Wir machen Unternehmen sicherer und IT effizienter!

TRIGONUM
consulting

TRIGONUM consulting

„Informationssicherheit mit System – Der Nutzen eines Informationssicherheits-Managementsystems nach ISO 27001“

Hamburg, 30.3.2011

Stephan Ernst, Trigonum GmbH

Agenda

01	Was bedeutet Informationssicherheit?
02	Welche Standards gibt es?
03	Informations-Sicherheits-Management-System
04	Wie können die TOM gem. BDSG umgesetzt werden?

Agenda

01 **Was bedeutet Informationssicherheit?**

02 Welche Standards gibt es?

03 Informations-Sicherheits-Management-System

04 Wie können die TOM gem. BDSG umgesetzt werden?

Status der Informationstechnologie im Unternehmen

- 97% aller deutschen Unternehmen mit mehr als 20 Mitarbeitern setzen Informationstechnologie ein*.
- Die Informationstechnologie unterstützt fast alle Unternehmensprozesse.
- Fast alle kritischen Unternehmensdaten werden elektronisch verarbeitet.
- Ein Ausfall wichtiger Systeme kann meistens maximal für 1 Tag toleriert werden.

Aber…

- Nur ca. ¼ der Unternehmen verfügt Notfallpläne**.
- Weniger als 50% der Unternehmen haben schriftlich fixierte Sicherheitsrichtlinien**.
- Mehr als 60% der Unternehmen erlauben die uneingeschränkte Nutzung der Hardware durch alle Mitarbeiter**.

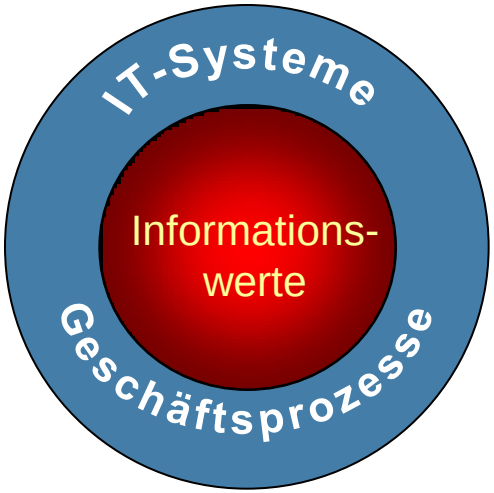
*Quelle: Statistisches Bundesamt, Wiesbaden 2008
** Quelle: Informationssicherheit im Unternehmen 2008, ECC-Handel

Informationswerte sind gefährdet

Katastrophen:
- Blitzeinschlag
- Brand
- Wassereinbruch

Fremdpersonal:
- Gebäudezutritt
- Systemzugang

Techn. Mängel:
- Serverausfall
- Datenverlust



Angriffe durch (Ex-)Mitarbeiter :
- Datenmanipulation
- Datendiebstahl
- Spionage

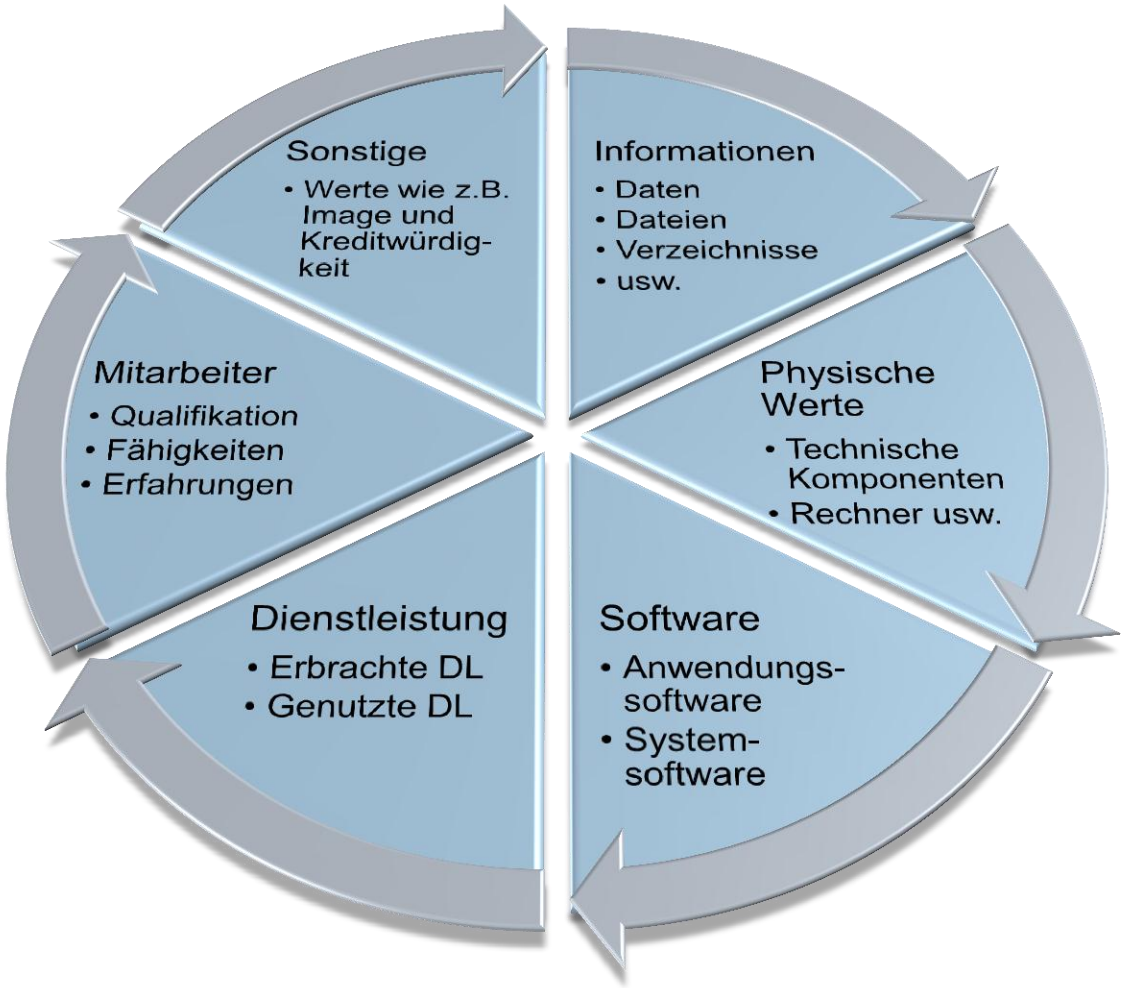
Industriespionage:
- Konstruktionsdaten
- Finanzdaten
- Forschungsergebnisse

Organ. Mängel:
- Berechtigungen
- Verschlüsselung
- Verantwortlichkeiten

Hacker:
- IT-Betrieb
- Datensicherheit

Ungeschulte Mitarbeiter:
- Internetnutzung
- Umgang mit Informationen
- Unachtsamkeit

Informationswerte im Unternehmen



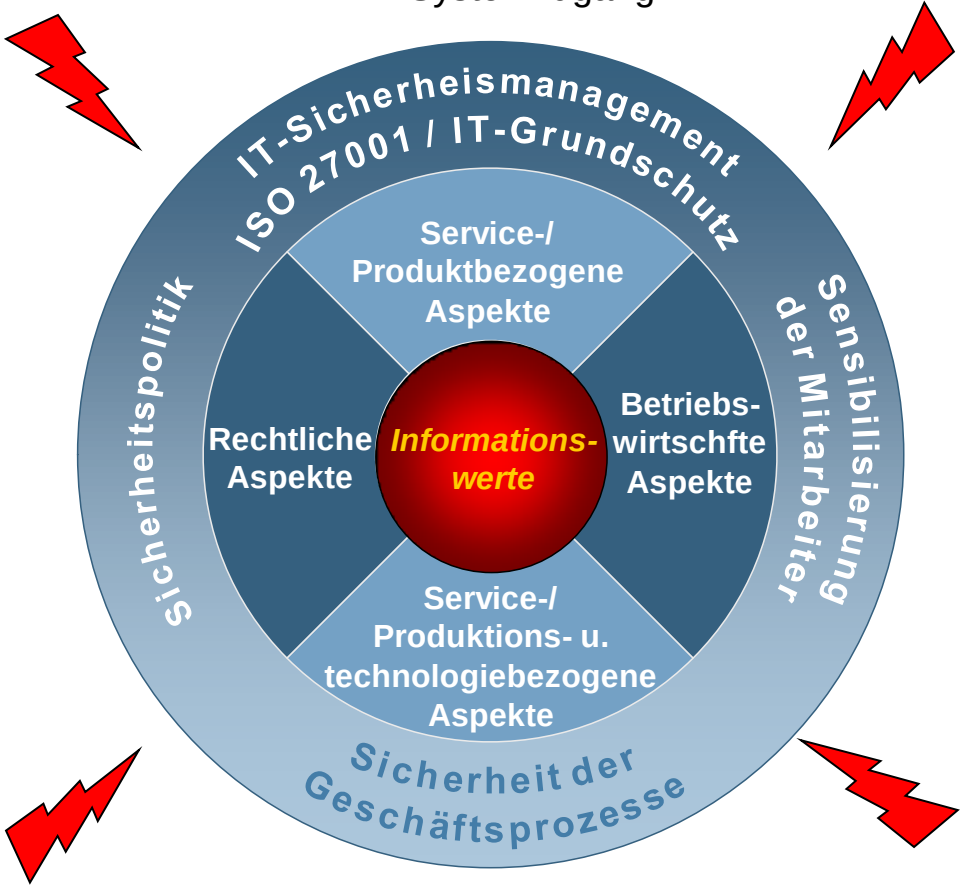
Informationswerte sind Gefahren ausgesetzt und müssen geschützt werden!

Informationswerte müssen geschützt werden

Katastrophen:
- Blitzeinschlag
- Brand
- Wassereinbruch

Fremdpersonal:
- Gebäudezutritt
- Systemzugang

Techn. Mängel:
- Serverausfall
- Datenverlust



Angriffe durch (Ex-)Mitarbeiter :
- Datenmanipulation
- Datendiebstahl
- Spionage

Industriespionage:
- Konstruktionsdaten
- Finanzdaten
- Forschungsergebnisse

Organ. Mängel:
- Berechtigungen
- Verschlüsselung
- Verantwortlichkeiten

Hacker:
- IT-Betrieb
- Datensicherheit

Ungeschulte Mitarbeiter:
- Internetnutzung
- Umgang mit Informationen
- Unachtsamkeit

Folgen fehlender Informations- und IT-Sicherheit

Risiken

Finanzielle Risiken:
1. Umsatz
2. Liquidität
3. Kredit-Rating
4. Kapitalumschlag
5. Börsenkurs

Strategische Risiken:
1. Marktanteile
2. Kunden
3. Business Partner
4. Lieferanten
5. Rechtliche Entwicklungen

Operative Risiken:
1. Produktionsrisiken
2. Qualität
3. Unbeschäftigte Mitarbeiter
4. IT-Verfügbarkeit

Externe Risiken:
1. Infrastruktur (z.B. Strom u. Datenleitungen)
2. Technische Veränderungen
3. Spionage u. Sabotage
4. Feuer, Wasser etc.

Folgen

Image, Umsatz-Verlust, mangelndes Vertrauen der Kunden und des Marktes

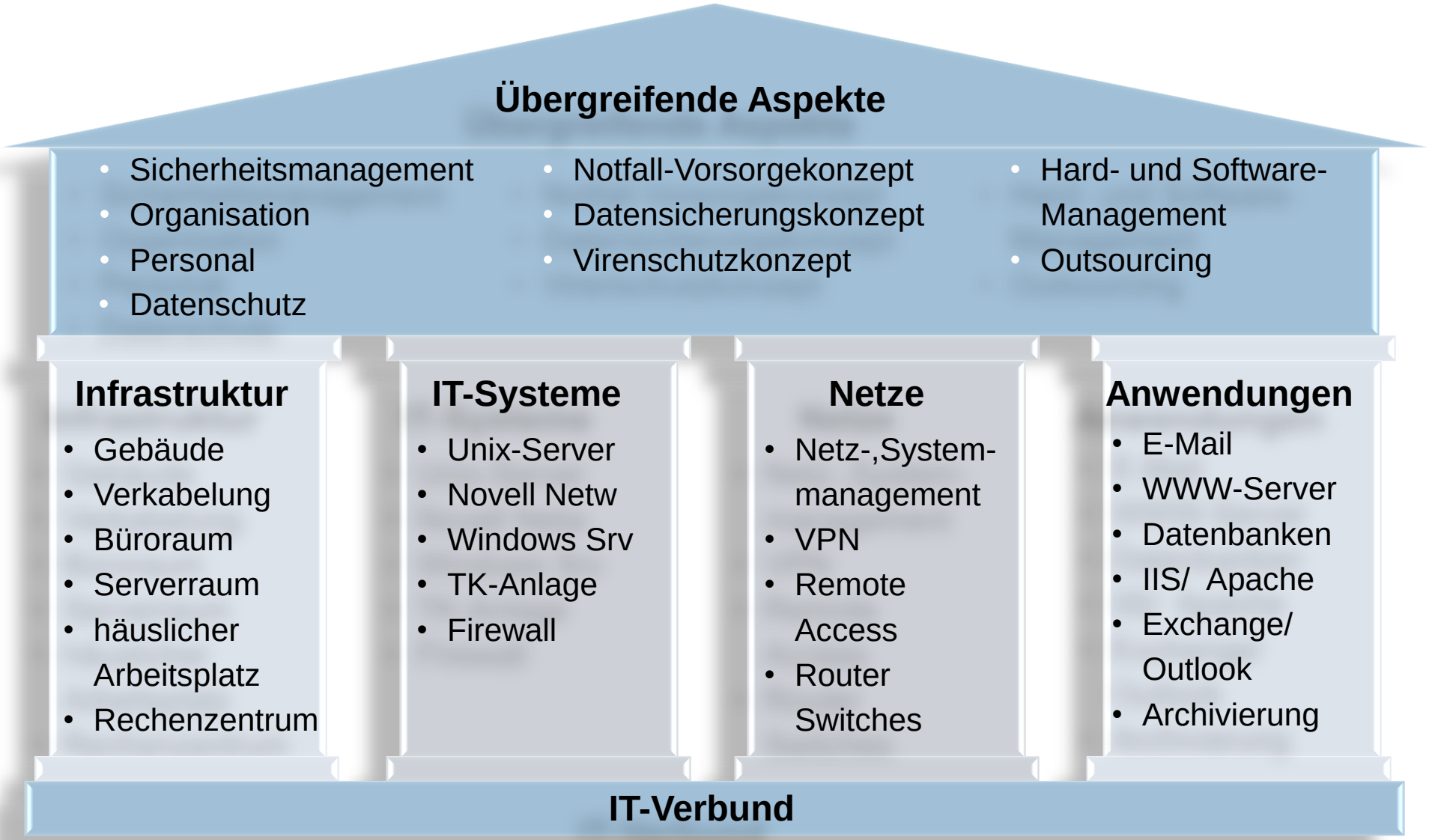
Gesetzesverstöße, z.B. BDSG
Verlust von Marktanteilen

Grundfunktion und Prozesse im Unternehmen sind gefährdet

Fundamentale Infrastruktur des Unternehmens ist gefährdet

Schichten und Bausteine der Informationssicherheit

(IT-Grundschutz auf Basis ISO27001)



Agenda

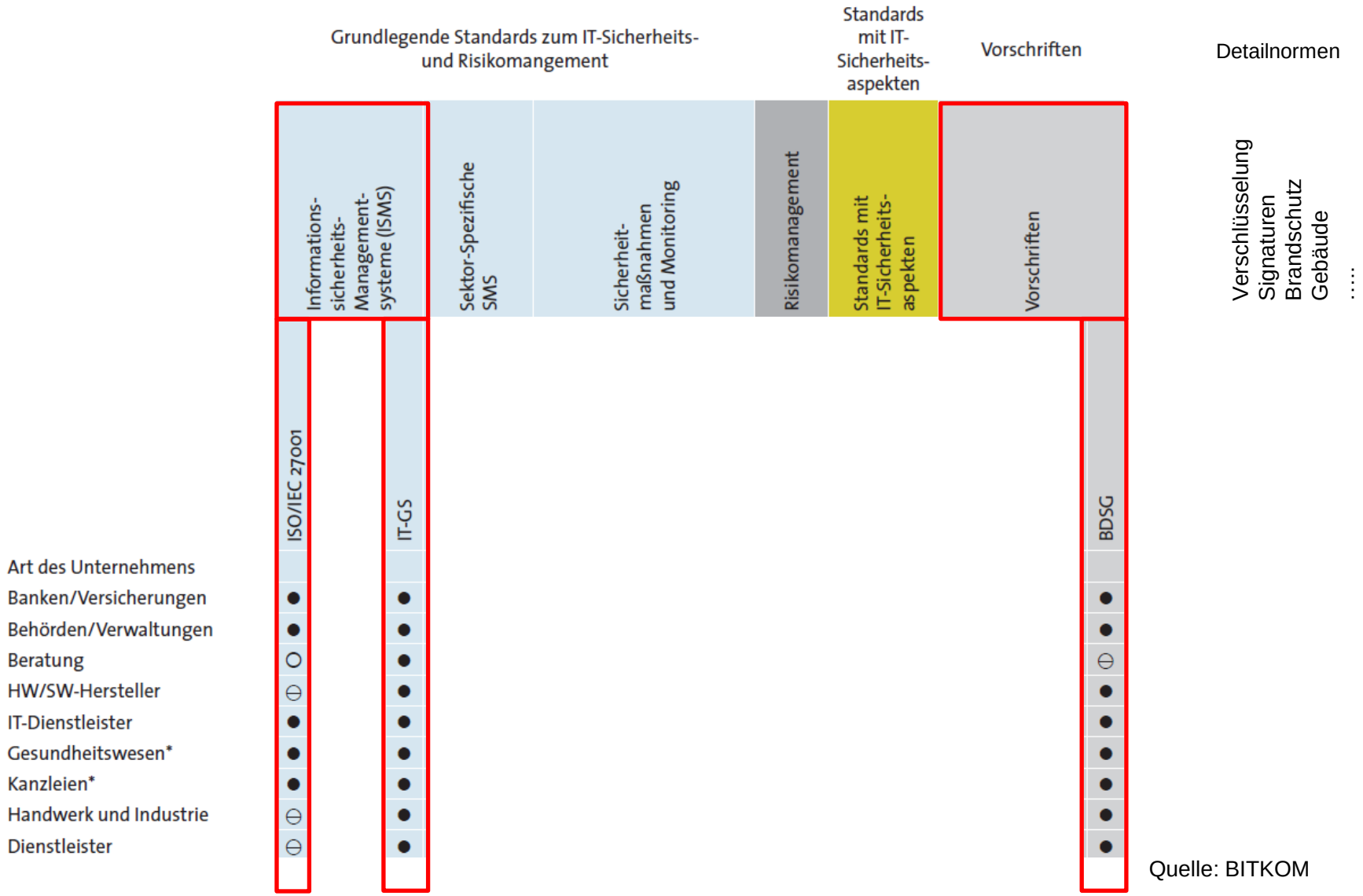
01 Was bedeutet Informationssicherheit?

02 **Welche Standards gibt es?**

03 Informations-Sicherheits-Management-System

04 Wie können die TOM gem. BDSG umgesetzt werden?

Standards im Bereich Informations- und IT-Sicherheit



Quelle: BITKOM

Alternativen zur Erlangung einer ISO 27001 Zertifizierung

Für den Aufbau und die Umsetzung eines zertifizierungsfähigen Informationssicherheitsmanagementsystems, gibt es die folgenden unterschiedlichen Ansätze:

ISO 27001:2005 (ergänzt um ISO 27002)

→ Die Auswahl und Umsetzung der Maßnahmen erfolgt anhand der vorher durchgeführten detaillierten Risikoanalyse. Diese basiert wiederum auf den ermittelten Informationswerten des Anwendungsbereichs.

→ 135 Kontrollziele

→ **Wenig Hilfe zur konkreten Umsetzung**

IT Grundschutz (ISO 27001 auf Basis IT Grundschutz)

→ Der IT Grundschutz verzichtet auf eine Risikoanalyse. Hier werden die erforderlichen Maßnahmen über die Modellierung des IT – Verbunds bestimmt.

→ Mehr als 70 Bausteine mit mehr als 1.100 Maßnahmen

→ **Detaillierte Vorgaben zur Umsetzung aber dadurch konkretere Hilfe zur Umsetzung**

Agenda

01 Was bedeutet Informationssicherheit?

02 Welche Standards gibt es?

03 **Informations-Sicherheits-Management-System**

04 Wie können die TOM gem. BDSG umgesetzt werden?

Ziele eines IT-Sicherheitsmanagements

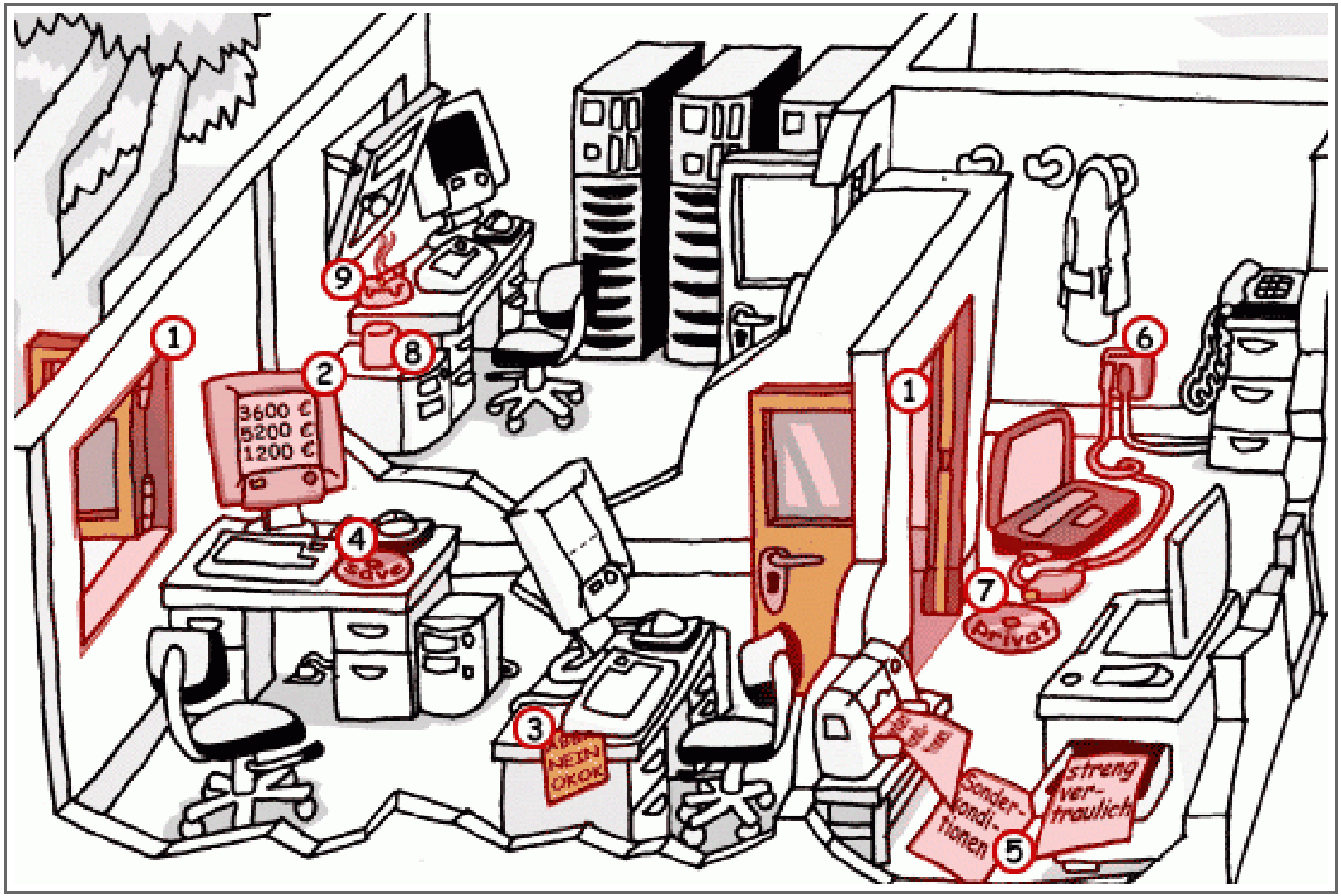
- **Gesteigerte Sicherheit** als integraler Bestandteil der Geschäftsprozesse
- **Einhaltung von gesetzlichen Anforderungen**
- **Kenntnis** und **Kontrolle** über IT-Risiken / -Restrisiken erlangen
- **Dokumentation** von Strukturen und Prozessen
- Sicherheit des Geschäftsbetriebes sicherstellen durch: **Business Continuity Management**
- **Kostenreduktion** durch transparente und optimierte Strukturen (ggf. auch Versicherungen)
- Gesteigertes **Sicherheitsbewusstsein** der Mitarbeiter
- **Beurteilung** der Organisation und Prozesse nach Sicherheitsgesichtspunkten
- **Weltweit anerkannter Standard** erlangen (Nachweis der Sicherheit gegenüber Kunden und Partnern)
- **Wettbewerbsvorteil**: "Dokumentierte Qualität" durch eine unabhängige Instanz

Viele Wege führen zur IT-Sicherheit...

Welcher Weg ist der effektivste?

BSI IT-Grundschutz
Die Idee … IT ist in vielen Unternehmen ähnlich.

BSI IT-Grundschutz
Die Idee … IT ist in vielen Unternehmen ähnlich.

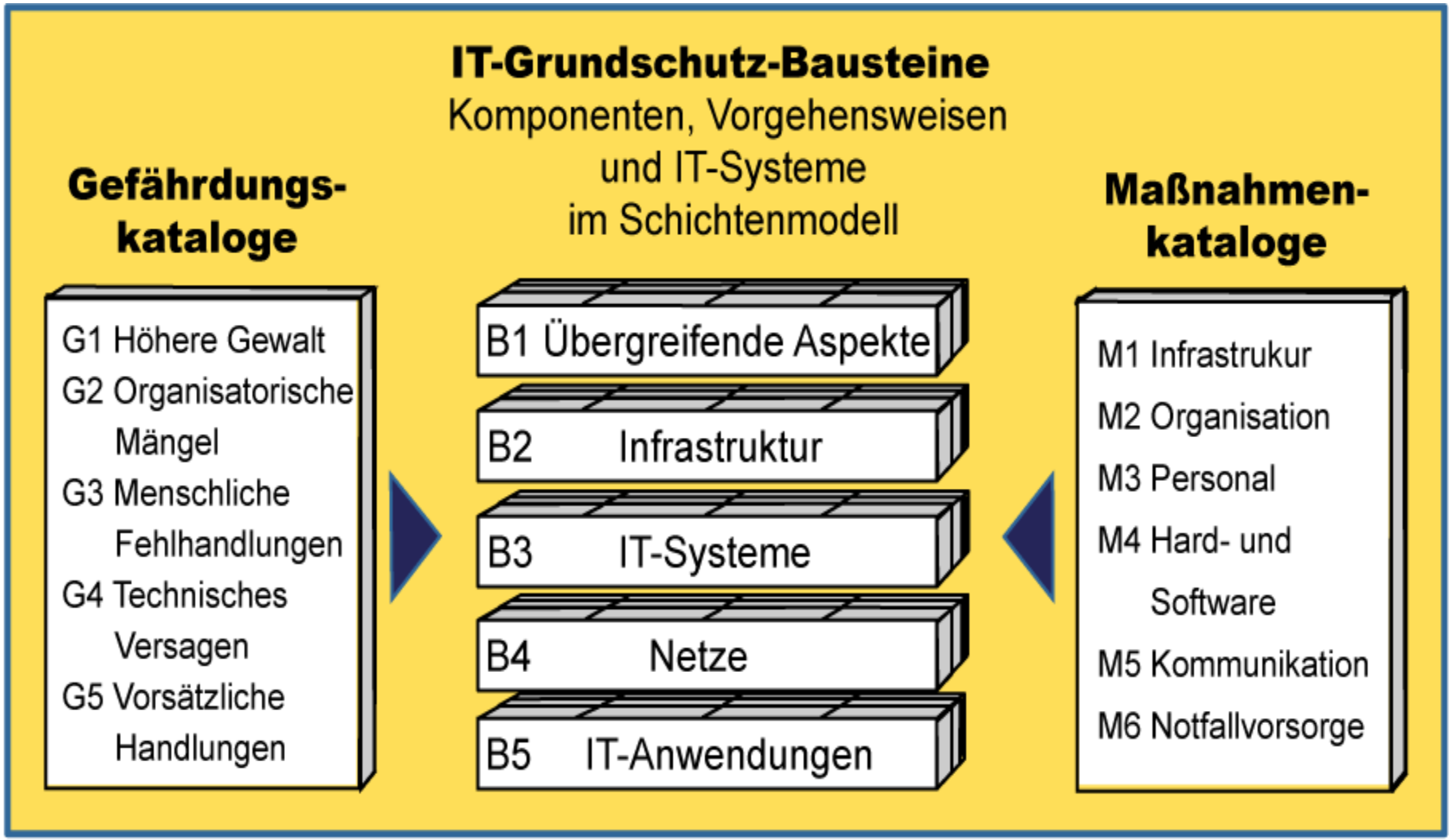


BSI IT-Grundschutz
Die Idee … IT ist in vielen Unternehmen ähnlich.

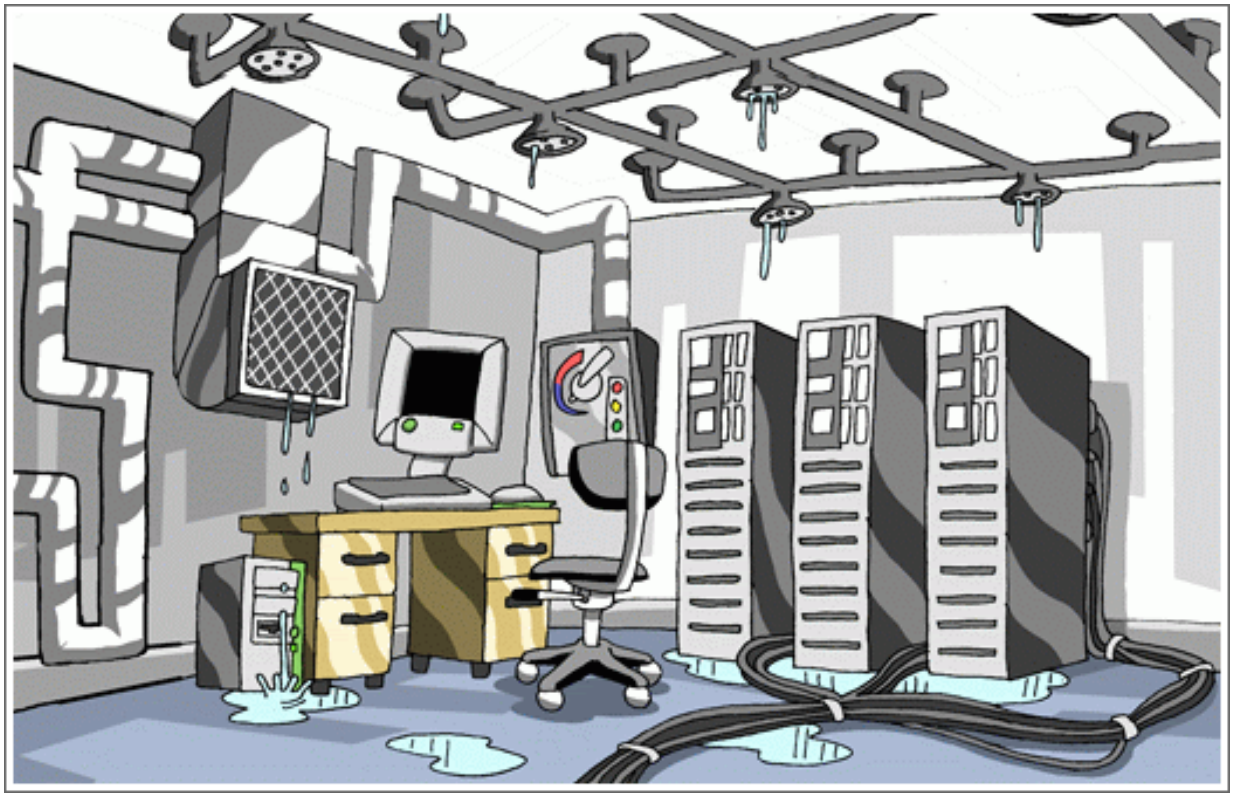
- **Typische** Abläufe und IT-Komponenten überall ähnlich
- Wichtig:
  - Wiederverwendbarkeit
  - Anpassbarkeit
  - Erweiterbarkeit

- Typische Gefährdungen, Schwachstellen und Risiken
- Typische Geschäftsprozesse und Anwendungen
- Typische IT-Komponenten
- Gerüst für das IT-Sicherheitsmanagement wird gebildet

Aufbau der IT-Grundschutz-Kataloge



Beispiel: BSI-Baustein Rechenzentrum



Beispiel BSI-Baustein: B2.9 Rechenzentrum

B 2.9 Rechenzentrum

Beschreibung

In den meisten Institutionen werden alle wesentlichen strategischen und operativen Funktionen und Aufgaben durch Informationstechnik (IT) maßgeblich unterstützt oder sind sogar ohne IT nicht auszuführen. Die IT-Systeme der Institution selbst und auch deren Anbindung an externe Netze müssen in einer angemessenen Umgebung und Infrastruktur betrieben werden. Nur so lässt sich die nötige Verfügbarkeit der IT sicherstellen. Die Anforderungen an die Leistungsfähigkeit dieser Systeme und der Netzumgebung steigen stetig an. Um diesem Leistungsbedarf gerecht zu werden, um entsprechende Reserven vorzuhalten und um die IT auch wirtschaftlich betreiben zu können, haben Behörden und Unternehmen jeglicher Größe ihre IT-Landschaft in Rechenzentren konzentriert.

Gefährdungslage

Für den IT-Grundschutz eines Rechenzentrums werden folgende ty

Höhere Gewalt

G 1.2	Ausfall von IT-Systemen
G 1.3	Blitz
G 1.4	Feuer
G 1.5	Wasser
G 1.6	Kabelbrand
G 1.7	Unzulässige Temperatur und Luftfeuchte
G 1.8	Staub, Verschmutzung
G 1.11	Technische Katastrophen im Umfeld

Maßnahmenempfehlungen

Planung und Konzeption

M 1.3	(A)	Angepasste Aufteilung der Stromkreise
M 1.7	(A)	Handfeuerlöscher
M 1.10	(C)	Verwendung von Sicherheitstüren und -fenstern
M 1.12	(A)	Vermeidung von Lagehinweisen auf schützenswerte Gebäudete
M 1.13	(Z)	Anordnung schützenswerter Gebäudeteile
M 1.18	(B)	Gefahrenmeldeanlage
M 1.24	(C)	Vermeidung von wasserführenden Leitungen
M 1.25	(B)	Überspannungsschutz
M 1.26	(W)	Not-Aus-Schalter

Beispiel BSI Maßnahme:
M 1.24 Vermeidung von wasserführenden Leitungen

M 1.24 Vermeidung von wasserführenden Leitungen

Verantwortlich für Initiierung: Leiter Haustechnik, Leiter IT

Verantwortlich für Umsetzung: Administrator, Haustechnik

In Räumen oder Bereichen, in denen sich IT-Geräte mit zentralen Funktionen wie z. B. Server befinden, sollten wasserführende Leitungen aller Art vermieden werden. Die einzigen wasserführenden Leitungen sollten, wenn unbedingt erforderlich, Kühlwasserleitungen, Löschwasserleitungen und Heizungsrohre sein. Zuleitungen zu Heizkörpern sollten mit Absperrventilen, möglichst außerhalb des Raumes oder Bereiches, versehen werden. Außerhalb der Heizperiode sind diese Ventile zu schließen.

Sind wasserführende Leitungen unvermeidbar, müssen Vorkehrungen getroffen werden, einen Wasseraustritt möglichst frühzeitig zu erkennen bzw. die negativen Auswirkungen zu minimieren. Als Minimalschutz kann eine Wasserauffangwanne oder -rinne unter der Leitung angebracht werden, deren Ablauf außerhalb des Raumes führt. Günstig ist es, dazu den Flur zu nutzen, da so ein eventueller Leitungsschaden schnell entdeckt werden kann. Zur frühzeitigen Erkennung von Wassereinbrüchen oder undichten Leitungen hat es sich bewährt, Decken hell zu streichen. Durch Sichtprüfungen müssen die vorhandenen Wasserleitungen regelmäßig auf ihre Dichtigkeit hin überprüft werden.

Es ist zu erwägen, wasserführende Leitung durch Wassermelder zu überwachen. Dafür können besondere Meldekabel unterhalb von Leitungen verlegt werden. Werden diese an eine Wassermeldeanlage angeschlossen, ist darüber eine schnelle und recht genaue Lokalisierung des Wasseraustritts möglich. Eine solche Anlage muss auf eine ständig besetzte Stelle aufgeschaltet werden, um in Verbindung mit entsprechenden Reaktionsplänen und einer aktuellen Dokumentation ein schnelles Eingreifen möglich zu machen. Optional können Wassermelder mit automatisch arbeitenden Magnetventilen eingebaut werden. Diese Magnetventile sind außerhalb des Raumes bzw. Bereiches einzubauen. Damit die Ventile auch bei Stromausfall ihre Schutzfunktion erfüllen, müssen sie im stromlosen Zustand geschlossen sein.

Als zusätzliche oder alternative Maßnahme empfiehlt sich eine selbsttätige Entwässerung (siehe M 1.14 *Selbsttätige Entwässerung*).

Alle Mitarbeiter im Bereich der IT und der Haustechnik sollten darüber informiert sein, dass in Gebäudeteilen mit IT-Systemen mit hohen Verfügbarkeitsanforderungen wasserführende Leitungen problematisch sind und was zu beachten ist. Es sollten Reaktionspläne vorhanden sein, in denen beschrieben ist, welche Maßnahmen bei Wasserleckagen zu ergreifen sind.

Prüffragen:

- Werden eventuell vorhandene Wasserleitungen regelmäßig auf ihre Dichtigkeit hin überprüft (Sichtprüfung)?
- Gibt es Reaktionspläne, die zielgerichtete Handlungen bei Meldung von Wasserleckagen vorgeben?

Übersicht BSI IT-Grundschutz

IT-Grundschutzhandbuch

ca. 75 Bausteine
ca.1.100 Maßnahmen
mehr als 2.000 Seiten

Übersicht über den IT-Sicherheitsprozess

1 **Initiative der Geschäftsführung**

- Analyse: Geschäftsprozesse, Unternehmensziele
- IT-Sicherheitsleitlinie
- IT-Sicherheitsorganisation

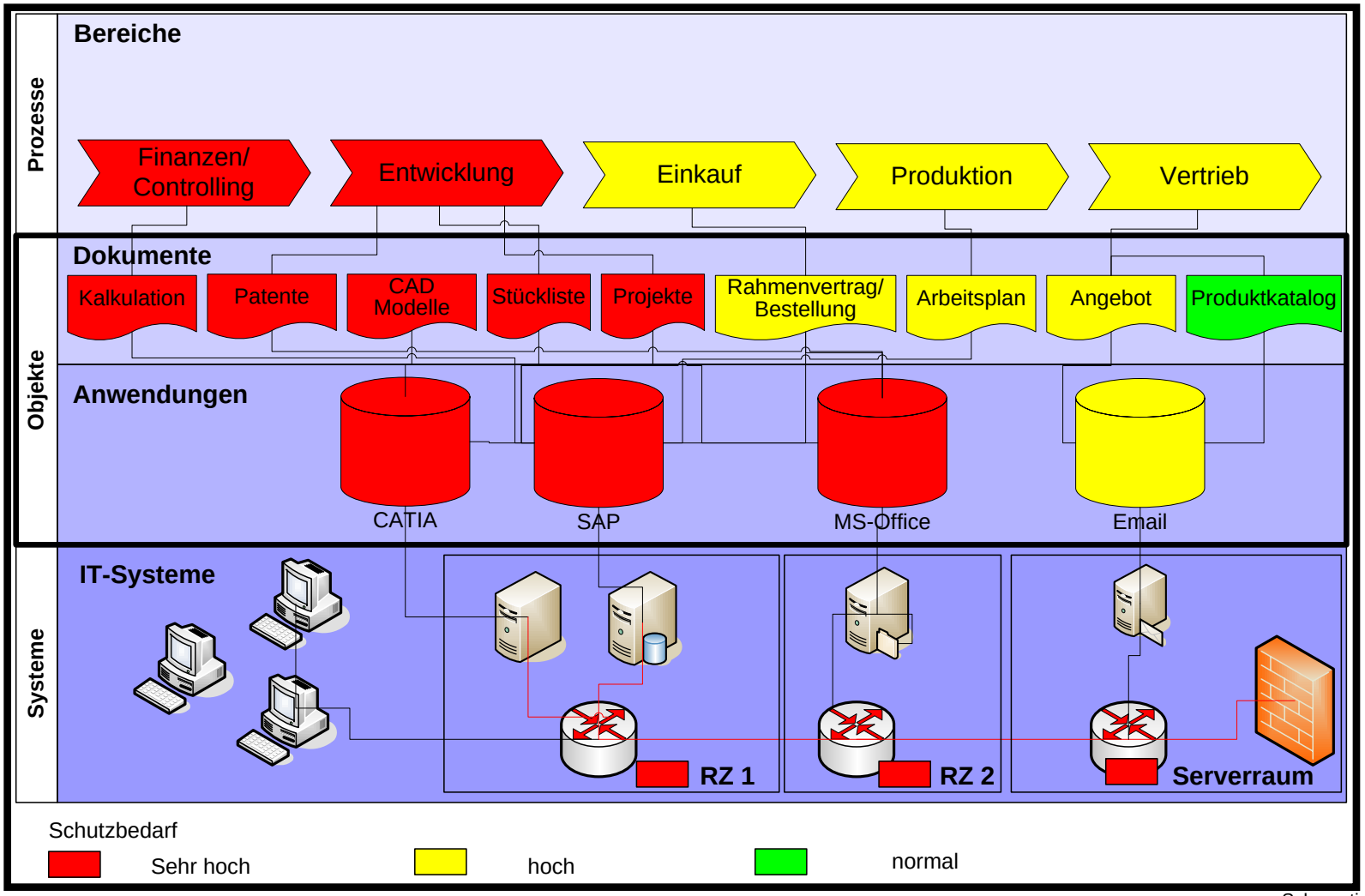
2 **Analyse der Rahmen-bedingungen**

- Informationen, IT-Systeme, Anwendungen
- Schutzbedarf (Szenarien)

3 **Sicherheitscheck**

- Sicherheitsmaßnahmen
- Identifikation von Sicherheits-lücken

Business- und Schutzbedarfsanalyse

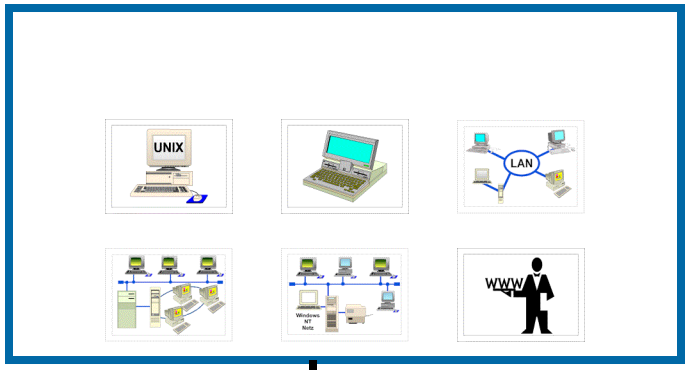


Schematische Darstellung

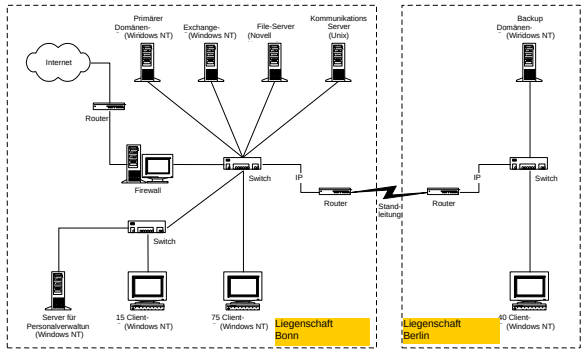
Sicherheitscheck – Statusbestimmung im Unternehmen

Anforderungen

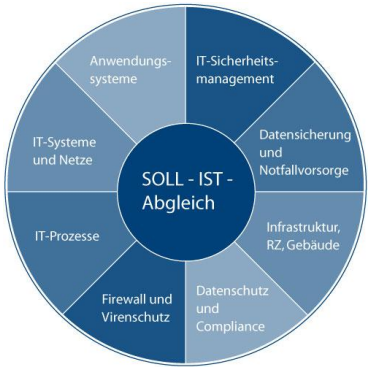
- **Gesetzliche Forderungen**
- **ISO Norm**



Umsetzung im Unternehmen



Maßnahmen-empfehlungen



Realisierte Maßnahmen

umzusetzende Maßnahmen

TRIGONUM consulting

Übersicht über den IT-Sicherheitsprozess

4 Planung von Maßnahmen

- Liste geeigneter Maßnahmen
- Kosten- und Nutzenanalyse
- Auswahl umzusetzender Maßnahmen
- Dokumentation des Restrisikos

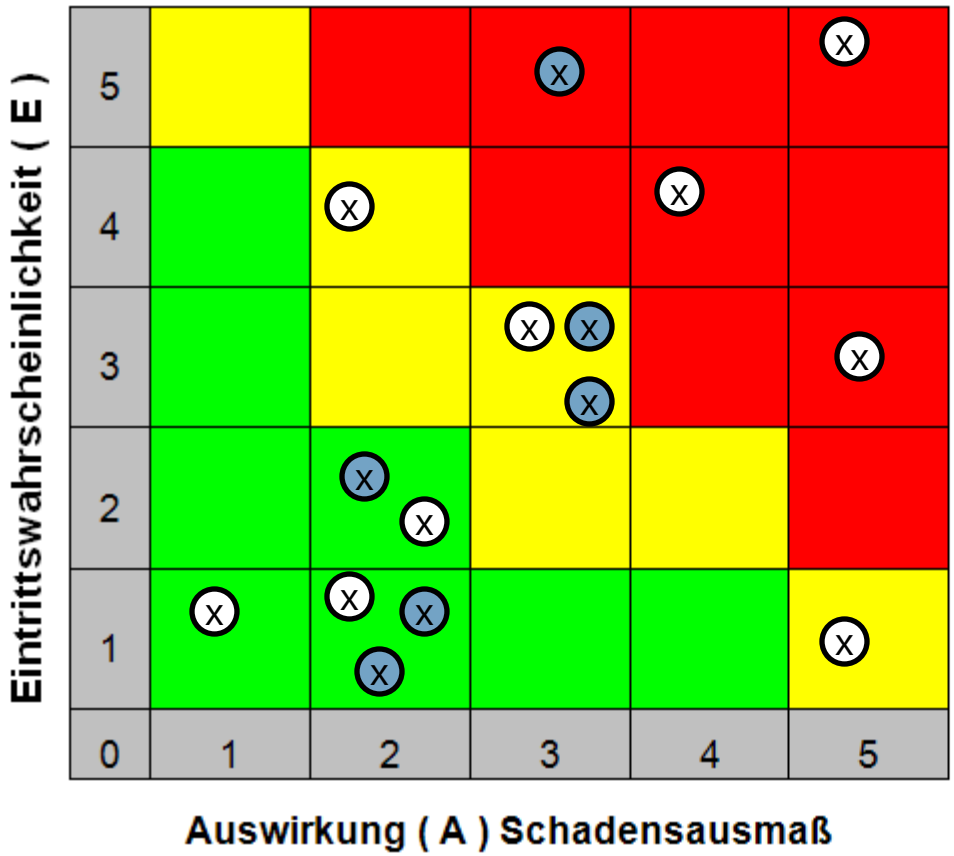
5 Umsetzung von Maßnahmen

- Implementierung
- Test
- Notfallvorsorge

6 Sicherheit im laufenden Betrieb

- Sensibilisierung
- Schulung
- Audit, Kontrollen, Monitoring, Revision
- Notfallvorsorge

Risikoanalyse und Maßnahmenplanung



Risikobewertung	
Wertebereich (A*E)	**Risiko**
1 – 4	gering/ mittel
5 – 9	hoch
10 – 25	sehr hoch

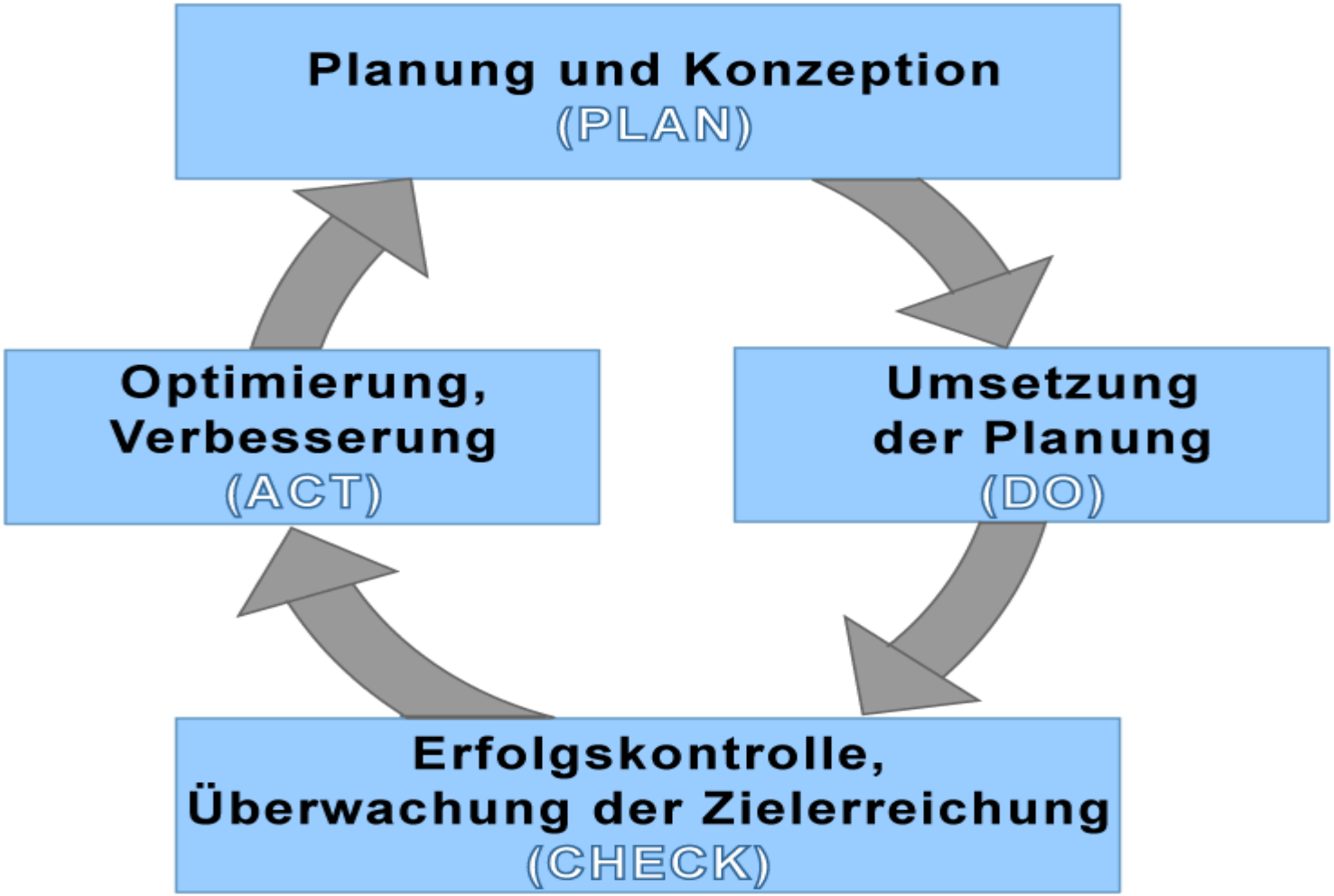
Legende:

grün = Bereich mit akzeptablen Risiken.

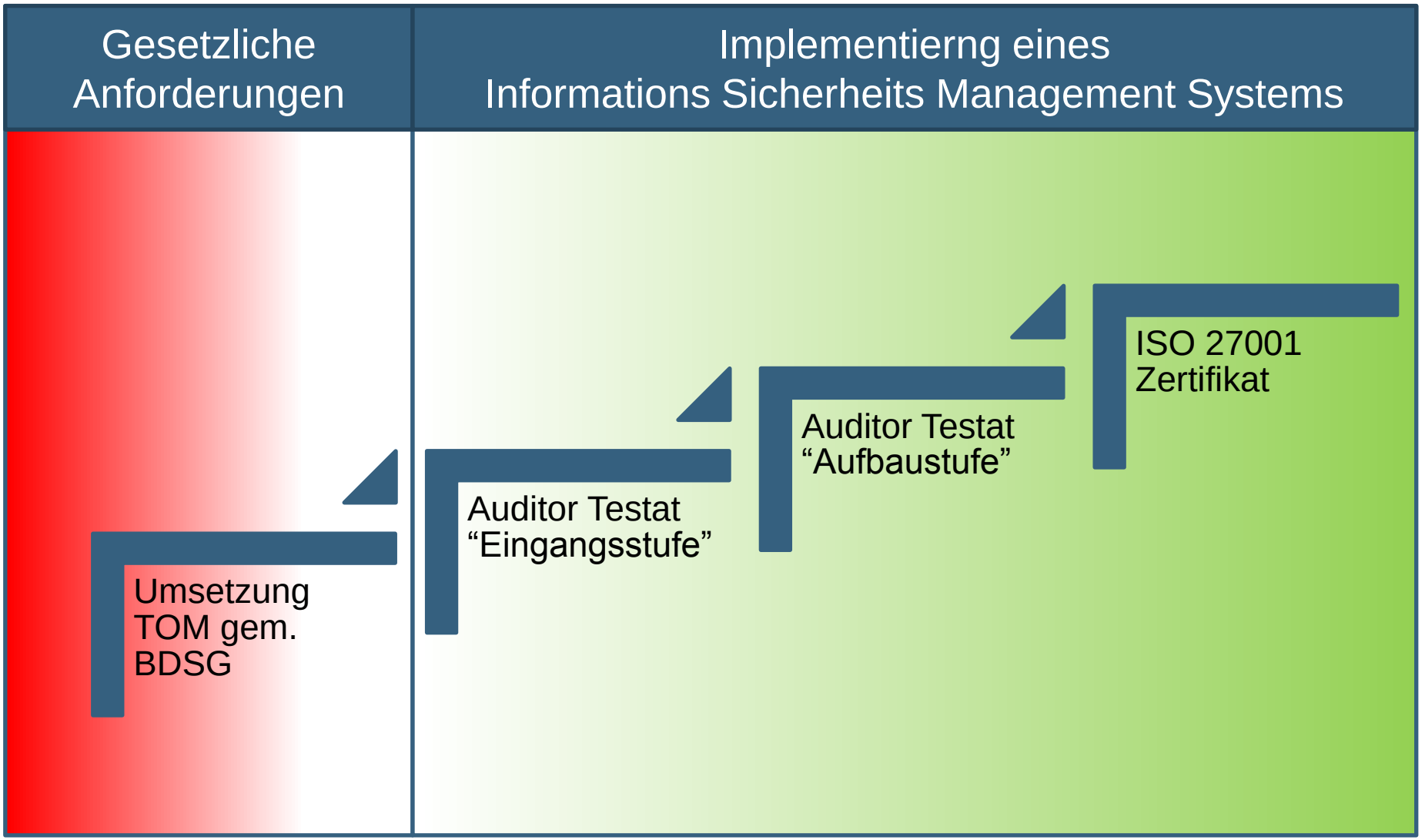
gelb = Bereich mit mittleren Risiken, welche nicht akzeptiert werden sollten und Maßnahmen erfordern.

rot = Bereich mit inakzeptablen Risiken, welche umgehend auf ein erträgliches Maß reduziert werden müssen.

Informations-Sicherheits-Management-System



Der Weg zum Informations-Sicherheits-Management auf Basis IT Grundschutz



Agenda

01 Was bedeutet Informationssicherheit?

02 Welche Standards gibt es?

03 Informations-Sicherheits-Management-System

04 **Wie können die TOM gem. BDSG umgesetzt werden?**

Schutz personenbezogener Daten

Fremdpersonal:
- Gebäudezutritt, Systemzugang

Techn. Mängel:
- Serverausfall
- Datenverlust

Katastrophen:
- Blitzeinschlag
- Brand
- Wassereinbruch

Angriffe durch (Ex-)Mitarbeiter :
- Datenmanipulation
- Datendiebstahl
- Spionage

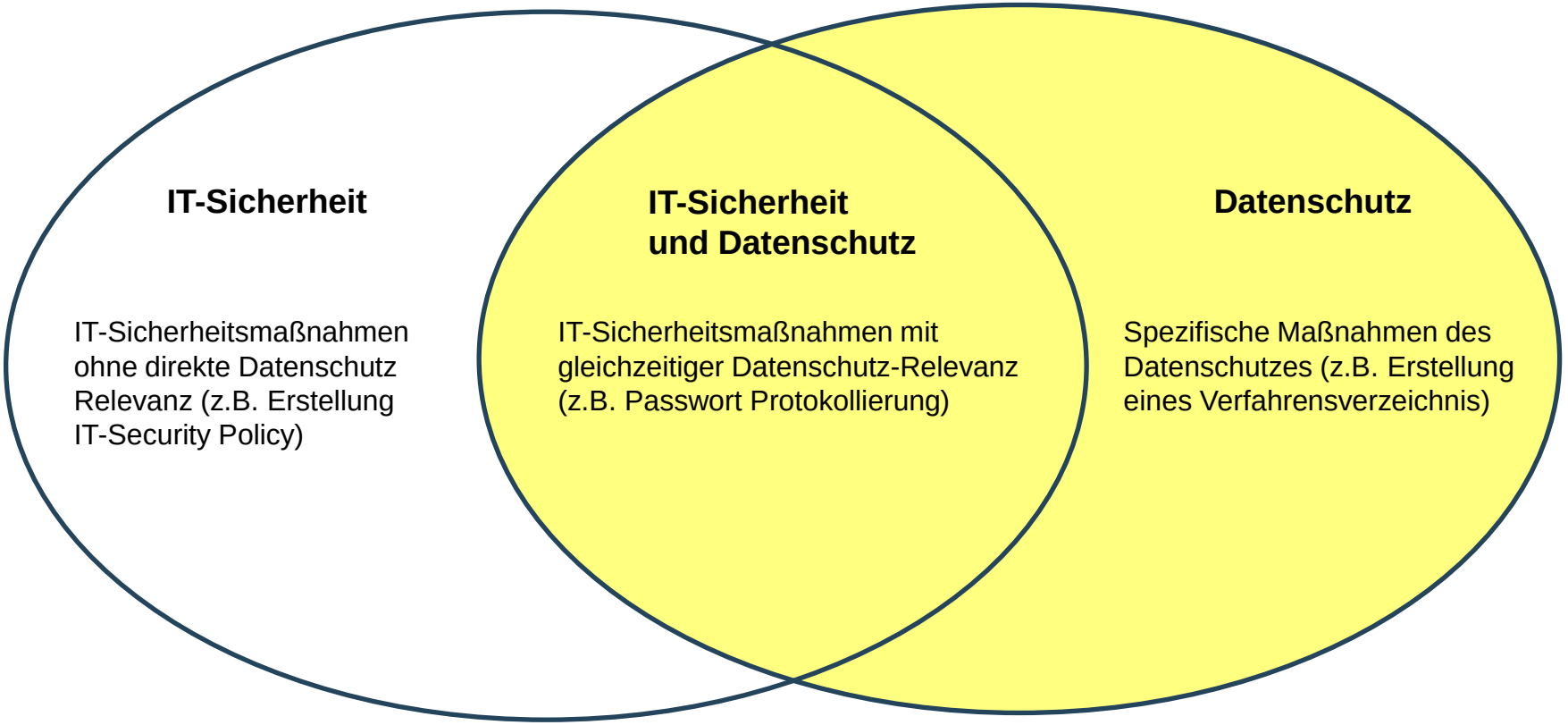
Hacker:
- IT-Betrieb
- Datensicherheit

Organ. Mängel:
- Berechtigungen
- Verschlüsselung
- Verantwortlichkeiten

Industriespionage:
- Konstruktionsdaten
- Finanzdaten
- Forschungsergebnisse

Ungeschulte Mitarbeiter:
- Internetnutzung
- Umgang mit Informationen
- Unachtsamkeit

Das Verhältnis von Datenschutz und IT-Sicherheit



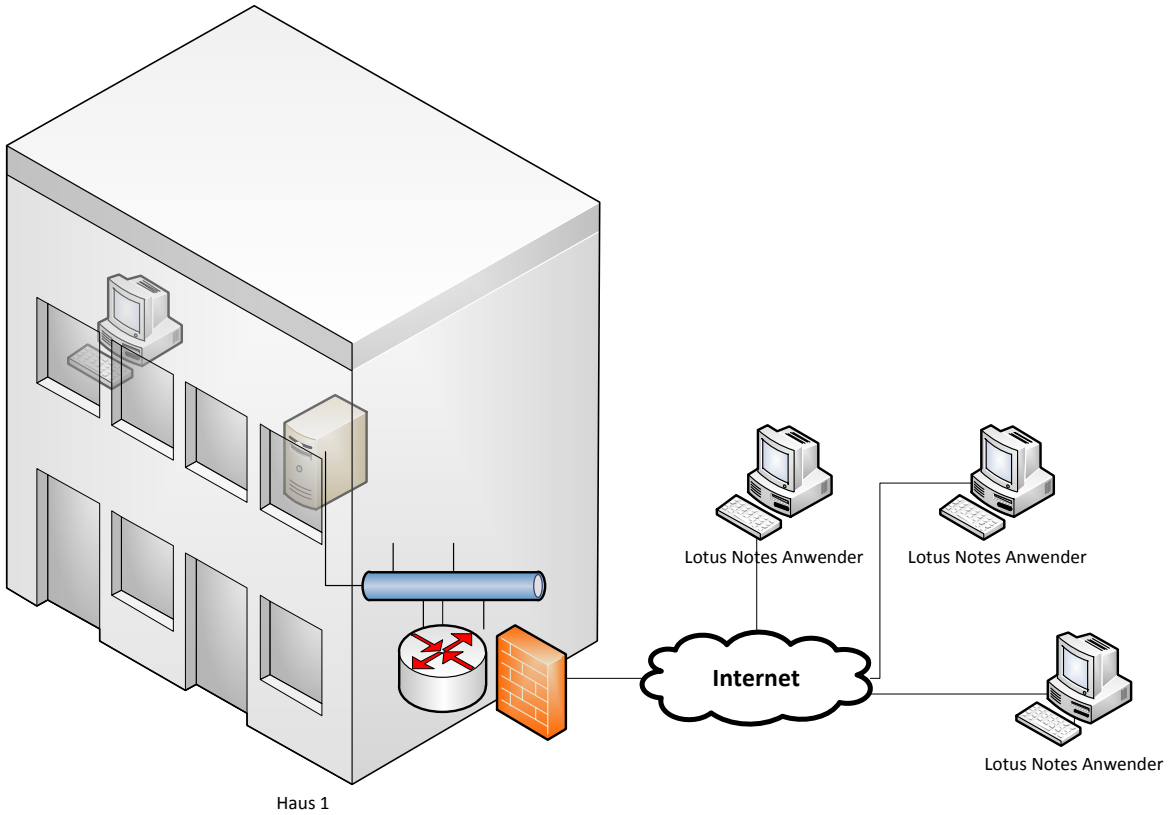
Datenschutz und BSI

Die Datenschutzbeauftragten des Bundes und der Länder haben eine Zuordnung der IT-Grundschutz-Maßnahmen zu den Zielsetzungen des Datenschutzes vorgenommen.

Zuordnung der Maßnahmen der IT-Grundschutz-Kataloge zu den datenschutzrechtlichen Kontrollzielen des Bundesdatenschutzgesetzes BDSG:

Maß-nahme aus GSK	Zutritts-kontrolle	Zugangs-kontrolle	Zugriffs-kontrolle	Weitergabe-Kontrolle	Eingabe-kontrolle	Auftrags-kontrolle	Verfüg-barkeits-kontrolle	(Zweck-bindung)
M1.2	x							
M1.10	X							
M1.12	x							
M1.15	x							
M1.17	x							
M1.19	x							

Beispiel – Externer Lotus Notes Betrieb



IT Verbund:

- Gebäude
- Rechenzentrum
- Internes LAN
- Server mit Notes Anwendung
- Router und Firewall
- Zugriff über VPN

Übersicht der relevanten IT Grundschutz Maßnahmen

Schicht: übergreifende Aspekte

- B 1.000 Sicherheitsmanagement
- B 1.001 Organisation
- B 1.002 Personal
- B 1.003 Notfallmanagement
- B 1.004 Datensicherungskonzept
- B 1.005 Datenschutz
- B 1.006 Schutz vor Schadprogrammen
- B 1.007 Kryptokonzept
- B 1.008 Behandlung von Sicherheitsvorfällen
- B 1.009 Hard- und Software-Management
- B 1.010 Standardsoftware
- B 1.011 Outsourcing
- B 1.012 Archivierung
- B 1.013 Sensibilisierung und Schulung zur Informationssicherheit
- B 1.014 Patch- und Änderungsmanagement
- B 1.015 Löschen und Vernichten von Daten
- B 1.016 Anforderungsmanagement

Schicht: Infrastruktur

- B 2.001 Gebäude
- B 2.002 Elektrotechnische Verkabelung
- B 2.009 Rechenzentrum
- B 2.012 IT-Verkabelung

Schicht: IT-Systeme

- B 3.101 Allgemeiner Server
- B 3.301 Sicherheitsgateway (Firewall)

Schicht: Netze

- B 4.001 Heterogene Netze
- B 4.004 VPN

Schicht: Anwendungen

- B 5.003 E-Mail
- B 5.005 Lotus Notes

27 Bausteine
mit 566 Maßnahmen !!!

Erstellung Umsetzungkonzept für TOMs

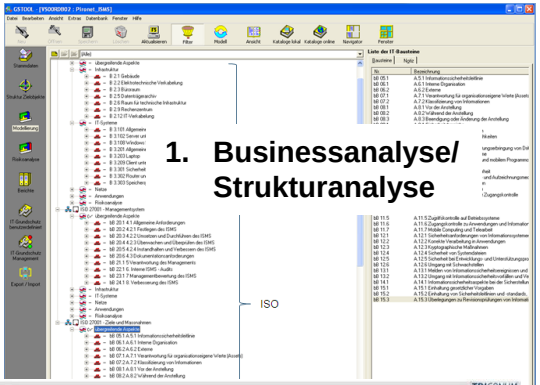
- Die IT-Grundschutz Maßnahmen liefern die Basis für ein Umsetzungskonzept für die technisch organisatorischen Maßnahmen.

Schicht: Anwendungen
Baustein: E-Mail
Zielobjekt: Lotus Notes Anwendung

Maßnahme		Status
Zugangskontrolle		
	M 6.90 Datensicherung und Archivierung von E-Mails	unbearbeitet
Zugriffskontrolle		
	M 2.46 Geeignetes Schlüsselmanagement	unbearbeitet
	M 2.118 Konzeption der sicheren E-Mail-Nutzung	unbearbeitet
	M 2.119 Regelung für den Einsatz von E-Mail	unbearbeitet
	M 2.120 Einrichtung einer Poststelle	unbearbeitet
	M 4.64 Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen	unbearbeitet
	M 5.56 Sicherer Betrieb eines Mailservers	unbearbeitet
	M 5.57 Sichere Konfiguration der Mail-Clients	unbearbeitet
	M 5.63 Einsatz von GnuPG oder PGP	unbearbeitet
	M 5.67 Verwendung eines Zeitstempel-Dienstes	unbearbeitet
	M 6.38 Sicherungskopie der übermittelten Daten	unbearbeitet
Weitergabekontrolle		
	M 2.42 Festlegung der möglichen Kommunikationspartner	unbearbeitet
	M 2.46 Geeignetes Schlüsselmanagement	unbearbeitet
	M 2.118 Konzeption der sicheren E-Mail-Nutzung	unbearbeitet
	M 2.119 Regelung für den Einsatz von E-Mail	unbearbeitet

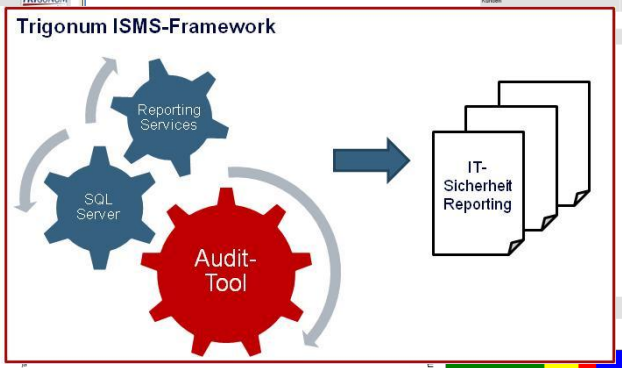
27 Bausteine
mit 173 Maßnahmen !!!

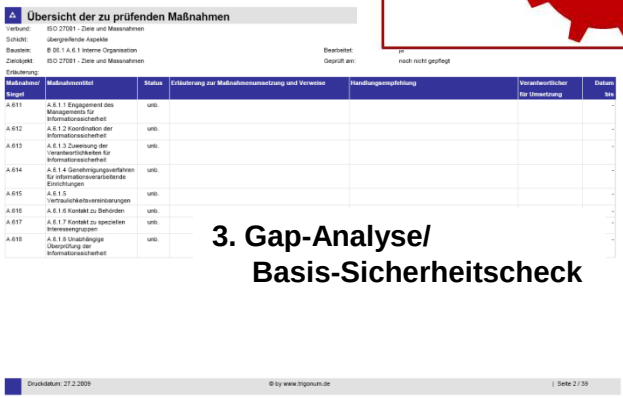
Trigonum ISMS-Framework zur Umsetzung



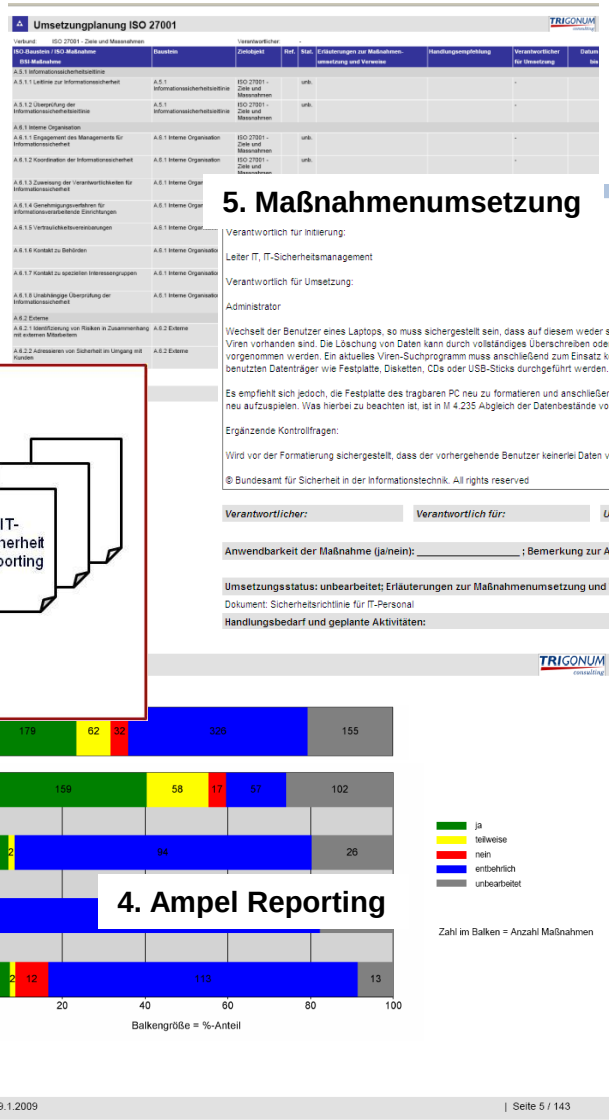
1. Businessanalyse/ Strukturanalyse

2. Schutzbedarfsfeststellung & ggf. Risikoanalyse





3. Gap-Analyse/ Basis-Sicherheitscheck



4. Ampel Reporting

5. Maßnahmenumsetzung

Nutzen

- Erfüllung der gesetzlichen Anforderungen
- Nachweis eines aktiven Risikomanagements
- Orientierung an international anerkannten Standards
- Klares definiertes und auch von Externen nachvollziehbares Vorgehen
- „Rad muss nicht neu erfunden werden“
- Höhere Betriebssicherheit und Minimierung des Ausfallrisikos
- Umsetzung wesentlicher Empfehlungen von ITIL und der ISO 20000
- Erschließen neuer Kundengruppen (ISO 27001 Zertifikat wird bereits in einigen Branchen bei Ausschreibungen gefordert)
- Abheben vom Wettbewerb durch nachgewiesene (zertifizierte) IT-Sicherheit als Zusatznutzen für Ihre Produkte / Dienstleistungen gegenüber Ihren Kunden

Für weitere Fragen stehen wir Ihnen jederzeit gern zur Verfügung.

TRI*GONUM GmbH*
Notkestrasse 11
22607 Hamburg
www.trigonum.de

Peter Bodino
Dipl. Wirtschaftsinformatiker
Telefon: +49(0)40 3199 1618 3
Fax: +49(0)40 3199 1618 8
E-Mail: Peter.Bodino@trigonum.de

Stephan Ernst
Dipl. Wirtschaftsingenieur
Telefon: +49(0)40 3199 1618 1
Fax: +49(0)40 3199 1618 8
E-Mail: Stephan.Ernst@trigonum.de