

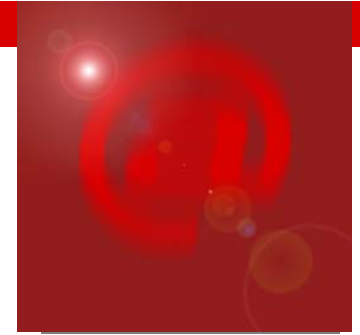


Information Security Management Systems

Peter Wimmer, Fiona Pattinson

ISO/IEC 27001 and related topics

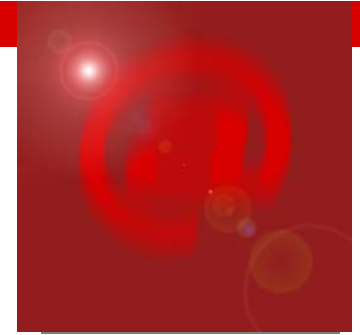
Services offered by atsec - Overview



Where we can help you	You need information	You need advice	You need support
You don't have an ISMS	We educate you about what is an ISMS, about the world of security standards and how they can support your business	We check your readiness for ISO/IEC 27001.	We develop a plan for implementing an ISMS and calculate the costs.
You are implementing an ISMS	We train your people on how to implement an ISMS and its various components	We help you developing methods and strategies for risk management, auditing, training and other strategic processes of an ISMS.	We design and implement all required components of an ISMS: documents, process, technology, organization. We support you preparing for a certification and guide through the certification audits,
You operate an ISMS	We train your experts on internal audits and risk assessments We help you improving security know how and awareness of your staff	We support you when you need to extend the scope of yours ISMS. We help you integrating the ISMS in your operational processes - and your other management systems.	We coach your staff during the pilot phase. We do independent reviews and audits. We check the efficiency of your security controls

ISO/IEC 27001 and related topics

Services offered by atsec - Overview



Information and Training

- General Information, Introduction to the world of security standards
- Implementation and auditing
- Awareness trainings, audit preparation



Readiness Assessment and ISMS Design

- Readiness Assessment
- ISMS Design
- Extensions of Existing Security Management Systems



ISMS Implementation

- Policies, Methods, and Processes
- Risk Assessment
- Implementation of Security Controls
- Integration Into IT Management Processes
- Coaching ISMS operation



Audits and Certification

- Internal Audits
- Independent Audits / Dry Run Audit
- Certification



Information and Training



Subject	Level	Duration
Information Security Standards – Overview	Basic	3-6 hours
ISO/IEC 27001 – Introduction	Basic	1 day
ISO/IEC 27001 – Implementation	Advanced	2 days
Auditing	Advanced	2 days
IT Continuity Management / Disaster Recovery	Advanced	2days
Information Security Awareness	Basic	2-4 hours

- *All training can be adapted to individual requirements*

Information Security Standards – Overview



▪ Contents

- Overview on standards important when designing and implementing information security controls
- Audience
Management, Project Managers, Security Staff
- Required Knowledge
None
- Recommended Length
Half day / 1 Day

Topics

- What is a standard and why should one use it?
- Which standards exist?
- Which standard for which task?
- A look at particular security standards: Origin, status, development, objectives, elements
- Certification: benefits, procedure
- How to implement standards: a project plan
- Questions and answers

ISO/IEC 27001 Introduction



- Contents
- Overview of the ISO/IEC 27001 standard
- Audience
Management, Project Managers, Security Staff
- Required Knowledge
None
- Recommended Length
1 Day

Topics

- What is an information security management system?
- What you should know about ISO/IEC 27001
- Major requirements of the standard
- Required security controls – an overview
- Certification: benefits, procedure
- How to implement ISO/IEC 27001
- Questions and answers

ISO/IEC 27001 Implementation



▪ Contents

- How to proceed when implementing an information security management system

- Audience
Security Staff

- Required Knowledge
Basic understanding of ISO/IEC 27001

- Recommended Length
2 Days

Topics

- What is an information security management system?
- ISO/IEC 27001 – Recap
- How to prepare a project plan
- Efforts and costs
- Major steps when implementing an ISMS
- Work products: required documents, processes, security organization etc.
- Roll out, integration in operating processes, training
- Certification

Auditing



- Contents
 - How to prepare and conduct compliance audits
- Audience
Auditors, CISO
- Required Knowledge
Basic understanding of ISO/IEC 27001
- Recommended Length
2 Days or
 - 5 Days to become a certified lead auditor; this training is offered by accredited partners

Topics

Objectives of audits and certificates

Audit plan

Initiation, planning and preparation of an audit

Step 1: What can/should be done before starting the audit

Step 2: Desktop audit

Step 3: System audit

Analysis of results

Reporting

Next steps

Information Security Awareness



Contents

Awareness training for people who work in an area which is governed by an ISMS

Audience

Staff

Required Knowledge

None

Recommended Length

2 hours - ½ Day

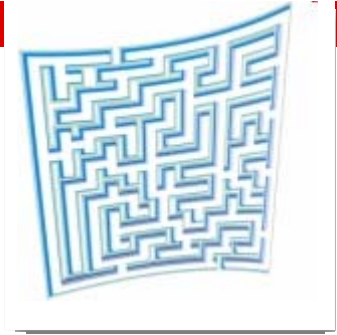
Topics

- Importance of information security – objectives and goals
- Information Security Management - Overview
- Policies and regulations
- Personal responsibilities
- Question and answers

NOTE:

This training is usually referring to the customer's own ISMS: its policies, documentation, processes and implemented security controls.

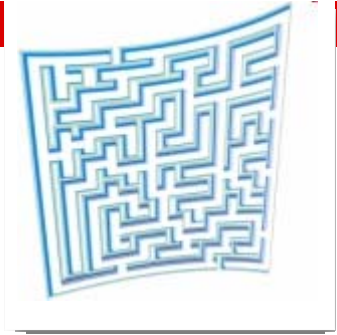
Readiness Assessment & ISMS DESIGN



Subject	Duration
Readiness Assessment	2 days
ISMS Design	1-3 weeks
Extension of existing ISMS	Varies

- *All training can be adapted to individual requirements*

Readiness Assessment



Deliverables

GAP Analysis
Project Plan
Calculation
Presentation
Workshop

Recommended Length

2 Days+

Topics

- Survey of the status quo: documentation, processes, technology
- GAP analysis: which required parts of an ISMS are missing or insufficient?
- Project Plan: specification of required tasks and resulting deliverables
- Calculation: effort and other costs. What can be done by the customer? Which task require special skills?
- Workshop: presentation of results

ISMS Design



Deliverables

Scope
Initial Risk
Assessment

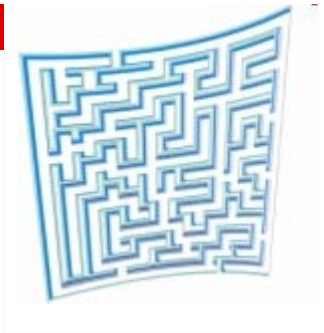
Recommended Length

1-3 Weeks

Topics

- Certification Strategy
- Process Improvements
- Integration with other management systems
- Review of other regulatory or legislative requirements

- Workshop: presentation of results



Extension of ISMS Scope

Deliverables

GAP Analysis
Project Plan
Calculation
Presentation
Workshop

Recommended Length

1 Days+

Topics

- Survey of the status quo: documentation, processes, technology
- GAP analysis: which required parts of the extended ISMS are insufficient or need to be performed?
- Project Plan: specification of required tasks and resulting deliverables
- Calculation: effort and other costs. What can be done by the customer? Which task require special skills?
- Workshop: presentation of results

Readiness Assessment & ISMS DESIGN



Subject	Duration
Policies, Methods, and Processes	2 days
Risk Assessment	1 Week +
Implementation of Security Controls	Varies
ISMS Integration	Varies
Coaching ISMS operation	Varies

- *All durations are specific to each project*

Policies Method and Process



Deliverables

Policies, Guidelines
Process
descriptions and
workflows
Workplace
descriptions
Training material

Recommended Length

Variable

Topics

Depending on the project plan: design and implementation of all required components of an ISMS, e.g.

- Documents like policies and guidelines
- Processes, roles and workplace description
- Methods like risk assessment methodology
- Concepts like training and audit plans
- Other topics as required

Risk Assessment



Content

Risk Identification
Vulnerability
Analysis
Threat Analysis
Risk Assessment
Risk Treatment
Planning

Deliverables

Risk Assessment
Report
SOA

Topics

Risk Assessment for any kind of IT system and supporting device (personnel, facilities, technical infrastructure, third party services)

- Risk Identification
- Vulnerability Analysis
- Threat Analysis
- Risk Assessment
- Risk Treatment Planning

*Based on the customer's own method and tools
- or on atsec's own approach. We have the
method, metrics and tools.*

Security Controls



Deliverables

Specifications
RFI / RFO
Technical
documentation

Operative security
controls

Topics

- Design of technical security controls based on current technologies and products
- Evaluation of products, request for information, request for offer
- Installation and configuration
- Training the operational staff
- Documentation

ISMS Integration



Content

Integration analysis

Deliverables

Miscellaneous

Topics

Survey of existing

- Management System(s)
- Processes and work flows
- Methods and reporting procedures

Integration of ISMS processes into existing

- IT management, Quality management
- Corporate risk management
- Crisis/disaster management
- Audit, training, documentation systems

Coaching IT Operations



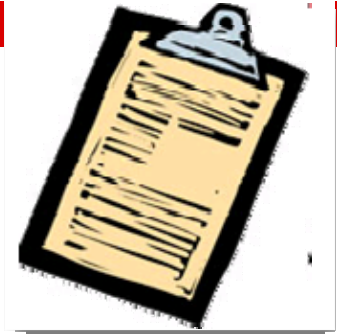
Deliverables

Miscellaneous

Topics

- Coaching the security staff during the pilot phase of the operational ISMS
- Corrective actions resulting from observations from the ISMS operations
- Corrective actions from audits (dry run, certification audits)
- Supporting the installation and operation of security controls

Independent / Dry-run Audit



Deliverables

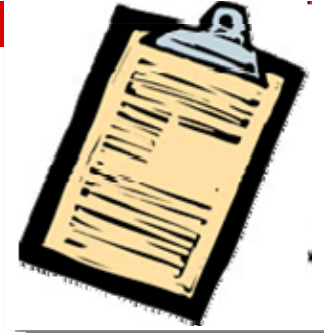
Audit report

Topics

A dry run audit is an audit which is executed under the conditions of a certification audit in order to verify the readiness for certification.

- Preparation, e.g., agreeing the schedule
- Desktop Audit: checking documents, processes, plans etc.
- Implementation (System) Audit
- Preparing the report
- Final workshop to discuss the results

Audit Support



Deliverables

Audit Planning
Selection of Auditor
Audit Preparation
Support during
audit

Topics

atsec does not provide certification services

Selection of the certification body and the auditor

- Audit planning
- Audit Preparation
 - Briefing the staff
 - Collecting material like documents / records
- Participation in audit interviews, site visits etc. in order to support the customer's staff
- Handling findings from audits



Corporate Certification Strategy

- For companies where formal certification of products is a key marketing or customer requirement, atsec assists with
 - Determining the strategy for gaining and maintaining compliance for a variety of certifications including both product and organizational IT security
 - Synchronizing certification and re-certification with the product release cycle
 - Helping customers develop efficient development processes for one or more products saving money and time.

Commitment to Quality



- atsec ensures all internal processes are certified with the leading international standards
 - ISO 9001 for quality
 - ensures ALL internal business processes meet recognized standards, mature and improve.
 - covers everything from back-office processes to “lessons learned”
 - ISO/IEC 27001 for information security
 - ensures that information and IP entrusted to us stays safe at all time
 - ISO 17025 for laboratory services
 - ensures our formal laboratory procedures are world-class



Why do business with atsec?

- atsec delivers results on time and at a fair price
- atsec provides unique synergies:
 - Experience with many compliance schemes
 - ISO/IEC 27001
 - FISMA
 - SOX, COBIT etc
- atsec has global reach
- atsec employs experts with internationally-recognized track records
- atsec leads the industry
 - contributing to development of standards
 - advising schemes and programs about the state-of-the-art for information security



Confidence in atsec

- We offer gratitude to the many companies, large and small, who help atsec thrive and trust us with their IT security needs...

