



# DIN ISO/IEC 27001:2005

## Informationssicherheits-Managementsysteme

hitforum.de am 29.04.2009

Helmut Elschner  
Senior Consultant Information Security



[www.materna.com](http://www.materna.com)

## Informationssicherheit – Definitionen

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

en.wikipedia.org based on [44 U.S.C § 3542 \(b\)\(1\) \(2006\)](#)

Informationssicherheit ist das Ergebnis eines Systems von Strategien und Verfahren zur Identifizierung, Kontrolle und zum Schutz von Informationen und Geräten, die im Zusammenhang mit ihrer Speicherung, Übermittlung und Verarbeitung genutzt werden

Source: ISO/IEC 20000-2 Clause 6.6.1

## Informationssicherheit – und noch eine Definition

### Informationssicherheit nach ISO / IEC 17799

Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen;  
andere Eigenschaften wie Authentizität, Zurechenbarkeit, Nicht-Abstreitbarkeit  
und Verlässlichkeit können ebenfalls berücksichtigt werden

## „Informationssicherheit“ ist mehr als nur „IT-Sicherheit“

### **IT-Sicherheit**

fokussiert sich traditionell auf den Schutz von IT-Systemen und den dort gespeicherten Daten

### **Informationssicherheit**

betrachtet Information in jeder Form:  
auf Datenträgern, auf Papier, gesprochen, ...

## Informationen sind Werte

Mehr denn je ist uns bewusst: Informationen sind Werte. Wir besitzen sie aus unterschiedlichen Gründen - weil wir für ihre Verwahrung oder Verarbeitung Verantwortung tragen, weil wir aus ihnen einen Vorteil ziehen, weil ihre Kenntnis uns vor Schaden bewahrt und noch viel mehr. Gehen sie uns verloren, werden sie gestohlen, sind sie falsch oder einfach nicht auffindbar, wenn wir sie benötigen, dann erleiden wir Schaden - die Palette reicht von geringfügig bis existenzbedrohend.

Österreichisches Informationssicherheitshandbuch (April 2007)

## Informationssicherheit im Detail

Alle Organisationen betreiben Geschäftsprozesse

Geschäftsprozesse werden durch IT-Services  
unterstützt oder auch erst ermöglicht

Geschäftsprozesse nutzen Anlagen und Werte (Assets)  
(Kundendaten, Patente, IT-Systeme / -Einrichtungen, ...)

Risiken bedrohen die Prozesse, Anlagen, Werte

Informationssicherheit hat den Schutz der Werte zum Ziel

# Grundwerte der Informationssicherheit

## **Verfügbarkeit**

von EDV-Systemen, Anwendungen, Daten

## **Vertraulichkeit**

Geschäftsgeheimnisse, Sensitive Daten

## **Integrität**

Nicht autorisierte Änderungen gespeicherter oder übertragener Daten ausschließen bzw. erkennen

# Bedrohungen

## Höhere Gewalt

Ausfall, Blitz, Feuer, Wasser, Kabelbrand, ...

## Organisatorische Mängel

Fehlende oder unzureichende Regelung  
Mangelhafte Kontrolle, Unbefugter Zutritt, ...

## Menschliche Fehlhandlungen

Fehlbedienung, fehlerhafte Administration,  
Übertragen falscher Datensätze, ...

## Technisches Versagen

Ausfall der Stromversorgung, Ausfall von  
Netzkomponenten, Datenverlust

## Vorsätzliche Handlungen

Manipulation, Diebstahl, Vandalismus,  
Missbrauch, „Trojanische Pferde“, ...

# Schutzmaßnahmen

## **Infrastrukturelle Maßnahmen**

Blitzschutz, Feuerlöscher, Klimatisierung, Räume

## **Organisatorische Maßnahmen**

Festlegen von Verantwortlichkeiten, Zugangs- und Zugriffsrechte, Firewallkonzept, Kontrolle, ...

## **Personelle Maßnahmen**

Einarbeitung, Einweisung, Schulung, Sicherheitsbewusstsein schaffen, ...

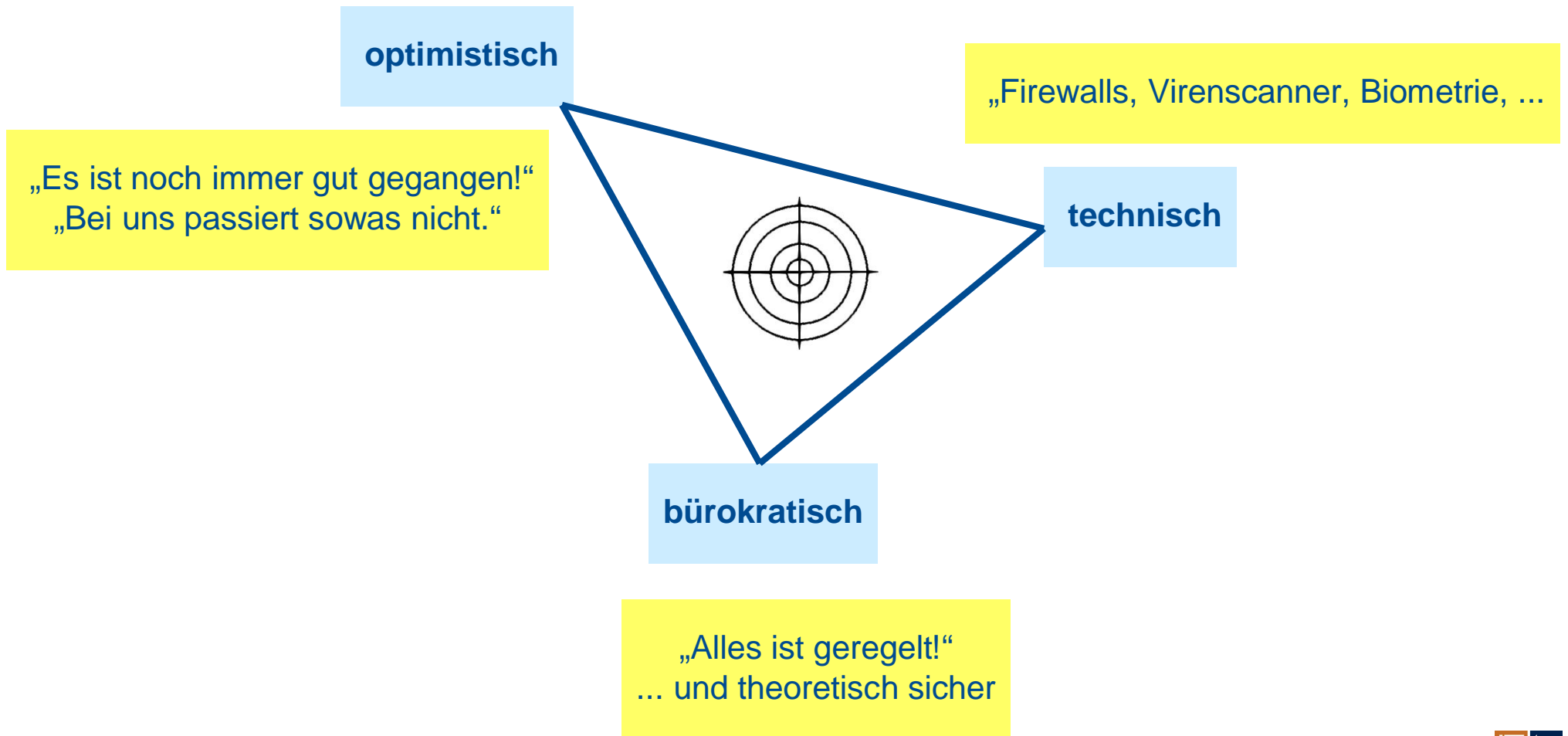
## **Technische Maßnahmen**

Passwortschutz, Bildschirmsperre, Firewalls, Virenschutz, Verschlüsselung, ...

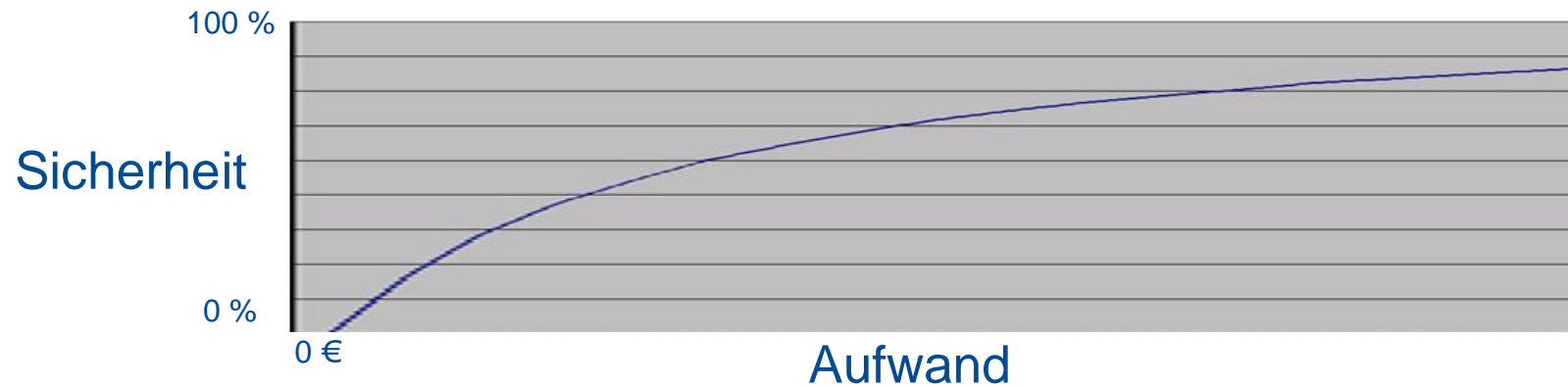
## **Notfall Vorsorgemaßnahmen**

Notfallhandbuch, Alarmierungsplan, Datensicherungsplan, Ersatzsysteme, ...

# „Informations-Sicherheits-Strategien“



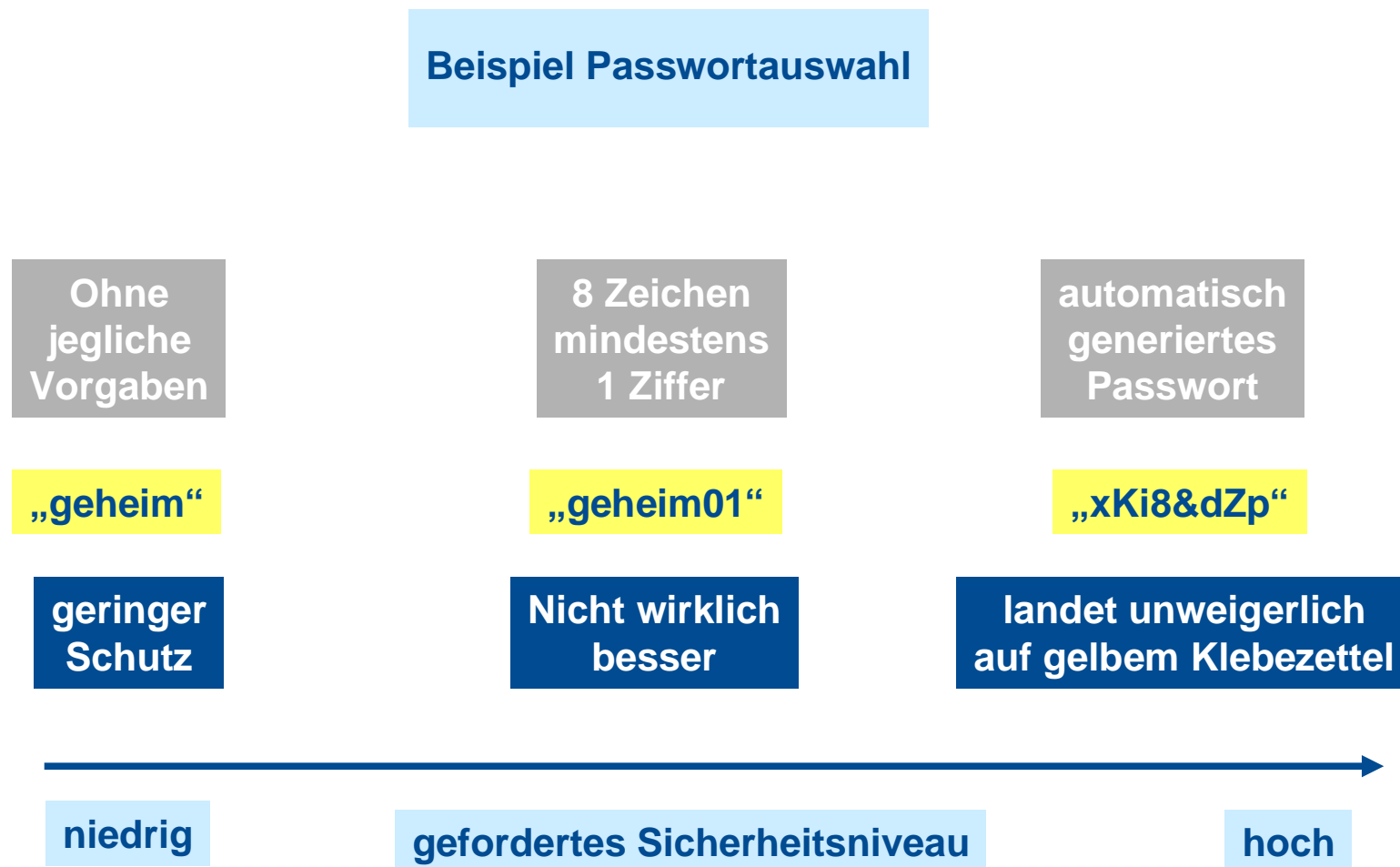
## Kosten / Nutzen - Relation



**100-prozentige Sicherheit ist nicht erreichbar  
Aber wie weit müssen wir gehen?  
Was ist das „passende“ Sicherheitsniveau?**

## Wahl eines realistischen Sicherheitsniveaus

### Beispiel Passwortauswahl



## Sicherheitsmaßnahmen im praktischen Einsatz



# Komponenten der Informations-Sicherheit

## TECHNIK

Firewalls, Virens Scanner, Kryptografie,  
Intrusion Detection, Smartcards, Token, ...

## ORGANISATION

Sicherheitsleitlinien, Sicherheitsrichtlinien,  
Sicherheitskonzepte, Regelung von Verantwortlichkeiten, ...

## MENSCHEN

Mitdenken, Verstehen, Beobachten, Melden, Reagieren, ...

**!!!** *Unkoordinierte Einzelmaßnahmen allein  
können nicht die benötigte Wirkung erzielen.*

*Gebraucht wird*

- *ein ganzheitlicher Ansatz*
  - *eine methodische Vorgehensweise*
  - *eine sinnvolle Koordination*
  - *kontinuierliche Verbesserung*
- ein Managementsystem für Informationssicherheit**

# Informationssicherheits-Managementsystem

## Informationssicherheits-Managementsystem (ISMS)

Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt

ANMERKUNG Das Managementsystem enthält die Struktur, Grundsätze, Planungsaktivitäten, Verantwortung, Praktiken, Verfahren, Prozesse und Ressourcen der Organisation.

(ISO 27001, Begriffe 3.7)

## Drei Normen aus der Normenreihe ISO 27000

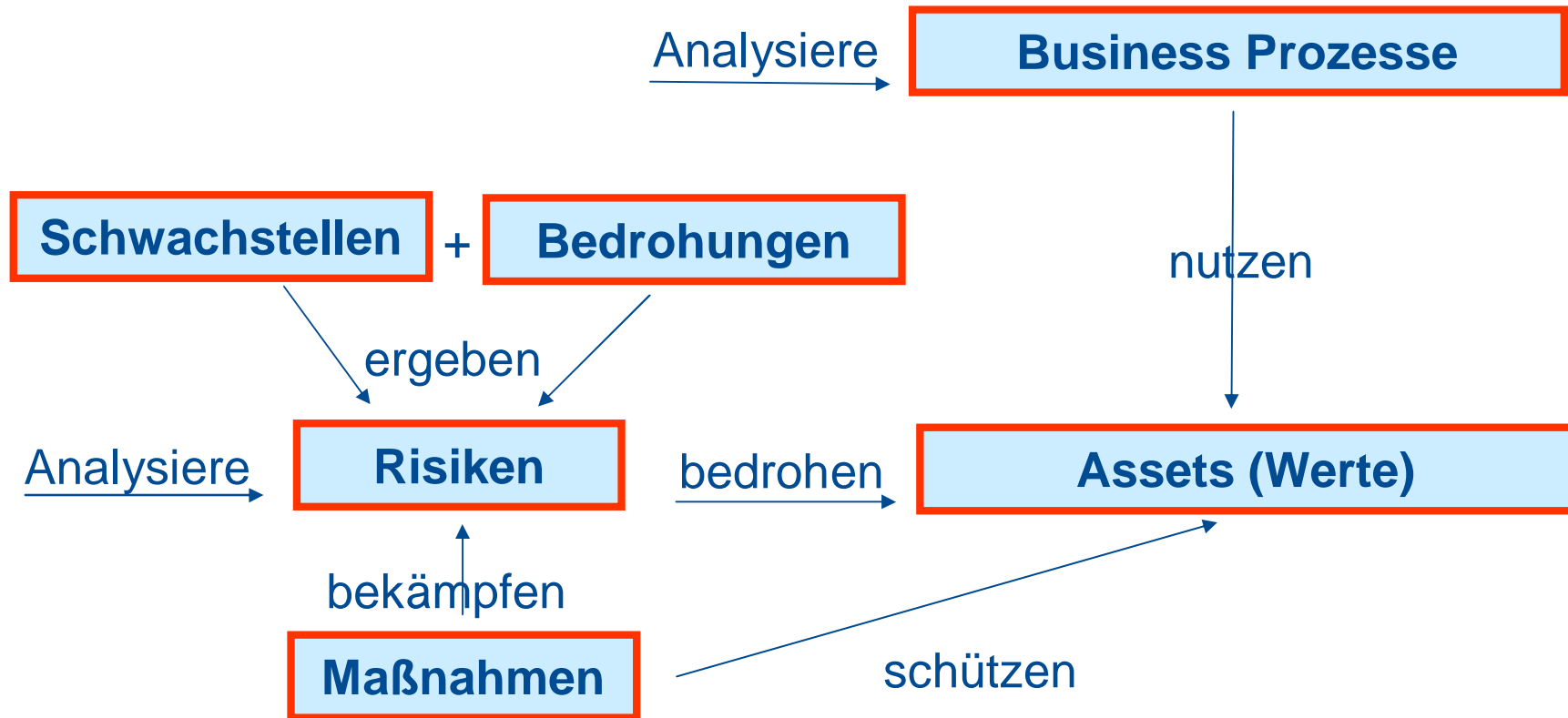
- ISO 27001 Informationssicherheits-Managementsysteme – **Anforderungen**
  - Enthält die formale Spezifikation und die normativen Anforderungen, **was** für die Einrichtung, Umsetzung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung eines Informationssicherheits-Managementsystems realisiert werden muss (ca. 45 Seiten)
- ISO 27002 **Leitfaden** für das Informationssicherheits-Management
  - Enthält Empfehlungen und Anleitungen zur Umsetzung, **wie** die Maßnahmenziele realisiert werden können (ca. 138 Seiten)
- ISO 27005 Informationssicherheits-**Risikomanagement**
  - Enthält einen der möglichen und systematischen Ansätze zum Aufbau eines Informationssicherheits-Risikomanagements, wie er zur Realisierung eines Informationssicherheits-Managementsystems gefordert wird

“Die Internationale Norm ISO 27001 ist mit ISO 9001 (Qualitätsmanagementsysteme) und ISO 14001 (Umweltmanagementsysteme) abgestimmt worden, um die konsistente und integrierte Umsetzung und Durchführung mit verwandten Managementsystemen zu unterstützen.”

## Historische Entwicklung

- **1992: Information Security Best Practices**  
Kommission des Department of Trade and Industry (UK)
- **1993: „Code of Practice“ veröffentlicht**
- **1995: BS 7799:1995 (British Standard Institute)**
- **1999: BS 7799-1 (Best Practices)**
- **1999: BS 7799-2 (Specifications) Zertifizierungsgrundlage**
- **2000: ISO 17799:2000 (Best Practices - BS 7799-1)**
- **2002: BS 7799-2:2002 (Einführung PDCA)**
- **2005: ISO/IEC 17799:2005 (Code of practice)**
- **2005: ISO/IEC 27001:2005 (Requirements) Zertifizierungsgrundlage**
- **2007: ISO/IEC 27002 (durch Umbenennung der ISO/IEC 17799 in 27002)**

# Risikomanagement



## Der prozessorientierte Ansatz und das PDCA Modell

ISO 27001 verwendet das PDCA Modell zur Strukturierung der ISMS Prozesse. Informationssicherheit ist ein kontinuierlicher Verbesserungsprozess (KVP).



## Das Management-Rahmenwerk für ein ISMS

ISO 27001 strukturiert den ISMS Prozess in fünf Phasen:



## Wie die Festlegung und Verwaltung eines ISMS erfolgt

Die Anforderungen und die vier Phasen aus Abschnitt 4 im Detail:



## Die normativen Maßnahmenziele der ISO 27001

- **A.5 Sicherheitsleitlinie**
  - A.5.1 Informationssicherheitsleitlinie
- **A.6 Organisation der Informationssicherheit**
  - A.6.1 Interne Organisation
  - A.6.2 Externe Beziehungen
- **A.7 Management von organisationseigenen Werten**
  - A.7.1 Verantwortung für organisationseigene Werte
  - A.7.2 Klassifizierung von Informationen
- **A.8 Personelle Sicherheit**
  - A.8.1 Vor der Anstellung
  - A.8.2 Während der Anstellung
  - A.8.3 Beendigung oder Änderung der Anstellung
- **A.9 Physische und umgebungsbezogene Sicherheit**
  - A.9.1 Sicherheitsbereiche
  - A.9.2 Sicherheit von Betriebsmitteln
- **A.10 Betriebs- und Kommunikationsmanagement**
  - A.10.1 Verfahren und Verantwortlichkeiten
  - A.10.2 Management der Dienstleistung von Dritten
  - A.10.3 Systemplanung und Abnahme
  - A.10.4 Schutz vor Schadsoftware und mobilem Code
  - A.10.5 Backup
  - A.10.6 Management der Netzwerksicherheit
  - A.10.7 Handhabung von Speichermedien
  - A.10.8 Austausch von Informationen
  - A.10.9 E-Commerce-Anwendungen
  - A.10.10 Überwachung
- **A.11 Zugangskontrolle**
  - A.11.1 Geschäftsanforderungen für Zugangskontrolle
  - A.11.2 Benutzerverwaltung
  - A.11.3 Benutzerverantwortung
  - A.11.4 Zugangskontrolle für Netze
  - A.11.5 Zugriffskontrolle auf Betriebssysteme
  - A.11.6. Zugangskontrolle zu Anwendungen und Information
  - A.11.7 Mobile Computing und Telearbeit
- **A.12 Beschaffung, Entwicklung und Wartung von Informationssystemen**
  - A.12.1 Sicherheitsanforderungen an Informationssysteme
  - A.12.2 Korrekte Verarbeitung in Anwendungen
  - A.12.3 Kryptographische Maßnahmen
  - A.12.4 Sicherheit von Systemdateien
  - A.12.5 Sicherheit bei Entwicklungs- und Unterstützungsprozessen
  - A.12.6 Schwachstellenmanagement
- **A.13 Umgang mit Informationssicherheitsvorfällen**
  - A.13.1 Melden von Ereignissen und Schwachstellen
  - A.13.2 Umgang mit Vorfällen und Verbesserungen
- **A.14 Sicherstellung des Geschäftsbetriebs (BCM)**
  - A.14.1 Informationssicherheitsaspekte bei BCM
- **A.15 Einhaltung von Vorgaben (Compliance)**
  - A.15.1 Einhaltung gesetzlicher Vorgaben
  - A.15.2 Einhaltung von Sicherheitsregelungen und -standards sowie technischer Vorgaben
  - A.15.3 Überlegungen zu Revisionsprüfungen

## Die fünf möglichen Schritte zur Zertifizierung

“Die Einführung eines ISMS sollte eine strategische Entscheidung (...) sein.”  
Informationssicherheit ist weder ein Produkt noch ein Projekt, sondern ein Prozess.



## Von der TGA akkreditierte Zertifizierungsstellen für ISO 27001



Anforderungen für Zertifizierungsstellen: ISO/IEC 17021:2006 und 27006:2007

TGA – Trägergemeinschaft für Akkreditierung German Association for Accreditation GmbH



### ISO 27001 (alphabetisch)


Zertifizierungsstelle	Land PLZ Ort
Comgroup GmbH	D-97980 Bad Mergentheim
DEKRA Certification GmbH	D-70565 Stuttgart
DQS GmbH	
Deutsche Gesellschaft zur Zertifizierung von Managementsystemen	D-60433 Frankfurt/Main
TÜV CERT - Zertifizierungsstelle der TÜV Rheinland Industrie Service GmbH	D-51105 Köln
TÜV CERT-Zertifizierungsstelle des TÜV Saarland e.V.	D-66280 Sulzbach
TÜV NORD CERT GmbH	D-45141 Essen
TÜV Rheinland Cert GmbH	D-51105 Köln
TÜV SÜD Management Service GmbH	D-80339 München
UIMCert GmbH	D-42115 Wuppertal

In diesem Bereich akkreditierte Zertifizierungsstelle(n): 9

[Zurück](#)

## ISO 27001 „live!“ – Blick in den Normentext

Detailanzeige für:  
DIN ISO/IEC 27001:2008-09

Variante	Download	Versand	Abo
Originalsprache: de	<input type="checkbox"/> EUR 108,80	<input type="checkbox"/> EUR 108,80	<input type="checkbox"/>
Übersetzung: en	<input type="checkbox"/> EUR 116,90	<input type="checkbox"/> EUR 116,90	<input type="checkbox"/> 

Aus Gründen des Urheberrechts bzw. Copyrights enthalten diese Folien lediglich einen Verweis auf eine mögliche Bezugsquelle anstelle der im Vortrag „live“ vorgestellten Normen. Wir bitten um Ihr Verständnis!

Dokumentenart: Norm

Ausgabe: 2008-09

Titel (deutsch): Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (ISO/IEC 27001:2005)

Titel (englisch): Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2005)

Inhaltsverzeichnis: [Inhaltsverzeichnis einsehen \(de\)](#) 

Originalsprachen: Deutsch

Preis: EUR 108,80

### DIN ISO/IEC 27001 (deutsch)


Bezug z.B. hier: <http://www.beuth.de/langanzeige/DIN+ISO%2FIEC+27001/103960154.html>

**Hinweis: Für Zertifizierungen ist der englische Text maßgeblich!**

## ISO 27001 „live!“ – Blick in den Normentext

Detailanzeige für:

ISO/IEC 27001:2005-10

Variante	Download	Versand	Abo
Originalsprache: en	<input type="checkbox"/> EUR 103,10	<input type="checkbox"/> EUR 103,10	<input type="checkbox"/>
Übersetzung: fr	<input type="checkbox"/> EUR 103,10	<input type="checkbox"/> EUR 103,10	

Aus Gründen des Urheberrechts bzw. Copyrights enthalten diese Folien lediglich einen Verweis auf eine mögliche Bezugsquelle anstelle der im Vortrag „live“ vorgestellten Normen. Wir bitten um Ihr Verständnis!

Dokumentenart: Norm

Ausgabe: 2005-10

Titel (deutsch): Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen

Titel (englisch): Information technology - Security techniques - Information security management systems - Requirements

Originalsprachen: Englisch

Preis: EUR 103,10


### ISO/IEC 27001 (Original, englisch)

Bezug z.B. hier: <http://www.beuth.de/langanzeige/ISO%2FIEC+27001/de/85689528.html>

**Hinweis: Für Zertifizierungen ist der englische Text maßgeblich!**

## ISO 27002 „live!“ – Blick in den Normentext

Detailanzeige für:  
**DIN ISO/IEC 27002:2008-09**

Variante	Download	Versand	Abo
Originalsprache: de	<input type="checkbox"/> EUR 204,10	<input type="checkbox"/> EUR 204,10	<input type="checkbox"/>
Übersetzung: en	<input type="checkbox"/> EUR 232,80	<input type="checkbox"/> EUR 232,80	<input type="checkbox"/> 

Aus Gründen des Urheberrechts bzw. Copyrights enthalten diese Folien lediglich einen Verweis auf eine mögliche Bezugsquelle anstelle der im Vortrag „live“ vorgestellten Normen. Wir bitten um Ihr Verständnis!

Dokumentenart: Norm

Ausgabe: 2008-09

Titel (deutsch): Informationstechnik - IT-Sicherheitsverfahren - Leitfaden für das Informationssicherheits-Management (ISO/IEC 27002:2005)

Titel (englisch): Information technology - Security techniques - Code of practice for information security management (ISO/IEC 27002:2005)

Inhaltsverzeichnis: [Inhaltsverzeichnis einsehen \(de\)](#) 

Originalsprachen: Deutsch


Preis: EUR 204,10

### DIN ISO/IEC 27001 (deutsch)

Bezug z.B. hier: <http://www.beuth.de/langanzeige/DIN+ISO%2FIEC+27002/de/110488964.html>

## ISO 27002 „live!“ – Blick in den Normentext

Detailanzeige für:  
ISO/IEC 27002:2005-06

Variante	Download	Versand	Abo
Originalsprache: en	<input type="checkbox"/> EUR 165,00	<input type="checkbox"/> EUR 165,00	<input type="checkbox"/>
Übersetzung: fr	<input type="checkbox"/> EUR 165,00	<input type="checkbox"/> EUR 165,00	

Aus Gründen des Urheberrechts bzw. Copyrights enthalten diese Folien lediglich einen Verweis auf eine mögliche Bezugsquelle anstelle der im Vortrag „live“ vorgestellten Normen. Wir bitten um Ihr Verständnis!

Dokumentenart:	Norm
Ausgabe:	2005-06
Titel (deutsch):	Informationstechnik - IT-Sicherheitsverfahren - Leitfaden für das Management der Informationssicherheit
Titel (englisch):	Information technology - Security techniques - Code of practice for information security management
Originalsprachen:	Englisch
Berichtigungsinformation:	Im DIN-Anzeiger für technische Regeln 10/2007, ICS 35.040, wurde dieses Dokument irrtümlich als zurückgezogen gemeldet. Die Ausgabe 2005-06 der ISO/IEC 27002 (ehemals ISO/IEC 17799) ist weiterhin gültig und enthält jetzt auch das Technical Corrigendum 1:2007-07.
Änderung:	Dieser Artikel wurde <b>geändert durch »</b>
Preis:	EUR 165,00

### ISO/IEC 27002 (Original, englisch)

Bezug z.B. hier: <http://www.beuth.de/langanzeige/ISO%2FIEC+27002/de/83099069.html>

## Vielen Dank für Ihre Aufmerksamkeit!

Name

Helmut Elschner

Funktion

Senior Consultant Information Security

E-Mail

[helmut.elschner@materna.de](mailto:helmut.elschner@materna.de)