

Dokumentation der Informationssicherheit

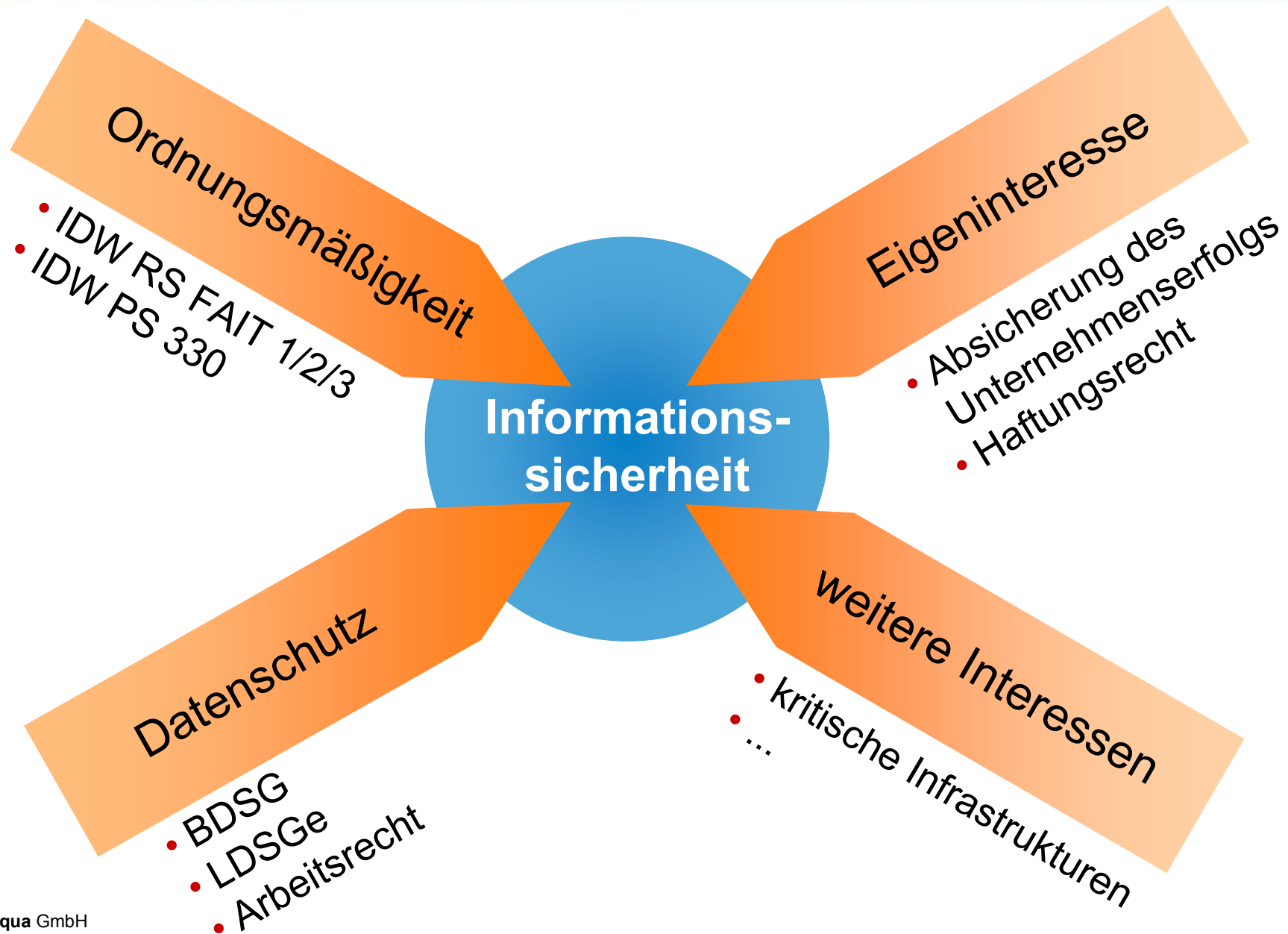
Systems 2007
Security Area

Lothar Goecke



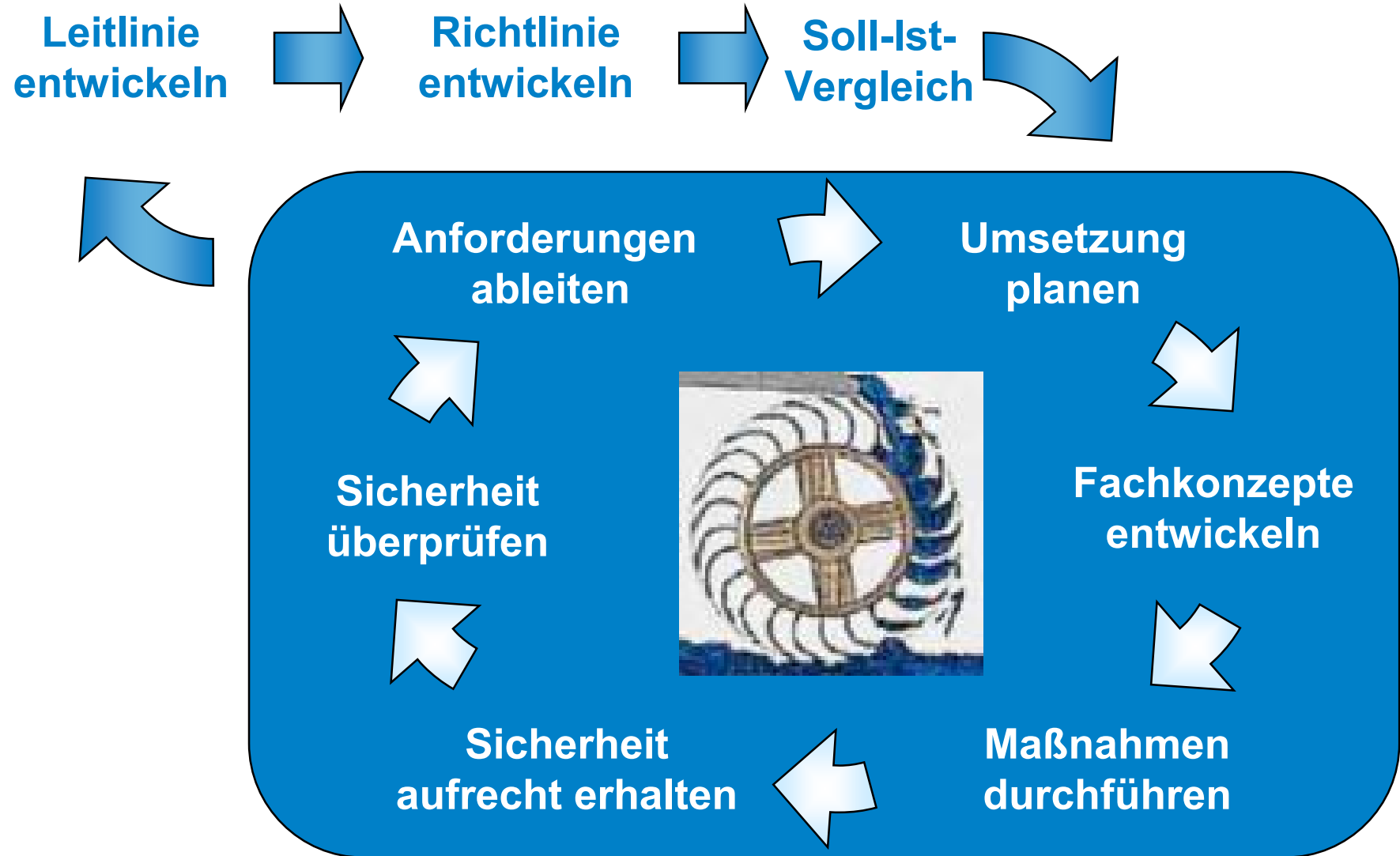


Informationssicherheit als Diener mehrerer Herren



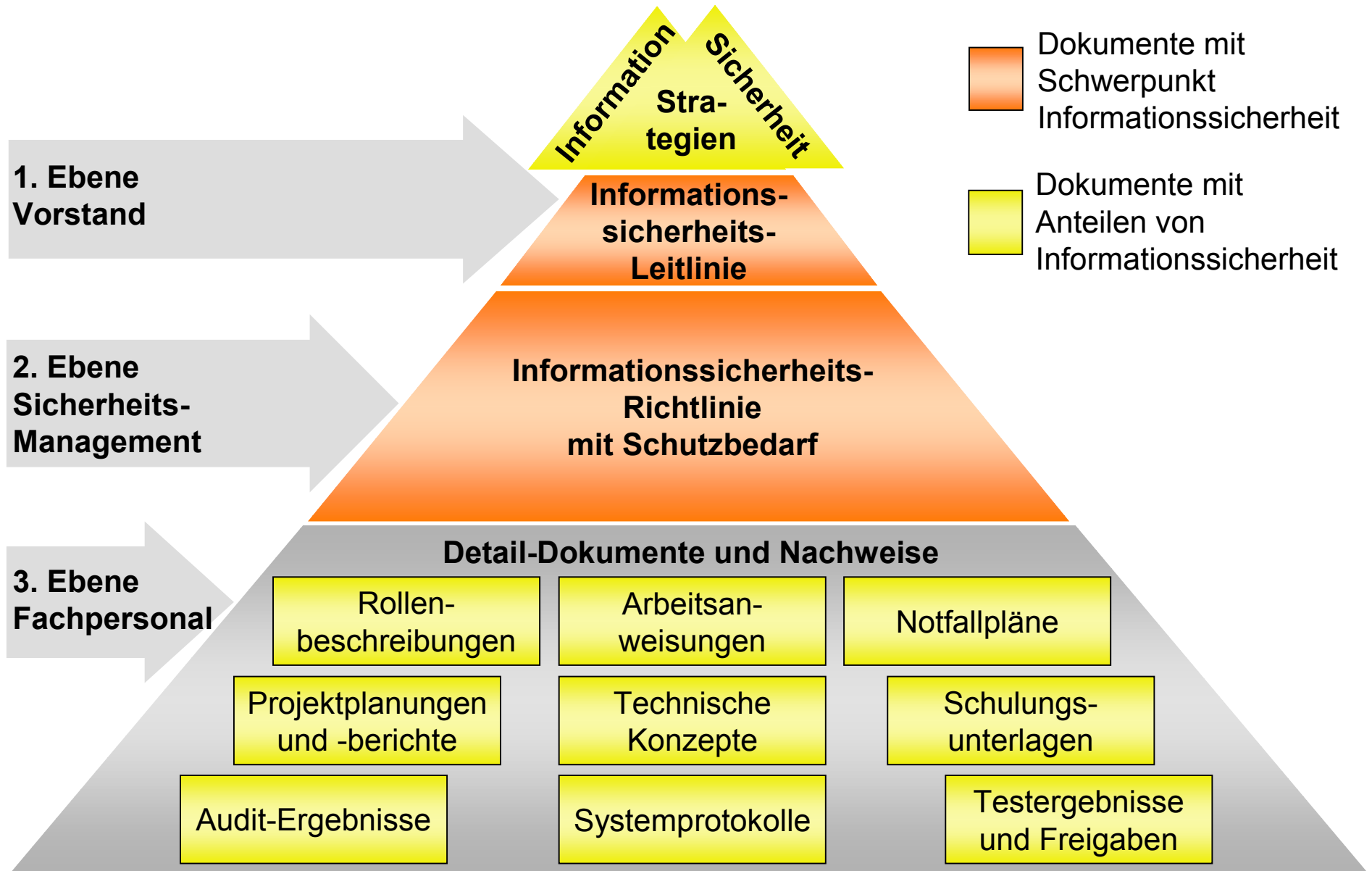


Informationssicherheit: Regelkreis





Dokumentationspyramide Informationssicherheit





Dokumentationsanforderungen

- Informationssicherheits-Leitlinie
 - gesetzliche Vorgaben
 - Verankerung Informationssicherheits-Management
 - zur Verdeutlichung der Unternehmensaufgabe
- Informationssicherheits-Richtlinie
 - Schutzbedarf
 - Anforderungen an Maßnahmen
 - zur Absicherung der Angemessenheit (ausreichend, wirtschaftlich)
- Detaildokumentation
 - Prozessbeschreibungen, Arbeitsanweisungen
 - Fachkonzepte, Produktbeschreibungen
 - für tägliche Arbeit
- Nachweise
 - Systemprotokolle, Tätigkeitsnachweise
 - Audit-Protokolle
 - für Vorfallsbearbeitungen und Prüfungen



Dokumentationsstrategie der consequence

- Informationssicherheits-Leitlinie
- Informationssicherheits-Richtlinie
 - enthält Regeln für die Informationssicherheit
 - verweist auf Detaildokumentation
 - Anwenderkreis sind Mitarbeiter mit besonderer Sicherheits-verantwortung (z.B. Stabsfunktionen, Orga-Bereich) und Prüfer
- Detaildokumentation
 - Einbindung detaillierter Prozessbeschreibungen, Arbeitsanweisungen, Konzepte usw. zur Informationssicherheit nach Möglichkeit in bereits existierende Dokumentation
 - z.B. in Organisationshandbuch oder Betriebshandbuch
 - Vermeidung eines zusätzlichen, parallelen Dokumentations-Universums
 - erhöhte Nutzer-Akzeptanz
- Nachweise
 - Unterlagen für Prüfungen oder Forensik



Informationssicherheits-Richtlinie: Textbeispiele

RIM000

Die Steuerung der IT-Risiken ist in das operationelle Risikomanagement des Unternehmens integriert:

- Der IT-Sicherheits-Beauftragte wird rechtzeitig über veränderte Risikolagen und -beurteilungen im Rahmen des operationellen Risikomanagements informiert.
- Ergebnisse aus der Steuerung der IT-Risiken fließen regelmäßig in das operationelle Risikomanagement ein.
- Die IT-Risiken sind dokumentiert und bewertet.

Die gegenseitigen Informationen können direkt zwischen dem Informationssicherheits-Beauftragten und dem Manager für operationelle Risiken ausgetauscht werden. Ein regelmäßiger Dialog ist sinnvoll.

SKA000

Der Zugang zum öffentlichen Internet ist im Rahmen von Arbeitsanweisungen oder Dienstvereinbarungen geregelt. Darin werden mindestens folgende Aspekte behandelt:

- Beantragung und Einrichtung eines Internet-Zugangs,
- zulässige Zugangswege,
- zulässige Anwendungen für den Internet-Zugang,
- zulässiger Nutzungsumfang,
- Veränderung von Browser-Einstellungen,
- Verwendung von Plug-Ins und Erweiterungen,
- Down- und Upload von Dateien.



Informationssicherheits-Richtlinie: Textbeispiele

VIS300

Alle Meldungen, die auf einer zentralen Meldestelle auflaufen, werden angemessen ausgewertet. Eine Reaktion erfolgt gemäß dokumentierter Verfahren.

Alarmer werden direkt an die Meldestelle des Dienstleisters geleitet. Zusätzlich können Polizei und Feuerwehr direkt einbezogen werden.

ITI300

Die Verfügbarkeit von IT-Komponenten ist entsprechend der ihnen zugeordneten Verfügbarkeits-Schutzbedarfs-Klasse (**SBK sehr hoch, hoch** oder **mittel**) für teilweise und komplette Hardware-Ausfälle einzelner Komponenten abgesichert.

Bei einem Ausfall eines Servers müssen z.B. folgende Aktionen innerhalb der durch die Schutzbedarfs-Klasse festgelegten Verfügbarkeitsziele stattfinden:

- Beschaffung und Aufbau von Ersatzkomponenten,
- Einspielen von Software und Daten,
- Vornehmen von Konfigurationseinstellungen.

Abhängig von der jeweiligen Komponente und ihrem Schutzbedarf können Absicherungskonzepte angefangen von räumlich aufgeteilten Cluster-Systemen über Wartungsvereinbarungen bis hin zu keinerlei vorsorglichen Maßnahmen angemessen sein.



Informationssicherheits-Richtlinie: Gliederung I

0 Dokumentenkontrolle

1 Einleitung

- 1.1 Ziele des Dokuments
- 1.2 Kurzbeschreibung des Inhalts
- 1.3 Grundlagen des Dokuments
- 1.4 Verbindlichkeitsregelung
- 1.5 Anwendung des Dokuments
- 1.6 Abgrenzungen

2 Regeln zu Organisation und Personal

- 2.1 Aufgaben der Vorstandsebene
- 2.2 Aufgaben spezieller Rollen im Rahmen der Informationssicherheit
- 2.3 Aufgaben der Fachbereiche im Rahmen der Informationssicherheit
- 2.4 Informationssicherheits-Aspekte in der Personalpolitik
- 2.5 Sicherheitsbewusstsein und IT-Schulung

3 Regeln für Fachbereiche zum Umgang mit Informationen und der IT

- 3.1 Schutz sensibler Dokumente
- 3.2 Sicherer Umgang mit Sprache
- 3.3 Genereller Umgang mit der IT-Infrastruktur
- 3.4 Nutzung sicherheitskritischer Anwendungen

4 Regeln für IT-relevante Steuerungs- und Verwaltungsprozesse

- 4.1 Steuerung von IT-Risiken
- 4.2 Steuerung von externen Dienstleistern und Partnern
- 4.3 Planung und Entwicklung von IT
- 4.4 Beschaffung und Bereitstellung von IT
- 4.5 Steuerung von Änderungen in der IT
- 4.6 Behandlung von IT-Vorfällen
- 4.7 Notfallvorsorge
- 4.8 Verwaltung von Benutzerkonten
- 4.9 Verwaltung der IT-Sicherheits-Dokumentation
- 4.10 Überprüfung der IT-Sicherheit



Informationssicherheits-Richtlinie: Gliederung II

5 Regeln für die Administration der IT-Infrastruktur

- 5.1 Übergreifende Regeln für die IT-Infrastruktur
- 5.2 Datennetzwerke
- 5.3 Zentrale Server
- 5.4 Arbeitsplatzeinrichtungen
- 5.5 Telefon-Systeme

6 Regeln zur Bereitstellung räumlicher Infrastruktur und von Versorgungseinrichtungen

- 6.1 Standortwahl
- 6.2 Perimeterschutz
- 6.3 Brandverhütung
- 6.4 Schutz gegen Wassereintritt
- 6.5 Klimatisierung
- 6.6 Stromversorgung
- 6.7 Kabelführung
- 6.8 Meldelinien

7 Sicherheitsrelevante Objektklassen

- 7.1 Schutzbedarfsklassen
- 7.2 Wiederanlaufklassen
- 7.3 Informationsklassen
- 7.4 Schadensklassen
- 7.5 Vorfälleklassen
- 7.6 Änderungsklassen
- 7.7 Account-Klassen
- 7.8 Software-Klassen
- 7.9 Netzklassen
- 7.10 PC-Klassen
- 7.11 Raumklassen

A Verweise und Anhänge

- A.1 IT-Struktur und IT-Risiken
- A.2 Aufgaben und Verantwortlichkeiten
- A.3 Informationssicherheits-Dokumentation
- A.4 Literaturverzeichnis
- A.5 Glossar



Informationssicherheits-Richtlinie: Ergebnisse

- konsistente, vollständige Dokumentation der Anforderungen für die Steuerung der Informationssicherheit
 - auf die Voraussetzungen und Bedürfnisse des Unternehmens zugeschnitten
 - kurze, verständliche Regeln
 - klar identifizierbar
 - klare Zuordnung
 - organisatorisch
 - technisch
 - strukturierter Dokumentenaufbau
=> leichte Auffindbarkeit
 - keine organisatorischen oder technischen Details
- Zusatzdokumente
 - Schutzbedarfsfeststellung
 - Nennung von Verantwortlichkeiten
 - Verweise auf nachfolgende Dokumentationsebene



Erleichterung
der Prüfbarkeit



Projekttablauf I

Projektstart

- Durchsicht vorhandener Unterlagen
- Grundlegende Festlegungen

Aufnahme der IT-Umgebung und Dokumentation

- IT-Strukturanalyse
- Überblick vorhandene Schutzmaßnahmen
- Überblick Dokumentationswesen
- Überblick IT-Dienstleister

Schutzbedarfsermittlung

- Ermittlung des Schutzbedarfs kritischer IT-Anwendungen und -Daten
- Festlegung von Sensitivitätsklassen für Informationen

Ableitung des Schutzbedarfs der IT-Umgebung

- Übertragung des Schutzbedarfs auf Server und Netzkomponenten



Beispiel Schutzbedarfsfeststellung

Schutzbedarfsanalyse

ZV-Belegverarbeitung

Schadensbeschreibung

Schadensart	Schadenhöhe
1 Beeinträchtigung des Geschäftsablaufs	1 Beschwerden
2 Negative Außenwirkung / Wettbewerbsnachteile	2 spürbare Kundenverluste
3 Direkte finanzielle Auswirkungen	3 existenzbedrohliche Marktverluste
4 Verstoß gegen Gesetze / Vorschriften / Verträge	
5 Materialverluste	
6 Physische und psychische Schädigung von Personen	

SBK Verfügbarkeit

hoch

Beeinträchtigung des Geschäftsablaufs: deutliche Einschränkungen
Verstoß gegen Gesetze / Vorschriften / Verträge: geringe Strafen / Haftungsschäden
Negative Außenwirkung / Wettbewerbsnachteile: Beschwerden

SBK Integrität

hoch

Direkte finanzielle Auswirkungen: gering
Negative Außenwirkung / Wettbewerbsnachteile: spürbare Kundenverluste

SBK Vertraulichkeit

hoch

Negative Außenwirkung / Wettbewerbsnachteile: spürbare Kundenverluste

Kundendaten Informations-Schutzklasse



Beispiel Maßnahmen

	Verfügbarkeit	Vertraulichkeit	Integrität
sehr hoch	Personenschleusen / videoüberwachte Unterbringung 24/7		
	Abschirmung durch interne Firewall		
	proaktive 24/7 Überwachung der IT-Systeme		
	geographisch verteilter Failover Cluster mit synchr. Datenspiegelung	sicher verschlüsselte Datenspeicherung & -übertragung	
	Notstromaggregat	starke 2-Faktor Authentisierung	
hoch		elektromagnetische Schirmung	
	Notfall-Liefervertrag	Intrusion Detection System	
	nächtliche Rufbereitschaft	verschlüsselte Datenübertragung über unsichere Medien	
	redundante Komponenten (z.B. RAID, NIC, Netz)	erweitertes / abgesichertes Logging mit Auswertung	
	lokale Vorhaltung von Ersatzkomponenten		USV-gesteuerter Shut-Down
mittel		verschlüsselte UserID / Passwort Authentisierung	
	Wartungsvertrag	differenzierte Zugangsrechte	
		einfaches Logging	



Projektlauf II

Verfassen der Richtlinie

- Ermittlung der Sicherheitsregeln

Zuordnung von Verantwortlichkeiten / Integration von Dokumenten

- Zuweisung von Verantwortungsträgern für Sicherheitsregeln
- Verweise auf vorhandene Dokumentation einarbeiten

Abstimmung der Richtlinie

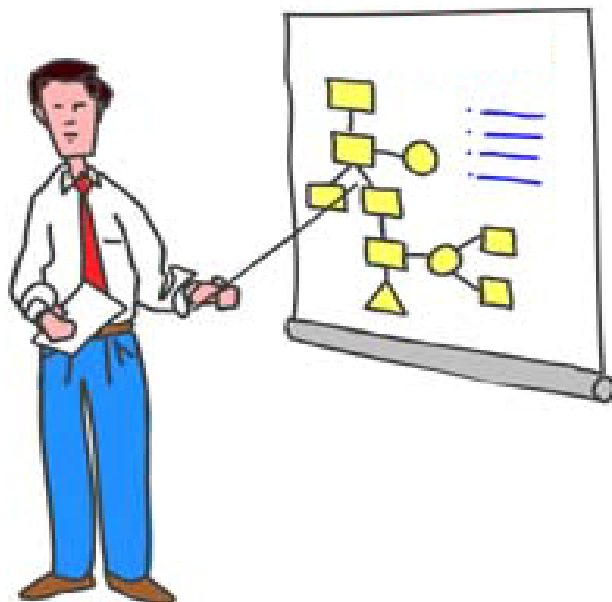
- Abstimmung der Regeln mit Verantwortlichen

Präsentation / Freigabe der Richtlinie

- Vorstellung der Richtlinie
- Inkraftsetzen der Richtlinie durch Geschäftsleitung



Vielen Dank für Ihre Aufmerksamkeit!



Dipl.-Math.

Lothar Goecke

Geschäftsführer

consequa GmbH
Süderstraße 73
20097 Hamburg
www.consequa.de

Tel.: 040 / 78 89 70 62
Fax: 040 / 78 89 70 66
Mob: 0171 / 863 50 17
lothar.goecke@consequa.de