

# ISMS-Standards aus Kundensicht

## Impulsreferat AG 8

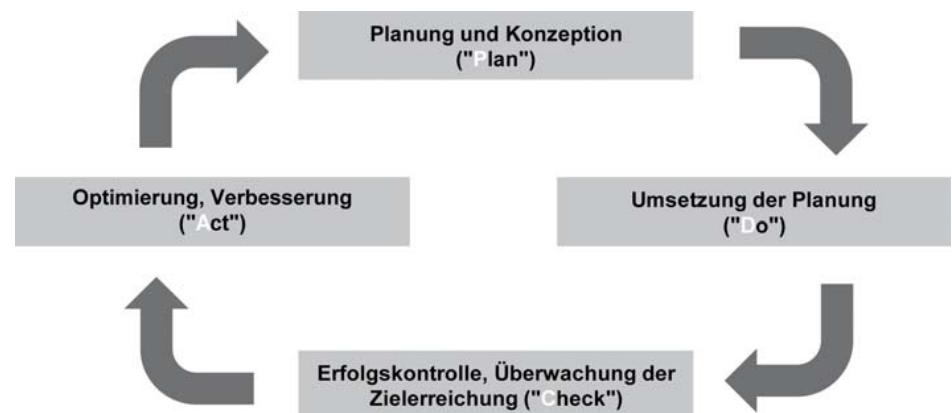
Dr. Michael Gehrke (TTS GmbH)

Berlin, den 27.11.2008

Workshop „E-Government-Standards für  
Wirtschaft und Verwaltung“

# Ziele eines Informationssicherheitsmanagementsystems (ISMS)

- Definieren, Umsetzen und Aufrechterhalten geeigneter Sicherheitsmaßnahmen passend zum Schutzbedarf der Organisation
- Dabei Gewährleistung von
  - Wirtschaftlichkeit
  - Benutzbarkeit
  - Transparenz
  - Compliance

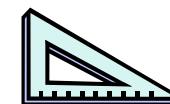


Quelle: BSI-Standard 100-1 / Denning

- Beispiele für ISMS-Standards
  - ISO/IEC 27001/2 Information security management systems
  - Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 100-1/2
  - Information Security Forum's „Standard of Good Practice“
  - National Institute of Standards and Technology SP 800-53 Recommended Security Controls for Federal Information Systems
  - ...

# Kundenmotivation: Geht ISMS nicht auch ohne Standards?

- Grundsätzlich ist ein ISMS ohne Orientierung an Standards implementierbar
- Kunden haben natürlich gute Gründe auf Standards zu setzen
  - Orientierungshilfe
  - Messlatte
  - Praxisreservoir
  - Verbesserung der Darstellbarkeit nach innen und außen
  - Vereinfachung der Durchsetzbarkeit nach innen und außen
  - Zertifizierbarkeit / Marketing
- ISMS Standards werden z. T. auch von den Kunden der Kunden gefordert



Wenn Sie ein ISMS implementieren müssten, welches wäre Ihr Grund, auf einen Standard zu setzen?



# Erfahrungen mit / von Kunden: Punkte, an denen ich herumdenke

- Vergleichbarkeit ISMS-zertifizierter Unternehmen nicht gegeben
- Auswirkung von Kostendruck auf ein ISMS
- Auswirkung von M&A / Umstrukturierungen auf ein ISMS
- Vorhandene Erfahrungen der CISOs beim Aufbau eines ISMS
- Wodurch wird die Qualität des ISMS mehr beeinflusst
  - Orientierung am Standards
  - Motivation der Schlüsselpersonen (CISO, CIO, Management, ...)
  - Vorhandenes Budget

# Mein persönlicher Resümee-Versuch

- Es ist eine sehr gute Idee, sich an Standards für ein ISMS zumindest zu orientieren
- Fast alle unserer Kunden tun dies auch
- Es ist schwieriger, „Scheunentore“ offen zu lassen
- Ein ISMS ist selber häufig bedroht durch die Ereignisse der realen Welt wie M&A, Kostendruck, etc.
- Vergleichbarkeit / Benchmarking wäre zu begrüßen, Effekt ähnlich wie bei Energiebenchmarking A++, A+, A, B
- Mal abwarten, was uns ISO 27004 „Measurements“ bringt

- Vielen Dank für Ihre Aufmerksamkeit

[www.tts-security.com](http://www.tts-security.com)

[michael.gehrke@tts-security.com](mailto:michael.gehrke@tts-security.com)

The screenshot shows the TTS website homepage. At the top right, there is a banner with a blue background featuring a computer monitor icon. Below the banner, the TTS logo and tagline are displayed. A navigation bar contains links for HOME, KONTAKT, and SITEMAP. The main content area includes a sidebar with links to Home, Unternehmensprofil, Philosophie, Alleinstellungsmerkmale, Designkriterien, News, Leistungen, Informationssicherheit, Publikationen, Karriere, and Kontakt. The main content area features three sections: 'Vision' (describing the company's goal to help companies worldwide), 'Mission' (describing the company's strategy to develop security solutions), and 'In bin interessiert an ...' (listing various security topics). The footer contains a copyright notice for 2005 TTS GmbH.

**Vision**  
In 5 Jahren werden Unternehmen weltweit auf die Beratungskonzepte der TTS vertrauen, um jegliche Art von Angriffen auf die Informationssicherheit beherrschen zu können.

**Mission**  
Die Berater der TTS entwickeln Strategien, Pläne, Architekturen und Konzeptionen, damit unsere Kunden Informationssicherheit beherrschen. Dabei setzen wir die besten Organisationskonzepte und Technologien ein, und passen diese an die Kundenbedürfnisse an. Professionalität, Qualität und Kompetenz sind die wesentlichen Eigenschaften unserer Arbeit und gleichzeitig das höchste Ideal für unsere Mitarbeiter.

**In bin interessiert an ...**

Antivirus	Rollenbasierter Zugriffsschutz - RBAC
Firewall	Security Awareness
Grundschutz	Security Guidelines
Identity & Access Management	Security Policy
Incident Handling	Security Review
Intrusion Detection	Sicherheitshandbuch
ISO17799/ BS7799	Sicherheitslösungen
Kontrag	Sicherheitsorganisation
Notfallplanung	Sicherheitsprozesse
Penetrationstest	Single Sign-On
Provisioning	Verschlüsselung
Risikoanalyse	Vertrauenswürdige Geschäftsprozesse
Risikomanagement	