

# Zertifizierte IT - Sicherheit

eine grundlegende Unternehmensentscheidung

Dr. Jörg Bode, tti Magdeburg GmbH – MD-ECZ

Der Vortrag beinhaltet auszugsweise Inhalte des Vortrages „Informationssicherheit - Pflicht, Kür und ein Mittel zur Kundenbindung“ von Andreas Gabriel, MECK -Mainfränkisches Electronic Commerce Zentrum

Gefördert durch:



aufgrund eines Beschlusses  
des Deutschen Bundestages



# IT – Sicherheitslage

## Lagebericht 2. Quartal 2009 des BSI

- Im Themenbereich **Angriffe & Ereignisse** wird die IT-Sicherheitslage mit **erhöhtem** Risiko eingeschätzt. Grund dafür sind unter anderem mehrere Angriffe auf Systeme der US-Flugkontrolle und der Diebstahl von Datenträgern der britischen Luftwaffe.
- Im Themenbereich **Bedrohungen & Gefahren** wird die IT-Sicherheitslage aufgrund der fortschreitenden Ausbreitung des Conficker-Wurms weiterhin mit **hohem** Risiko beurteilt.
- Im Themenbereich **Trends** wird die IT-Sicherheitslage mit einem **normalen** Risiko bewertet. Im Mai 2009 wurde Google Wave, eine neuartige Plattform zur webbasierten Kommunikation in Echtzeit, vorgestellt, eine Veröffentlichung ist für die zweite Jahreshälfte 2009 vorgesehen. Aus IT-sicherheitstechnischen Gründen und auch aus Sicht des Datenschutzes ist die Verwendung allerdings aktuell nicht zu empfehlen.

# Gesetzeslage zur Informationssicherheit – eine Auswahl

- Betriebsverfassungsgesetz
- BGB
- Bundesdatenschutzgesetz
- Informations- und Kommunikationsdienstegesetz
- KntraG
- Signaturgesetz
- Telekommunikationsgesetz
- Telemediengesetz
- GmbH Gesetz
- Aktiengesetz
- .....

## IT-Sicherheit – strategische Aufgabe des Managements

- Unternehmenszielen, wie Umsatzsteigerung, Gewinn, Image usw. stehen Unwägbarkeiten und Bedrohungen gegenüber.
- Die Abhängigkeit der Unternehmen von der IT-Infrastruktur wächst ständig. Immer mehr Geschäftsprozesse werden nur noch elektronisch abgewickelt.
- Risikomanagement muss IT-Sicherheit als wichtigen Bestandteil beinhalten.
- Verantwortlich hierfür ist das Management !!!



# Informationssicherheitsmanagement

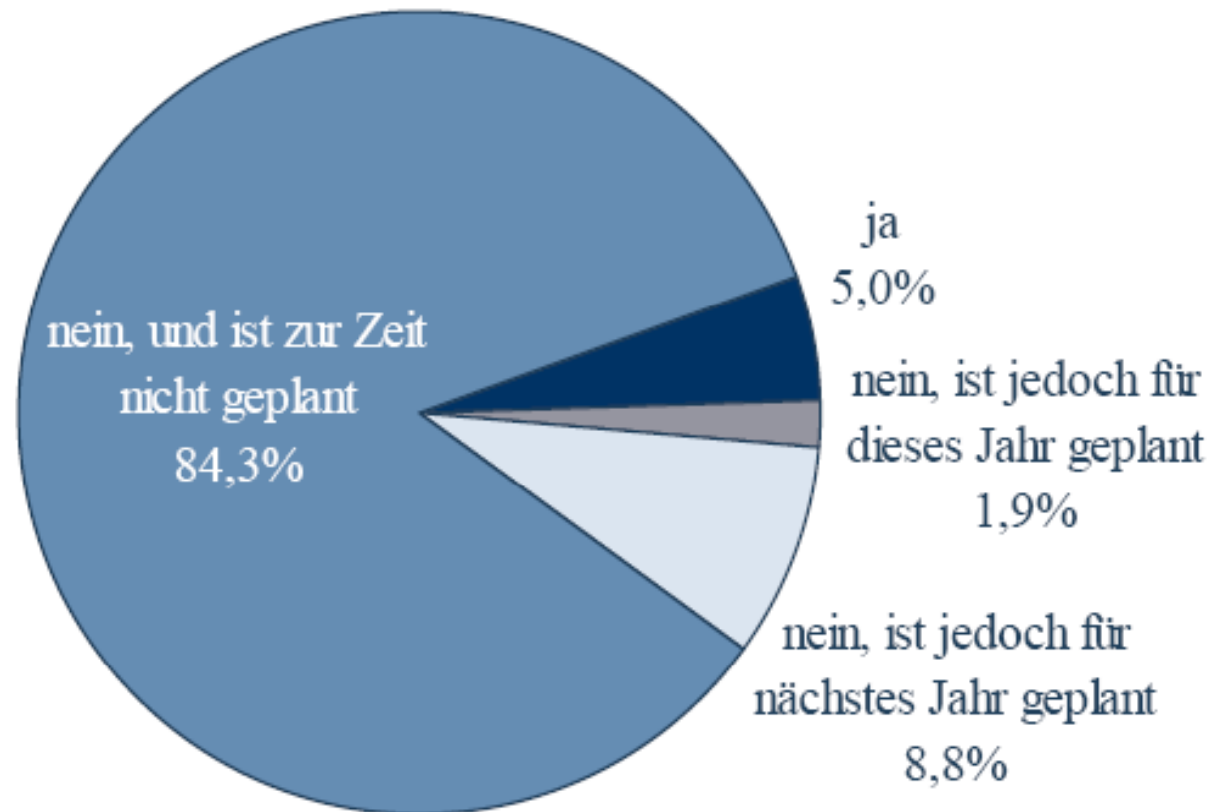
- Informationssicherheitsmanagement ist mehr als IT-Sicherheit
- ISMS ist ein integriertes Managementsystem, das Sicherheits- und Risikomanagement umfasst und in das Unternehmensmanagementsystem eingebunden werden muss
- Management muss für Umsetzung sorgen, wie bei anderen Managementsystemen auch, ggf. Einführung incl. Zertifizierung

# Was ist eine Zertifizierung

Gemäß EN 45011 ist Zertifizierung der **Konformität** eine Maßnahme durch einen **unparteiischen Dritten**, die aufzeigt, dass angemessenes Vertrauen besteht, dass ein ordnungsgemäß bezeichnetes Erzeugnis, Verfahren oder eine ordnungsgemäß bezeichnete Dienstleistung in **Übereinstimmung** mit einer bestimmten **Norm** oder einem bestimmten anderen normativen Dokument ist.

**Oder einfacher: Sie ist die Bestätigung der Übereinstimmung mit einer vereinbarten Vorgabe durch eine unabhängige Stelle.**

## Wie steht der deutsche Mittelstand zum Thema „Zertifizierung im Bereich Informationssicherheit“?



Quelle: ECC Handel:  
Elektronischer  
Geschäftsverkehr in  
Mittelstand und Handwerk –  
Ihre Erfahrungen und Wünsche  
2008, Oktober 2008.

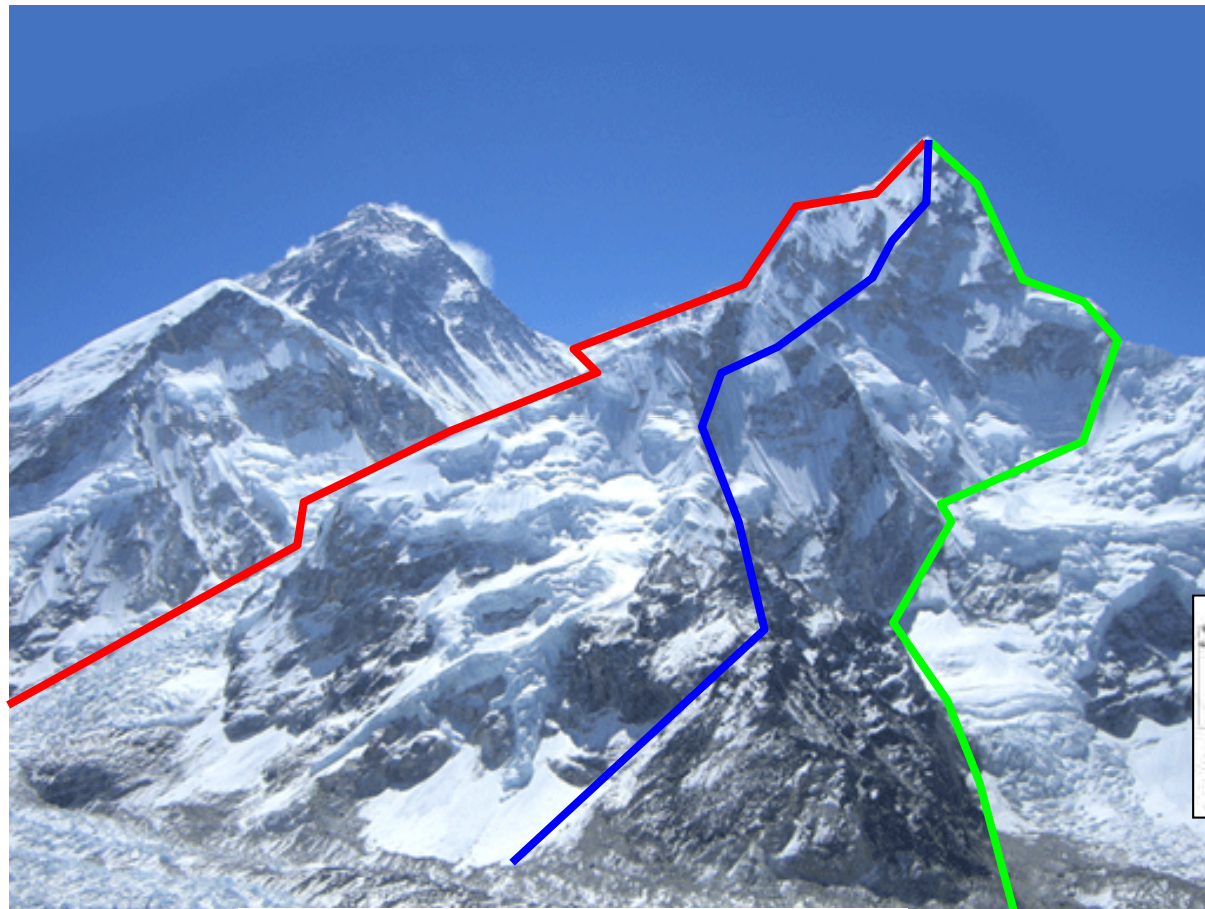
# 3 Möglichkeiten für Informationssicherheitsmanagement

ISO/IEC 27001 : Definition der Anforderungen an ein Informationssicherheitsmanagementsystem; prozessorientierter Ansatz; auditierbar und damit auch zertifizierbar

IT-Grundschatz des BSI: Basis für die Konzeption der Informationssicherheit bestehend aus dem IT-Grundschatzhandbuch und BSI-Standards; Ausgangspunkt ist Strukturanalyse, nicht prozessorientiert;  
Zertifizierung auf Basis IT-Grundschatz gemäß ISO/IEC 27001

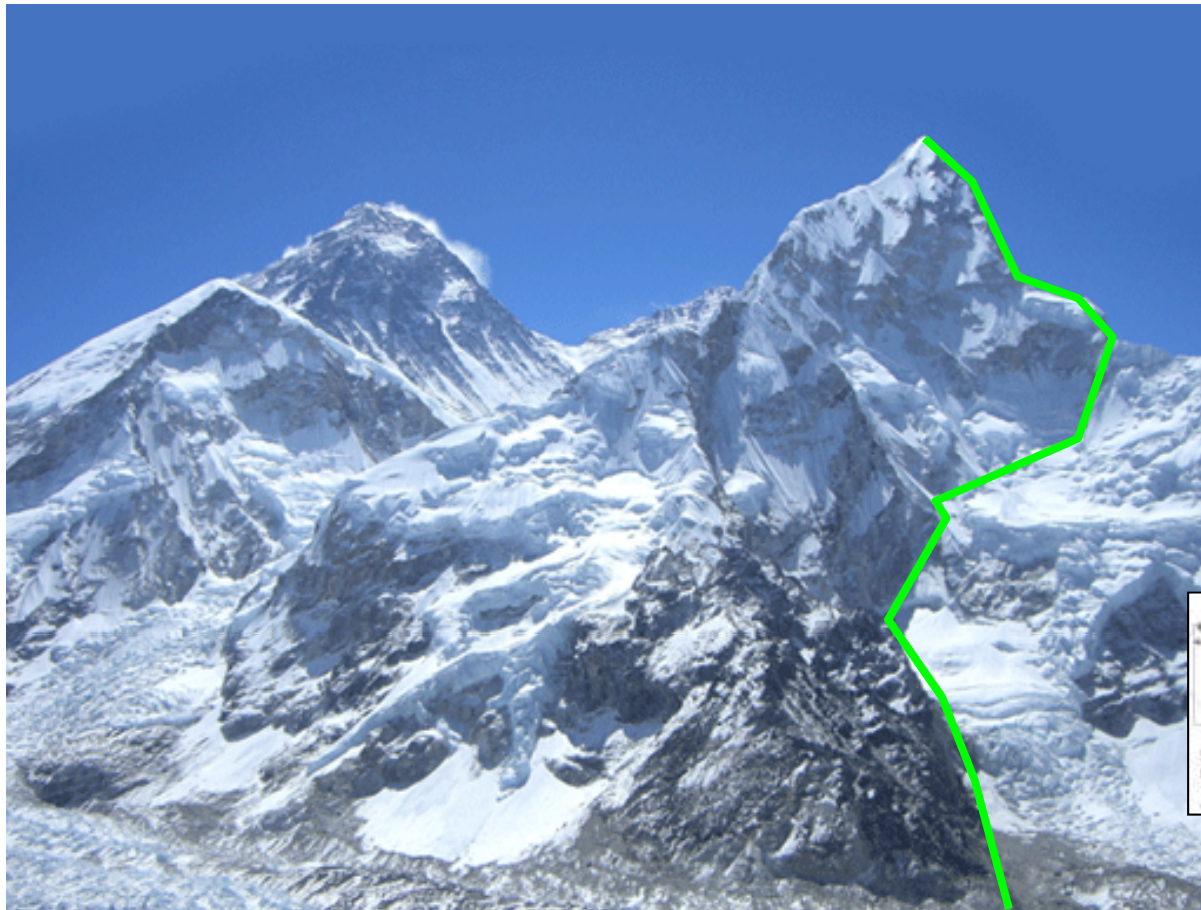
ISO 9000 ff.: Anforderungen an Qualitätsmanagementsysteme mit Komponenten der IT-Sicherheit; kein ISMS; keine Zertifizierung der Informationssicherheit

# Das hohe Ziel: Zertifizierung im Bereich Sicherheit



## Vergleich ISO 9001

# Das hohe Ziel: Zertifizierung im Bereich Sicherheit



Quelle: <http://www.nepalhiking.com/images/mount-everest.gif>, [http://www.jurowl.de/images/de\\_mail\\_buergerportale\\_logo.jpg](http://www.jurowl.de/images/de_mail_buergerportale_logo.jpg)

# Beispiel Gesundheitskarte

## Die Gesundheitskarte



Umsetzung durch die



Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Quellen: <http://www.bmg.bund.de>; <http://www.gematik.de>

## Forderungen der Gematik

„Die Aktivitäten im Rahmen des Sicherheitsmanagements **MÜSSEN** in Anlehnung an **ISO 27001/27002:2005** gestaltet werden. Sowohl Dienstbetreiber, die Teile der Telematikinfrastruktur betreiben, als auch die gematik **MUSS** ein **Informationssicherheitsmanagementsystem (ISMS)** implementieren.

Auf dieser Basis soll die Verzahnung der Prozesse und die Optimierung der Schnittstellen kontinuierlich verbessert werden.“  
(S.184)

Entnommen aus:

„Gematik: Einführung der Gesundheitskarte – Übergreifendes Sicherheitskonzept der Telematikinfrastruktur. Version 2.3.0 vom 17.07.2008 “

Quelle: [http://www.gematik.de/upload/gematik\\_DS\\_Sicherheitskonzept\\_V2\\_3\\_0\\_3802.pdf](http://www.gematik.de/upload/gematik_DS_Sicherheitskonzept_V2_3_0_3802.pdf)

## Was heißt das nun?

### Die „schlechte“ Nachricht

„Der Betreiber von Infrastrukturdiensten und -netzen MUSS ein Informationssicherheitssystem mind. nach ISO 27001 implementieren.“  
(S. 274)

### Die „gute“ Nachricht

„Anmerkung: Dies bedeutet, dass der Betreiber nach ISO/IEC 27001 arbeiten MUSS. Es bedeutet nicht, dass der Betreiber eine Zertifizierung nach ISO/IEC 27001 besitzen MUSS.“ (S. 274)

Entnommen aus:

„Gematik: Einführung der Gesundheitskarte – Übergreifendes Sicherheitskonzept der Telematikinfrastruktur. Version 2.3.0 vom 17.07.2008 “

Quelle: [http://www.gematik.de/upload/gematik\\_DS\\_Sicherheitskonzept\\_V2\\_3\\_0\\_3802.pdf](http://www.gematik.de/upload/gematik_DS_Sicherheitskonzept_V2_3_0_3802.pdf)

# Das hohe Ziel: Zertifizierung im Bereich Sicherheit



Quelle: <http://www.nepalhiking.com/images/mount-everest.gif>, [http://www.jurowl.de/images/de\\_mail\\_buengerportale\\_logo.jpg](http://www.jurowl.de/images/de_mail_buengerportale_logo.jpg)

Das Video zu de-mail finden Sie unter:

[http://www.cio.bund.de/cln\\_094/SharedDocs/Videos/DE/de\\_mail\\_video.html?  
nn=55498#download=%201](http://www.cio.bund.de/cln_094/SharedDocs/Videos/DE/de_mail_video.html?nn=55498#download=%201)

# Der neue Dienst für Deutschland: De-Mail

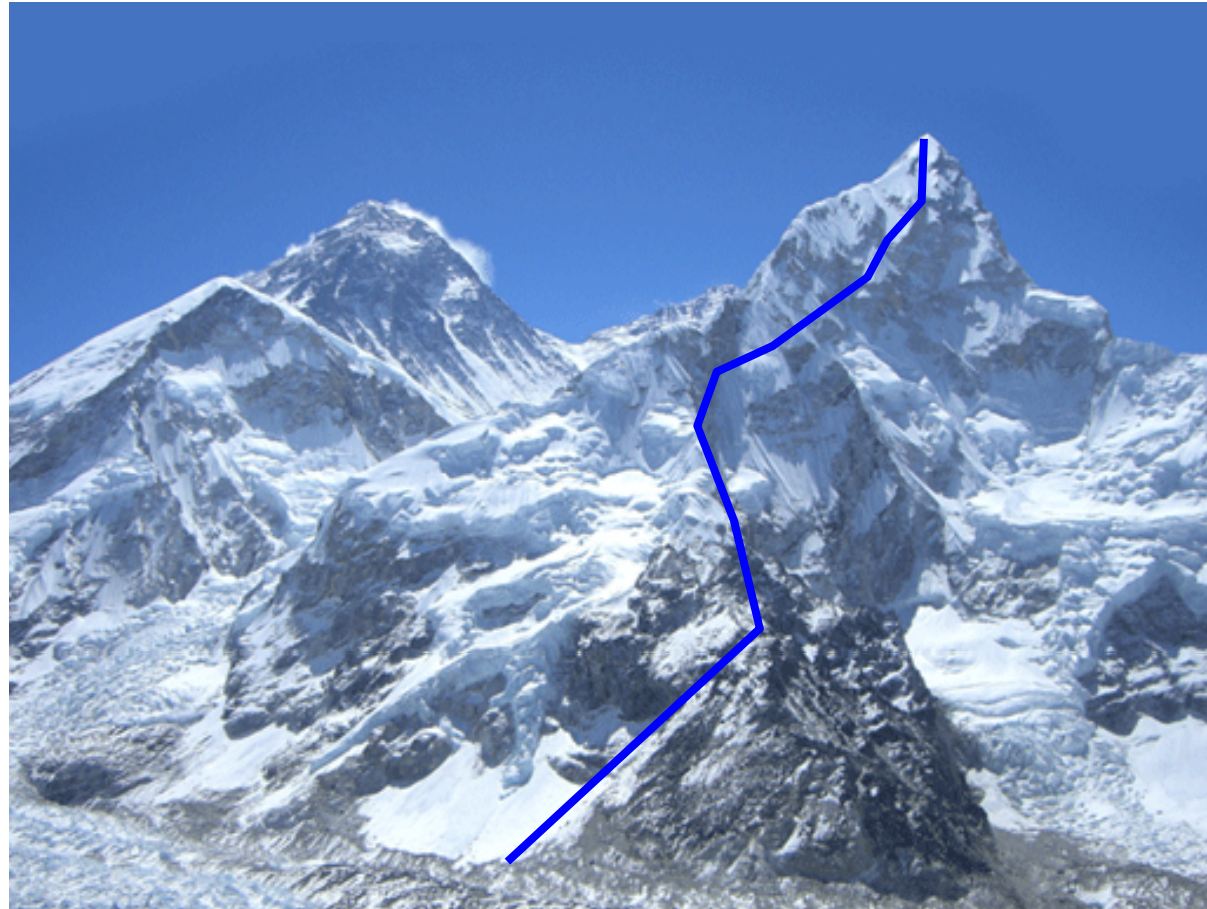
„Erfüllung der Pflichten nach §§ 3 bis 13 sowie § 16, Zusammenwirken mit anderen akkreditierten Diensteanbietern (Interoperabilität), ständige Verfügbarkeit, sicheres Erbringen der Dienste durch Sicherheitszertifikate (§ 18 Absatz 2 Nummer 3) und Erfüllung der datenschutzrechtlichen Anforderungen (§ 18 Absatz 2 Nummer 4).

**Dafür sind folgende Prüfungen erforderlich:**

- Interoperabilität der angebotenen Dienste
- IT-Sicherheit der eingesetzten sicherheitsrelevanten Hard- und Softwarekomponenten
- Datenschutz
- IT-Sicherheit nach ISO 27001 auf der Basis von IT-Grundschutz (für Organisation und Prozesse)

Quelle: Entwurf eines Gesetzes zur Regelung von Bürgerportalen und zur Änderung weiterer Vorschriften, S. 19

# Das hohe Ziel: Zertifizierung im Bereich Sicherheit



## Vergleich ISO 9001

Quelle: <http://www.nepalhiking.com/images/mount-everest.gif>, [http://www.jurowl.de/images/de\\_mail\\_buergerportale\\_logo.jpg](http://www.jurowl.de/images/de_mail_buergerportale_logo.jpg)

# Wikipedia über die ISO 9001 (Qualitätsmanagementnorm)

„Aus marktstrategischer Sicht dient einem in Konkurrenz stehenden Unternehmen ein Zertifikat, um die Qualität seiner Produkte oder Dienstleistungen nachweisen zu können. Für Hersteller, Zulieferer und große internationale Unternehmen kann das Zertifikat als „**zwingend**“ betrachtet werden, **um überhaupt Aufträge** einer gewissen Größenordnung **zu bekommen**.“

## Was sollten Sie tun?

- Erfassung aller Schutzgegenstände
- Durchführung einer Risikoanalyse
- Erkennen von Schwächen und Implementierung geeigneter Gegenmaßnahmen
- Etablierung des Datenschutzes und der Rechtskonformität
- Dokumentation aller Maßnahmen
- Sensibilisierung aller Mitarbeiter

# Informationsmöglichkeiten

[www.ec-net.de](http://www.ec-net.de) ; [www.md-ecz.de](http://www.md-ecz.de) ; [www.tti-md.de](http://www.tti-md.de)

[www.bsi.de](http://www.bsi.de) ; [De-mail](mailto:De-mail)

„Information Security Management“  
Loseblattsammlung der TÜV Media GmbH

[www.tuev-media.de](http://www.tuev-media.de)

Vielen Dank für Ihre Aufmerksamkeit

MD-ECZ

Magdeburger Electronic Commerce Zentrum

Dr. Jörg Bode

Roland Hallau

Wilfried Müller

03941 567007  
jbode@tti-md.de

0391 7443524  
rhallau@tti-md.de

0391 7443537  
wmueller@tti-md.de

[www.md-ecz.de](http://www.md-ecz.de)  
[www.ec-net.de](http://www.ec-net.de)