Schritt für Schritt zur IT-Spitzenleistung

Vortrag 2K06 - Zertifizierung eines ISMS nach ISO27001 aus Sicht eines Auditors

Agenda

- Betrachtung des Umfeldes und Begriffserklärung
- ISMS – Management der Informationssicherheit
- ISMS – Warum? Fallbeispiele
- Zertifizierung des ISMS – Wer, Wie und vor allem Warum?
- Fragen

Was passiert denn so? Und was sind Herausforderungen?

- Vorfälle
  - Design des neuen Modells erscheint 5 Monate vor Markteinführung in Publikationen – Wettbewerber können wesentliche Designelemente imitieren
  - Im Internet veröffentlichte Produktkataloge werden von chinesischen „Herstellern“ kopiert, Modelle erscheinen zeitgleich im Fachhandel (Original) und im „Baumarkt“ (Fälschung)
  - Rückrufaktionen aufgrund falsch ausgelegter Bauteile
  - Barcode-Label können nicht gedruckt werden – Assembly Band muss angehalten werden (je Stunde ca. €150.000 Pönale)
- Herausforderungen
  - Lieferverträge nach China müssen mit Konzessionen erkauft werden (BMW, Airbus, …) => Technologietransfer?
  - Fertigungstiefe soll wieder verringert werden – OEM bauen Modelle doch wieder selbst
  - Compliance Management. Übereinstimmung mit Anforderungen von Gesetzen, Regelungen -> u.a. SOX
  - Permanente Besuche durch Auditoren: interne Revision, OEM, SOX, QMS, UMS, SAS70, …..

Kurzer Ausflug: Beispiel Automobil-Hersteller („OEM“)

- Für OEM ist IT vom Support Prozess zum Enabler geworden
  - Produktentwicklungsprozess 1990 = 7 Jahre, 2005 = 20 Monate
  - „Concurrent Engineering“ und Virtualisierung
  - Change Management - Änderungen können bis zuletzt in laufende Produktion überführt werden
  - Konfigurations Management – Mehrwert für Kunden durch aktuelle Informationen zum eigenen Fahrzeug und damit verbessertem Service
- OEM fordern einen Qualitätsnachweis … der Supportprozesse
  - Fähigkeit zur Geheimhaltung – Schutz der Produkte
  - Fähigkeit zur Verfügbarkeit – Lieferung JIT / JIS
  - Fähigkeit zur Integrität – richtiger Barcode, korrekte Zuordnung der Produktdetails
- Zurück zu den Thesen
  - These 1: Management ist verantwortlich für Informationssicherheit
  - These 2: IT ist verantwortlich für Informationssicherheit?
  - Vertraulichkeit?; Integrität?; Verfügbarkeit? – Ja wie denn?

Was ist ein ISMS und weitere wichtige Begriffe

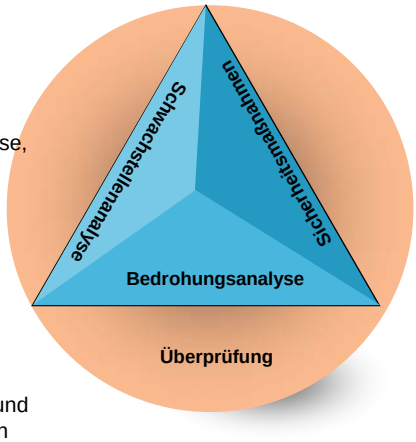
- IS – Informationssicherheit
  - Schutz von Informationen, die einen Wert für das Unternehmen darstellen
  - Informationen? Gespeichert, gesprochen, geschrieben , gesagt, …
  - Schutz gegen Verlust von **VIV(A)**
- Sicherheitsziele - **VIV(A)**
  - Vertraulichkeit („geheim halten“)
  - Integrität („korrekt“)
  - Verfügbarkeit („vorhanden wann und wo benötigt“)
- ISMS – Informationssicherheits-Managementsystem
  - These 1: Management ist verantwortlich für Aufbau, Betrieb, Kontrolle und Verbesserung der Informationssicherheit
  - These 2: IT ist verantwortlich für Informationssicherheit im Unternehmen.
  - ..ich bitte um Ihre Meinung

Agenda

- Betrachtung des Umfeldes und Begriffserklärung
- ISMS – Management der Informationssicherheit
- ISMS – Warum? Fallbeispiele
- Zertifizierung des ISMS – Wer, Wie und vor allem Warum?
- Fragen

Informationsschutz Management System:
Analysieren, Handeln, Überwachen

- Ermittlung der gefährdeten Informationen und Bewertung der möglichen Schadensfolgen
- Erfassung und Kontrolle aller Informationsflüsse, Schnittstellen (organisatorisch und technisch)
- Ermittlung aller organisatorischen und technischen Sicherheitslücken
- Aufbau von Sicherheitskonzepten und Realisierung von Maßnahmen
- Regelmäßige Kontrolle der Angemessenheit und Funktionsfähigkeit der Sicherheitsmaßnahmen



ISO 17799 / ISO 27001 – Analysieren, Handeln Überwachen

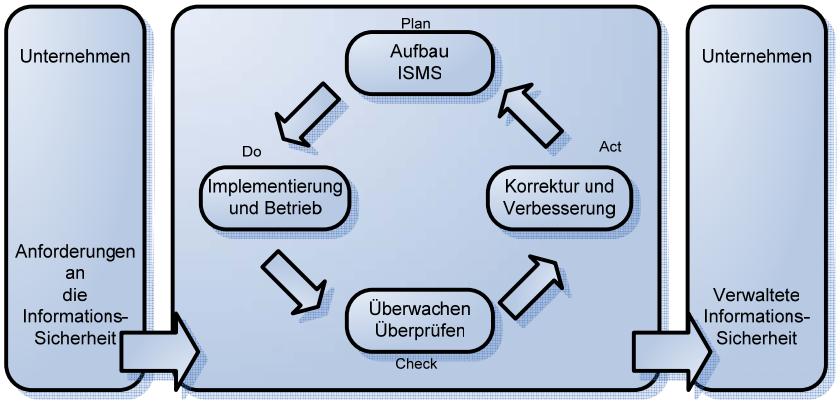
- **ISO 17799:2005**
- „Code of practice for information security management“
- Referenz Dokument oder “Best Practice“

→ **Implementierung**

- **ISO/IEC 27001:2005 (vorher BS7799-2)**
- „Information Security Management Systems - Requirements“
- Anforderungen an Informationssicherheit;
- IS ist ein Prozess
  - **Risiko Management** ist wichtigste Aktivität
  - Prozessmodell Plan – Do – Check – Act
  - Anforderungen an Dokumentation
  - Management Review
- Appendix A: Auswählbare Maßnahmenkomplexe

→ **Zertifizierung**

Prozessmodell des ISMS



ISO 27001 Prozessmodell

Appendix A: systematische Abfrage IS relevanter Themen

Management
-Informationssicherheits-Politik (**A.5**)
-Organisation der Sicherheit (**A.6**)
-Klassifizierung und Kontrolle der Unternehmenswerte / Asset Management (**A.7**)
-Management von Informationssicherheits-Vorfällen (Incidents, **A.13**)
-Einhaltung der Verpflichtungen / Gesetze, Vorschriften, Vereinbarungen (**A.15**)

Geschäftsprozesse
-Risiko Management (vor allem in P-Phase des PDCA - **4.2.1c…h**)
-Business Continuity Management (**A.14**)

Gebäude / Umgebung
Physische und umgebungsbezogene Sicherheit (**A.9**)

Tagesgeschäft
Management der Kommunikation und des Betriebes (**A.10**)

Planung / Projekte
System -beschaffung, -entwicklung und -wartung (**A.12**)

Zutritt / Zugang / Zugriff / Zulassung
Access Control (**A.11**)

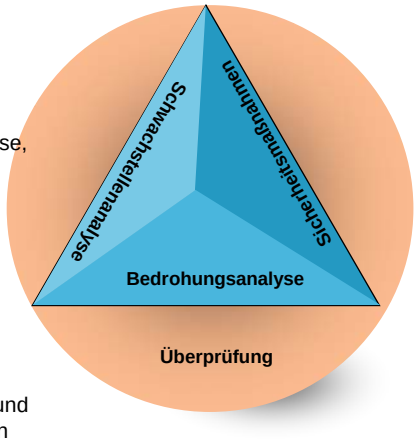
Personal
Personelle Sicherheit (**A.8**)

Agenda

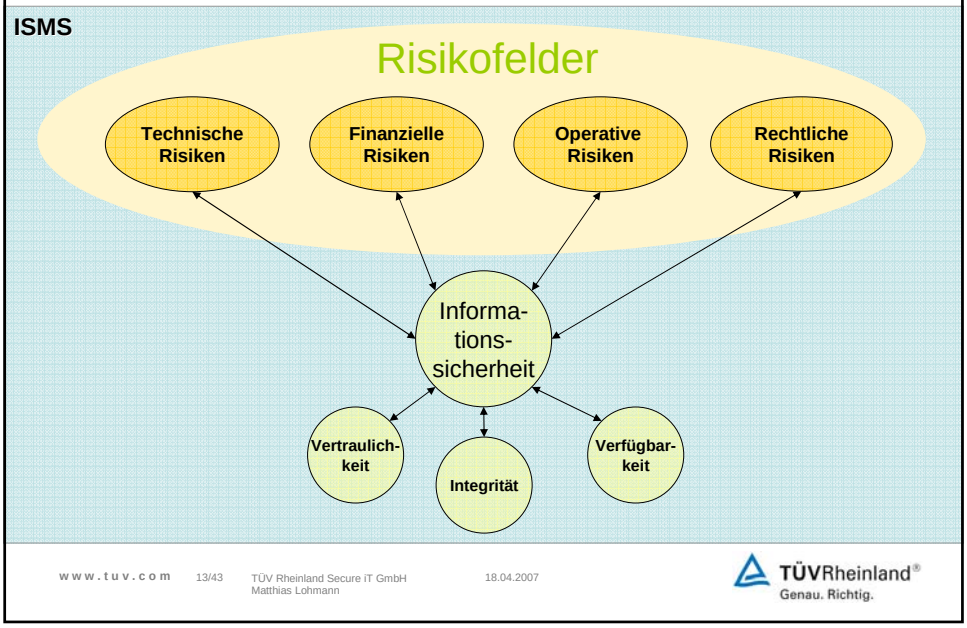
- Betrachtung des Umfeldes und Begriffserklärung
- ISMS – Management der Informationssicherheit
- ISMS – Warum? Fallbeispiele
- Zertifizierung des ISMS – Wer, Wie und vor allem Warum?
- Fragen

Informationsschutz Management System: Wiederholung
Analysieren, Handeln, Überwachen

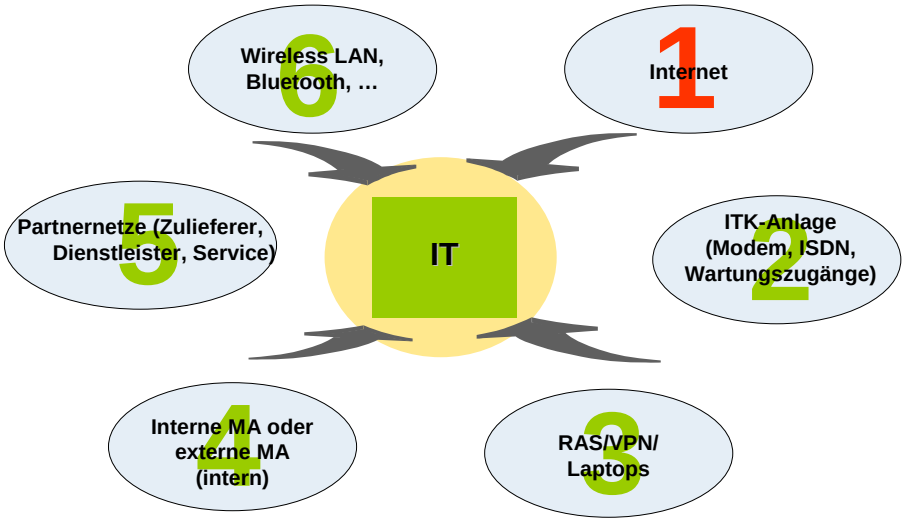
- Ermittlung der gefährdeten Informationen und Bewertung der möglichen Schadensfolgen
- Erfassung und Kontrolle aller Informationsflüsse, Schnittstellen (organisatorisch und technisch)
- Ermittlung aller organisatorischen und technischen Sicherheitslücken
- Aufbau von Sicherheitskonzepten und Realisierung von Maßnahmen
- Regelmäßige Kontrolle der Angemessenheit und Funktionsfähigkeit der Sicherheitsmaßnahmen



- **Warum ist Informationssicherheit ein Qualitätsmerkmal?**



- **Wege der Bedrohung**



Fall 1: Outsourcing eines Services

- Alltägliches Beispiel
  - Unternehmen A möchte ein Webportal
  - A beauftragt B der Erstellung.
    - B beauftragt C, D und E mit der Entwicklung
      - C und E beauftragen Komponenten bei F
  - …
  - Sicherheitstest nach(!) der Integration

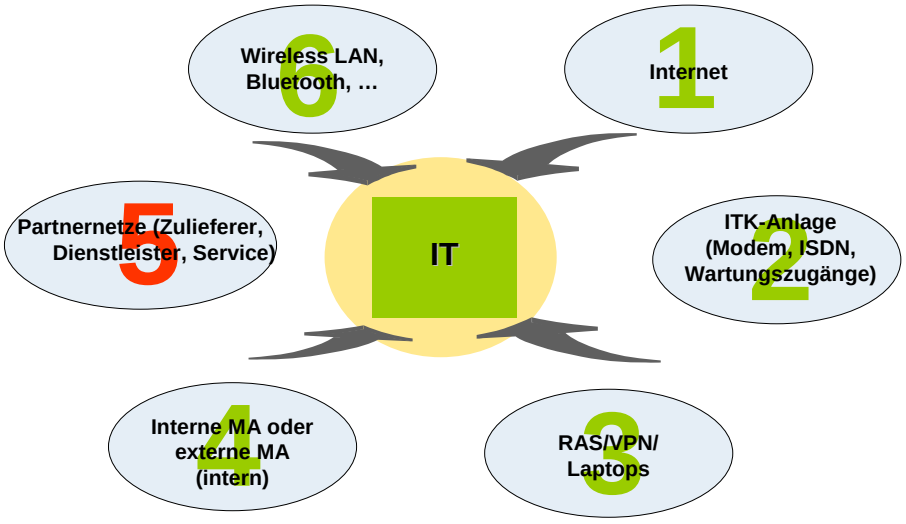
Fall 1

- Ergebniss:
  - Fehler in der Applikation (B) -> Zugriff auf die Webroot
  - Fehler im Serveraufbau (C) -> Zugriff auf den gesamten Server
  - Fehler in der Serversicherung (C, D) -> Zugriff auf alle DMZs
    - … auch der Kunden != A ;)
  - Fehler in der DMZ-Anbindung (D) -> Zugriff auf die interne Infrastruktur von (A)
    - Und A2 und A3 und A4 …
  - …mal ganz davon abgesehen, dass das „Rechenzentrum“ bei F ein besserer Raum ohne jede Redundanz der Versorgung ist.…

Ursache

- Fehler im Entwicklungsprozess
- Fehlende SecLA
- Implizite Sicherheitsannahme
- „Wir gingen davon aus, dass XY für die Sicherheit sorgt.“
- Beispiel aus 2002 (Verifikation in 2004, 2005, 2006)

Wege der Bedrohung



Fall 2: Ein Unternehmen teilt sich, die Sicherheit auch

- IT-Sicherheit verlangt die Kenntnis der Grenzen des Netzwerkes (Schnittstellen mit fremden Netzen)
- Szenario: (Anzahl der (externen und internen) IT-DL)
  - Aus Unternehmen AB (1) wird A und B (2)
  - Aus A wird A1, A2, A3 und B wird B1, B2, B3, B4 (4)
  - Aus B2 wird B21, B22 und B23 wird wieder in A2 eingegliedert (7)
  - …
- Problem: Als AB gab es ein physikalisches IT-Netz
- … jetzt immer noch!

Technische und organisatorische Analyse

- Beauftragt von A2
- Ergebnis: Organisatorische Analyse
  - Hohes Sicherheitsbewusstsein
  - Definierte Sicherheitsprozesse
  - Vollständige Dokumentation
- Ergebnis: technische Analyse
  - Fast beliebige Anzahl von Zugängen zum Internet
  - Keine logische oder gar physikalische Trennung der Netze
  - Zentrale Systeme mit „unbekannter“ Administration
  - Grenzen des Netzwerkes kannte selbst der IT-Dienstleister nicht

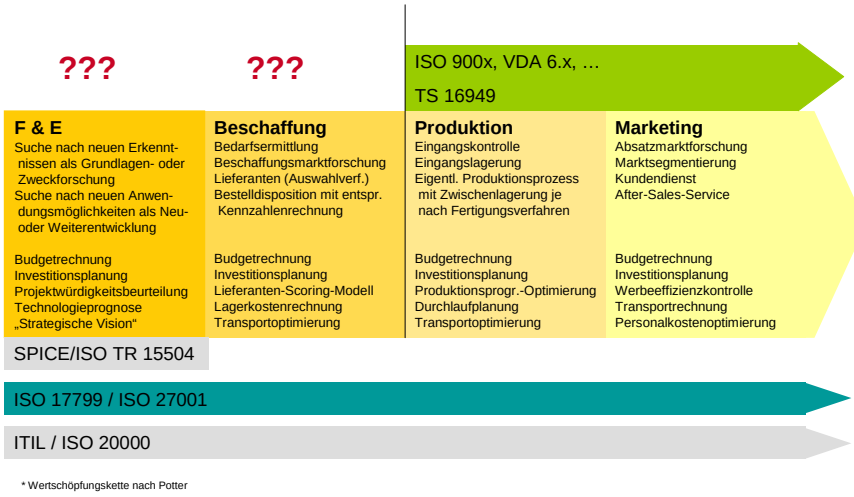
Ursache

- Zerfall des Zentralunternehmen -> Verkauf von Teilunternehmen
- IT wurde bei der Zerteilung des Unternehmens nicht betrachtet
- Verantwortlichkeit für die IT-Sicherheit nicht geklärt (keine Vorgaben)
  - Netzwerk
  - Anbindung an Fremdnetzen
  - Serverbetrieb
  - Clientbetrieb
  - Applikationsentwicklung
  - …

Fallbeispiel 3: Outsourcing in der Automobilindustrie

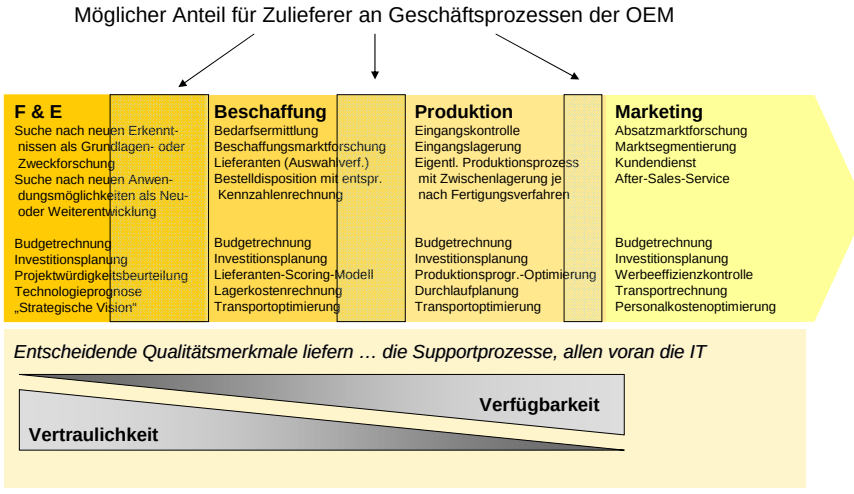
- Motivation
  - Kosten
  - Know How
- Realität
  - Ingenieurs-Ansatz: Erst muss es funktionieren, dann wird an Sicherheit gedacht ☺
- Strategie der Automobilindustrie
  - Es funktioniert…
  - …jetzt machen wir es sicher!
- Frage: Was sourcen denn die OEM aus???

Wertschöpfungskette* und Qualitätssicherung



* Wertschöpfungskette nach Potter

Wertschöpfungskette* - Chancen für Zulieferer



Agenda

- Betrachtung des Umfeldes und Begriffserklärung
- ISMS – Management der Informationssicherheit
- ISMS – Warum? Fallbeispiele
- Zertifizierung des ISMS – Wer, Wie und vor allem Warum?
- Fragen

Für wen ist ein ISMS eigentlich zutreffend und anwendbar?

- Groß oder Klein?
  - Von 15 Mitarbeitern bis zu 60.000 Mitarbeitern
  - …egal
- Beschränkt auf Branchen?
  - IT Dienstleister
  - Telekommunikation
  - Pharma
  - Automobilbau
  - Metallverarbeitung
  - Chemie
  - Luft- und Raumfahrt
  - … egal
- --> mindestens dort, wo Informationen wichtig für das Unternehmen sind
- **STOP: Das betrifft doch jedes Unternehmen, jede Behörde, … oder?**

Zurück zu Automobilindustrie: Zertifizierung wird Pflicht

- VDA
  - ISO27001:2005 wird Zulieferern derzeit empfohlen…
  - … und ist Pflicht für Entwicklungspartner, die zusätzlich noch PTS erfüllen müssen
  - PTS? Prototypen Schutz
- Anwendung
  - Zertifizierschema entwickelt von TÜV Rheinland Secure iT gemeinsam mit OEM
    - Prüfung der organisatorischen Sicherheit
    - Prüfung der technischen Sicherheit
    - Überwachung der Wirksamkeit (!)
  - OEM akzeptiert nur Anbindung ans eigene Netz für zertifizierte Unternehmen
- Vorteil
  - Bisher hat jeder OEM eigene Prüfer geschickt, künftig wird eine Prüfung ausreichen → Kosteneinsparung

Gründe für Zertifizierung: Compliance and Awareness

Kunden verlangen Nachweise
- VDA
- Service Provider
- Rechenzentrum
- …

Management fordert (sudden awareness)
- Vorfälle mit hohem Schaden (Virus, Diebstahl, Feuer, …)
- „Medienwirksame“ Vorfälle: geringer Schaden aber die „richtigen“ Personen (VIP, Stakeholder)
- …

Andere Gründe
- Gesetzliche Forderung: Medizin / FDA, SOX, KonTraG, BDSG, TKKG, Freedom of Information act, Electronic Communications Act, …
- Vertragliche Vereinbarungen: Qualitätszusagen, Sicherheitsvereinbarungen
- Zusicherung an / von Handelspartnern
- Kundenbindung
- Verbesserung des Ansehens (Reputation)
- Wirtschaftlichkeit und Wettbewerbsfähigkeit

Vorteile einer ISMS Zertifizierung (1/3)

- Bewertung der Geschäftsprozesse aus der Sicht der Sicherheit von Informationen
- Integration von Informationssicherheit in Geschäftsprozesse
- Management der Risiken der Informationsverarbeitung
- Management Weiterführung der Geschäfte (Ausfallsicherheit)
- Dokumentation von Strukturen und Prozessen
- Bessere Sicherheits-Awareness der Angestellten

Vorteile einer ISMS Zertifizierung (2/3)

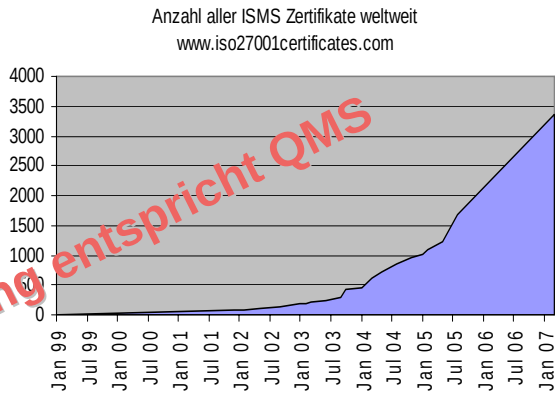
- “Competitive advantage” durch eine Zertifizierung
- Weltweit anerkannter Standard
- Einsparungen durch sinkende Versicherungsprämien
- Klare Strukturen → Sinnvoller Einsatz der Ressourcen
- ITIL verweist auf BS 7799
- ISO 27001:2005 ist ISO 9000-“Kompatibel“
  Synergien durch integrierte Audits (QMS, UMS, TS16949, OHSAS, ISMS, PTS, …)

Vorteile einer ISMS Zertifizierung (3/3)

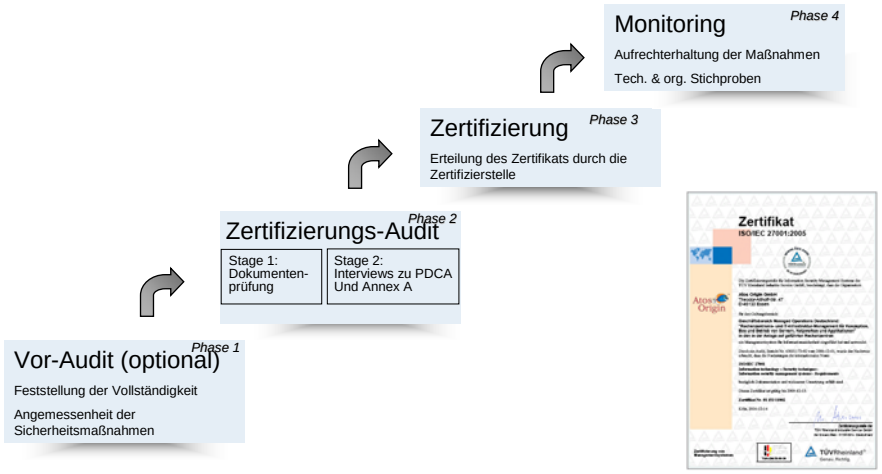
- Aktuelle Studien zeigen, dass Organisationen, welche eine BS7799:2 bzw. ISO27001 Zertifizierung halten, als vertrauenswürdig und respektabel angesehen werden.
- Zukünftige Geschäftsbeziehungen werden vereinbart in der Gewissheit, dass aus Informationssicherheit resultierende Risiken effektiv gemanagt werden.
- Informationssicherheit ist damit ein essentieller Bestandteil für ein stabiles Wachstum von Unternehmen und ein Wettbewerbsvorteil.

Anzahl von ISMS Zertifikaten – ISMS User Group

- Dez. 2005
  - Magic 1000
- März 2007
  - 3350
- Wer interessiert sich dafür?
  - Japan: 1910
  - UK: 326
  - India: 279
  - Taiwan: 124
  - Germany: 74
  - Hungary: 57
  - Korea: 49
  - China: 47
  - USA: 47
  - Italy: 42
- **TÜV Rheinland: erster akkreditierter TÜV (März 2003)**
  >100 Zertifikate weltweit
- …und wo sind Ihre Geschäftspartner?



ISO 27001-Zertifizierung durch die TÜV Secure iT



TÜVRheinland® Genau. Richtig.

Untersuchungsgrundlagen

- Verfahren zur Auditierung eines Informationssicherheits-Managements nach
  - ISO 27001:2005 “Information security management systems –
  - specification with guidance for use” vom 15.11.2005
  - ISO 27001 Fragenliste, Version 1.2 vom 14.12.2005
  - Akkreditiertes Verfahren seit 2003, Aktualisierung auf ISO 27001 im Januar 2006 durch TGA bestätigt

TÜVRheinland® Genau. Richtig.

Durchführung des Zertifizierungsaudits

- Stage 1: Dokumentenprüfung
  - SoA und alle darin referenzierten (Prozess-) Dokumente
- Stage 2: Interviews mit Verantwortlichen und Mitarbeitern
  - Innerhalb ihres Verantwortungsbereiches
  - Auditplan definiert Datum, Zeit, Dauer für jeden Beteiligten
  - Identifikation von Prozessabweichungen
  - Keine Identifikation von Fehlverhalten
  - Stichproben
    - Sammlung von weiteren Nachweisen für Wirksamkeit und Vollständigkeit
    - Nachvollziehen von Vorgängen: Einsicht in Unterlagen, Formulare, Dateien und Listen
  - Ortsbegehungen
    - Alle relevanten Örtlichkeiten
    - Gelände / Wache; Gebäude; Rechenzentrum; Versorgungseinrichtungen (Klima, Strom, Verkabelung, …); Verteilerschränke; F&E Bereiche; Projekträume;

Projektablauf

Zertifizierung geht schnell - Gesamtdauer ist abhängig von Ihrer Vorbereitung

Ausblick: Belastung durch Zertifizierungen

- ISO 27001 kann Teil von Systemzertifizierungen sein
  - MSFT: 5 Tage Audits – 8 Zertifikate
    - ISMS & PTS
    - QMS: QS 9000 / VDA 6.1 / TS 16949
    - UMS
    - OSHAS
    - …
  - → jährlich nur 1-mal Besuch durch externe Auditoren (vorher 8x)
- Wesentliche Elemente gemeinsam zwischen den „xMS“
  - PDCA
  - Anforderungen an Dokumenten-Management
  - …
- Die Pflicht wird zur Kür…

Agenda

- Betrachtung des Umfeldes und Begriffserklärung
- ISMS – Management der Informationssicherheit
- ISMS – Warum? Fallbeispiele
- Zertifizierung des ISMS – Wer, Wie und vor allem Warum?
- Fragen

Q&A

- Diskussion und Fragen

Wegbegleiter TÜV Rheinland Secure iT
Wer wir sind.

- **Tochtergesellschaft der TÜV Rheinland Group**
- **TÜV RG weltweit vertreten an 300 Standorten in 50 Ländern**
- **TÜV Secure iT: Spezialisten zur dauerhaften Sicherung von IT-Umgebungen**
- **Konzentration auf IT Services in den Bereichen IT- Security, IT-Prozesse und e-Business**

Portfolio (1/2)*

IT-Security

IT-Security Management
- Einführung eines IT-Security Managementsystems (Prozessmodell auf Basis BS 7799 & Security Process Framework)
- Definition und Erstellung von Security Policies
- Quick Checks & Bestandsaufnahmen
- Erstellung von Checklisten / Self Assessment
- Spezifische Detailanalysen innerhalb der IT-Security
- Bewertung des Firewallmanagements
- Schutzbedarfsfeststellungen / Risikomanagement
- Grundschutzaudit
- Konzeption & Aufbau von Notfallmanagement
- Einführung und Bewertung von Security Level Agreements
- Ermittlung von Kennzahlen / Internes Benchmarking
- Gestellung des Chief Information Security Officers (CISO)

Datenschutz
- Datenschutzaudit
- Gestellung externer Datenschutzbeauftragter

IT-Security Testing
- Application Testing / Technische Sicherheit von Anwendungen und Produkten
- Client-Hacking
- System-Hardening
- Scanning / Penetration von Netzwerken
- Technische Konzeptprüfung
- Telekommunikationsanlagen-Scanning (TK-Scanning), T-Kit

IT-Security Zertifizierung
- Zertifizierung nach BS 7799
- Zertifizierung nach IT-Grundschutzhandbuch
- Zertifizierung von Softwareentwicklungspartnern der Automobilindustrie (SEP-Sec)
- Zertifizierung von Data Centern nach BS 7799
- Zertifizierung von ISP's nach BS 7799
- Zertifizierung von ASP's nach BS 7799
- Zertifizierung von PSP's nach BS 7799

* BS7799 inzwischen vollständig durch ISO 27001 ersetzt

Portfolio (2/2)

IT-Prozesse / IT-Usability

IT-Service Management
- Einführung eines IT-Service Managementsystems (Prozessmodell auf Basis ITIL & BS 15000)
- Quick Checks / Schwachstellenanalysen im IT-Service Management
- Spezifische Detailanalysen zu Teilprozessen
- Assessment/Zertifizierung des IT-Service Management auf Basis von ITIL & BS 15000

Software-Entwicklung und -Beschaffung
- Erstellung von Lastenheften & Anforderungsspezifikationen
- Moderation von Reviews & Projektmeetings, Inhouse-Training
- Review / Abnahme von Projektergebnissen auf Basis von Lastenheft und Pflichtenheft
- Assessment / Zertifizierung von software-entwickelnden Unternehmen auf Basis von ISO 9001
- Assessment / Zertifizierung von Softwareentwicklungsprojekten auf Basis ISO TR 15504 (SPICE)
- Gestellung externer IT-Projektleiter für Entwicklungsprojekte, Beschaffungsprojekte, Einführungsprojekte

IT-Usability
- Analyse von Benutzerprofilen und Nutzungskontexten
- Erstellung von Nutzungskonzepten
- Anforderungsanalyse aus Benutzersicht
- Review von Prototypen und interaktiven Systemen (mit und ohne Benutzern)
- Prüfung & Zertifizierung der Nutzungsqualität / Gebrauchstauglichkeit von Software
- Prüfung & Zertifizierung der Barrierefreiheit / Accessibility von Software
- Assessment / Zertifizierung des Usability Management innerhalb von Software-Entwicklungsprojekten auf Basis von ISO 13407

* BS15000 inzwischen vollständig durch ISO 20000 ersetzt

- **Schritt für Schritt an die Spitze**
  Wir unterstützen Sie dabei.

Vielen Dank für Ihre Aufmerksamkeit.

Matthias Lohmann
TÜV Rheinland Secure iT GmbH
Tel.: 0221-806-2682
matthias.lohmann@de.tuv.com

TÜVRheinland®
Genau. Richtig.