ISO/IEC 27001 – Theory and Practice

Peter Schindecker / Udo Adlmanninger
Managing Director / Member of the Executive Board
M3 GmbH / Secaron AG

Internet Security Days, Brühl
14.09.2011

1. Motivation - spirit and purpose of the certification
2. Roadmap – the way we did it
3. Best Practices - a pragmatic approach
4. Lessons Learned - experience and hints
Roadmap – the way we did it

Kick-Off 06/2009

Init 04/2009

Step-1 11/2009

Step-2 05/2010

Pre-Audit 10/2010

Certification Audit TÜV Nord 12/2010

Consulting partner: 
secaron AG

duration: 18 month

costs: 34 PM (3 senior staff - internal) 95 TEUR (external) 225 TEUR (hw/system)

budget: 575 TEUR (total)

Best Practices – a pragmatic approach

- Security Policy
- Management Review
- Methodology
- Risk Analyses
- Incident Handling
- User Management
- Change document
- Visitor Book, ...
Certification Audit – a pragmatic approach

• M3 IT Security Officer
• Secaron senior consultant
• TÜV Nord ISO 27001 auditor

One point contact for Q&A
Pre-audit
findings
data protection compliance

Lessons learned – Must Haves for the Auditor

• Risk Management has to be part of the security policy
• Security Targets should be measurable
• Proof of the efficiency of safeguards
• Management Review – Review and Forecast
• Documentation of information and owner
• Policy Safeguards (where are the safeguards derived from?)
• Correlation between ISO controls, assets and safeguards
• Listing of relevant laws
• Appointment of security officer and data protection officer
• BCM (restart, testing)
• Documentation of the purchase process
• Documentation Logging Monitoring
• Patch concept
• Backup testing
• Documentation of system hardening
Lessons Learned – experience and hints

• First of all you have to awake the internal awareness of security risks

• Try to get the absolute support of the executive board as project owner

• Support from an competent ISMS-Consulting company at an early stage

• Close collaboration and early integration of all employees and executive board during the whole certification process

• Pragmatic ISMS process definition in consideration of the basic conditions of your company based on ITIL 3.0 framework
  
  • Must – easy „daily doing“ for the whole staff
  • Must – high level of standardization of processes
  • Must – high flexibility according to changes of policies and guidelines
  • Must – Implementation & maintainance of an self-contained ISMS Service Desk

• Additional competent support by appointment of an external data protection officer

• Consistently performance of the certification process based on competent team, which should be exempt for this major task

Thank you!