

Informationstag "IT-Sicherheit in der Marktforschung"

Gemeinsame Veranstaltung von TeleTrust und ADM

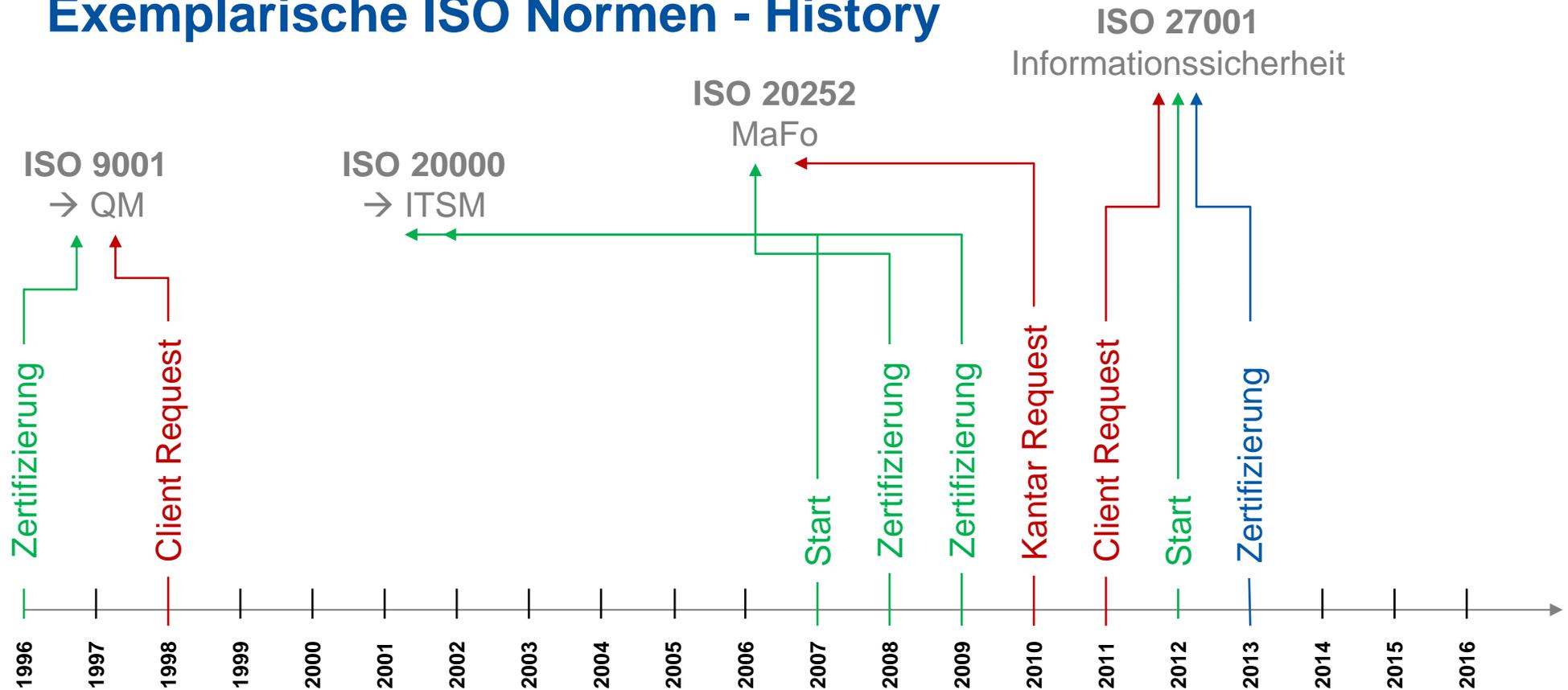
Berlin, 16.10.2013

ISO/IEC 27001ff. in der Marktforschung

Winfried Hagenhoff
COO TNS Infratest

Schon wieder eine neue Zertifizierung? Brauchen wir das?

Exemplarische ISO Normen - History



ISO 27001

Sie sind Gast
[Einloggen](#) | [Registrieren](#)

Suche

News

- 7-Tage-Alerts
- 7-Tage-News
- News-Archiv
- Newsletter
- English News
- PDF-Email

Aktuelle Meldungen

03.11.2009
Zugriff auf Rechnungen im Sparkassen-S'
Nach Libri hat nun den Deutschen Sparkassenverb
mit Kundenrechnungen erteilt. So konnten ange
anderer Kunden durch Ändern einer bestimm

03.11.2009
Neues Kryptosystem soll digitales
Resistent gegen Hackerangriffe und schr
der norwegischen University of Science

03.11.2009
Die Rückkehr der Computerw
Phishing hat im ersten
wie die Verbreitung von W
Security Intelligence Report 200
Unternehmensumgebungen anfallig-



<http://www.ontraxx.net/index.php>

Sie sind Gast
[Einloggen](#) | [Registrieren](#)

Suche

News

7-Tage-Alerts

News Security

Britisches Ministerium verliert USB-Stick mit Passwörtern

Von **Elinor Mills** und **Stefan Beiersmann**
CNET News.com
04. November 2008, 10:49 Uhr

Behörde schließt aus: Government-Portal

WDR.de | Fernsehen | Radio | Programmvorschau | Unter
suchen Mittwoch, 11.11.2009

Suchbegriff

Startseite
Nachrichten
Wetter
Verkehrslage
Politik
Wirtschaft
Kultur
Wissen
Panorama
Computer
Service
Medienseite
Studios in NRW
Kinder

Millionenfacher Datenmissbrauch
Fast täglich werden neue Fälle von Datenmissbrauch bekannt. Ansehens des Skandals um illegal gehandelte Kundendaten fordert die NRW-Datenschutzbeauftragte ein Verbot für den Handel mit persönlichen Daten.

Erneut Sicherheitsleck bei SchülerVZ
28.10.09: Zum zweiten Mal innerhalb weniger Tage ist ein Sicherheitsleck im Online-Netzwerk SchülerVZ bekannt geworden: Nun kursieren 1,8.000 Datensätze mit privaten Informationen wie Geburtsdaten, Blog-Einträge und E-Mail-Adressen. Eigentlich dürfen das nur Freunde sehen. (tagesschau)

US-Bericht: China verstärkt Spionageangriffe auf Unternehmen

China kurbelt seine Cyber-Spionage stärker an und geht dabei immer sorgfältiger und erfolgreicher vor. Das stellt die US-Kommission "China Economic and Security Review" nach [Angaben des Wall Street Journal](#) abschließend in einem Bericht fest. So gelänge es der chinesischen Regierung immer häufiger, über das Internet in Hightech-Unternehmen einzubrechen und in großen Mengen wertvolle Daten zu stehlen.

Consultingfirma verliert Auftrag nach Datenverlust

Von **Peter Marwan**
ZDNet
16. September 2008, 18:09 Uhr

Britisches J verschwind Hacker stellen E-Mail-Adressen von 52.000 Rewe-Kunden ins Netz

von Anita Klingler, 20. Juli 2011, 18:29 Uhr

FLEXISPY
Produkt Your Children | Open Marketing Spoores

Home | Produkte | Fragen | News | Über Uns | Demo

Die Leistungsfähigste Spionage-Software für Handys
FlexISPY ist ein Programm, das alle Aktivitäten des Handys auf dem es installiert ist, unbemerkt überwacht. Schützen Sie Ihre Kinder, finden Sie heraus ob Ihr Partner Sie betrügt. Die möglichsten sind: SMS, MMS, E-Mails, Internet, etc.
Sobald FlexISPY auf einen unterstützten Mobil installiert worden ist, empfangen Sie Kopien von SMS-Berichten die von dem aus generiert oder empfangen wurden, Anrufgeschichten, usw.
Verstecken Sie Symbole & jetzt verfügbar.
Verstecken Sie Pocket PC, und BlackBerry ab nächste Woche.
Schreiben Sie sich an der Heise Seite.
Diese Seite liefert noch nicht völlig auf Deutsch verfügbar.
Für alle weiteren Informationen: Die hier gezeigten Produkte sind als erfolgreichste

FLEXISPY-PRO	FLEXISPY-LIGHT
Produkt Überblick	Produkt Überblick
PRO	LIGHT

News | Hintergrund | Erste Hilfe

Security > News > 7-Tage-News > 2011 > KW 27 > Server der B

Server der Bundespolizei ausspioniert

EU-Flughäfen: 3.300 Laptops verschwinden wöchentlich

London Heathrow mit 900 verlorenen Geräten an der Spitze - Platz zwei belegt der Amsterdamer Airport Schiphol, gefolgt von Paris

Die Verlustrate von Notebooks auf europäischen Flughäfen liegt bei über 3.300 Stück pro Woche. Das geht aus einer Studie des **Panomon Institute** hervor, die vom PC-Hersteller **Dell** in Auftrag gegeben wurde. Diese Verlustrate bezieht sich jedoch lediglich auf die acht größten Airports des Kontinents ein. An der Spitze liegt der Flughafen London Heathrow, wo 900 Geräte pro Woche abhanden kommen. Platz zwei belegt der Amsterdamer Airport Schiphol, gefolgt von Paris Charles de Gaulle. Hier sind Notebook-Verluste von jeweils etwa 700 Stück wöchentlich zu beklagen.

Stiftung Warentest
test.de

Tests + Themen | Shop | Abo | Über uns | Presse

Suchen

Sie sind hier: [Startseite](#) > [Tests + Themen](#) > [Geldanlage + Banken](#) > [Meldungen](#)

Datenmissbrauch bei der Postbank Systematische Verstöße gegen den Datenschutz

27.10.2009
Die Postbank gewährt Tausenden von freien Handelsvertretern detailliertes Einblick in den Verkauf ihrer Produkte fördern. Laut der Datenschutzbehörde von Nordrhein-Westfalen ist das verboten. Finanztoxis liegen auch zahlreiche Kontoauszüge von Prominenten vor.
*) eigenen Angaben will die Postbank ihren Finanzberatern jetzt sperren.

Jedes ZWEITE deutsche Unternehmen wird ausspioniert!

2012 rechnet die deutsche Wirtschaft mit einem Schaden von über 4,2 Milliarden Euro.

China wird dabei nicht mehr als das Risikoland bewertet. Vor allem die ehemaligen GUS-Republiken werden in der Spionageszene immer aktiver und beschaffen auf diesem Weg Know-how für Ihre Firmen. Mehr als die Hälfte der Schäden entstehen dabei durch die eigenen Mitarbeiter, die oft ungeahnt Opfer von Social Engineering Angriffen werden.

Es
la
amt
g
ne
Me
ne
Kon
k
sch
s
dr
schä
Die
Ko
g
ding
we
Chi
re
In
die
hö
nicht immer, im Gegenteil. Der Verfassungsschutz geht davon aus, dass viele Geheimdienste, vor allem in Asien, die Wirtschaftsspionage privater Firmen decken und oft sogar unterstützen. Sie wissen. Die Server, von denen die meisten Computer-Spähangriffe ausgehen, stehen in Asien. Auf einem Symposium will

deutsche Unternehmen SZ-Grafik: Mainka / Quelle: BITKOM
der Bundesverfassungsschutz an diesem Montag über die Gefahren für die Wirtschaft berichten. Mittlerweile sind nach Angaben des BKA 750 000 Rechner in Deutschland mit sogenannten Trojanern infiziert, die vertrauliche Daten unbe-

Spionage betroffenen Unternehmen (44 Prozent), überhaupt nicht auf die Angriffe reagiert – weil sie Angst um ihren Ruf haben und Verluste auf dem Aktienmarkt befürchten. Außerdem wissen die Firmen gar nicht, an wen sie sich wenden sollen. 28 Prozent gaben an, das Problem intern zu lösen. Ob sie es lösen konnten,

uelle Angebote, um ihn zu unterbieten, und leiten seine Innovationen direkt in ihre Produktionsstätten weiter. Die gute alte Wirtschaftsspionage der Russen und Chinesen war gestern. Jetzt geht es um direkte Angriffe auf deutsche Firmen. Ein neues Arbeitsfeld für die eigene Behörde, findet der Verfassungsschutz.

Treiber für den Bedarf an nochmals erhöhter Informationssicherheit

Kundenanforderungen

- Zuverlässige Serviceleistungen
- sichere Infrastrukturen
- E-Business
- Entwicklungspartnerschaft
- Know-how Schutz
- Dazu: Besonderheiten öffentlich-rechtl. Kunden

Rechtliche Vorgaben

- Risk Management z.B. KontraG
- Datenschutz BDSG
- Haftungsfragen
- Regulierung / Corp. Governance (z. B. SOX, Basel III)
- Compliance

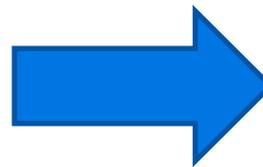
Eigeninteresse

- Schutz von Informationen und Wissen
- Schutz der Infrastrukturen
- Kooperation mit Wettbewerbern
- Image in der Öffentlichkeit

Die Informationsressourcen sind für ein wissensbasiertes Unternehmen von unschätzbbarer Wichtigkeit.

Warum ISO 27001 in der Marktforschung?

- **Positionierung beim Kunden**
 - Zunehmend häufig: Kundenanforderung i.V. mit Angebotsprozessen bzw. IT-Audits durch die Sicherheitsorga unserer Kunden
- **Orientierung an internationalen Standard**
- **Außenwirkung**
- **Risiken erkennen und reduzieren**
 - Haftungsrisiko (§ 276 BGB)
 - aus Verträgen, aus Delikten, aus Verpflichtungen (§ 9 BDSG)
- **Nachweis für Wirtschaftsprüfer**
- **Bestandsführung, Sorgfaltspflicht**



Vertrauen

Kompetenz

Werte sichern

Wettbewerbsvorteil

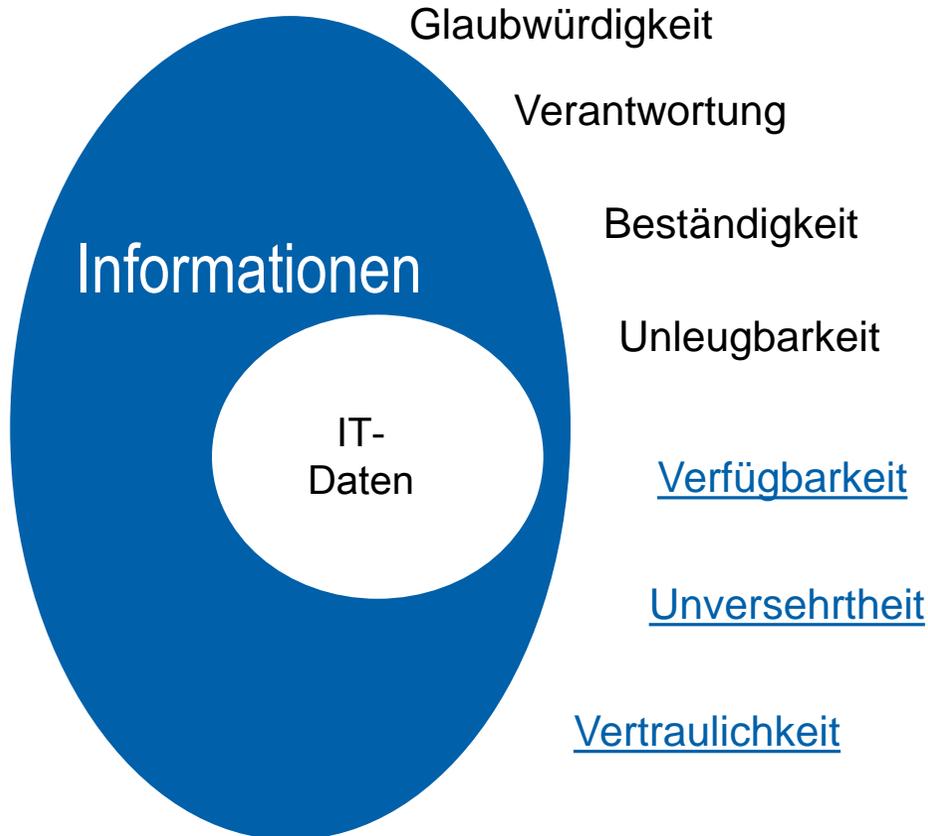
Bedrohungen erkennen

Glaubwürdigkeit

Wirtschaftlichkeit

Akzeptanz

Einige Fakten zu Informationen ...



- Information ist mehr als nur elektronisch gespeichert oder verarbeitet
- Informationssicherheit umfasst mehr als nur IT-Sicherheit
- Sicherheit bedeutet mehr als nur Vertraulichkeit – im geschäftlichen Umfeld ist in der Regel die Verfügbarkeit wichtiger
- Management ist mehr als nur technische Systeme und Werkzeuge

Über allem: Awareness!

Wo/Wie werden Informationen verarbeitet?

- Kundendaten
 - Mitarbeiterdaten
 - Konzepte
 - F&E
 - Verträge
 - Finanzdaten,
 - Strategien
 -
- Nicht nur „in der DV“!
 - alle Netzwerke
 - E-Mail, PC, Data Media
 - Drucker, Papier, Post, Sprache, Fax
 - Wichtig: Schutzklassen definieren

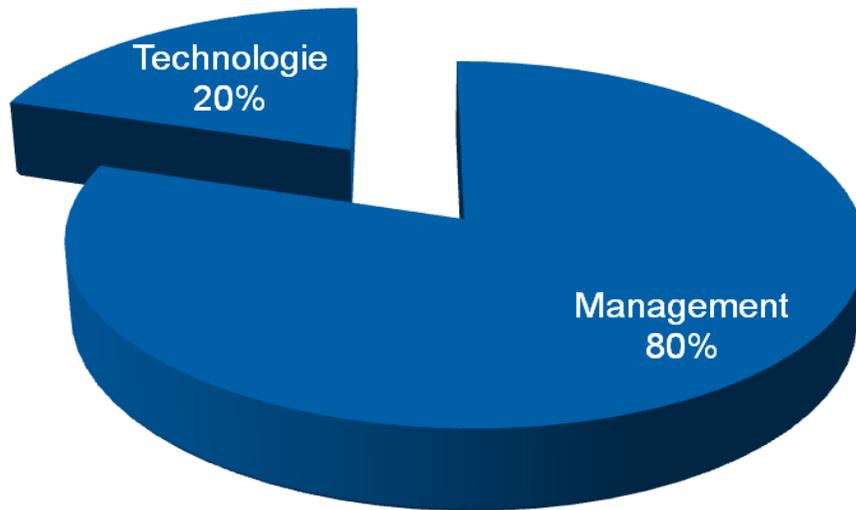
Lebenszyklus von Informationen

- Schutzklassen z.B.:
- Öffentlich
 - Intern
 - Vertraulich
 - Verbindliche Verhaltensanweisungen je Schutzklasse definieren und kommunizieren!

Informationen müssen entsprechend ihrer Schutzklasse über den gesamten Lebenszyklus sicher behandelt werden



Informationssicherheit ist ...

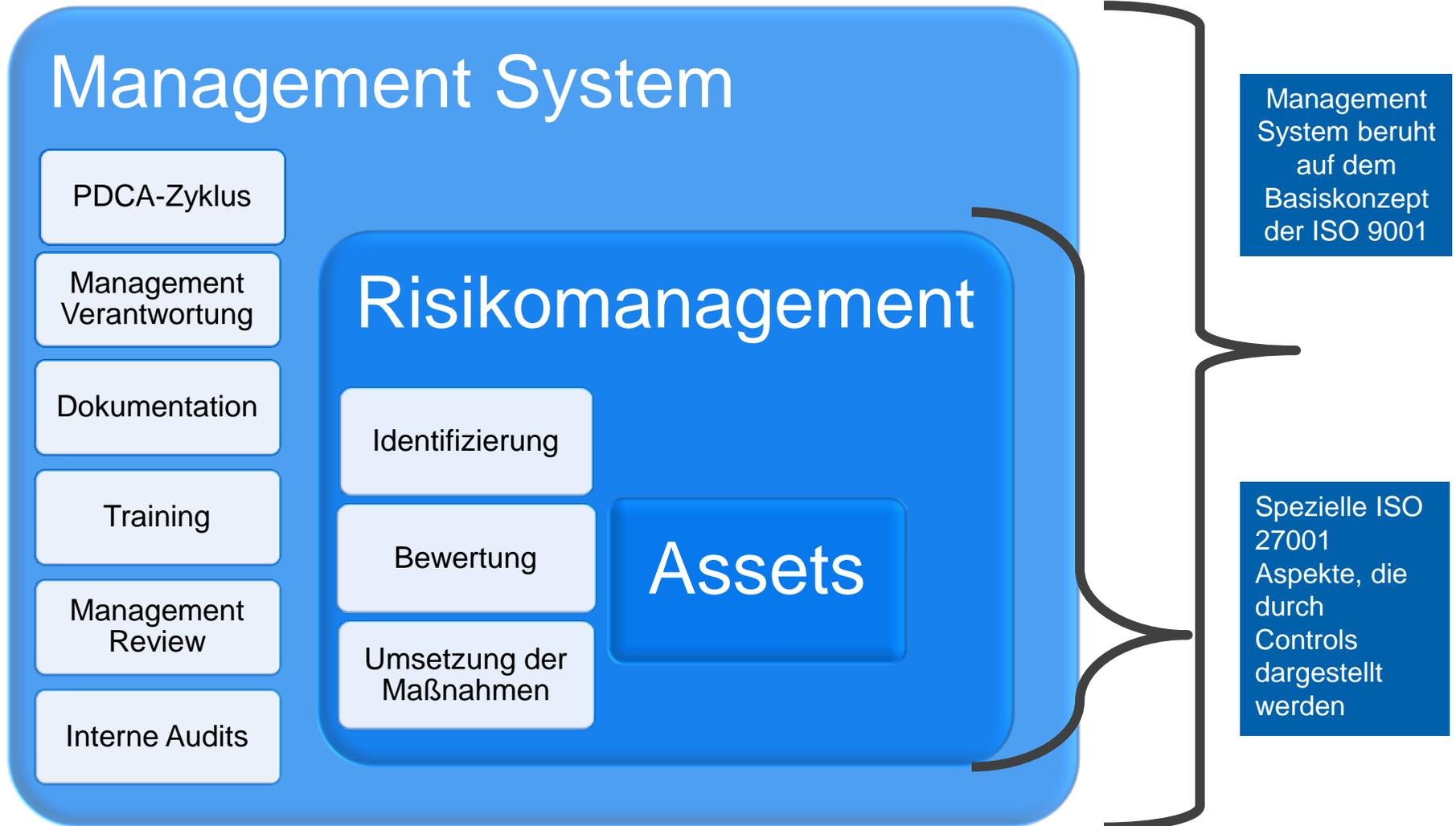


... 80 % Management

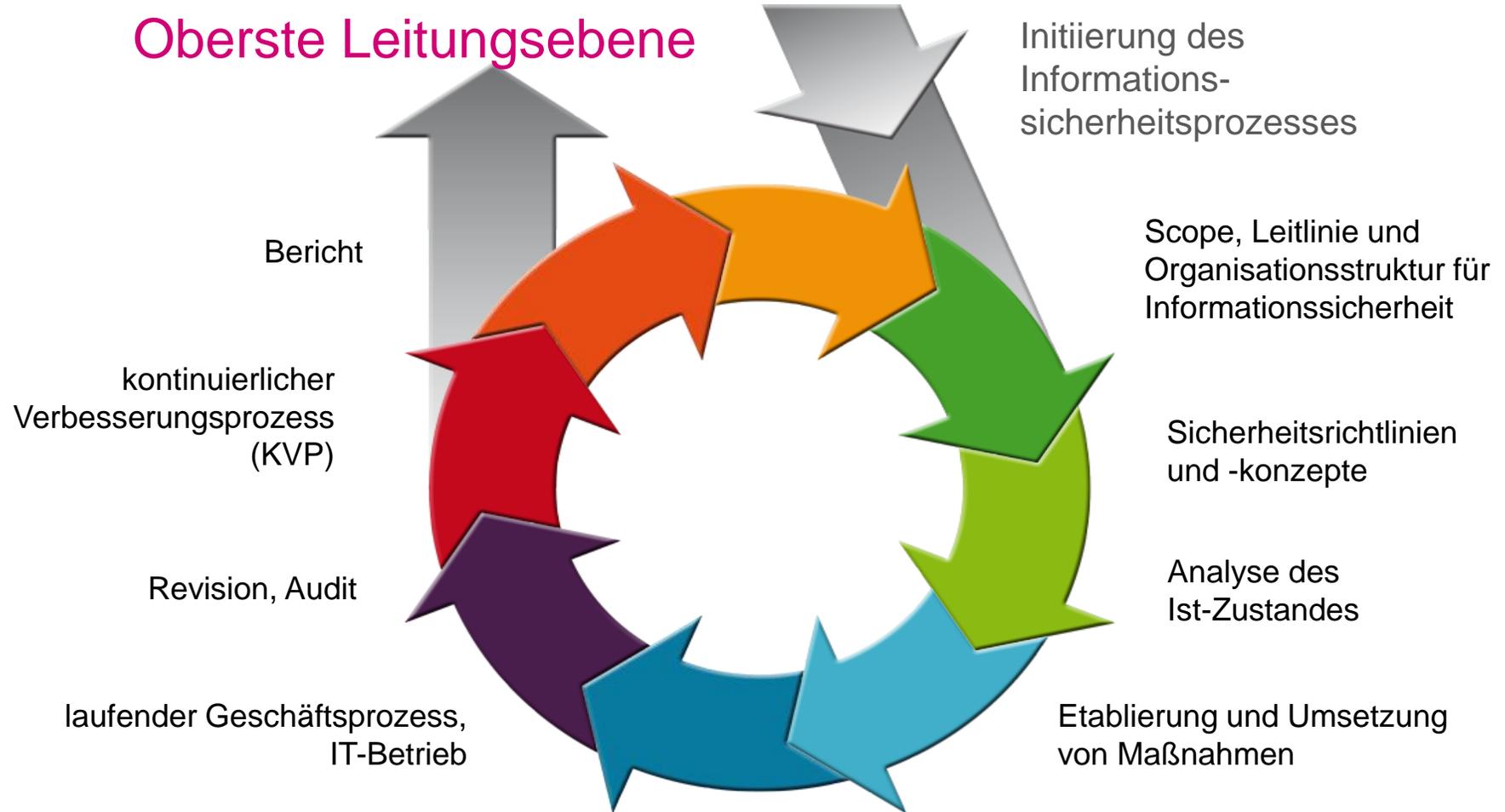
IS-Policy,
IS-Verantwortlichkeiten,
Bewusstsein & -Training, Reporting,
Business Continuity Planung,
Prozesse, etc.

... 20 % Technologie

Systeme, Tools,
Architektur etc.



Einführung des Informationssicherheitsprozesses



1. Unterstützung und Zustimmung des Managements

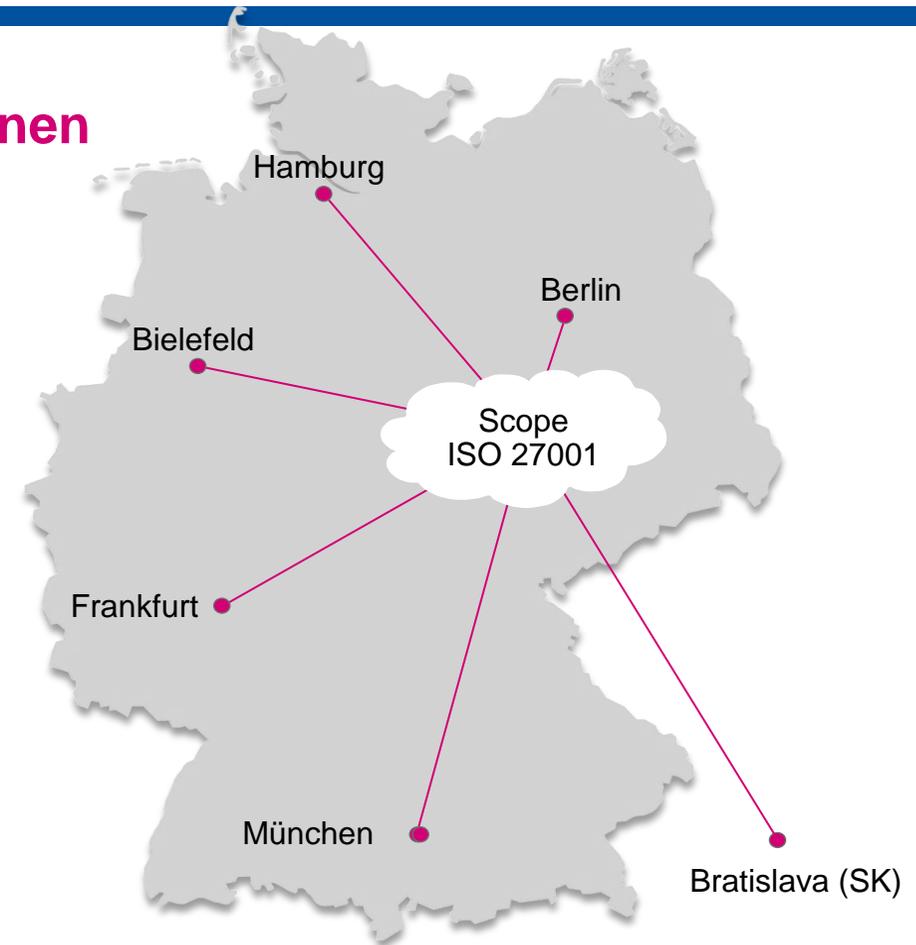
- zu den ISMS Leitlinien und Verbreitung im Unternehmen
- aus allen Hierarchie-Ebenen

2. Festlegung des Scopes

- Was fordern Kunden, Organisationen, Behörden?
 - Geltungsbereich im Unternehmen (Bereiche, Standorte, ...)
 - Prozesse: welche - welche nicht?
 - Ausschlüsse definieren!
 - Weite Möglichkeit der Eingrenzung (auch technisch)
 - Abwägung: Sinnhaftigkeit eines kleinen Scopes versus künftiger Wirksamkeit
- Scope/Geltungsbereich erscheint auf dem ISO/IEC 27001 Zertifikat und kann nachträglich nicht mehr geändert werden!

ISO 27001 bei TNS Infratest - Scope (Anwendungsbereich)

- **Umgang mit Daten und Informationen im Rahmen des Marktforschungsprozesses**
- Anwendung auf alle TNS Infratest Companies incl. der WPP Deutschland Holding GmbH & Co. KG
- 6 Standorte im Fokus: MUC, BFE, HAM, FRA, BER, BTS
- Involvierte Business Units: IT, IS, DS, DSE, FM, HR, Legal, BR, Geschäftsführung
- Relevanz für **alle** Mitarbeiter



3. Budgets für Informationssicherheits-Management Aktivitäten bereitstellen

→ realistische Kosten einplanen

4. Awareness schaffen im gesamten Geltungsbereich

- Training
- Präsenz, bereichsweite Reviews, Begehungen
- Interne Audits

5. Nachhaltige Implementierung eines kontinuierlichen Verbesserungsprozesses (KVP)

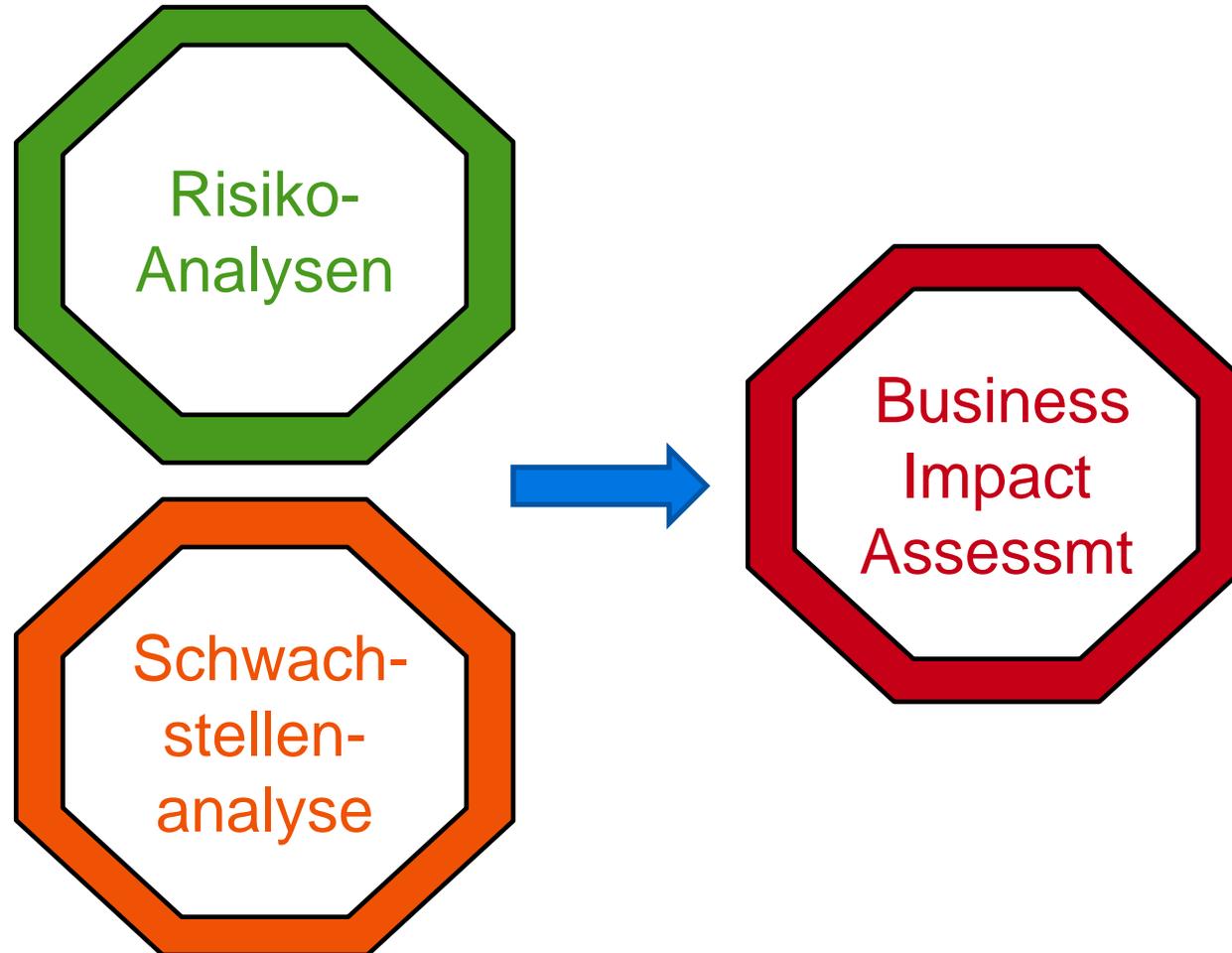
- Kennzahlen, Management Review

Awareness für Informationssicherheit

Was können **Sie** tun?

- **Vorbild sein!**
- Security Awareness Kampagne und Aktivitäten **positiv** kommunizieren und unterstützen
 - ▶ Bei allen Mitarbeitern eine **positive** Einstellung zum Thema Sicherheit erzeugen
- Suchen Sie nach Mitarbeitern, die als lokale Ansprechpartner für Informationssicherheit pro aktiv mitarbeiten wollen (Multiplikatoren)
 - ▶ Ansprechpartner zum Thema Sicherheit bekannt geben (an Projekt-Organisation)

Ausgewählte Schritte vor der Zertifizierung (von allen Bereichen einzufordern!)



Bewertung der Risiken und der Erforderlichkeit weiterer Maßnahmen



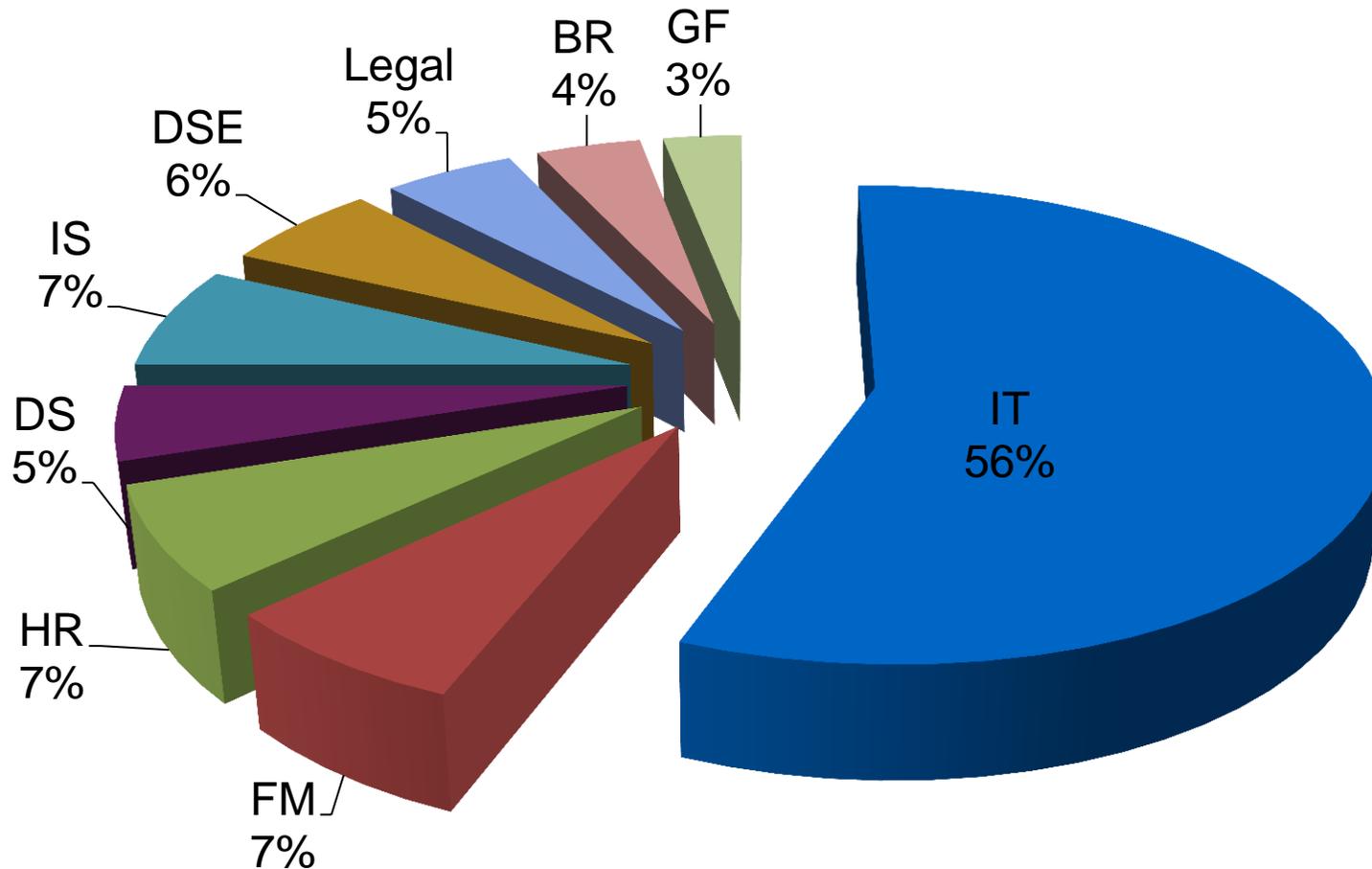
Identifizierte Risiken müssen beseitigt oder getragen werden
(Dokumentierte Akzeptanz des Restrisikos durch das Management)

Inhalte der Norm ISO 27001 und Verantwortlichkeiten im Projekt

11 Themengebiete der ISO 27001 133 Controls	Verantwortlich
Informationssicherheits-Politik (z.B. Security Policy, IKT-RBV, Scope)	GF , IT, BR
Organisation der Informationssicherheit	IT , IS, DS, DSE, Legal, HR, Alle Bereiche
Management von organisationseigenen Werten (Assets)	Alle Bereiche
Sicherheit der Personalressourcen	HR , Legal, FM, IT
Physische und umgebungsbezogene Sicherheit (z.B. Zutrittskontrolle/Zugangskontrolle)	FM , IT, IS
Management der Kommunikation und der Betriebsabläufe	Alle Bereiche
Zugriffskontrolle (z.B. auf Netze und Informationen/Daten)	IT , IS, DSE, FM
Beschaffung, Entwicklung und Wartung von Informationssystemen	IT , IS, DSE
Management von Informationssicherheitsvorfällen	IT , IS, DSE
Management des kontinuierlichen Geschäftsbetriebes (BCM)	Legal , Alle Bereiche
Einhaltung von Verpflichtungen und Gesetzen - Compliance	Legal , DS, IT, IS, DSE

Das Projekt ISO 27001

Anteile der Business Units an den Arbeitspaketen



ISO 27001 – Risikomanagement - Maßnahmen

Beispiele für vorgeschlagene bzw. umgesetzte Maßnahmen

- **Datenschutz**
 - Verpflichtende intensive Einführungsschulung für **neue** Mitarbeiter
 - Verpflichtende jährliche Schulungen für **alle** Mitarbeiter im e-learning mit Zertifikatserneuerung
- **Facility Management**
 - Besucher werden am Empfang abgeholt und auch dort verabschiedet
 - Zusätzliche Wachschutz-Maßnahmen bzw. Videoüberwachung Eingangsbereiche
 - Zusätzliche „Datenschutztonnen“ zur Dokumentenvernichtung
- **Human Resources**
 - Erarbeitung von Mitarbeiter-Bindungsstrategien

ISO 27001 - Vielen Dank für Ihre Aufmerksamkeit!



Fragen?

