

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages



Netzwerk Elektronischer Geschäftsverkehr

Würzburg, 14.07.2009

Informationssicherheit heute und in Zukunft

MECK Informationsveranstaltung
Teil 4 von 4 der MECK Veranstaltungsreihe Sicherheit

Andreas Gabriel
www.meck-online.de und www.ec-net.de/sicherheit



Netzwerk Elektronischer Geschäftsverkehr



Beratung für kleine und mittelständische Unternehmen durch
das Mainfränkisches Electronic Commerce Kompetenzzentrum


Das MECK-Team:



Herr Oliver Freitag
Projektleiter des MECK
Bereichsleiter
Innovation/Umwelt
IHK Würzburg-Schweinfurt



Herr Volker Dürrbeck
Bereich ERP/Software
Lehrstuhl Prof. Thome



Herr Ludwig Habersetzer
MECK Grundberatung
Lehrstuhl Prof. Thome



Herr Andreas Gabriel
Bereich Informationssicherheit und
Datenschutz
Lehrstuhl Prof. Thome



Herr Rüdiger Landeck
Handwerkskammer
für Unterfranken



Herr Urban Östreicher
Handwerkskammer
für Unterfranken

... und zahlreiche Partner

Sie erreichen uns unter: <http://www.meck-online.de>



Wir sind nicht alleine:
Netzwerk Elektronischer Geschäftsverkehr

- 27 regionale Zentren in ganz Deutschland
- 1 Branchenzentrum „Handel“ mit Sitz in Köln
- Projektträger:
Deutsche Gesellschaft für Luft- und Raumfahrt (DLR)
- Förderung durch das BMWi (Bundesministerium für Wirtschaft und Technologie)

<http://www.ec-net.de>



Verbundprojekt „Sichere E-Geschäftsprozesse in KMU und Handwerk“ – Kooperationspartner



Dr. Kai Hudetz,
Andreas Duscha



Andreas Gabriel



Ekkehard Diedrich
Harald Kesberg



Dagmar Lange
(Projektleiterin)
Prof. Dr. Günther Neef



Über meine Person



Andreas Gabriel
Jahrgang 1974

- BWL-Studium
- Certified Lead Auditor ISO 27001
- Datenschutzbeauftragter
- Selbstverteidigungs- & Selbstbehauptungslehrer

Der Schwerpunkt meiner Tätigkeit:

„Der kreative Umgang mit dem Thema Sicherheit“

- Referent an verschiedenen IHKs und HWKs
- Dozent an der Universität Würzburg;
u. a. beim Weiterbildungsstudiengang
MBA Business Integration
(<http://www.businessintegration.de>)



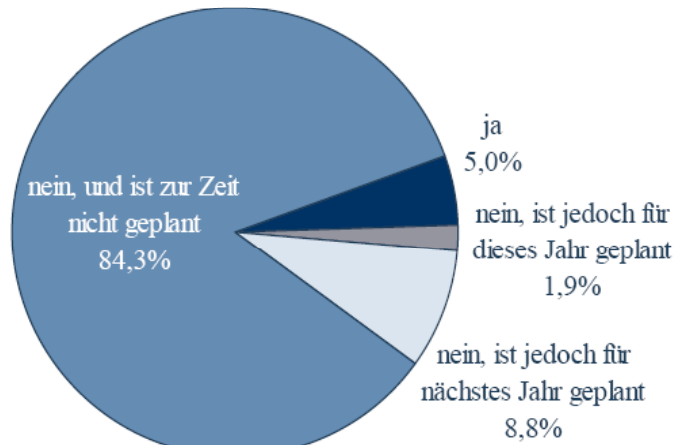
Was versteht man unter einer Zertifizierung?

„Nach 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.



Weil es der Markt von Ihnen fordern wird!

Warum überhaupt eine Sicherheitszertifizierung?

- „Verbesserung der Kundenzufriedenheit ...
... waren diese bis jetzt etwa unzufrieden?“
- „Zertifizierung als Marketinginstrument ...
... wie teuer darf Werbung überhaupt sein?“
- „Vorteil gegenüber Konkurrenten ...
... verlieren Sie gerade etwa Aufträge?“
- „Internationalisierung der Märkte ...
... wie weit reicht Ihr Geschäftsbereich?“
- „Verbesserung der Sicherheit ...
... waren Sie bisher etwa unsicher?“

Wenn...

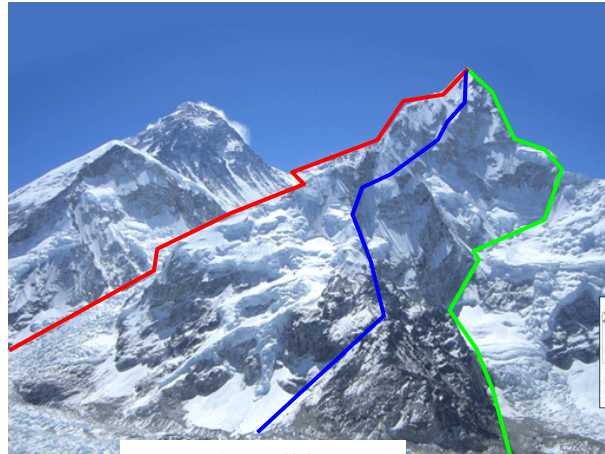
3

Bild: <http://www.nepalhiking.com/images/mount-everest.gif>

Quelle: In Anlehnung an G. Gumpo/F. Wallisch: ISO 9000 entschlüsselt



Warum überhaupt eine Zertifizierung im Bereich Informationssicherheit?



Wenn's wirklich sicher **Vergleich ISO 9001** Geschäftsverkehr

9

Quelle: <http://www.nepalhiking.com/images/mount-everest.gif>, http://www.jurowl.de/images/de_mail_buergerportale_logo.jpg



Begrifflichkeiten im Bereich EDV und Sicherheit

Definition „IT“:

„IT umfasst im Sinne des BSI-Errichtungsgesetzes alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen.“

Quelle: BSI Schulung IT-Grundschutz – Glossar

Definition „IT-Sicherheit“:

„Der Zustand eines IT-Systems, in dem die Risiken, die beim Einsatz dieses Systems aufgrund von Gefährdungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind.“

Quelle: BSI Schulung IT-Grundschutz – Glossar

Definition „Datenschutz“:

- (1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird
- (2) Dieses Gesetz gilt für die **Erhebung, Verarbeitung und Nutzung** personenbezogener Daten (...)

Quelle: § 1 Bundesdatenschutzgesetz

Wenn's wirklich sicher sein soll – Netzwerk Elektronischer Geschäftsverkehr

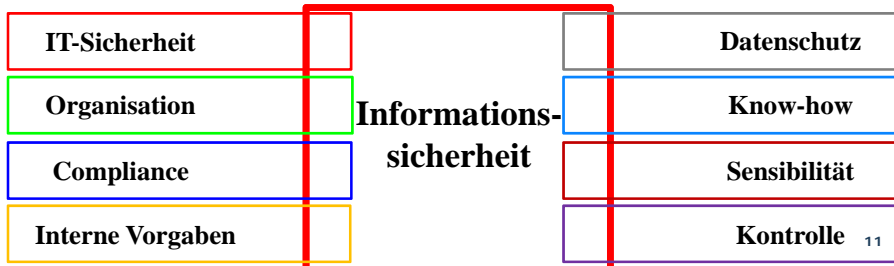
10



Definition „Informationssicherheit“

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

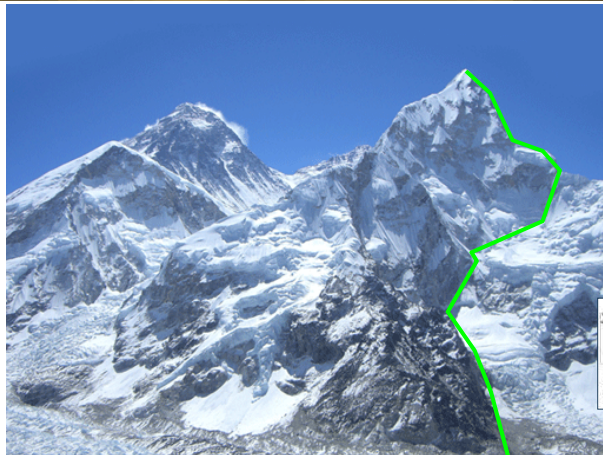
Quelle: ISO 27001, S. 8



© A. Gabriel



Das hohe Ziel: Zertifizierung im Bereich Sicherheit



Wenn's wirklich sicher sein soll – Netzwerk Elektronischer Geschäftsverkehr

12

Quelle: <http://www.nepalhiking.com/images/mount-everest.gif>, http://www.jurowl.de/images/de_mail_buergeportale_logo.jpg



Warum müssen Sie sich mit dem Thema Sicherheit beschäftigen?

Ulla Schmidt
Bundesministerin für Gesundheit



Die Gesundheitskarte



Umsetzung durch die



Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

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



Was die Gematik von ihren Geschäftspartnern fordert?

„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



Was versteht man unter einem Informations-Sicherheits-Management-System (ISMS)?

„Der 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.“

Quelle: ISO 27001, S. 8



Historische Betrachtung der ISO

DTI	=	Department of Trade and Industry	1993
CoP	=	Code of Practice	
BS 7799	=	British Standard Nr. 7799	
		Teil 1 → Best Practice	1995 bis
		Teil 2 → Zertifizierungsgrundlage	1998
BSi	=	British Standard Institution	
ISO	=	ISOS (griechisch) vergleichbar mit / equal as	
	=	International Organization of Standardization	
IEC	=	International Electrotechnical Commission	seit
DIN	=	Deutsches Institut für Normung	2000
		ISO 27001 → Zertifizierungsgrundlage	
		ISO 27002 → Best Practice (ehem. ISO 17799)	¹⁶



Die ISO 27001 besteht aus ...

Komponenten der ISO	Beschreibung/ Charakterisierung	Fachbegriffe der ISO
11 Elementen	Rahmenbedingungen des ISO 27001	Clauses
37 Maßnahmenzielen	Ziele, die durch den ISO 27001 vorgegeben werden	Objectives
133 detaillierte Maßnahmen	Detaillierte Umsetzungsanforderungen	Controls



11 Kategorien für 133 Controls

- A5: Sicherheitspolitik
- A6: Organisation der Sicherheit
- A7: Einstufung und Kontrolle der Werte
- A8: Personelle Sicherheit
- A9: Physikalische und umgebungsbezogene Sicherheit
- A10: Management der Kommunikation und des Geschäftsbetriebes
- A11: Zugangskontrollen
- A12: Beschaffung von IT-Systemen, Systementwicklung und -wartung
- A13: Behandlung von Vorfällen
- A14: Aufrechterhaltung des reibungslosen Geschäftsbetriebs
- A15: Einhaltung gesetzlicher und normativer Verpflichtungen

Quelle: ISO 27001



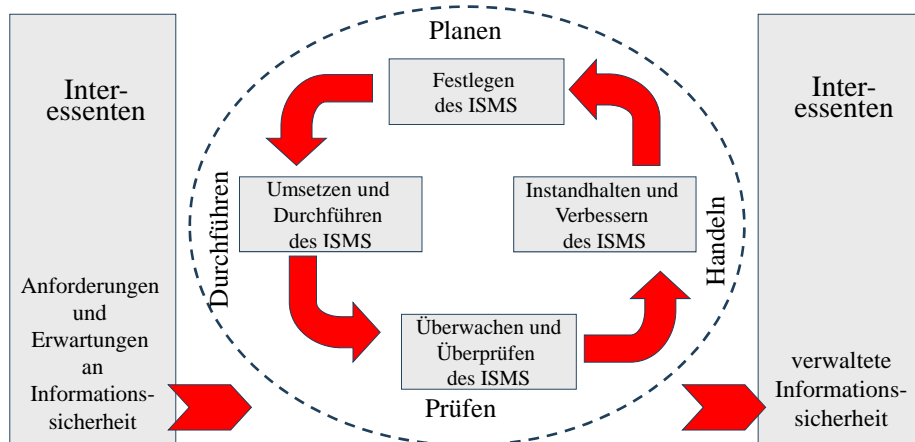
Die Normen der „ISO 27000 Familie“ im Überblick

Standard	Titel
ISO 27000	„ISMS – Fundamentals und vocabulary“
ISO 27001	„ISMS – Specification“
ISO 27002	„ISM – Code of Practice“
ISO 27003	„ISMS – Implementation Guidance“
ISO 27004	„ISM – Measurement“
ISO 27005	„IS – Risc Management“
ISO 27006	„ISMS – Requirements for bodies providing audit and certification“

Quelle: Brunnstein, J.; Pohl, H. (Hrsg.): ITIL. Security Management realisieren



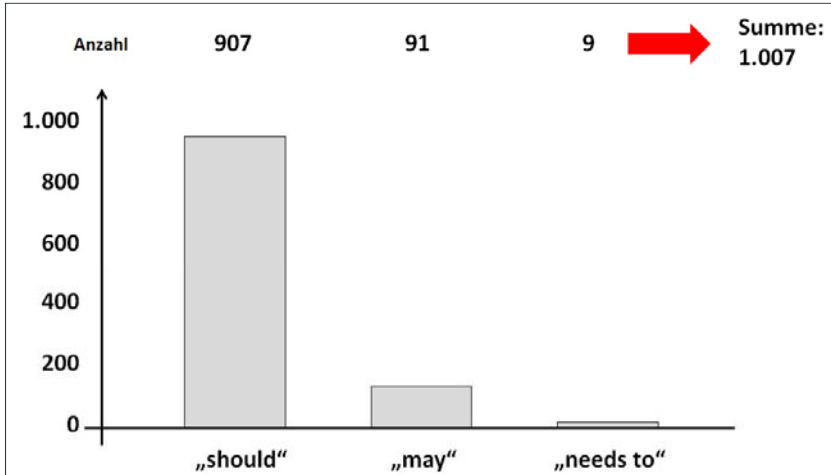
Die Vorgehensweise Das „Plan – Do – Check – Act – Modell“ (PDCA)



Quelle: ISO 27001



Kleiner Rückblick:
Wortwahl in der ISO 17799:2005



Quelle: M. Hauß, SRC Security Research & Consulting GmbH



Status Quo
ISO 27001

UK	400
China	190
D	119
USA	91
I	54
Spain	35
A	29
F	12
NL	12
CH	6
Summe	5.626

Japan	3191*	Iceland	12	Peru	3
India	451	Netherlands	12	Vietnam	3
UK	400	Pakistan	11	Belgium	2
Taiwan	321	Singapore	11	Isle of Man	2
China	190	Norway	10	Kazakhstan	2
Germany	119	Russian Federation	10	Morocco	2
USA	91	Saudi Arabia	10	Portugal	2
Korea	88	Slovenia	9	Ukraine	2
Czech Republic	68	Sweden	9	Argentina	1
Hungary	65	Bahrain	6	Armenia	1
Italy	54	Kuwait	6	Bangladesh	1
Poland	39	Slovakia	6	Belarus	1
Spain	35	Switzerland	6	Denmark	1
Hong Kong	30	Colombia	5	Kyrgyzstan	1
Australia	29	Croatia	5	Lebanon	1
Austria	29	Indonesia	5	Lithuania	1
Ireland	29	South Africa	5	Luxembourg	1
Mexico	27	Qatar	4	Macedonia	1
Malaysia	26	Sri Lanka	4	Mauritius	1
Brazil	22	Bulgaria	3	Moldova	1
Greece	22	Canada	3	New Zealand	1
Turkey	20	Chile	3	Sudan	1
UAE	18	Egypt	3	Uruguay	1
Thailand	16	Gibraltar	3	Yemen	1
Philippines	15	Iran	3		
Romania	15	Macau	3		
France	12	Oman	3	Total	5626

Quelle: <http://www.iso27001certificates.com>
Stand: 22.06.2009



Zertifizierungen nach ISO 27001 – Entwicklung im Laufe der letzten Jahre

Land	Anzahl der zertifizierten Unternehmen						Delta 12/06-01/09
	05.12. 2006	23.10. 2007	24.04. 2008	17.09. 2008	15.12. 2008	19.01. 2009	
China	28	74	102	161	174	182	+ 550%
Deutschland	60	87	89	108	108	108	+ 80%
Frankreich	3	5	10	12	9	10	+ 233%
Italien	42	45	46	54	54	55	+ 31%
Japan	1.715	2.317	2.554	2.645	2.863	2.994	+ 75%
Österreich	9	17	20	20	26	26	+ 189%
Spanien	8	12	13	25	26	27	+ 238%
UK	251	363	365	268	368	374	+ 49%
USA	42	54	60	71	82	85	+ 102%
Weltweit	2.814	4.036	4.457	4.802	4.987	5.190	+ 84%

Quelle: <http://www.iso27001certificates.com>



Wer darf ISO Zertifikate nach 27001 vergeben?

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](#)

Wenn's wirklich sicher sein soll – Netzwerk Elektronischer Geschäftsverkehr 24

Quelle: <http://www.tga-gmbh.de/scopes/index.php?id=0050&idsb=2>; Stand: Juni 2009



Was heißt das nun für Sie und Ihr Unternehmen?

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



Das hohe Ziel: Zertifizierung im Bereich Sicherheit



Wenn's wirklich sicher sein soll – Netzwerk Elektronischer Geschäftsverkehr

26

Quelle: <http://www.nepalhiking.com/images/mount-everest.gif>, http://www.jurowl.de/images/de_mail_buergerportale_logo.jpg



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)**



Das Bundesamt für Sicherheit in der Informationstechnik (BSI) – Auszüge aus dem Leitbild

Wer sind wir?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist der zentrale IT-Sicherheitsdienstleister des Bundes. Wir sind für IT-Sicherheit in Deutschland verantwortlich. Grundlagen unserer Arbeit sind Fachkompetenz und Neutralität.

Was wollen wir erreichen?

Unser Ziel ist der sichere Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft. Mit unserer Unterstützung soll IT-Sicherheit als wichtiges Thema wahrgenommen und eigenverantwortlich umgesetzt werden.

Wer sind unsere Kunden?

Mit unserem Angebot wenden wir uns an die Nutzer und Hersteller von Informationstechnik. Das sind heute in erster Linie öffentliche Verwaltungen in Bund, Ländern und Kommunen, aber auch Unternehmen und Privatanwender.

Was sind unsere Aufgaben?

Information
Entwicklung

Beratung
Zertifizierung



Die BSI Module im Überblick

BSI-Standards zur Informationssicherheit	IT-Grundschieutzkataloge
BSI Standard 100-1: Managementsysteme für Informationssicherheit	Bausteinkataloge <ul style="list-style-type: none"> - B1: Übergreifende Aspekte - B2: Infrastruktur - B3: IT-Systeme - B4: Netze - B5: IT-Anwendungen
BSI Standard 100-2: IT-Grundschieutz-Vorgehensweise	Gefährdungskataloge <ul style="list-style-type: none"> - G1: Höhere Gewalt - G2: Organisatorische Mängel - G3: Menschliche Fehlhandlungen - G4: Technisches Versagen - G5: Vorsätzliche Handlungen
BSI Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschieutz	Maßnahmenkataloge <ul style="list-style-type: none"> - M1: Infrastruktur - M2: Organisation - M3: Personal - M4: Hard- und Software - M5: Kommunikation - M6: Notfallvorsorge
BSI Standard 100-4: Notfallmanagement	

Quelle: http://www.bsi.bund.de/literat/bsi_standard/standard_1001.pdf



Informationen aus den BSI-Grundschieutzkatalogen

Gefährdungen	Katalogkürzel	Schicht	Anzahl Gefährdungen	Beispiel
	G 1	Höhere Gewalt	15	G 1.3 Blitz
	G 2	Organisatorische Mängel	101	G 2.5 fehlende/unzureichende Wartung
	G 3	Menschl. Fehlhandlungen	76	G 3.4 Unzulässige Kabelverbindungen
	G 4	Technisches Versagen	52	G 4.13 Verlust gespeicherter Daten
	G 5	Vorsätzliche Handlungen	126	G 5.4 Diebstahl
Summe:			370	

(Gegen-) Maßnahmen	Katalogkürzel	Schicht	Anzahl Maßnahmen	Beispiel
	M1	Infrastruktur	60	M 1.19 Einbruchschutz
	M2	Organisation	306	M 2.3 Datenträgerverwaltung
	M3	Personal	43	M 3.4 Schulung von Programmnutzung
	M4	Hard- und Software	232	M 4.15 Gesichertes Login
	M5	Kommunikation	121	M 5.66 Verwendung von SSL
	M6	Notfallvorsorge	95	M 6.12 Durchführung von Notfallübungen
Summe:			857	

Quelle: A. Pörnig



Kontaktmöglichkeiten und Informationsmaterialien 1/2

Gefährdungskataloge

Höhere Gewalt:	http://www.bsi.de/gshb/deutsch/g/g01.htm
Organisatorische Mängel:	http://www.bsi.de/gshb/deutsch/g/g02.htm
Menschliche Fehlhandlungen:	http://www.bsi.de/gshb/deutsch/g/g03.htm
Technisches Versagen:	http://www.bsi.de/gshb/deutsch/g/g04.htm
Vorsätzliche Handlungen:	http://www.bsi.de/gshb/deutsch/g/g05.htm

Maßnahmenkataloge

Infrastruktur:	http://www.bsi.de/gshb/deutsch/m/m01.htm
Organisation:	http://www.bsi.de/gshb/deutsch/m/m02.htm
Personal:	http://www.bsi.de/gshb/deutsch/m/m03.htm
Hardware und Software:	http://www.bsi.de/gshb/deutsch/m/m04.htm
Kommunikation:	http://www.bsi.de/gshb/deutsch/m/m05.htm
Notfallvorsorge:	http://www.bsi.de/gshb/deutsch/m/m06.htm



Kontaktmöglichkeiten und Informationsmaterialien 2/2

Weitere Angebote

Rollendefinition	http://www.bsi.de/gshb/deutsch/baust/03.htm
Anwendungsweisen	http://www.bsi.de/gshb/deutsch/baust/01004.htm
Modellierung	http://www.bsi.de/gshb/deutsch/baust/02001.htm
Datenschutz	http://www.bsi.de/gshb/baustein-datenschutz/index.htm
Das Grundschutz-Tool (kostenpflichtige Software)	http://www.bsi.de/gstool/index.htm
Zertifizierung	http://www.bsi.de/gshb/zert/index.htm
Schulung	http://www.bsi.de/gshb/webkurs/index.htm



Zertifizierungen, die auf der Webseite des BSI veröffentlicht wurden

ISO 27001-Zertifikate auf der Basis von IT-Grundschutz

- Rechenzentrum der Finanzverwaltung des Landes Nordrhein-Westfalen, Düsseldorf
- IBM Deutschland Mittelstand Services GmbH, Meerbusch
- Städtisches Klinikum Braunschweig gGmbH, Braunschweig
- Städtisches Landesamt für Steuern, München
- Städtisches Amt für Wirtschaftsinformatik, Berlin
- Ministerium für Wissenschaft und Kunst, Dresden
- Landesamt für Wirtschaftsinformatik NRW, Münster
- Landesamt für Wirtschaftsinformatik und Ernährung, Bonn
- Landesamt für Wirtschaftsinformatik, Bonn
- TLG IMMO
- Energiedienst Netz
- Landesbetrieb Daten und Informationsverarbeitung, Berlin
- Informations-Verarbeitende Unternehmen, Berlin
- TRUMPF Laser GmbH + Co. KG, Sprockhövel
- office direkt Service-Center GmbH, Remscheid
- Frama AG, Lauperswil, Schweiz
- Interoute Datacentre Germany GmbH, Kleinmachnow
- BT (Germany) GmbH & Co oHG, München
- Babiel GmbH, Düsseldorf
- neu-itec GmbH, Neubrandenburg
- Kommunales Rechenzentrum Minden-Ravensberg/Lippe (KRZ), Lemgo
- Gesamtverband der Deutschen Versicherungswirtschaft (GDV) e. V., Berlin
- BT Berlin Transport GmbH, Berlin

24 Unternehmen und Einrichtungen
Summe:

Prüfschema:

http://www.bsi.bund.de/gshb/zert/ISO27001/Pruefschema_V.2.1.pdf

Quelle: http://www.bsi.bund.de/gshb/zert/veroeffentl/iso27001_zertifikate.htm



Unternehmen, die sich aktuell im Zertifizierungsprozess befinden

- ekom21 – KGRZ Hessen
- Kommunales Rechenzentrum Minden-Ravensberg/Lippe
- make IT GmbH
- netzhaus AG
- Ministerium für Wirtschaft, Umwelt und ländliche Räume
- BITMARCK SERVICE
- messerknecht information
- SAG Consulting Services GmbH
- Bochum-Gelsenkirchener Straßenservicegesellschaft
- Evangelischer Oberkirchenrat Stuttgart

10 Unternehmen und Einrichtungen
Summe:

Prüfschema:

http://www.bsi.bund.de/gshb/zert/ISO27001/Pruefschema_V.2.1.pdf

Quelle: http://www.bsi.bund.de/gshb/zert/veroeffentl/iso27001_zertifikate_lfd.htm

Auditor des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Es werden mehr als 200 Personen auf der Webseite des BSI genannt, die eine entsprechende Ausbildung als **Auditor** vorweisen können.

Wenn's wirklich sicher

Anerkante ISO 27001-Auditorinnen für Audits auf der Basis von IT-Grundschutz

Zur Zeit sind mehr als 120 Auditorinnen beziehungsweise Auditorinnen für ISO 27001 Audits auf der Basis von IT-Grundschutz beim BSI anerkannt, deren Listen seit dem Jahr 2007 über 50 Auditors beziehungsweise Auditorinnen erfolgreich eine Anerkennung (Lizenz / Zertifikat) erwarben.

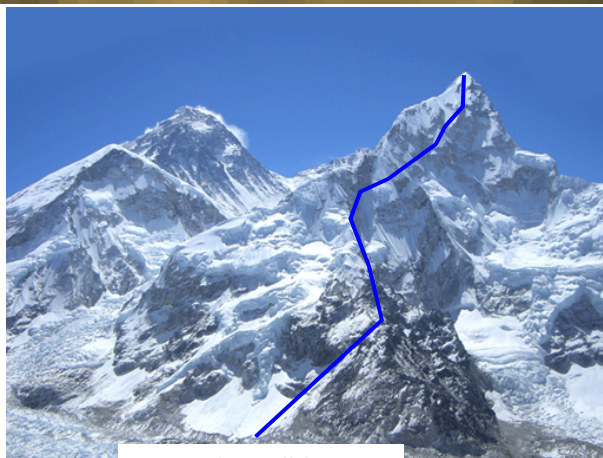
Nachfolgende Personen haben vom BSI eine Anerkennung (Lizenz / Zertifikat) als Auditor beziehungsweise Auditorinnen für ISO 27001 Audits auf der Basis von IT-Grundschutz erhalten. Die Personen mit einer **Lizenz als IT-Grundschutz-Auditor** sind separat aufgeführt. Hinweis: Die Tabelle ist nach Füllzeitszyklen sortiert.

Lizenz / Zertifikat-Nummer	Name	Privatanschrift	Dienstliche Adresse	gültig ab	gültig bis
0191-2008	Bucher, Michael	...		01.11.2008	31.10.2013
0192-2008	Teschner, Bernd	...		02.11.2008	31.10.2013
0200-2008	Johannsen, Dirk	...		15.11.2008	14.11.2013
0197-2008	Jersch, Jörg	...	04103 Lenging WVW-ServiceCenter - Beratung für Managementprozesse (ehemalig Jörg Jersch) www.mvz-consult.de (P)	15.07.2008	14.07.2013
0194-2008	Hemig, Thomas	...	04105 Lenging Sawene Enterprise Communications GmbH & Co. KG www.sawene.de/index.php (P)	30.06.2008	29.06.2013
0047-2006	Herbst, Bernd	...	04347 Lenging T&M&F GmbH www.tmf.com (P)	01.04.2006	31.03.2011
0093-2006	Brandt, Knud	...	10117 Berlin PERSSON AG www.persson.com (P)	15.08.2006	14.08.2011
0180-2008	Hauße, Knut	99425 Weimar	10117 Berlin PERSSON AG www.persson.com (P)	29.05.2008	29.05.2013
0003-2006	Gardonschek, Alexander	...	10117 Berlin Ernst & Young AG www.ey.com (P)	01.01.2006	31.12.2010
0164-2007	Köderman, Alexander	...	10178 Berlin SerNet - Service Network GmbH www.ser-net.de (P)	01.11.2007	31.10.2012
0160-2007	Mazdowski, Roman	...	10179 Berlin SerNet - Service Network GmbH www.ser-net.de (P)	15.08.2007	14.08.2012

35

Quelle: <http://www.bsi.bund.de/gshb/zert/veroeffentl/auditor27001.htm>

Das hohe Ziel: Zertifizierung im Bereich Sicherheit



Wenn's wirklich sicher

Vergleich ISO 9001 :schaftsverkehr

36

Quelle: <http://www.nepalhiking.com/images/mount-everest.gif>, http://www.juro1.de/images/de_mail_buergerportale_logo.jpg



Bedeutung der ISO für unsere Zukunft

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**.“

Quelle: http://de.wikipedia.org/wiki/ISO_9001



Entwicklung der ISO 9001 Zertifizierungen im Laufe der Zeit

Anzahl der ISO 9001-Zertifizierungen (weltweit)		davon	
Jahr	Anzahl	in Deutschland	Anzahl
2007	951.486	in Deutschland	45.195
		in Europa	386.284
		im Rest der Welt	520.007
2005	773.867	Vergleich mit ausgewählten Ländern	
2000	408.631	China	210.773
1995	127.349	Italien	115.359
		USA	36.192
		England	35.517
		Frankreich	22.981

Quelle: ISO; Stand: 31.12.2008



Die Forderungen Ihrer Kunden wachsen!

Österreich: IT-Sicherheit für Patientendaten

(...) „Einen Ausweg aus der Haftung bietet eine **Zertifizierung** nach dem Standard für **Informationssicherheit ISO 27001**. Das Zertifikat attestiert einer Organisation, alle der Sorgfaltspflicht entsprechenden Sicherheitsmaßnahmen nach anerkannten Methoden eingeführt zu haben.“ (...) Zitat von: CIS-Chef, Herrn Scheiber

Quelle: <http://www.e-health-com.de>

ITK-Sicherheitsmanagement strategisch angehen

„Die Bedrohung der Informations- und Kommunikationstechnologie (ITK) nimmt unvermindert zu. Die **ISO 27001-Zertifizierung** auf der **Basis von IT-Grundschutz** dient als Nachweis für ein erfolgreiches Sicherheitsmanagement im Unternehmen und schafft Wettbewerbsvorteile.“

Quelle: <http://www.funkschau.de>



Es existieren noch zahlreiche weitere Routen auf den höchsten Berg der Welt ...

Eigenkapitalvorschriften des Basler Ausschusses für Bankenaufsicht (BASEL II)

Datenschutz (BDSG)

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

PS 330 Institut für Wirtschaftsprüfer

Sarbanes Oxley Act

etc.

EuroSOX

Wenn's wirklich sicher sein soll – Netzwerk Elektronischer Geschäftsverkehr

40

Quelle: <http://www.nepalhiking.com/images/mount-everest.gif>, http://www.jurowl.de/images/de_mail_buergeportale_logo.jpg

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages



Netzwerk Elektronischer Geschäftsverkehr

Was müssen Sie nun in Ihrem Unternehmen umsetzen?

- Erfassung aller Schutzgegenstände,
- Durchführung einer Risikoanalyse,
- Erkennen von Schwächen und Implementierung geeigneter Gegenmaßnahmen,
- Etablierung des Datenschutzes/Rechtskonformität,
- Dokumentation aller Maßnahmen,
- Sensibilisierung aller Mitarbeiter u. v. m.



Netzwerk Elektronischer Geschäftsverkehr



Sicherheit mit Garantie für den Mittelstand?!

Titel des Artikels:

„Geprüfte Sicherheit“

„Vor allem KMU hinken bei der Sicherung Ihrer Informationen und Daten oft hinterher: Meist ist zwar die geeignete Technologie für den Schutz der IT-Infrastruktur vorhanden, aber es mangelt an einem übergreifenden **Management-Ansatz für Informationsrisiko, Datenschutz und Unternehmens-Compliance.**“



Wenn's wirklich sicher sein soll – Netz

Quelle: Business&IT, 4/2008, S. 76



Informationssicherheit – organisatorische Maßnahmen Teil 1/2

1 Ernennung eines Verantwortlichen

Es muss ein (IT-) Sicherheitsbeauftragter (engl. CISO) ernannt werden

2 Schriftliche Fixierung der Verantwortlichkeiten

Sowohl die Aufgaben und Pflichten als auch die Kompetenzen sind schriftliche festzuhalten

3 Sicherheitsleitlinie Sicherheitsrichtlinie

Erstellung eines „Verhaltenskodex“, der für alle Mitarbeiter bindend sein muss

4 Erstellung umfassender Dokumentationen

Betriebliche Vorgehensweisen, Sicherheitsverstöße, besondere Vorkommnisse etc.

© A. Gabriel



Informationssicherheit – organisatorische Maßnahmen Teil 2/2

5 Sicherstellung der Rechtskonformität

Alle neuen Verordnungen, Gesetze etc. sind zeitnah zu prüfen (engl. Compliance)

6 Erfüllung aller Vorgaben des Datenschutzes

Ernennung des Datenschutzbeauftragten, Erstellung eines Verzeichnisses etc.

7 Umgang mit den eigenen Risiken

Welche Bedrohungen und Schwachstellen wirken auf das Unternehmen?

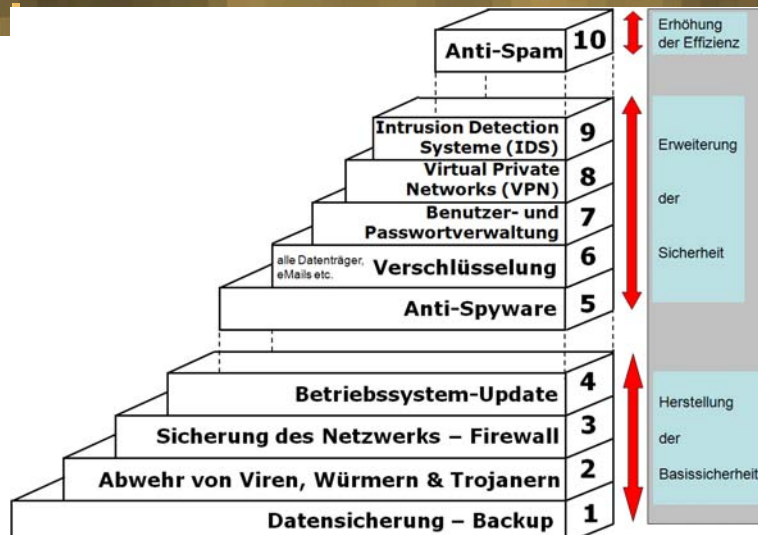
8 Regelmäßige Schulung aller Mitarbeiter

Alle Angestellten müssen sensibilisiert werden – auch die Geschäftsführung

© A. Gabriel



Informationssicherheit – technische Maßnahmen



© A. Gabriel



Definition des Begriffs „Risiko“

„Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab.“

Risiko wird auch häufig definiert als die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens.“

Quelle: BSI, IT-Grundschutzkatalog 2005, Glossar



Eingrenzung verschiedener Risikoarten

Technologische Risiken

- IT-Risiken
- Infrastrukturelle Risiken
- Datenrisiken
- Modellrisiken
- etc.

Personalbezogene Risiken

- Kriminelle Handlungen
- Unfallrisiken
- Fluktuationsrisiken
- etc.

Organisatorische Risiken

- Aufbauorganisation
- Ablauforganisation
- Management
- etc.

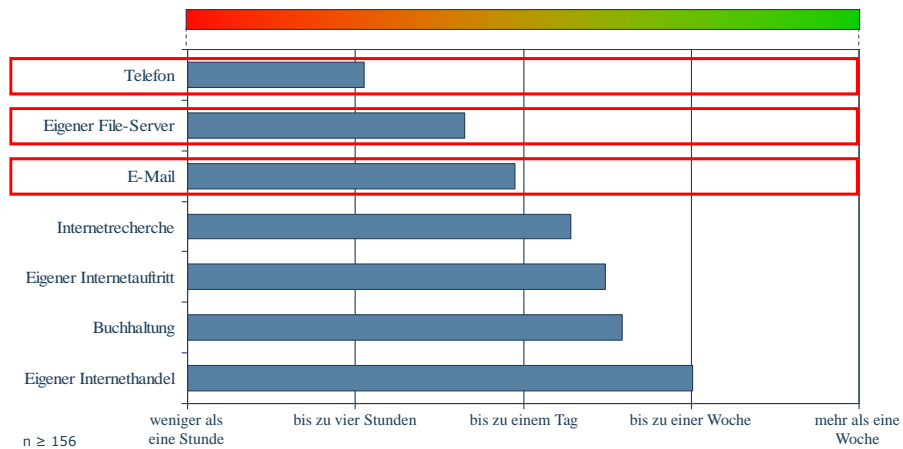
Externe Risiken

- Naturereignisse
- Politische Risiken
- Drittparteirisiken
- etc.

Quelle: in Anlehnung an Romeike, E.: Erfolgsfaktor Risikomanagement



Länge der Aufrechterhaltung des Betriebes ohne folgende Dienste

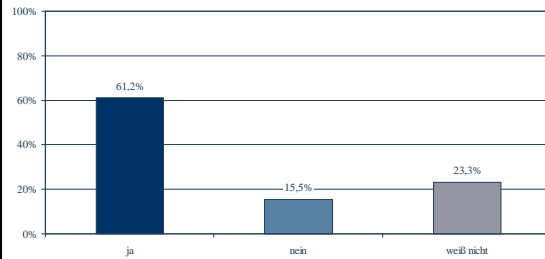


Die ganze Studie finden Sie unter:
<http://www.ec-net.de/sicherheit>

In Kooperation mit dem E-Commerce-Center Handel, Köln



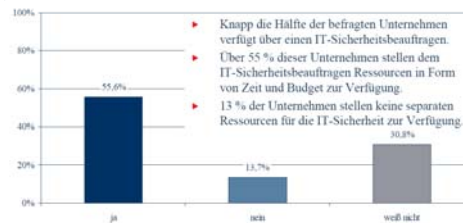
Bereitstellung zeitlicher und finanzieller Ressourcen für den „IT-Sicherheitsbeauftragten“



Ergebnis der Umfrage aus dem Jahr 2007

Ja	- 5,6 %
Nein	- 1,8 %
Weiß nicht	+ 7,5 %

Ergebnis der Umfrage aus dem Jahr 2008

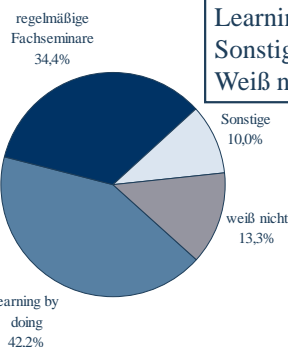


- Knapp die Hälfte der befragten Unternehmen verfügt über einen IT-Sicherheitsbeauftragten.
- Über 55 % dieser Unternehmen stellen dem IT-Sicherheitsbeauftragten Ressourcen in Form von Zeit und Budget zur Verfügung.
- 13 % der Unternehmen stellen keine separaten Ressourcen für die IT-Sicherheit zur Verfügung.

Quelle: ECC Handel: Elektronischer Geschäftsverkehr in Mittelstand und Handwerk, 2007 und 2008.



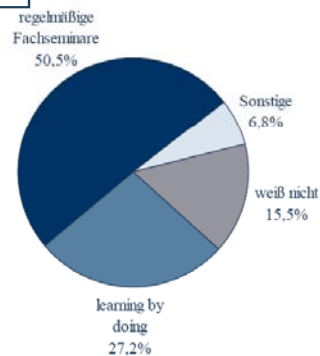
Weiterbildung des „IT-Sicherheitsbeauftragten“



Ergebnis der Umfrage aus dem Jahr 2007

Fachseminare	+ 16,1 %
Learning by doing	- 15 %
Sonstige	- 3,2 %
Weiß nicht	+ 2,2 %

Ergebnis der Umfrage aus dem Jahr 2008



Quelle: ECC Handel: Elektronischer Geschäftsverkehr in Mittelstand und Handwerk, 2007 und 2008.



Netzwerk Elektronischer Geschäftsverkehr



Vielen Dank für Ihre Aufmerksamkeit

Informationssicherheit heute und in Zukunft

Würzburg, 14.07.2009

Andreas Gabriel

Mainfränkisches Electronic Commerce Kompetenzzentrum
c/o Universität Würzburg

Neubastraße 66
97070 Würzburg

Tel.: 0931 / 3501-231
Fax: 0931 / 31-2599

gabriel@meck-online.de
www.meck-online.de
www.ec-net.de/sicherheit
www.wiinf.uni-wuerzburg.de

51