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

Internet Security Days 14.09.2011

Agenda

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

formware®

Technology & Innovation & Management for documentbased business processes & correspondence & forms

Company

- Founded 1988
- Employees 65
- Turnover 14 Mio. €
- Subsidiary M3 GmbH

Business

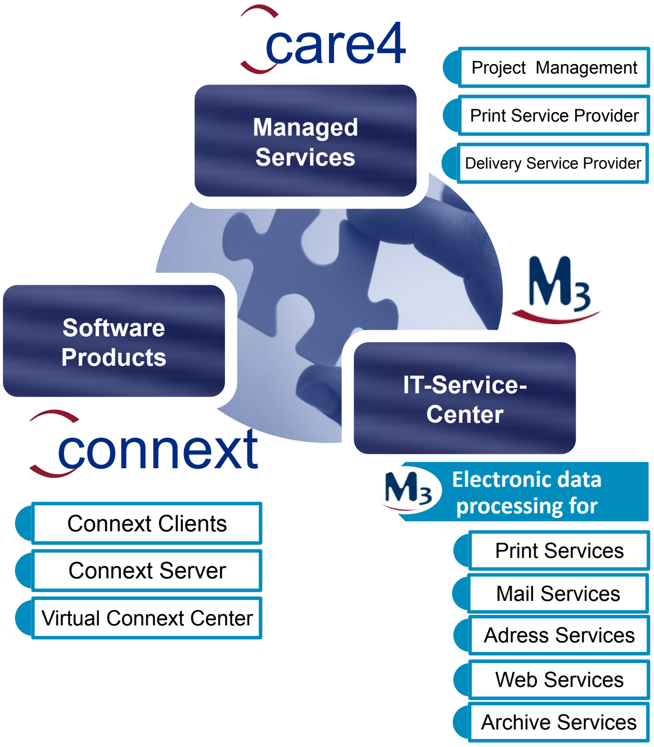
- Communication Management
- Business Process Solutions (BPM/BPO)

Portfolio

- Consulting
- SW-Development
- SW-Products & Solutions
- IT-as-a-Service

Locations

- Nußdorf am Inn (head quarter/data center)
- Ludwigsburg (sales office)
- Rosenheim (data center)



care4

Managed Services

- Project Management
- Print Service Provider
- Delivery Service Provider

Software Products

connext

- Connext Clients
- Connext Server
- Virtual Connext Center

M3

IT-Service-Center

M3 Electronic data processing for

- Print Services
- Mail Services
- Adress Services
- Web Services
- Archive Services

Portfolio

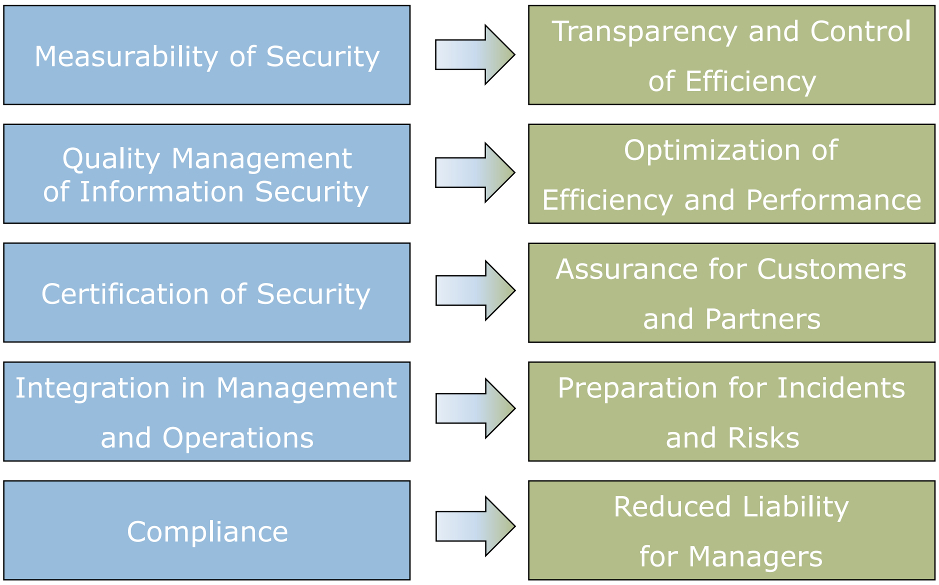
»|secaron

Secaron AG

Security / Risk Management	Concepts & Solutions	Compliance
Security Management ISO 27001 IT Risk Management Business Continuity Management	Network Security Identity Management and PKI Application Security Logging and Monitoring Data Leakage Prevention Information Rights Management	Organizational and Technical Audits Penetration Testing Testing of mobile Apps

e.security solutions

Motivation – spirit and purpose



Measurability of Security → Transparency and Control of Efficiency

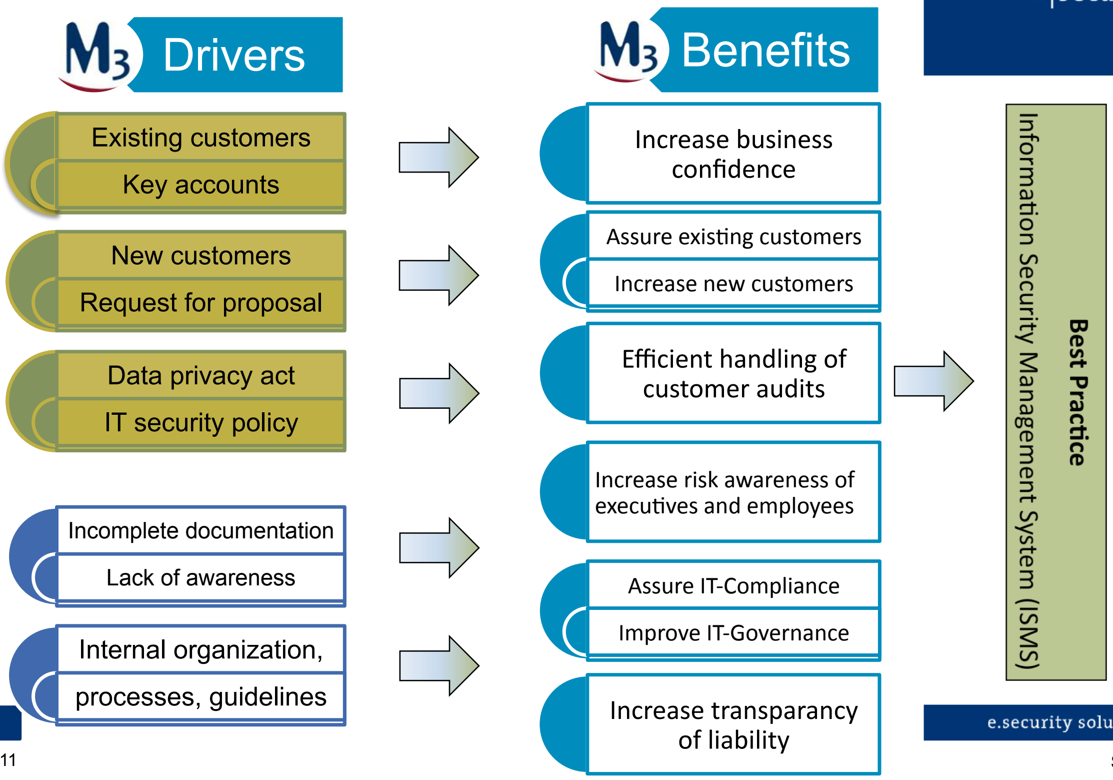
Quality Management of Information Security → Optimization of Efficiency and Performance

Certification of Security → Assurance for Customers and Partners

Integration in Management and Operations → Preparation for Incidents and Risks

Compliance → Reduced Liability for Managers

Motivation – spirit and purpose



M3 Drivers

- Existing customers
- Key accounts

- New customers
- Request for proposal

- Data privacy act
- IT security policy

- Incomplete documentation
- Lack of awareness

- Internal organization,
- processes, guidelines

M3 Benefits

- Increase business confidence

- Assure existing customers
- Increase new customers

- Efficient handling of customer audits

- Increase risk awareness of executives and employees

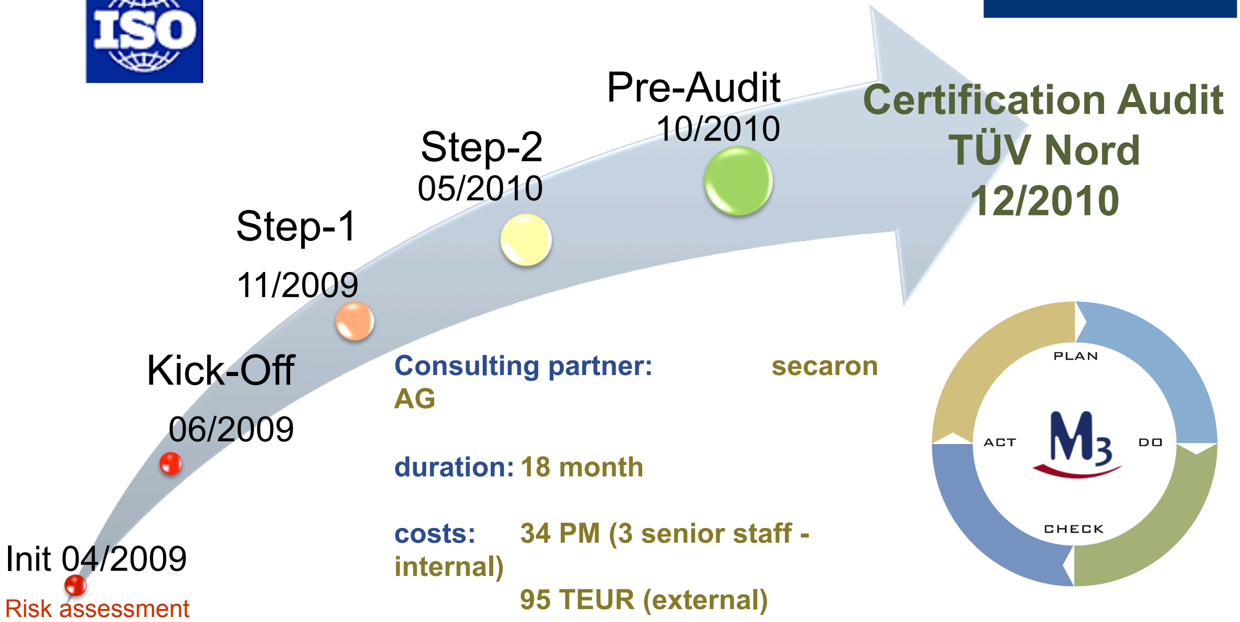
- Assure IT-Compliance
- Improve IT-Governance

- Increase transparancy of liability

→ Information Security Management System (ISMS)

Best Practice

Roadmap – the way we did it



Init 04/2009

Risk assessment

Kick-Off 06/2009

Step-1 11/2009

Step-2 05/2010

Pre-Audit 10/2010

Certification Audit TÜV Nord 12/2010

Consulting partner: secaron AG

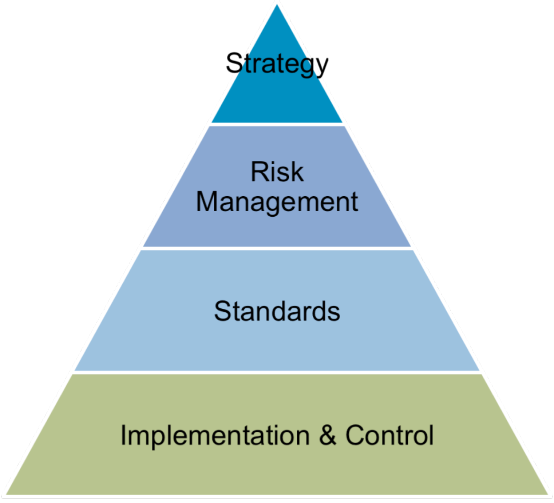
duration: 18 month

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, ...**



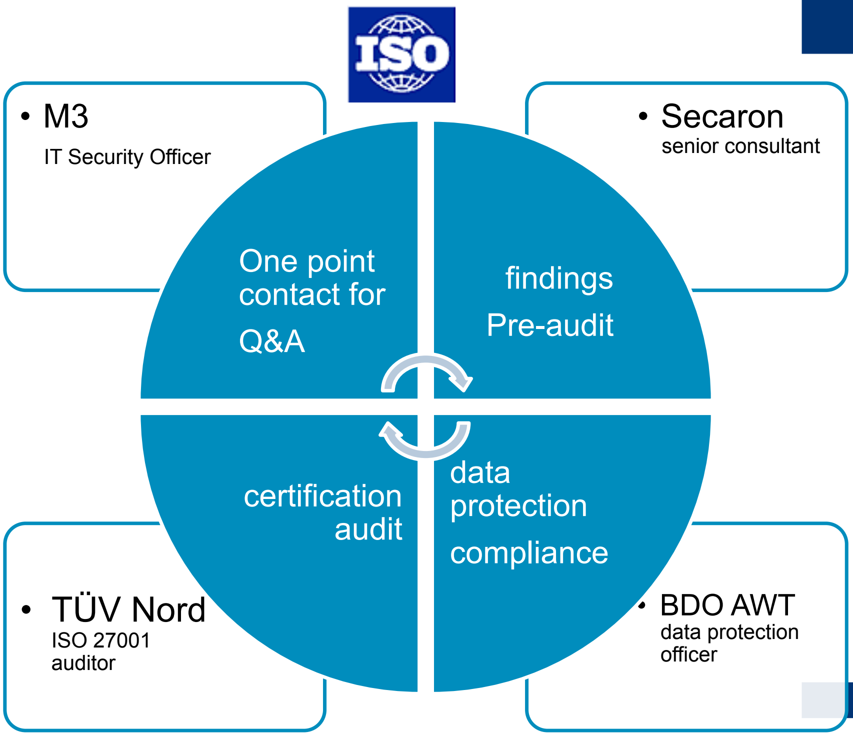
Strategy

Risk Management

Standards

Implementation & Control

Certification Audit – a pragmatic approach



- M3
  IT Security Officer

- Secaron
  senior consultant

One point contact for Q&A

findings Pre-audit

certification audit

data protection compliance

- TÜV Nord
  ISO 27001 auditor

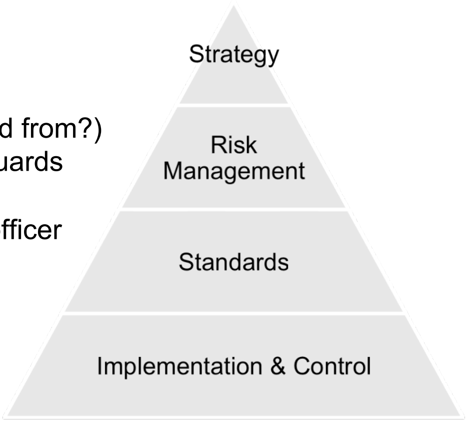
- BDO AWT
  data protection officer

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 conzept
- Backup testing
- Documentation of system hardening



Strategy

Risk Management

Standards

Implementation & Control

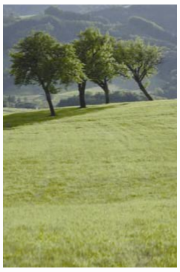
Lessons Learned – experience and hints

- 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 & maintanance 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!

Secaron AG
Ludwigstr. 45 (Building B)
D-85399 Hallbergmoos
Tel. +49 811- 9594 - 0
Fax +49 811- 9594 - 220
www.secaron.de

Contact:
Udo Adlmanninger
E-Mail: adlmanninger@secaron.de



Formware/M3 GmbH
Stangenreiterstr. 2
D-83131 Nußdorf am Inn
Tel. +49 8034-709 - 0
Fax +49 8034-709 – 1362
www.formware.de

Contact:
Peter Schindecker
E-Mail: peter.schindecker@m3-bs.de