a combination of continuous assessment and after-course feedback mechanisms.

For delegates attending this course who have already achieved IRCA or RAB-QSA Lead Auditor certification in an Accredited Management System Scheme, this course satisfies IRCA and RAB-QSA Certification requirements as a "Transitional" Auditor Course meeting ISO/IEC 27001:2005 scheme requirements for Lead Auditor certification.

## Method of Delivery and Timetable

This course is available for **Onsite** session and in the **Public Venue**. This is a three-day intensive course equivalent to 24 credit hours; the times will be 8:00 AM – 5:00 PM unless otherwise arranged.