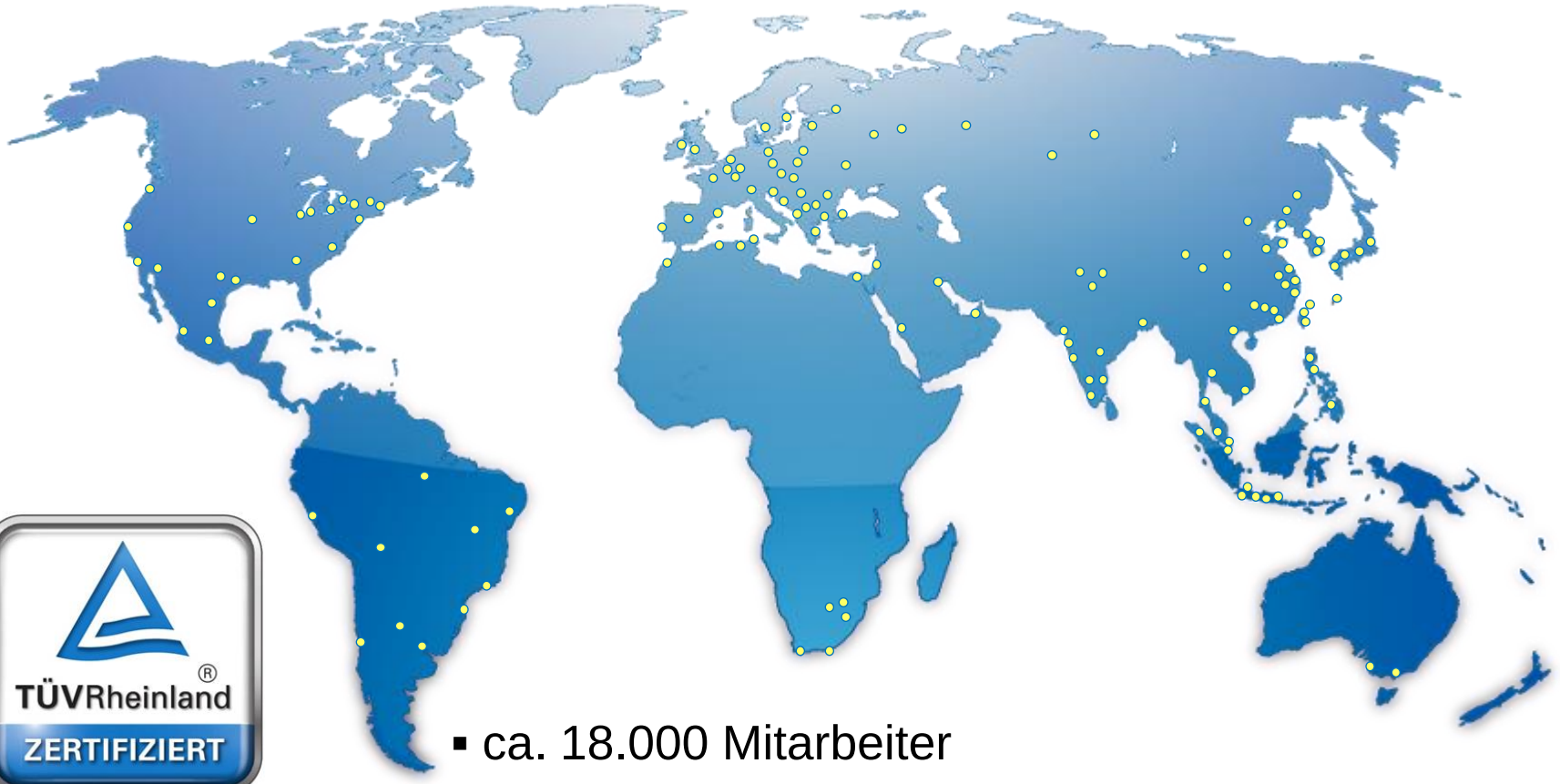
Aus Liebe zu Sicherheit und Qualität.

ECO Verband – Frankfurt – 30.01.2015

TÜVRheinland®
Genau. Richtig.

2013 - Auf allen Kontinenten zuhause.

- Ca. 600 Standorte in 65 Ländern
- ca. 1,6 Mrd. € Umsatz



- ca. 18.000 Mitarbeiter

Das Team zum Thema IT und Informationssicherheit


Bruno Tenhagen

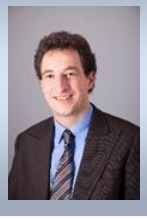

Bruno Tenhagen


Manfred Willems


Tim Nakamaru

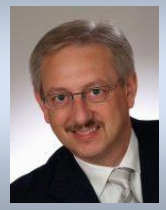

Torsten Jung


Patrick Rischar


Franz Obermayer


Christian Aust


Jürgen Ehmann


Andreas Lentwojt


Walter Schlegel


Sven Stephan


Thomas Kloos


Heiko Gossen


Thomas Lüttkemeyer


Stefan Braunshausen


Ralf Meschke


Peter Rothfeld

Referenzkunden Finance, Healthcare und IT

Finance

talanx. Versicherungen. Finanzen.
IKB Deutsche Industriebank
ING DiBa Die Bank und Du
FIDUCIA Ihr IT-Partner
HUK24 DIE ONLINE-VERSICHERUNG
DPS ENGINEERING
pbb DEUTSCHE PFANDBRIEFBANK
Postbank
bank-verlag zahlungssysteme
DZ BANK
Frankfurter Volksbank
BUNDESDRUCKEREI
EOS
Allianz

Healthcare

PVS holding GEMEINSAM BESSER.
DAK Unternehmen Leben
Gesellschaft für PATIENTENHILFE
VAMED health. care. vitality.
Techniker Krankenkasse
Malteser ...weil Nähe zählt.
Alles Gute. KVBW
OLYMPUS
BOSCH
CONSILIO
KKH
Allianz
GE Healthcare
ife Ihre freundlichen Experten.
HBSN AG Health Business Services Network

Informationstechnologie / Telekommikation

items
vodafone
Computacenter Services & Solutions
smava Der erste Kreditmarktplatz
Telefónica
QSC AG
IBM
conova.com THE IT COMPANY
IT-Consult Halle GmbH
consinto
TREND MICRO
GLOBAL SWITCH
r@tiodata IT-Lösungen & Services
BITMARCK®
Atos Origin
BORnet Kommunikation
QVC Ideen für mich!
OEVERMANN Networks GmbH
HKR Rechenzentrum GmbH
Herzlich Willkommen! Brandl
CONTENiT
LEITWERK
on line
adlon Empowering Business with IT
GAD IT für Banken
icubic The solution®
Deloitte.
DATIS®
uptime IT
TAS

TÜVRheinland®
Genau. Richtig.

Referenzkunden Automotive, Industrie & Sonstige

Industrie / Chemie / Pharma

Canon
GEA
LANXESS Energizing Chemistry
L'orange YOUR POWERFUL INJECTION
Envi Con Envi Con & Plant Engineering GmbH
WÜRTH
ThyssenKrupp
Freudenberg
OLYMPUS
ifm
enrichment technology a joint venture between Urenco and Areva
fischer elektronik
pharmaserv standortmanagement und services
EnBW Energie braucht Impulse

Automotive / Logistik

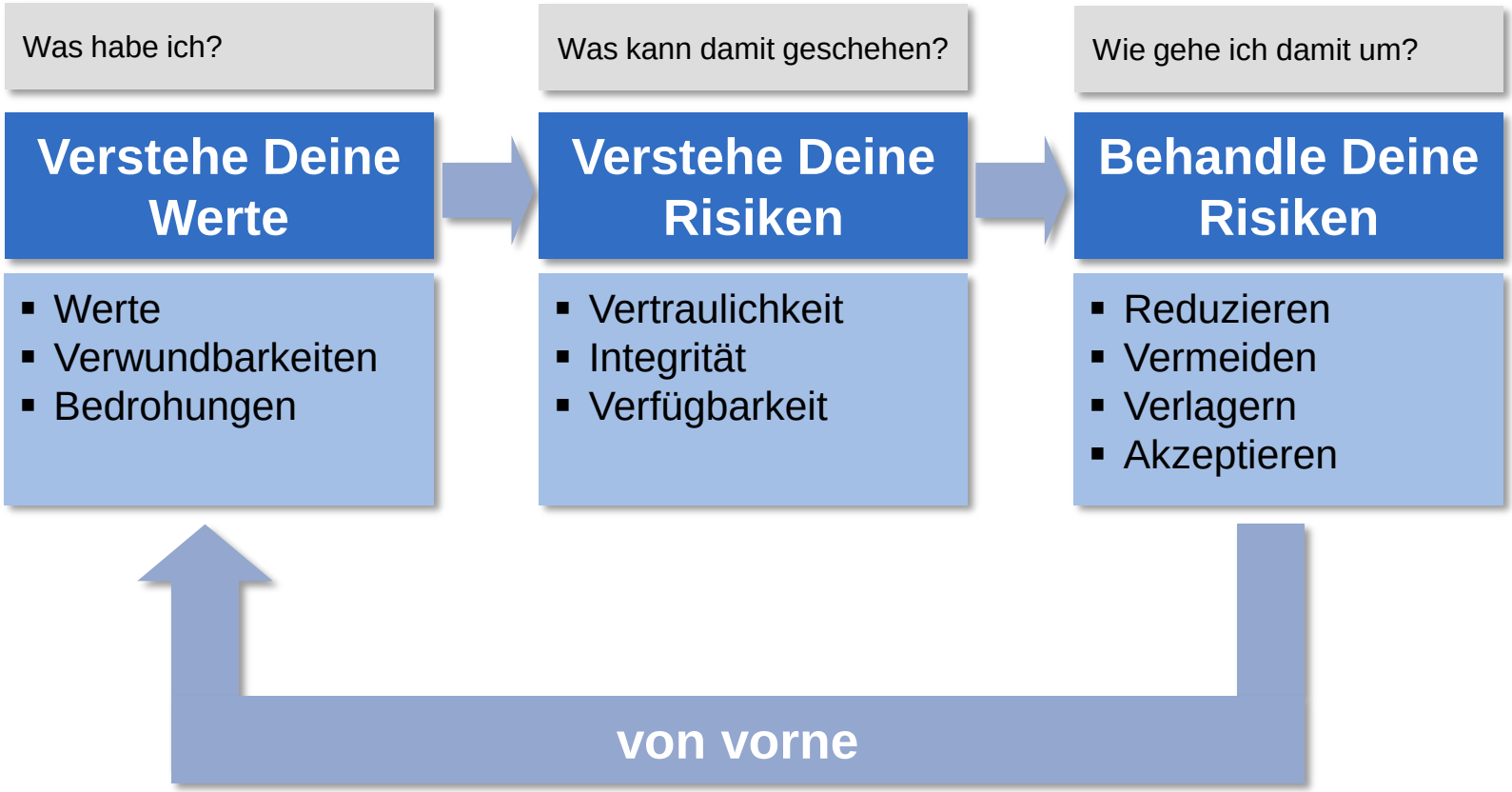
DAKOSY
outokumpu
delphi
LEAR CORPORATION
P+Z Engineering
BOSCH
DONATH International
IAV GmbH Ingenieurgesellschaft Auto und Verkehr
ZF
Audi Vorsprung durch Technik
Geis Global Logistics
AUTOSTADT
VAPS | ACS
LEXCOM We take care of IT for you.

Gouverment/ Sonstige

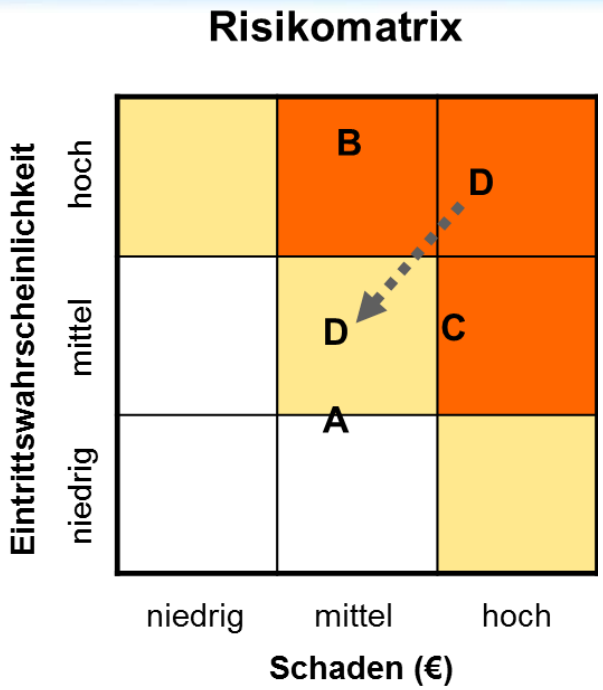
Google Deutschland
Lufthansa
STADTWERKE SOLINGEN
GDF SUEZ BY PEOPLE FOR PEOPLE
GREVEN'S Adreßbuch-Verlag Köln GmbH & Co. KG
mediamonitoring
ROLEX
SWE Stadtwerke Erfurt Gruppe
facelift
Bet3000
tipico
RTL
ERDGAS MÜNSTER Partner für Deutsches Erdgas
Tchibo
TOMORROW FOCUS
ADATO International GmbH
powered by GEOS
Lufthansa Cargo Networking the world.
Dumrath & Fassnacht www.duf-online.de

ISMS nach ISO/IEC 27001:2013

Risikobasierte Vorgehensweise



Risikomanagement
Risiko = Eintrittswahrscheinlichkeit x Schadenshöhe



Vorsicht an der Bahnsteigkante: Willkommen auf dem „gefährlichsten Marktplatz der Welt"

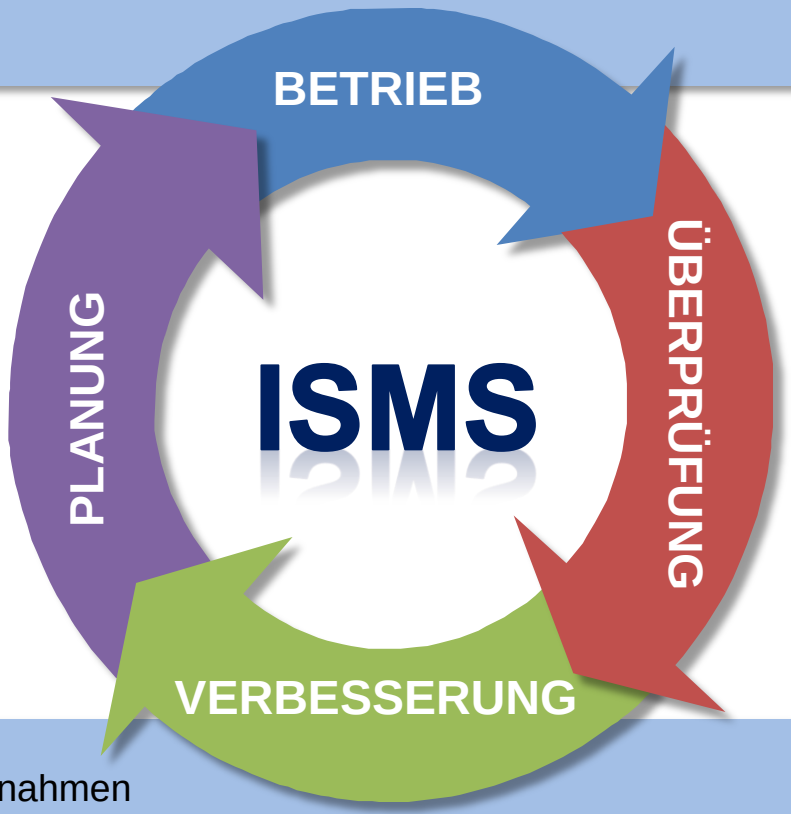
- Kritische Erfolgsfaktoren:
  - Vollständigkeit der Szenarien
  - Ermittlung realistischer Wahrscheinlichkeiten
  - Berechnung der Schadenshöhe

ISMS nach ISO/IEC 27001:2013

Sicherheitsmanagement als kontinuierlicher Prozess

- Implementierung und Betrieb von Maßnahmen

- Definition von Anwendungs-bereich und Zielen
- Risikoanalyse
- Maßnahmen-definition



- Überwachung und Überprüfung

- Verbesserung der Maßnahmen
- Vorbeugen von Fehlern

ISMS nach ISO/IEC 27001:2013
Gliederung

- IS-Themen

Management

- Informationssicherheitspolitik (5.2, A.5)
- ISMS-Organisation (5.3, A.6)
- Information Asset Management (A.8)
- IS Incident Management (A.16)
- Compliance (A.18)
- Leadership (5)
- Beziehungen zu Lieferanten (A.15)

Personal

- Personelle Sicherheit (A.7)

Zutritt / Gebäude / Umgebung

- Physische Sicherheit (A.11)

Tagesgeschäft

- Betrieb (A.12)
- Kryptographie (A.10)
- Kommunikations-sicherheit A.13)

Planung / Projekte

- Beschaffung, Entwicklung und Wartung von Systemen (A.14)

Zugang / Zugriff

- Zugangskontrolle (A.9)

Geschäftsprozesse

- IS Risiko Management (8.2, 8.3)
- Business Continuity Management (A.17)

Ihr Weg zu Ihrem ISO/IEC 27001 Zertifikat

Implementierung (evtl. mit Berater)

Bestands-
aufnahme

Scope
festlegen

Schutz-
bedarf
feststellen
und Risiken
bewerten

Controls auswählen
bzw. Maßnahmen
festlegen

Controls implementieren,
Management Review und
interne Audits durchführen

Zertifizierung
durchführen


Zertifikat

Standard ISO/IEC 27001:2005

Zertifikat-Registrier-Nr. xx xxx xxxx

TÜV Rheinland Cert GmbH bescheinigt:

Zertifikatsinhaber: <Logo>
<Kunde>
<Kundenanschrift
>

Geltungsbereich: Standort Musterstadt

Durch ein Audit, Bericht Nr. nnnnnnnn, wurde der Nachweis erbracht, dass die Anforderungen des Prüfkataloges für ISO/IEC 27001:2005, der TÜV Rheinland Cert GmbH bezüglich Dokumentation und wirksamer Umsetzung erfüllt sind.

Das Fälligkeitsdatum für Folgeaudits ist der dd. mmm.

Gültigkeit: Dieses Zertifikat ist gültig bis yyyy-mm-dd
vom yyyy-mm-dd bis zum yyyy-mm-dd.

yyyy-mm-dd

Bruno Tenhagen
TÜV Rheinland Cert GmbH
Am Grauen Stein · 51105 Köln

www.tuv.com

TÜVRheinland®


TÜVRheinland®
ZERTIFIZIERT

Management
System
ISO 27001:2013

www.tuv.com
ID 0000000001

TÜVRheinland®
Genau. Richtig.

Relevanz der ISO 27001 Zertifizierung

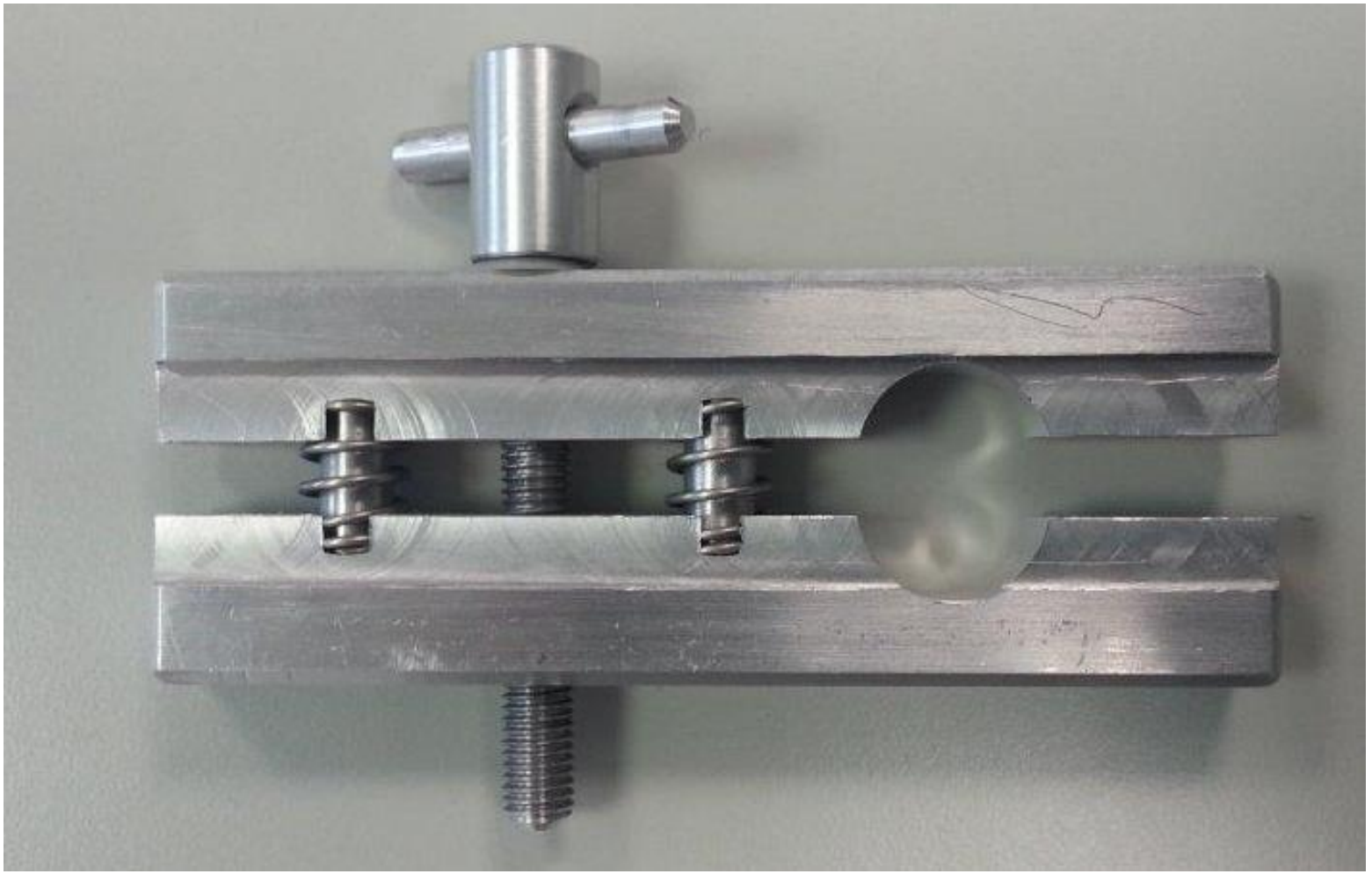
Unter allen weltweit themenspezifischen Normen verzeichnete die Norm ISO/IEC 27001:2005 2012 mit 23 % den größten Zuwachs

Beispiel Personelle Sicherheit

Auszug aus ISO 27001, Anhang A

A.7	**Human resource security**	
A.7.1	**Prior to employment**	
. . .		
A.7.2	**During employment**	
Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.		
A.7.2.1	Management responsibilities	*Control* Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
A.7.2.2	Information security awareness, education and training	*Control* All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

Wie gehen wir mit Widerspruch im Audit um …..



Rollenspiel Personelle Sicherheit

Rollenspiel „Wie sinnvoll sind Social Media Guidelines?“

Ca. 15 Minuten

Am Audit-Interview nehmen außer dem Auditor teil:
- Leiter IT (kontra)
- Leiter Vertrieb (pro)
- Leiter Personal (kontra)

Situation:

Ein Mitarbeiter hat in xing und linkedin gepostet, dass er Projektleiter Expansion Südamerika geworden ist. Der Vertriebsleiter hat diese Information durch seine Vernetzung mit dem Projektleiter erfahren.

Rollenspiel
Es werden die Vor- und Nachteile einer Social Media Policy diskutiert

Feedback an ...

Bruno Tenhagen
Produktmanager ISO 27001
Senior Auditor ISO 27001
IRCA Lead-Tutor/ Lead-Auditor
Lead-Auditor (BSI)

E-Mail bruno.tenhagen@de.tuv.com