

Verantwortlichkeiten und Risiken im Umfeld der Informationssicherheit

Kreiswirtschaftsförderung Mettmann
27. Oktober 2009

Osfried Tillmanns, Business Consulting, Informationssicherheit

Zur Person

SIEMENS

Siemens Enterprise
Communications GmbH & Co KG

Zweigniederlassung Essen
Paul-Klinger-Straße 7 - 11
45127 Essen

Osfried Tillmanns

Business Consulting

Tel.: +49 89 7007-21281
Fax: +49 89 7007 14 -21281
E-Mail: osfried.tillmanns
@siemens-enterprise.com

Geschäftsmäßige Anforderungen, Verpflichtungen und Interessen

SIEMENS

Informationen sind in modernen
„**wissensbasierten Organisationen**“
von unschätzbarem Wert

Rechtliche Vorgaben Compliance	Eigeninteresse	Anforderungen Dritter
<ul style="list-style-type: none">• Gesetz zur Kontrolle und Transparenz in Unternehmensbereichen, Sorgfaltspflichten (KonTraG, AktG, GmbHG, BGB)• Datenschutz (BDSG, TKG, etc.)• Allgemeine Geheimhaltungspflichten / Bankgeheimnis, Fernmeldegeheimnis (KWG, StGB, HGB, BGB)• Auskunft- und Nachweispflichten (GoBS/BMF, HGB, Steuerrecht, GDPdU ...)• Sarbanes Oxley Act - SOX	<ul style="list-style-type: none">• Sichere Geschäftsprozesse• Schutz von Informationen und Wissen (Spionage)• Schutz der Investitionen und Infrastrukturen• Image in der Öffentlichkeit• Anpassung an verändertes Umfeld: W wie Wireless!• Kredit-Rating, Basel II• Risikoabsicherung Solvency II	<ul style="list-style-type: none">▪ Kunden fordern zuverlässige Serviceleistungen▪ Kunden fordern Schutz der Daten▪ Investoren fordern Corporate Governance▪ e-business Security Anforderungen

Beispiele ohne Anspruch auf Vollständigkeit

Über welche Risiken reden wir?

- x unbefugter Zugriff auf Informationen**
- x Gesetzliche Vorgaben und Verbindlichkeiten**
- x Sicherheit der Geschäftsprozesse**

- Die **Wirtschaftsspionage** hat weiter an Bedeutung gewonnen.
- Fremde Nachrichtendienste versuchen von deutschen Wirtschaftsunternehmen illegal Know-how zu erlangen.
- Nach aktuellen Opfer- und Dunkelfeldstudien wurde ein großer Teil aller Firmen bereits ausspioniert, **kleine** und **mittelständische** ebenso wie große **Konzerne**.
- Die Schäden für das ausgespähte Unternehmen können **existenzbedrohende Ausmaße** annehmen.
- Man schätzt den jährlichen Schaden im Bereich der Wirtschaftsspionage derzeit auf rund **30 Milliarden Euro** sowie **70.000 Arbeitsplätze**, aufgrund der hohen Dunkelziffer ist der Schaden eher höher.

Das Bundesamt für Verfassungsschutz

- Starke **Zunahme von elektronischen Angriffen**, Maßnahmen mit und gegen die IT-Infrastrukturen.
- Aktivitäten, die neben der Informationsbeschaffung auch zur **Schädigung und Sabotage dieser Systeme** geeignet sind.
- Der überwiegende Teil der Betroffenen **erkennt die illegalen Handlungen** im Zusammenhang mit Wirtschaftskriminalität und Wirtschaftsspionage, zum Beispiel Einsatz professioneller Spionagesoftware, **nicht**.
- Ein besonderer **Risikofaktor** in der digitalisierten Welt sind die **modernen IuK-Systeme**.
- **Kritische Unternehmensdaten** liegen in elektronischer Form vor und werden bei Bedarf in Sekundenschnelle übertragen.
- Starker Zuwachs bei der Überwachung und Analyse von Markt und Konkurrenz - **Competitive Intelligence (CI)** – als (cio.de vom 13.07.2009)

Datenschutz & Bußgeld

Freitag, 23. Oktober 2009, 16:12 Uhr

manager-magazin.de

Home **Unternehmen** Finanzen Technologie Karriere Lifesty

Home > Unternehmen

23.10.2009

Datenaffäre

Bahn akzeptiert Millionenbußgeld

Die Deutsche Bahn zahlt wegen jahrelangen Missbrauchs ihrer Mitarbeiterdaten mehr als 1,1 Millionen Euro Bußgeld - das höchste Bußgeld, das eine deutsche Daten-Aufsichtsbehörde jemals verhängte. Sonderermittler der Affäre fordern jetzt strafrechtliche Konsequenzen.

Berlin - Einer der Sonderermittler in der Affäre, der frühere Bundesinnenminister Gerhart Baum, forderte die Staatsanwaltschaft auf, nun zügig gegen die Straftäter vorzugehen. Das Bußgeld beträgt genau 1.123.503,50 Euro, wie Dix mitteilte. Damit würden alle "bekanntgewordenen Datenschutzverstöße bei der Deutschen Bahn geahndet, soweit sie nicht verjährt sind", wie der Berliner Datenschutzbeauftragte Alexander Dix am Freitag mitteilte.

- Die Deutsche Bahn zahlt wegen jahrelangen Missbrauchs ihrer Mitarbeiterdaten mehr als 1,1 Millionen Euro Bußgeld.
- Ein Sonderermittler forderte die Staatsanwaltschaft auf, nun zügig gegen die Straftäter vorzugehen.
- Grube schuf beim Umbau der Konzernspitze einen eigenen Vorstandsposten für die Ressorts Compliance, Datenschutz und Recht.
- Werden nun verantwortliche frühere Bahnbeschäftigte von dem Konzern in Regress genommen?

**Die Verantwortlichkeiten
beim Betrieb von Informations- und
Kommunikationssystemen
ergeben sich aus den
rechtlichen Rahmenbedingungen**

Rechtliche Rahmenbedingungen ...

... ergeben sich aus einer Vielzahl von Gesetzen und Vorschriften mit unterschiedlichen Zielrichtungen.

Zu unterscheiden sind:

- **öffentlich rechtliche Vorgaben,**
z.B. Datenschutz oder FernmeldeRecht
- **zivilrechtliche Haftung,**
z.B. §§ 91,93 AktG ⇒ KontraG,
oder § 43 GmbHG,
- **Branchenspezifische Vorgaben und Verpflichtungen,**
- **strafrechtliche Verantwortlichkeit,**
z.B. §§ 14, 201, 202a, 203, 204, 206, 303a, 303b StGB
(Handeln für andere, Vertraulichkeit des Wortes, Brief- oder Fernmeldegeheimnis, Ausspähen von Daten, Verletzung-/ Verwertung von Geheimnissen, Datenverfälschung, Computersabotage)

Hintergrund und Auswirkungen von KonTraG

SIEMENS

Mit der Einführung des **G**esetzes zur **K**ontrolle und **T**ransparenz im Unternehmensbereich (KonTraG) am 1.5.1998 wurde gesetzlich festgelegt, dass Aktiengesellschaften **ein Risiko-Früherkennungssystem zu implementieren** haben (gem. §91 Abs. 2 AktG).

Der §91 Abs. 2 ist auch vor dem Hintergrund von Schadensersatzverpflichtungen (gem. §93 Abs. 2 AktG) und der erleichterten Möglichkeit zur **Geltendmachung von Ersatzansprüchen** (gem. §147 AktG) zu sehen.

Im Zusammenhang mit §76 Abs. 1 des AktG ergeben sich hieraus **Organisationspflichten des Vorstandes** zur Sicherung des Unternehmensfortbestandes.

Lt. Aktiengesetz kommt eine **persönliche Haftung des Vorstandes** dann in Betracht, wenn er Entwicklungen im Unternehmen, nicht durch ein Risikomanagement überwacht und durch geeignete Maßnahmen vorbeugt (§ 91 Abs. 2 und § 93 Abs. 2 AktG).

Verantwortlichkeiten zur Informationssicherheit



Auch **Geschäftsführer** einer GmbH sind persönlich haftbar, sie haben die "**Sorgfalt eines ordentlichen Geschäftsmannes**" aufzubringen (§ 43 Abs. 1 GmbHG). In dieser Formulierung wird eine entsprechende Folgerung für das Risikomanagement impliziert, in Analogie zu KonTraG.

Ähnliches gilt für **andere Gesellschaftsformen**, wie etwa für Kommanditgesellschaften oder die Offene Handelsgesellschaften. **Gleichstellung bezüglich der Rechtspflichten zur Informationssicherheit gegenüber den Kapitalgesellschaften**, sofern keine natürliche Person als persönlich haftender Gesellschafter eingesetzt ist.

Kommen die Verantwortlichen - Vorstand oder Geschäftsführung - der beschriebenen Risikovorsorgepflicht nicht nach und entsteht dadurch dem Unternehmen ein finanzieller Schaden, kann dies zu einer **persönlichen Haftung** der Mitglieder des Vorstands und der Geschäftsführung, unter Umständen auch der Aufsichtsratsmitglieder führen.

Verantwortlichkeiten von Geschäftsführern, Vorständen

SIEMENS

Haftungsrelevante Gesetze:

- KonTraG
 - §§ 91, 93 **AktG**
 - § 43 **GmbHG**
Sorgfaltspflicht, Haftung & Schadensersatzpflicht
- § 289 HGB, Lagebericht
- § 78 BBG Schadensersatzpflicht bei vorsätzlicher oder grob fahrlässiger Pflichtverletzung von Beamten.
- § 14 StGB, Handeln für andere als vertretungsberechtigtes Organ oder als vertretungsberechtigter Gesellschafter.

Ableitung der Verantwortlichkeiten ...

1. ... aus der Funktion

- Vorstand der Aktiengesellschaft (§ 93 Abs. 1 AktG)
- Geschäftsführer der GmbH (§ 43 Abs. 1 GmbHG)

„... die **Sorgfalt eines ordentlichen Geschäftsmanns** anzuwenden.“

2. ... aus dem Arbeits- oder Anstellungsvertrag (§ 276 BGB)

„Der Schuldner hat **Vorsatz** und **Fahrlässigkeit** zu vertreten. **Fahrlässig handelt**, wer die im Verkehr **erforderliche Sorgfalt** außer Acht lässt.“

3. ... aus weiteren Gesetzen

- Produkthaftung
- Datenschutz
- Urheberrecht
- Vertrauenshaftung ...

Haftung der Organe und deren Vertreter

Eigenes Verschulden

- **Organisationsverschulden** – mangelnde Organisation bei der Positionierung relevanter Entscheidungskompetenzen und Prüfungspflichten von wichtigen bzw. kritischen Aufgabengebieten bei den „**verfassungsgemäß berufenen Vertretern**“ oder deren Organen (Geschäftsführer oder Vorstände).
- § 14 StGB, Handeln für eine andere Person als vertretungsberechtigtes Organ einer juristischen Person oder als Mitglied eines solchen Organs oder als vertretungsberechtigter Gesellschafter einer rechtsfähigen Personengesellschaft.

Datenschutzbeauftragter

§ 4g BDSG Aufgaben des Beauftragten für den Datenschutz

§ 3a BDSG Grundsatz der **Datenvermeidung**

§ 4 BDSG **Verbot der Erhebung** personenbezogener Daten

§ 5 BDSG Festlegung des **Datengeheimnisses**

§ 9 BDSG **Notwendige technische & organisatorische Maßnahmen**
> insbesondere Anlage zu § 9 BDSG

§ 28 Datenerhebung nur für **eigene Zwecke**

§ 823 I, II BGB **Haftung gegenüber Betroffenen**

Betroffene Rollen

- Geschäftsführer, Vorstände
- CIO
- Betriebsrat, Personalrat
- Datenschutzbeauftragte
- IT-Leiter, Administratoren,
- IT Sicherheits-Beauftragte
- IT Dienstleister
- interne Revision

Weitere Anforderungen und Auswirkungen

Ordnungsmäßiger IT-Betrieb

(gemäß Revisionshandbuch GoB/GoDV)

SIEMENS

Einhaltung gesetzlicher Vorgaben und ordnungsgemäßer Betrieb der Informations- und Kommunikationssysteme (ICT) bezüglich der:

- **Auftragsbindung**
Ordnungsmäßigkeit, Erkennung der Kosten- bzw. Ertragsentwicklung und Vermeidung unregelter Arbeitsweise mangels Vorgaben.
- **Urschrifttreue**
Sicherstellung ordnungsgemäßer Führung von Beleg- und Buchnachweisen.
- **Kontrollierbarkeit**
Vermeidung fehlerhafter Datenbestände, inkonsistenter Prozesse oder Daten, fehlerhafter Gebrauch und Auswertung von Daten oder Programmen.
- **Transparenz**
Sicherstellung geregelter Arbeitsweisen, kontrollierte Aufgabenerfüllung, Auskunftsfähigkeit, beweiskräftige Nachweise, geordnete Pflege von Verfahren und Programmen sowie geregeltes und ordnungsgemäßes Reporting.
- **Funktionssicherheit**
Schutz vor Betriebsunterbrechungen, Datenverlust, Systemausfällen, nicht möglicher Datenwiederherstellung, Katastrophenanfälligkeit, Festlegung auf unwirtschaftliche oder störanfällige Arbeitsweisen, Fehler für die sich keiner verantwortlich fühlt und erhöhte Kosten.

Steuerliche Anforderungen GDPdU

GDPdU

Grundsätze zum Datenzugriff und die Prüfung digitaler Unterlagen

- Ziel - Beschleunigung und höhere Effizienz der Außenprüfungen
- Umsetzung - Zugriff der Finanzverwaltung auf die Teile der Unternehmens-DV, in denen steuerlich relevante Daten erzeugt oder verarbeitet werden

Betroffene Daten:

- Finanzbuchhaltung
- Anlagenbuchhaltung
- Lohn- und Gehaltsbuchhaltung
- aber auch...
... steuerlich relevante Daten in anderen Bereichen des DV-Systems, welche Einfluss auf das Betriebsergebnis haben

Wirtschaftsprüfung nach IDW PS 330/331

Gesetzlicher Auftrag:

Der Jahresabschluss eines Unternehmens hat unter Beachtung der Grundsätze ordnungsgemäßer Buchführung ein den tatsächlichen Verhältnissen entsprechendes Bild der Vermögens-, Finanz- und Ertragslage zu vermitteln (§264 HGB).

Ein Wirtschaftsprüfer hat seine Prüfung so anzulegen, dass Unrichtigkeiten und Verstöße gegen diese Pflicht erkannt werden (§§ 317 HGB).

Prüfungsumfang ist eingeschränkt auf IT-Systeme die dazu dienen, Daten zu verarbeiten die direkt oder indirekt „rechnungslegungsrelevant“ sind, d.h. für:

- Buchführung
- Jahresabschluss
- Lagebericht

Das heißt: alle IT-Systeme, durch deren Gefährdung dem Unternehmen oder dessen Eigentümern ein wirtschaftlicher Schaden entstehen könnte.

Der Sarbanes-Oxley Act (SOX)

Internes Kontroll-System

SIEMENS

Der Sarbanes-Oxley Act (SOX) betrifft alle Unternehmen, deren Aktien an US-amerikanischen Börsen notiert sind. SOX soll nach den Bilanzskandalen in Amerika (Enron) und Europa (Parmalat) das Vertrauen der Anleger wieder stärken. Die zwei wichtigsten Paragraphen dieses Gesetzes sind Section 302 und Section 404.

Section 302

- Die erforderlichen Veröffentlichungen (**Bilanzen etc.**) müssen **vollständig** und **richtig** sein.
- **CEO und CFO** müssen eine **eidesstattliche Erklärung** bei der Börsenaufsichtsbehörde (SEC) für die Korrektheit der Finanzberichte abgeben.

Section 404

- Das Management muss ein **effizientes internes Kontrollsystem** für finanzielles Reporting implementieren und warten.
- Unternehmen sind dazu verpflichtet die **Wirksamkeit** des **internen Kontrollsystems (IKS)** für die Finanzberichterstattung explizit zu bestätigen.

Gesetze alleine schützen nicht

Gibt es dennoch Einbrecher, obwohl Einbruch strafbar ist?

Beispielsweise:

§ 303a StGB Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§ 303b StGB Computersabotage

(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht oder

2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

Täterschaft

In Deutschland gehen gemäß Bundeskriminalamt zwei Drittel aller beabsichtigten oder unbeabsichtigten Systemangriffe auf das Konto von **eigenen Angestellten.**

(Quelle: <http://finanzen.focus.msn.de/D/DA/DAE/DAE47/dae47.htm>)

Probleme im IT-Betrieb: Viren-/ Spam-Filterung

SIEMENS

Der NICHT-Einsatz von Antiviren- oder Antispamsoftware kann für die Geschäftsleitung haftungs- und strafrechtliche Konsequenzen haben (LG Hamburg 401 O 63/00 vom 18.07.2001).

Ohne arbeitsrechtlich wirksame Regelungen des betrieblichen Einsatzes von Antiviren- oder Antispamsoftware ist ein **Straftatbestand** erfüllt.

Strafrechtstatbestände

§ 206 StGB, Verletzung des Post- oder Fernmeldegeheimnisses

Tathandlung:

Unterdrücken einer dem Unternehmen zur Übermittlung anvertraute Sendung.

Strafe:

Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

Ein konkreter Fall

OLG Karlsruhe 1Ws 152/04 (vom 10. Januar 2005)

Das Tatbestandsmerkmal des „Unterdrückens“ im Sinne des § 206 StGB wird durch das Ausfiltern von Emails erfüllt.

Gibt es Rechtfertigungsgründe dennoch zu filtern?

theoretisch ja, praktisch nein.

„Die Herausfilterung kann gerechtfertigt sein, wenn die Emails mit Viren behaftet sind.“

Weitere Urteile

Manager haften bei Nichteinführung eines Risikomanagementsystems für den Datenverlust persönlich;
"ARAG-Garmenbeck"-Entscheidung des BGH v. 21.04.1997

Schadensersatz bei Verbreitung eines Computervirus, aufgrund des Einsatzes eines veralteten Virenprogramms;
- LG Hamburg, Urteil vom 18.07.2001, Az: 401 O 63/00

Provider ist für Schadensersatz bei Serverausfall haftbar (Web-hosting Vertrag)
Amtsgericht Charlottenburg 208 C 192/01

Urheberrecht: Problem Unterlizenzierung

SIEMENS

§§ 15 ff, § 69 c Abs. 1 Nr. 1 UrhG Vervielfältigungsverbot

Problem: Die Anzahl der tatsächlich genutzten Lizenzen ist höher als die Anzahl der berechtigt genutzten Lizenzen.

Rechtsfolgen:

- zivilrechtliche Haftung
- handelsrechtliche Verantwortung
- strafrechtliche Verantwortung

Urheberrecht: Zivilrechtliche Haftung

SIEMENS

Bereits fahrlässiges Handeln begründet Haftung

Rechtsprechung hat strengen Haftungsmaßstab aufgestellt:
Der Handelnde muss alle zumutbaren Maßnahmen ergreifen, um die Rechtmäßigkeit sicher zu stellen.

Wer haftet?

- § 97 Abs. 1 UrhG
Haftung des Unternehmens auf Schadensersatz
- § 100 UrhG
Verschuldensunabhängige **Mithaftung des Unternehmensinhabers**
- Bei Personengesellschaften:
Der persönlich haftende Gesellschafter

Urheberrecht: Verantwortlichkeit und Rechtsfolge

SIEMENS

Verpflichtung zur Errichtung eines **Risikomanagements** und zur ordnungsgemäßen Unternehmensführung

Lizenzkonformität fällt unter die Risikoüberwachung

Eine Unterlizenzierung erfüllt nicht die Anforderungen an eine Unternehmensführung hinsichtlich der zu erbringenden „**Sorgfalt eines ordentlichen Kaufmanns**“

§ 106 Abs. 1 UrhG

Rechtsfolge: Geldstrafe oder Freiheitsstrafe bis zu 3 Jahren

Achtung: Dabei reicht es aus, wenn der Täter die Rechtswidrigkeit der Nutzung für möglich hält und sie billigend in Kauf nimmt.

Operatives Risikomanagement in der IuK-Technik

Zum Auftrag des operativen Risikomanagements

SIEMENS

- **Identifizieren**
Erkennen der Unternehmenswerte und Evaluierung der Risiken.
- **Schützen**
Schutz des Unternehmens.
- **Gegensteuern**
Vorbeugen der Bedrohungen und angemessen Entgegenen.
- **Verbessern**
Evaluierung von technologischen Neuerungen und organisatorischer Veränderungen und Treiben der fortlaufenden Verbesserung.

Business Impact

Feststellung der kritischer Auswirkungen (Business Impact)

- **Quantitativ** nach monetären Gesichtspunkten,
 - wie z. B. nach KonTraG meldepflichtige Wertgrenzen
 - existenzbedrohende Werte

- **Qualitativ** z. B. Compliance-Erfüllung
 - gesetzlich
 - behördlich
 - vertraglich

- Skalierung nach Schadensklassen

- Zuordnung des möglichen Schadens bei Verlust der
 - Vertraulichkeit – Confidentiality (**C**)
 - Integrity – Integrität (**I**)
 - Verfügbarkeit – Availability (**A**) und der kritischen Ausfallzeiten

Gebräuchliche Standards zum Risikomanagement in der IT

SIEMENS



CobiT

Ursprünglich 1995 von der (U.S.) Information Systems Audit Control Association (ISACA) entwickelt (Seit 2004: Version 4.0)

- IT Governance Framework einschließlich IT-Sicherheit
- Überwiegend in den USA genutzt

IT Grundschutz

Entwickelt vom Bundesamt für Sicherheit in der Informationstechnologie (BSI) basierend auf dem „OrangeBook“ seit 1994, beinhaltet:

- ISO/IEC 27001 (ISMS) mit
- BSI-Standard Serie 100-1, 100-2 und 100-3
- Grundschutzkatalog



ISO/IEC 27001 Informationssicherheitsmanagementsystem (ISMS)

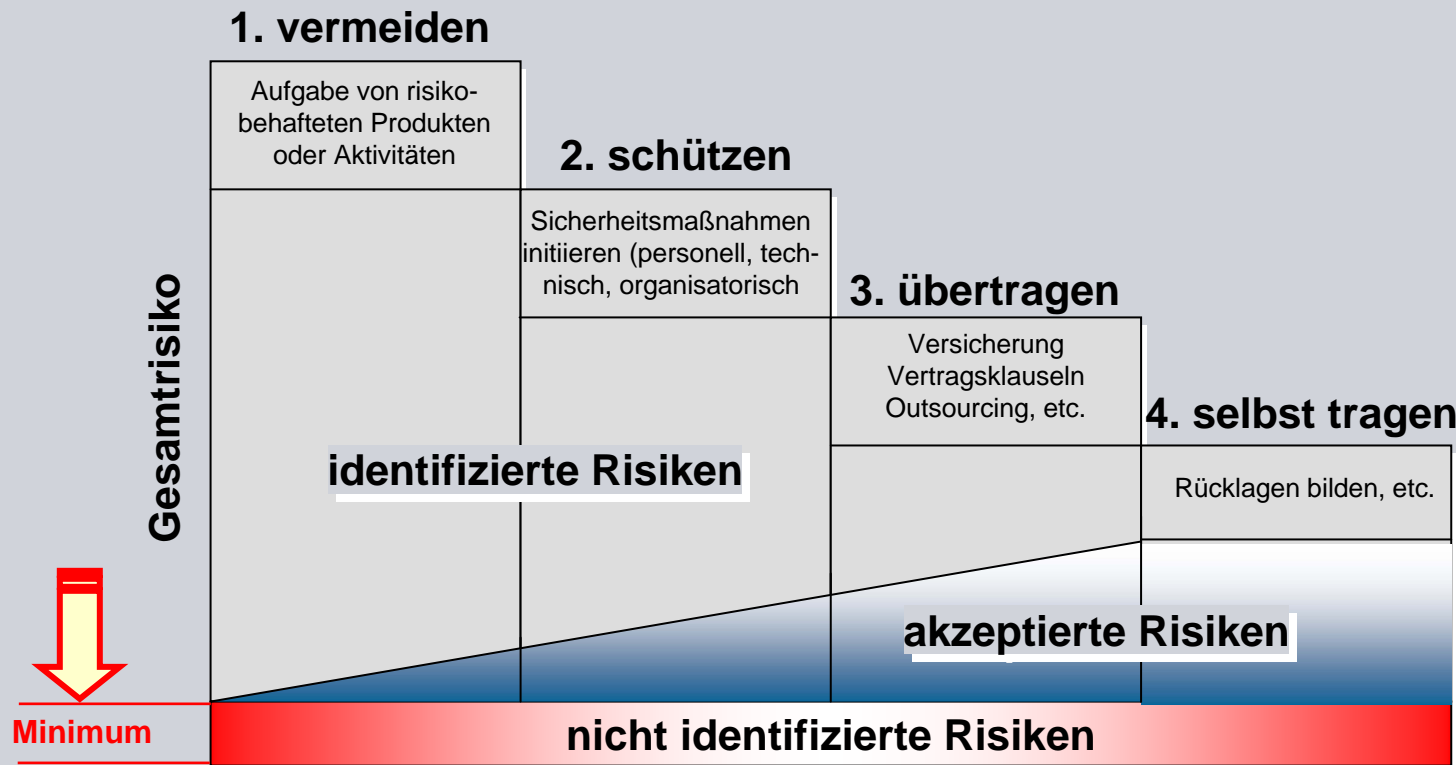
Entwickelt vom British Standards Institute (BSi) im Jahr 1995 als BS 7799 (Teil 1 und 2)

- ISO/IEC 27001:2005 basierend auf Teil 2: „Information Security Management System“
- ISO/IEC 17799:2005 basierend auf Teil 1: „Code of Practice“
- (zus. BS 7799-3:2006 „Guidelines for Information Security Risk Management“)



Risikobehandlung

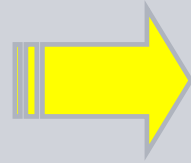
Die Handlungsalternativen beim Risikomanagement lassen sich in vier Klassen einteilen:



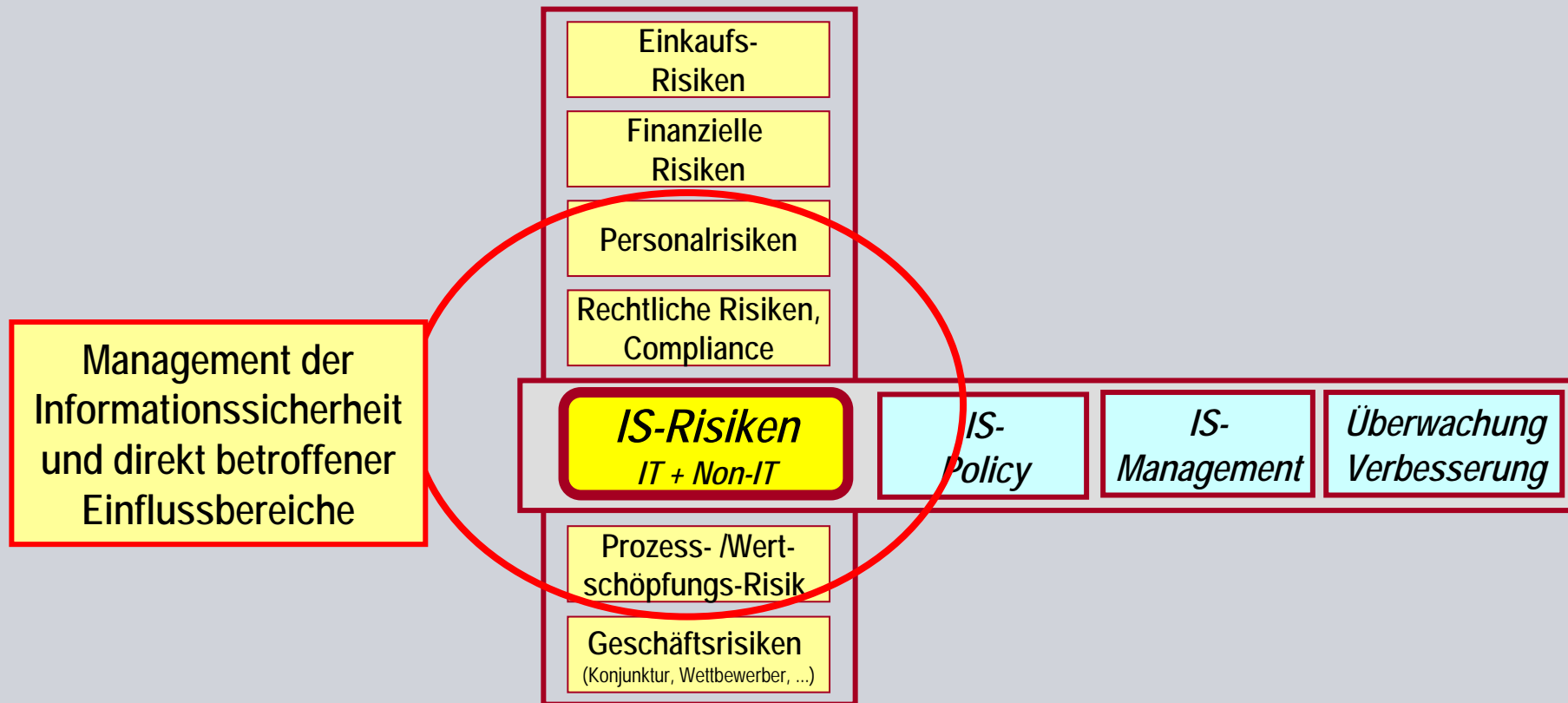
Der Risikoidentifikation kommt höchste Bedeutung zu!

Informationssicherheit im Fokus des Risikomanagements

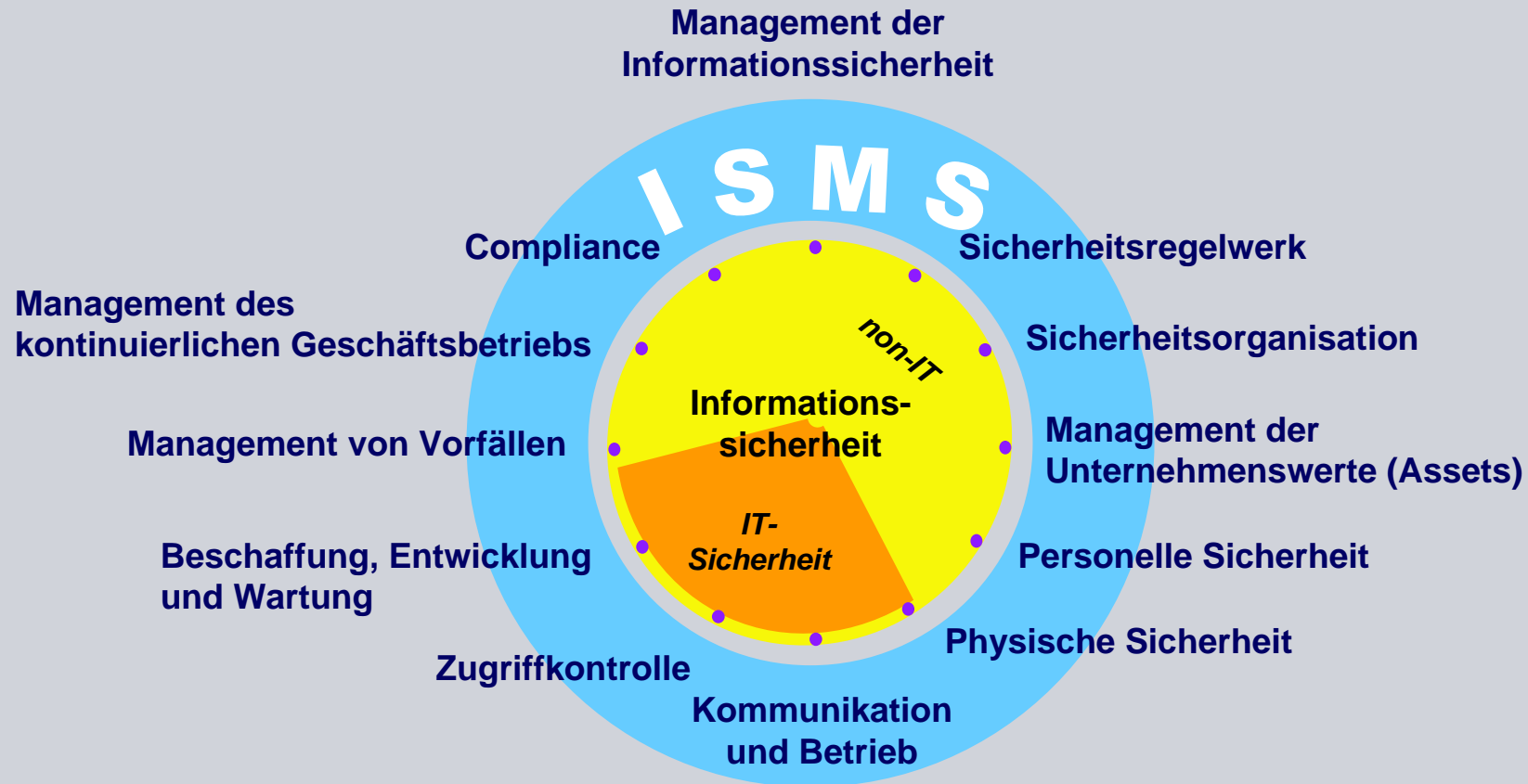
KonTraG
fordert:



Corporate
Risk Management

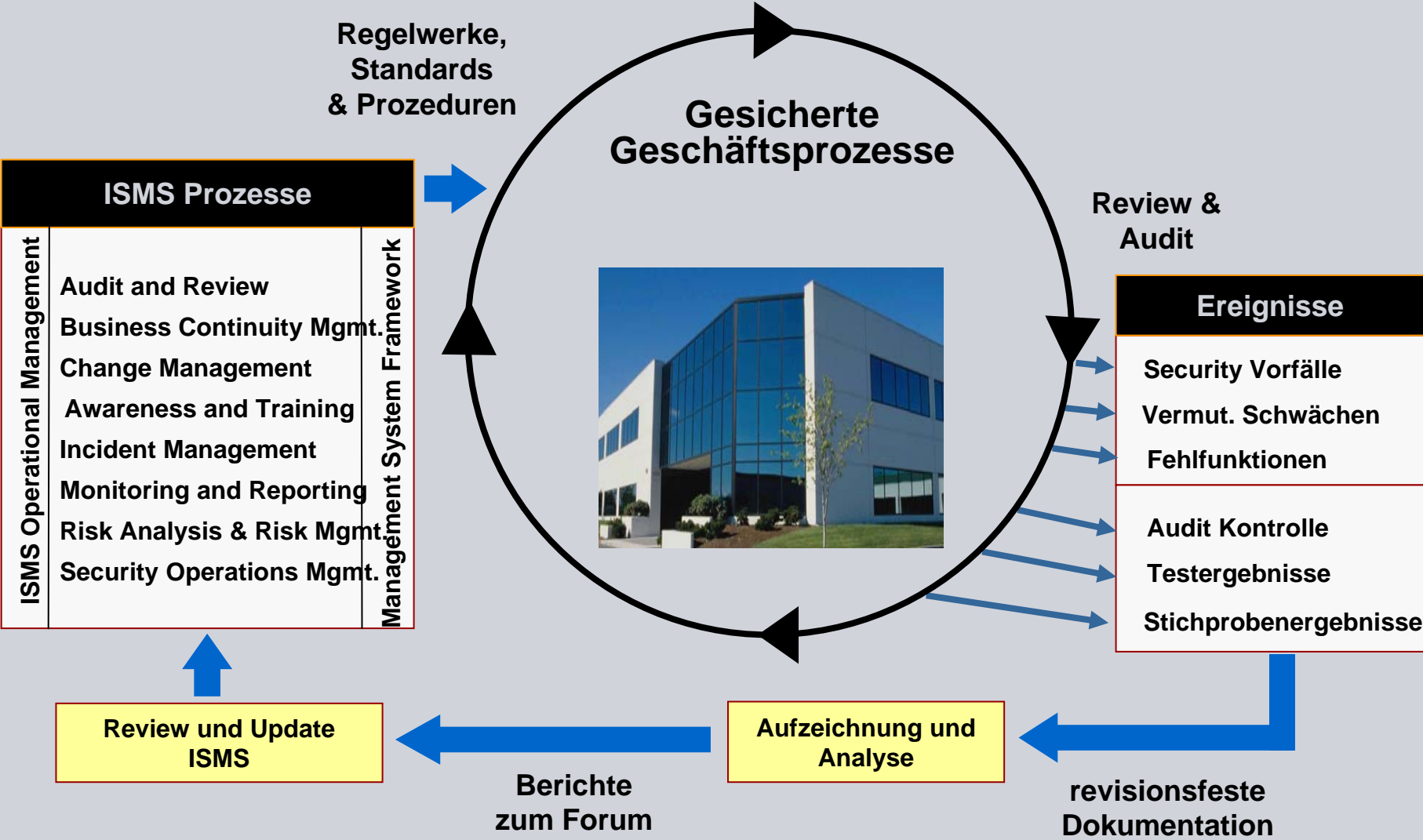


Informationssicherheit oder IT-Sicherheit ?



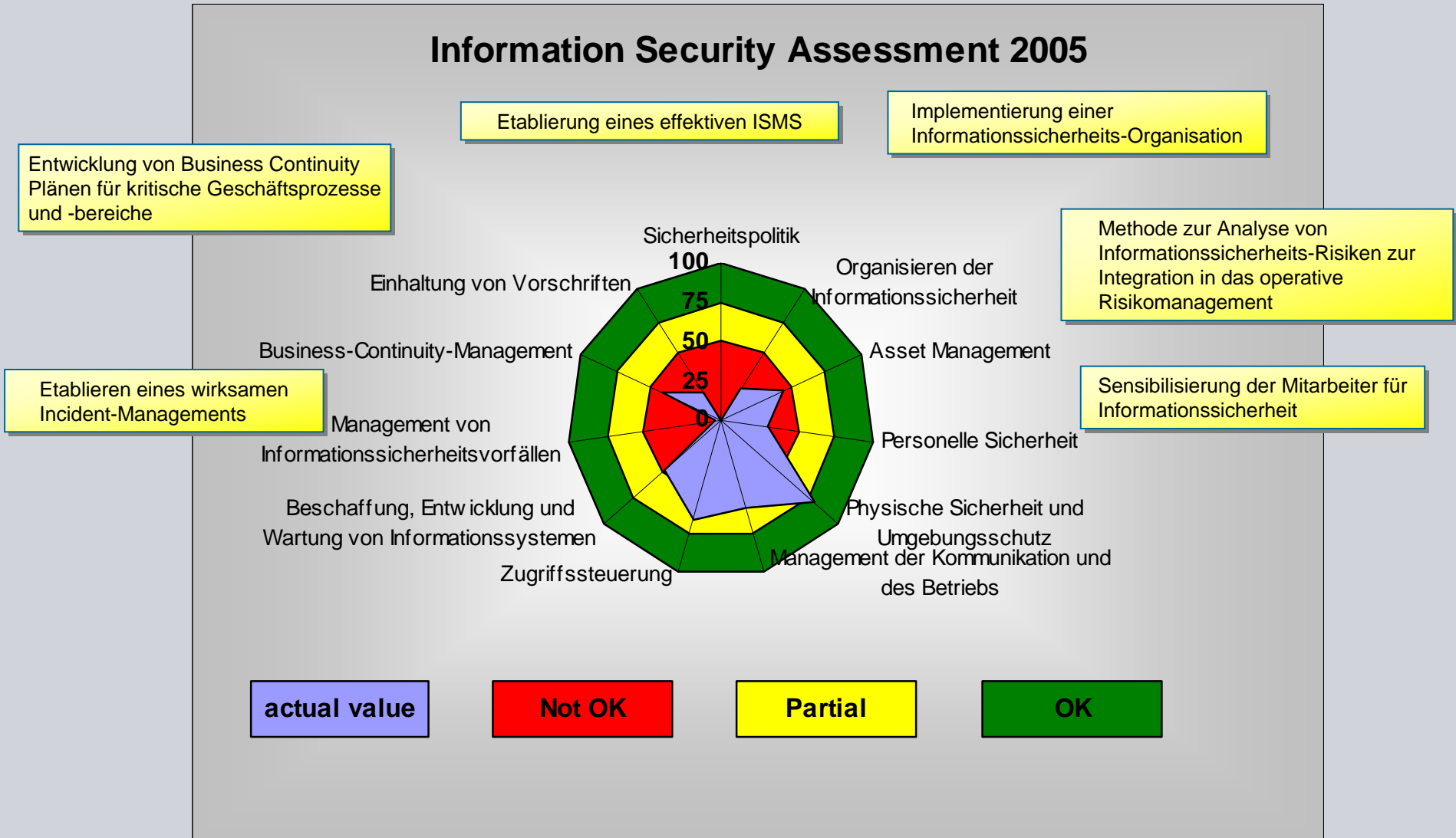
Die Informationssicherheit – gemäß ISO 27001 - umfasst die Geschäftsprozesse und damit den Geschäftsbetrieb.

**Qualitätsmanagementprozess:
Informationssicherheit, Plan –Do – Check – Act**



Assessment, Beispiel für identifizierte Handlungsfelder

Information Security Assessment 2005



**Danke für Ihre Aufmerksamkeit,
Fragen?**

SIEMENS

