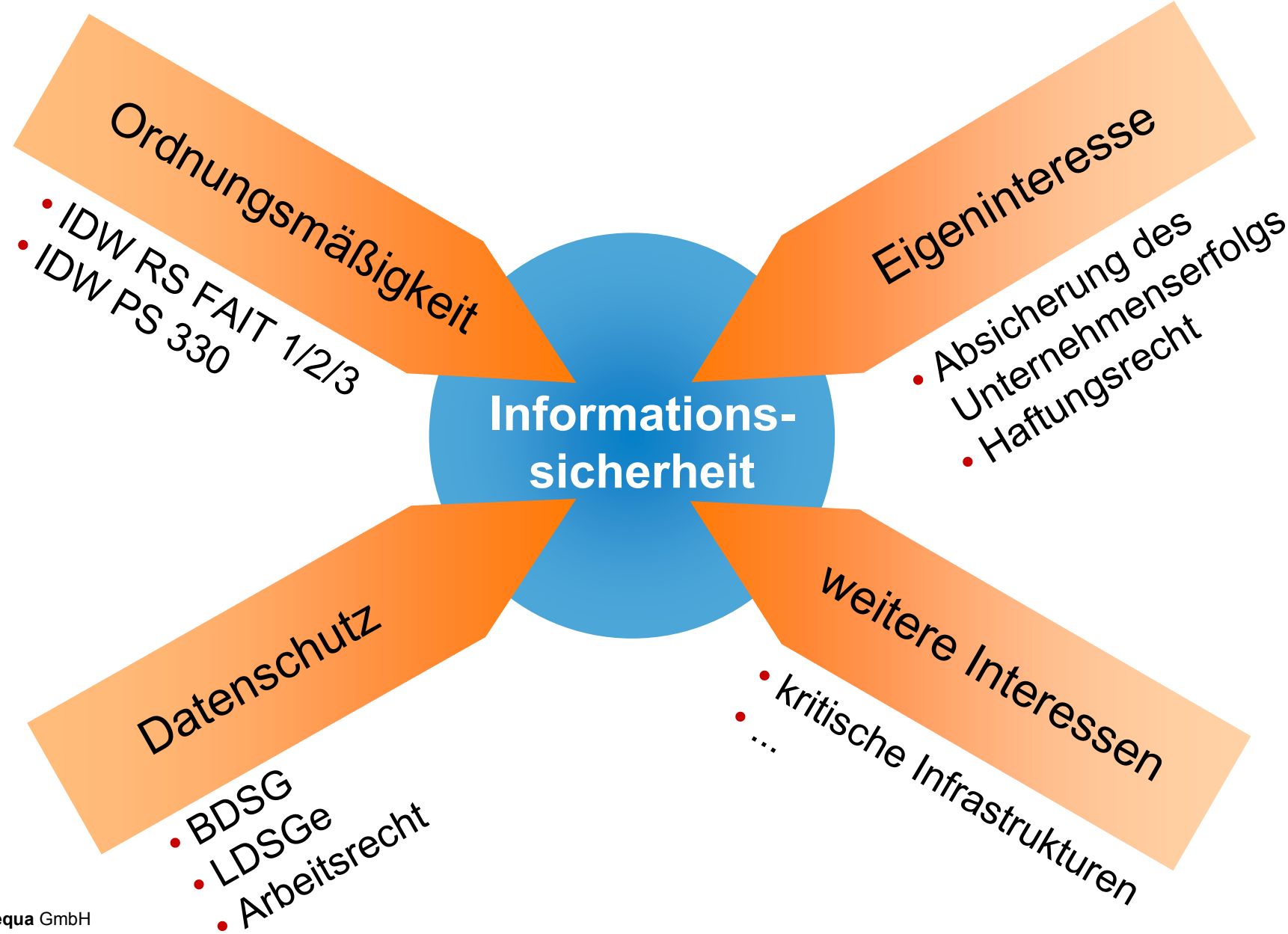
Dokumentation der Informationssicherheit

iSocietyWorld

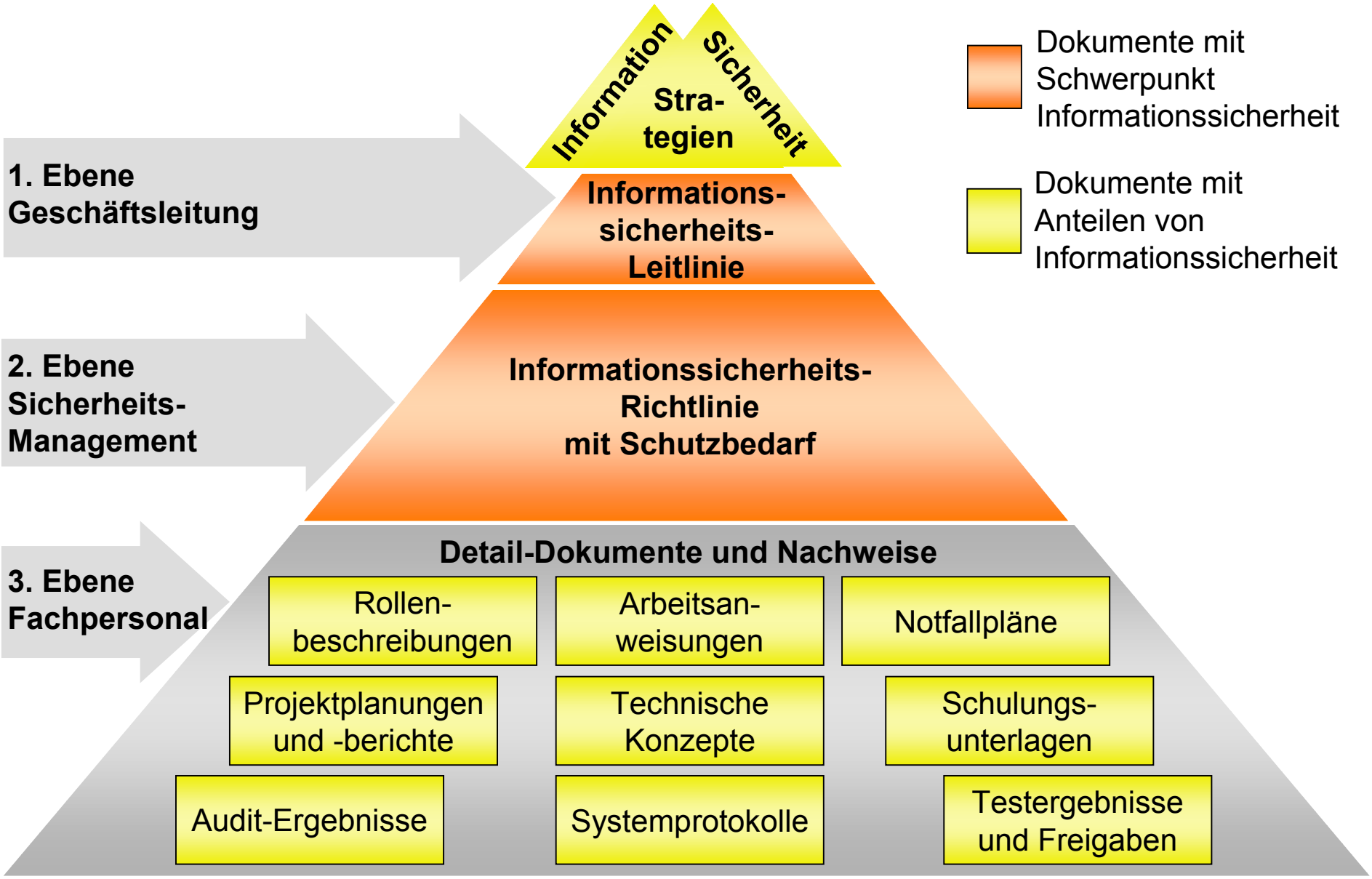
14. November 2007

Lothar Goecke

Informationssicherheit als Diener mehrerer Herren



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 consequa

- Informationssicherheits-Leitlinie
- Informationssicherheits-Richtlinie
  - enthält Regeln für die Informationssicherheit
  - verweist auf Detaildokumentation
  - Anwenderkreis sind Mitarbeiter mit besonderer Sicherheitsverantwortung (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-Leitlinie

Informationssicherheits-Leitlinie

- Dokument auf Strategieebene
  - nimmt Anforderungen aus IT-Strategie und evtl. vorhandener allgemeiner Sicherheitsstrategie auf
  - von Geschäftsleitung erlassen
- Überbau für die IT-Sicherheit im Unternehmen
  - schafft Grundverständnis
  - benennt Verantwortlichkeiten und Rollen
- Sensibilisierung
  - wird an gesamtes Personal des Unternehmens und eventuelle IT-Dienstleister veröffentlicht

Informations- Sicherheits-Leitlinie: Textbeispiel

2.3 Persönliche Verantwortung•

Es ist die gemeinsame Pflicht von Vorstand, Mitarbeitern und Dienstleistern, das Maß an Sicher heit zu gewährleisten, das Kunden und andere Geschäftspartner von der Firma erwarten.
Die Einhaltung der Sicherheitsgrundsätze ist daher eine **Aufgabe aller Mitarbeiter** und anderer für das Haus Tätigen.

Deshalb gelten folgende Anforderungen:

- Alle Mitarbeiter, unabhängig von Position und Aufgabenbereich, tragen Verantwortung für die Informationssicherheit in ihrem Aufgabenbereich.
- Jeder Dienstleister ist analog den vorliegenden Standards zu verpflichten und zu kontrollie ren.
- Jeder Mitarbeiter soll selbständig im Falle von Sicherheitsproblemen oder entsprechenden Vorfällen die Initiative ergreifen. Zumindest ist unmittelbar der Vorgesetzte zu informieren.

Informations- Sicherheits-Leitlinie: Gliederung

1 Dokumentenkontrolle

2 Informationssicherheit als strategische Aufgabe
- Bedeutung der Informationssicherheit
- Reichweite der Grundsätze
- Persönliche Verantwortung
- Durchsetzung

3 Grundlagen und Ziele der Informationssicherheit
- Rechtliche Normen und Standards
- Operationelle Risiken und Schutzbedarf
- Sicherheitskriterien für die Informationsverarbeitung
- Randbedingungen

4 Aufgaben und Verantwortlichkeiten
- Sicherheit als Führungsaufgabe
- Verantwortliche für die Informationsverarbeitung
- IT-Sicherheits-Beauftragter und Arbeitskreis IT-Sicherheit
- Weitere spezielle Verantwortlichkeiten

5 Regelkreis zur Informationssicherheit
- Ermittlung der Anforderungen
- Überprüfung der Informationssicherheit
- Planung der Umsetzung
- Durchführung der Maßnahmen
- Aufrechterhaltung der Informationssicherheit

6 Grundlegende Schutzmaßnahmen
- Objekte der Informationssicherheit
- Maßnahmen für Infrastruktur und IT-Equipment
- Maßnahmen für Daten und Anwendungen
- Maßnahmen für Prozesse

Informationssicherheits-Leitlinie: Rollen

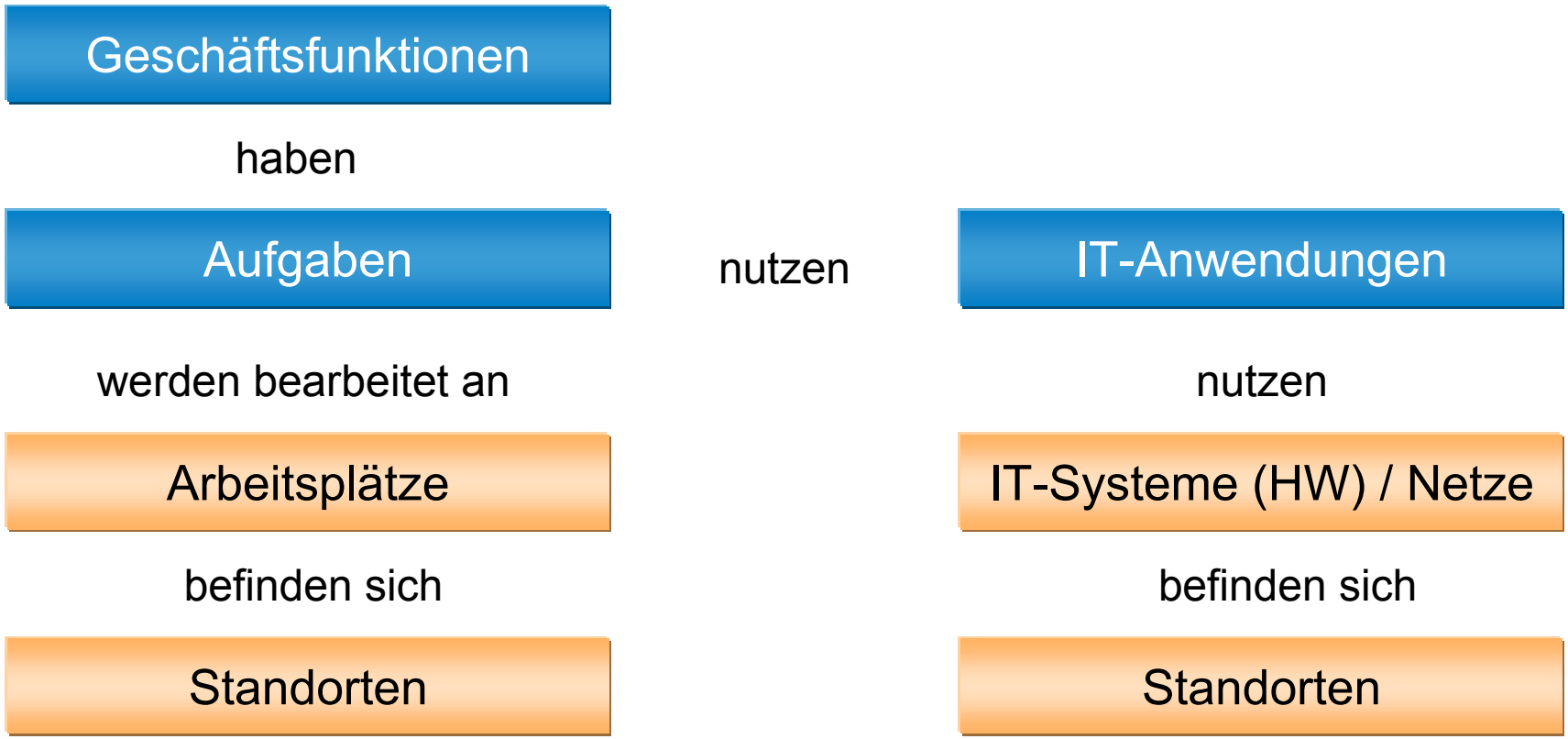
- Geschäftsleitung
  - Gesamtverantwortung
  - erlässt Informationssicherheits-Leitlinie
  - definiert und besetzt alle Rollen
- IT-Leitung
  - Verantwortung für ordnungsgemäßen IT-Betrieb
  - setzt Informationssicherheits-Leitlinie um
- Informationssicherheits-Beauftragter
  - Verantwortung für Informationssicherheits-Management
  - berichtet an Geschäftsleitung
  - berät IT-Leitung
- IT-Revision
  - Verantwortung für Prüfung des ordnungsgemäßen IT-Betriebs
  - berichtet an Geschäftsleitung
  - prüft IT-Leitung

Informationssicherheits-Richtlinie

Struktur- und Schutzbedarfsanalyse der IT

- Anwendungen und IT-Komponenten
- Abhängigkeiten
  - der Anwendungen untereinander
  - der Anwendungen von den IT-Komponenten
  - der IT-Komponenten untereinander
- Schutzbedarf der Anwendungen
  - Erhebung in Workshop
- Schutzbedarf der IT-Komponenten
  - Ableitung aus Anwendungen
  - individuelle Anpassungen

Strukturanalyse für IT-Komponenten

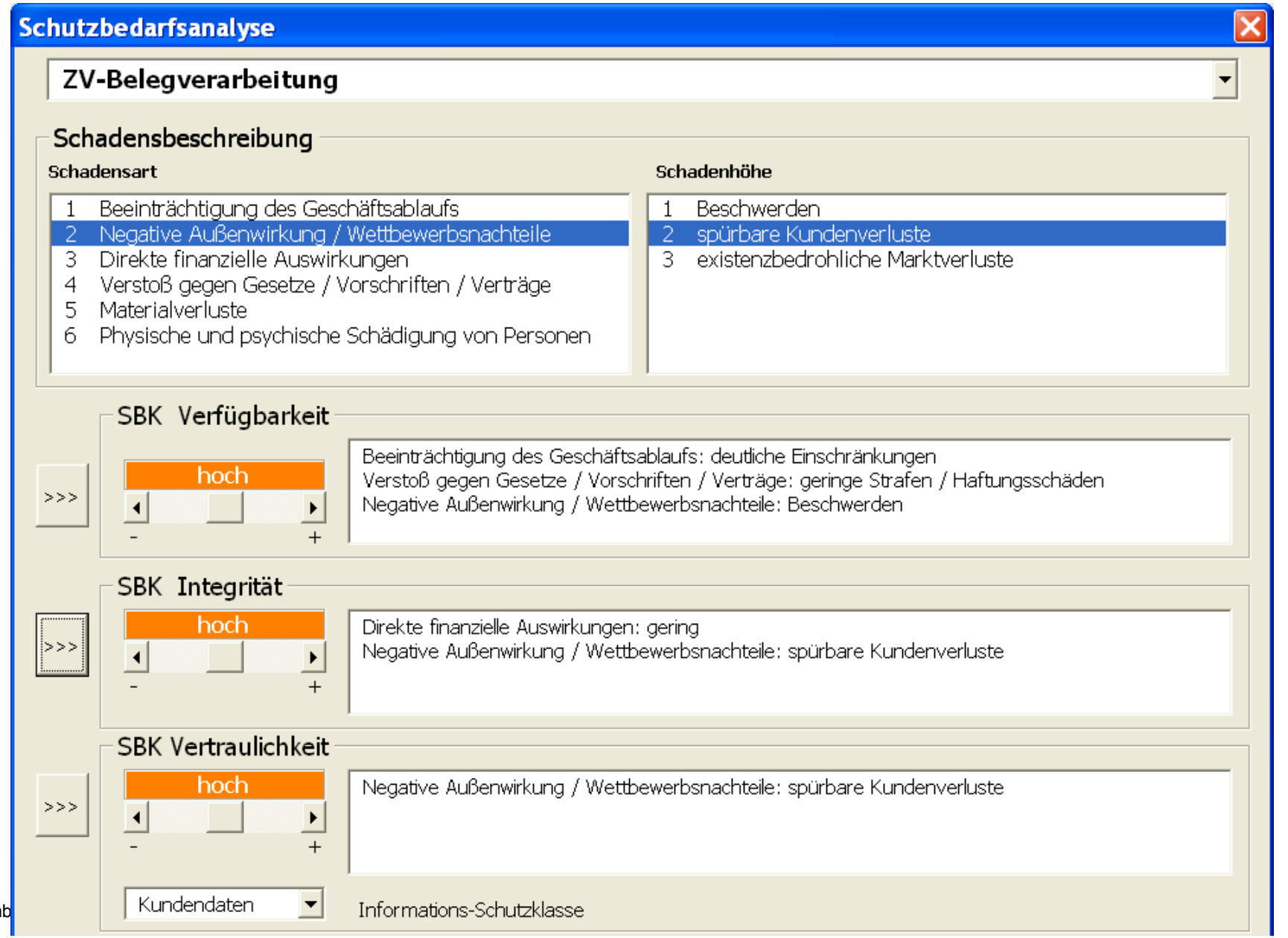


Schutzbedarfs-Klassen

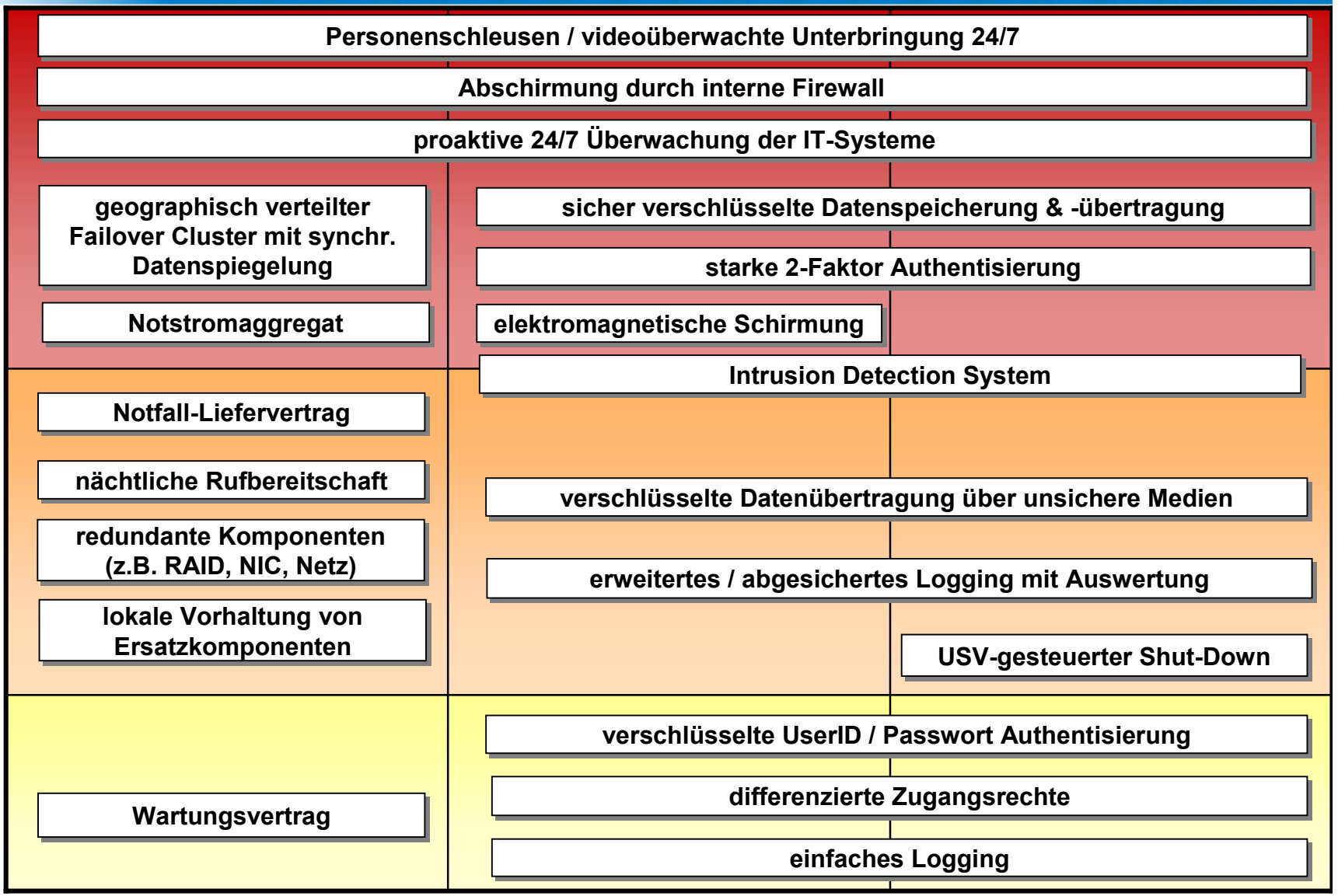
Schutzbedarfs-Klasse Schadensart	mittel	hoch	sehr hoch
Beeinträchtigung des Geschäftsablaufs	Betriebsbehinderung	deutliche Einschränkung	existenzbedrohende Handlungsunfähigkeit
negative Außenwirkung/ Wettbewerbsnachteile	Beschwerden	spürbare Kundenverluste	existenzbedrohende Marktverluste
direkte finanzielle Auswirkungen	geringe Beträge	deutliche Bilanzauswirkung	existenzbedrohend / Konkurs
Verstoß gegen Gesetze / Vorschriften / Verträge	geringe Strafen u. Haftungsschäden	hohe Strafen u. Haftungsschäden	existenzbedrohende Strafen u. Haftungsschäden

anzuwenden auf Verfügbarkeit, Vertraulichkeit und Integrität

Beispiel Schutzbedarfsfeststellung



Beispiel Maßnahmen



Verfügbarkeit aus verschiedenen Blickwinkeln

Verfügbarkeit allgemein

Redundanz	voll mit sofortiger Umschaltung	vorhanden mit merkbaren Umschaltzeiten	nur teilweise vorhanden, Aufbauzeiten erforderlich
Schutzbedarfsklasse Verfügbarkeit	sehr hoch	hoch	mittel

Wiederanlaufklasse	0	1	2	3	4	5
maximale Ausfallzeit	<= 4 Std.	<= 1 Tag	<= 2 Tage	<= 3 Tage	<= 7 Tage	> 7 Tage
maximale Datenverlustzeit	ca. 0 Std.	ca. 0 Std.	ca. 0 Std.	ca. 24 Std.	ca. 24 Std.	ca. 24 Std.

Verfügbarkeit im Notfall

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.

Alarme 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 Geschäftsleitungsebene
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 Versorgungs-einrichtungen
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 Vorfallsklassen
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

Projektablauf 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

Projektablauf II

Verfassen der Richtlinie

- Ermittlung der Sicherheitsregeln

Zuordnung von Verantwortlichkeiten / Integration von Dokumenten

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

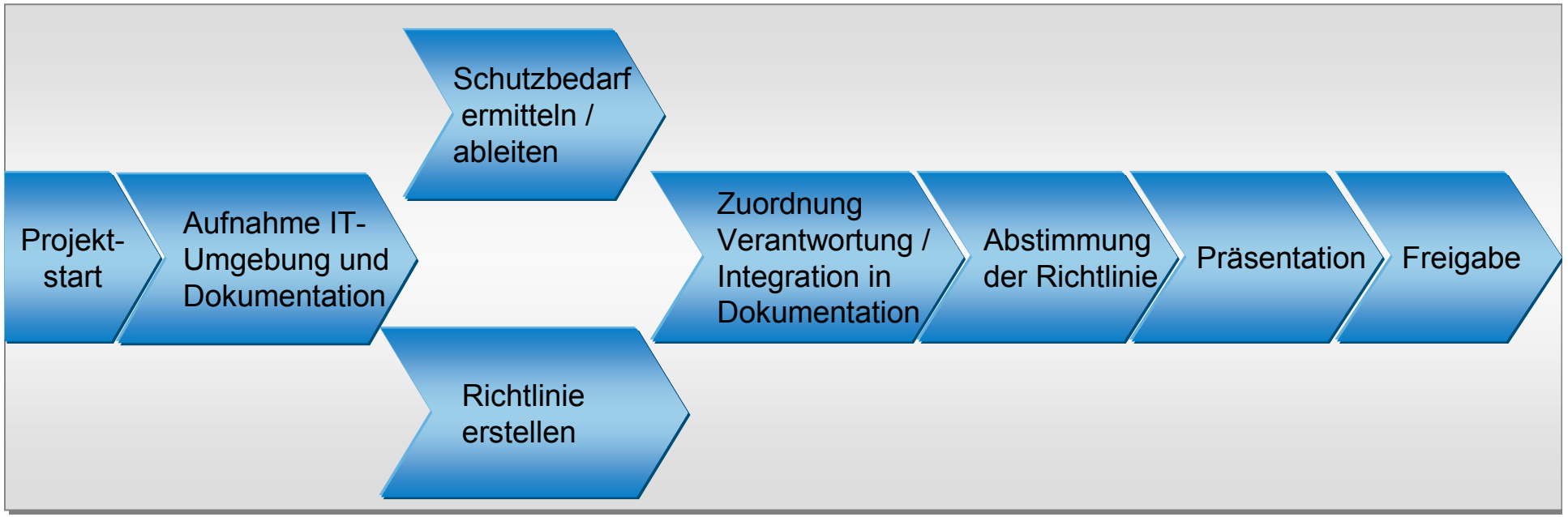
Abstimmung der Richtlinie

- Abstimmung der Regeln mit Verantwortlichen

Präsentation / Freigabe der Richtlinie

- Vorstellung der Richtlinie
- Inkraftsetzen der Richtlinie durch Geschäftsleitung

Informationssicherheits-Richtlinie: Vorgehen



Dauer ca. 6 Monate

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

  Erleichterung der Prüfbarkeit

  - keine organisatorischen oder technischen Details
- Zusatzdokumente
  - Schutzbedarfsfeststellung
  - Nennung von Verantwortlichkeiten
  - Verweise auf nachfolgende Dokumentationsebene

Informationssicherheits-Audit

Informationssicherheits-Audit

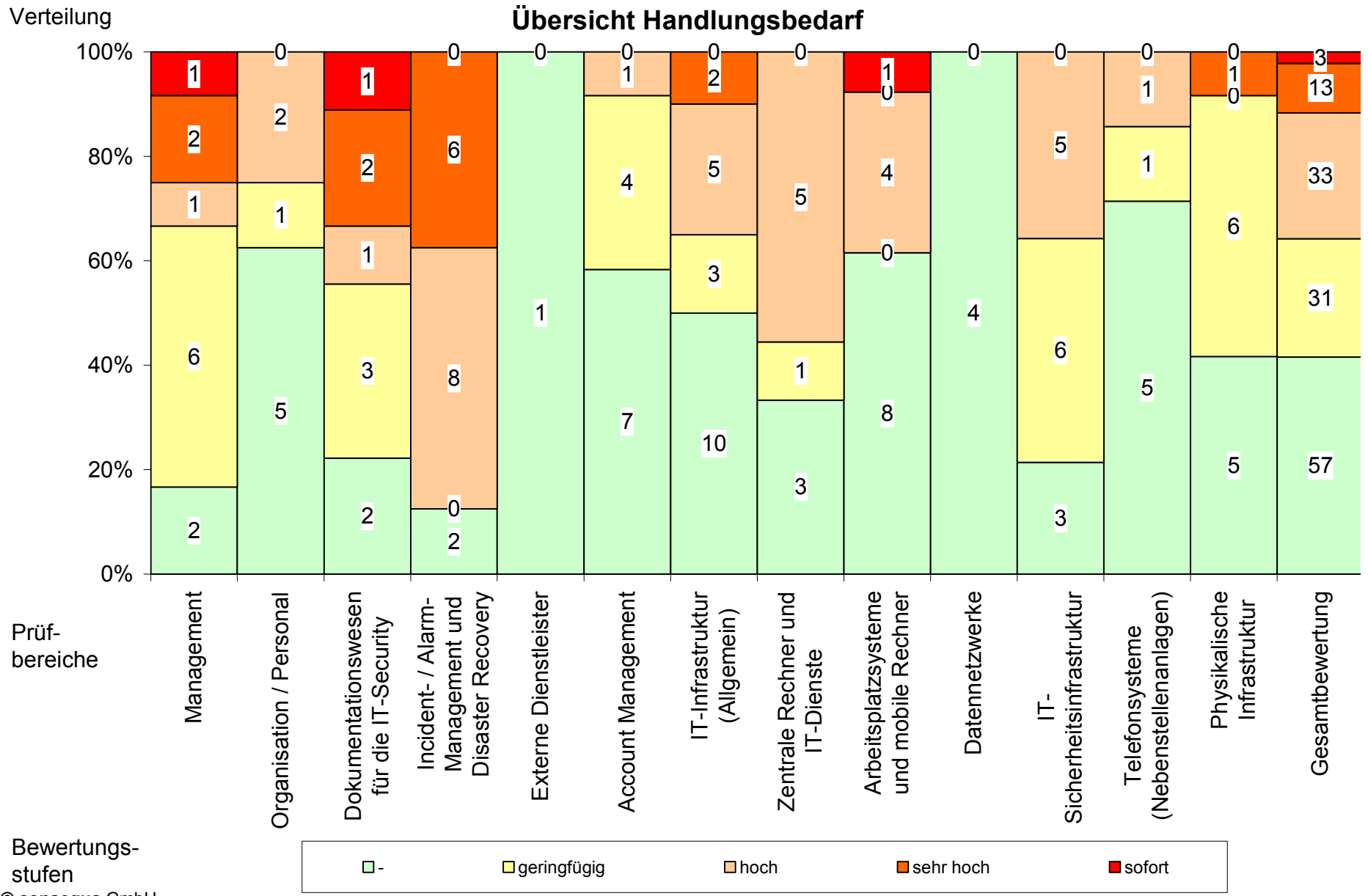
- **Ziele**
  - Überprüfung der Vollständigkeit, Angemessenheit und Umsetzung der Maßnahmen
  - Aufzeigen von Handlungsbedarf
- **Grundlagen**
  - eigene Informationssicherheits-Richtlinie des Unternehmens
- **Methoden**
  - Interviews
  - Dokumentenprüfungen
- **Abgrenzungen**
  - keine technische Detailprüfung
  - keine Hands-On Prüfungen
  - keine 100% Sicherheit

Methode: Fragenkatalog

Datei Bearbeiten Ansicht Einfügen Format Extras Daten Fenster ?

1	2	3	4	5	6	7	8	9	10	11
Bereich		Rücksprung Intro	**10** Prüfpunkte				Sparkasse			
RI	***Risikomanagement***		**100%** beantwortet							
Gemittelte Bewertung des Sicherheitsniveaus										
4,4	***unkritisch - wenig kritisch***									
SIZ-Nr.	**SIZ-Konzept & ...mmentare**	**Bewertungsfrage**	**Priorität**	**...ümethode**	**Erfüllungsgrad**		**Erläuterung**	**Handlungsbedar...f**	**...3-Wert**	**Empfohlene Maßnahme**
O.20	K003	Wurden bereits Risiko-, Bedrohungs- und Schutzbedarfsanalysen für die IT-Systeme und IT-Anwendungen durchgeführt?	8	DE	In einigen Teilen	2	nur für Wiederanlaufziele im Notfall existent	sehr hoch	16	Schutzbedarfsanalyse ergänzen
O.21	K003	Werden einheitliche Methoden zur Risiko- Bedrohungs- und Schutzbedarfsanalyse speziell für die IT-Systeme und IT-Anwendungen eingesetzt?	5		n.a.	x	noch nicht erfolgt, außerdem siehe RI-W.20			
O.22	K026	Werden bestehende Restrisiken durch geeignete Versicherungen minimiert?	4		Vollständig	0		-	0	
W.20	K401	Existiert ein formal implementiertes übergreifendes Management operationeller Risiken? - a. Sind die Ziele des Risikomanagements von den Unternehmenszielen abgeleitet? - b. Wie ist das operationelle Risikomanagement mit dem IT-Sicherheitsmanagement verknüpft? - c. Ist es bzgl. der IT-Sicherheit mit anderen (Planungs-)Prozessen geeignet verknüpft?	4		In einigen Teilen	2	noch keine Risikolandkarte, Projekt zur Einführung für 2007 geplant	geringfügig	8	Anpassung des Risikomanagements und Etablierung einer Kommunikationsstruktur
W.21	K401	Werden die Maßnahmen zur IT-Sicherheit auch als Beiträge zur Risikosteuerung verstanden und entsprechend bewertet? - a. Wird das IT-Sicherheitsmanagement rechtzeitig über veränderte Risikolagen und -beurteilungen informiert und wie wird dessen Fachkompetenz hierbei genutzt? - b. Werden die Einflüsse von Planungen und Projekten auf die Wirksamkeit und Eignung der Maßnahmen zur Risikosteuerung geeignet berücksichtigt?	8		In einigen Teilen	2	siehe RI-W.20	sehr hoch	16	
W.22	K402	Ist der Informationsaustausch zwischen Risikomanagement und IT-Sicherheitsmanagement gewährleistet?	8	DE	Vollständig	0		-	0	

Informationssicherheits-Audit: Ergebnisse



consequa-Methode: Maßnahmenkatalog

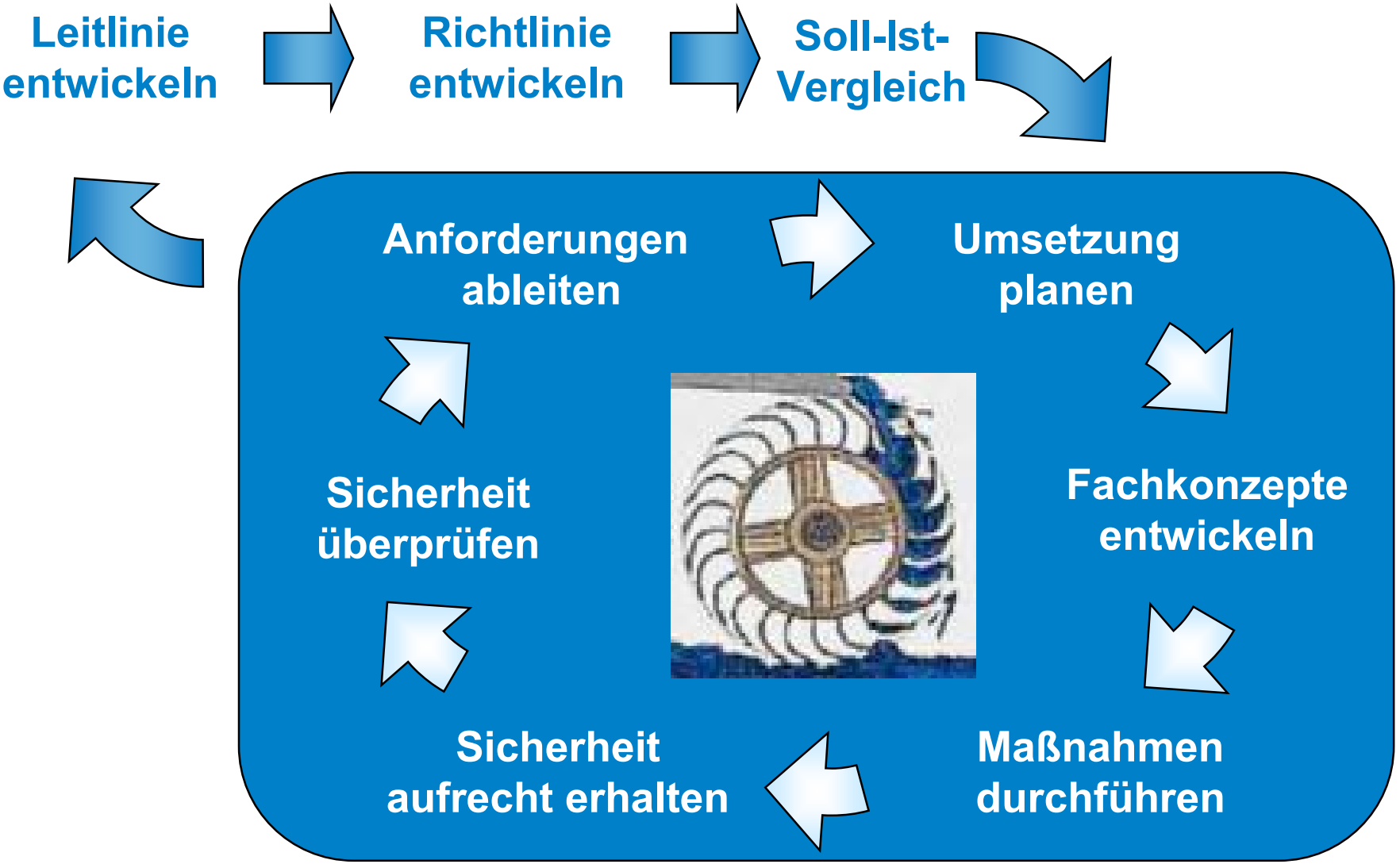
Datei Bearbeiten Ansicht Einfügen Format Extras Daten Fenster ?

2	3	4	5	7	8	9	10	11	12	16	21
Beschreibung der Maßnahme	Maßnahmentyp	Priorität	Priorität	Bezug	Audit-Bereich	Ref. Regelnummer Sicherheitsrichtlinie	Regel	Begründung der Maßnahme	Durchführung	Kosten	Planung
Change Management und Anwendungsentwicklung											
Freigabeverfahren überarbeiten, Anweisung zur Eigenentwicklung um Testverfahren und Verfahren der Abnahme ergänzen	do		sehr hoch		CM	B.32	Gibt es geregelte Test- und Freigabeverfahren? - a. Werden neu einzusetzende Hard- und Software-Komponenten getestet? - b. Werden Patches, Updates und Upgrades getestet? - c. Werden die Vorgaben bzgl. der IT-Sicherheit bei den Freigabeverfahren berücksichtigt? - d. Wird die Freigabe/Verweigerung der Freigabe revisionssicher dokumentiert?	Tests bei von der OPDV freigegebenen Programmen und bei Patches nicht vorgesehen, Freigabe auf Checklisten dokumentiert			
			geringfügig		CM	B.30	Existieren Entwicklungs-, Test - und Produktionsumgebungen und sind diese voneinander getrennt? - a. Sind die einzelnen Umgebungen getrennt? - b. Werden außerhalb der Produktionsumgebung nur anonymisierte Daten verwendet? - c. Ist genau festgelegt welche Aktivitäten in den Umgebungen erfolgen dürfen?	für Notes-Entwicklung und -Test existiert eine separate Datenbank, weitere Möglichkeiten nicht vorgesehen, Testumgebung unterliegt gleichen Sicherheitsregeln wie Produktion			
			geringfügig		AE	B.06	Gibt es Vorgaben für neu einzusetzende Anwendungen? - a. Gibt es Richtlinien für die einzusetzenden Werkzeuge in der Anwendungsentwicklung? - b. Gibt es sicherheitstechnische Vorgaben für die Anwendungen? - c. Gibt es sicherheitstechnische Vorgaben speziell für Web-Anwendungen? - d. Wird bei den Anwendungen das im Hause etablierte Rollen-/Rechtekonzept berücksichtigt? - e. Werden neue Anwendungen einer sicherheitstechnischen Abnahme unterzogen?	Anweisung existiert, Werkzeuge technisch erzwungen, Entwicklungsverantwortung bei anderer Person als Vorgabenerstellung, Abnahme nicht immer dokumentiert			
Externe Dienstleister											
Anforderung an FinanzIT für genauere Regelungen stellen	do		sehr hoch		ED	V.14	Sind IT-Sicherheitsanforderungen und deren Umsetzung zwischen den Vertragspartnern geregelt? - a. Ist der Vertragspartner bzgl. der Einhaltung branchenspezifischer Anforderungen verpflichtet worden? - b. Wurde das Recht zum Audit vertraglich zugesichert?	nur in allgemeiner Form vertraglich geregelt			

IT-Sicherheits-Audit: Ergebnisse

- **ausgefüllte Audit-Prüflisten**
  - nach Audit-Bereichen
- **Maßnahmenkatalog**
  - konsolidiert aus Handlungsbedarf
  - mit grober Kosten- / Aufwandsschätzung
- **Kurzbericht mit Bewertung des Sicherheits-Status**
  - Ausgangspunkt und Vorgehensweise
  - ermittelter Status
  - Vorschläge zu Maßnahmen
  - Fazit
  - Anhang: Bewertungsgrundlagen

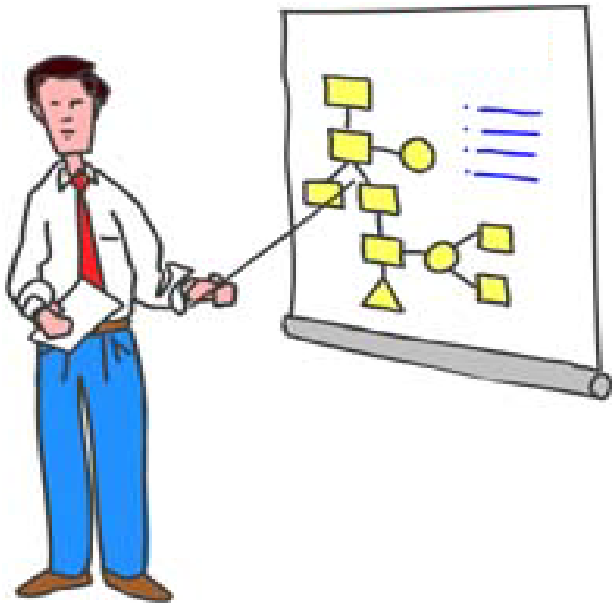
Informationssicherheit: Regelkreis



Reifegrad der Steuerung

Stufe		Merkmale
5	**optimal**	integraler Bestandteil der Unternehmenskultur (Integration in das allg. Risiko-Management und das Unternehmens-Benchmarking)
4	**gesteuert**	systematisches IT-Risikomanagement (Schutzbedarfsanalyse) Fokus auf Ganzheitlichkeit (Abstimmung aller betroffenen Bereiche) definierte Regelkreise (Audit, Reports)
3	**definiert**	Informationssicherheitspolitik definierte Organisationsstruktur für Informationssicherheit (ISB, ...) Maßnahmen aufbauend auf IT-Strukturanalyse
2	**wiederholbar**	dokumentierte Konzepte und Arbeitsabläufe (Datensicherungskonzept, Ablauf Accountverwaltung, ...)
1	**initial**	technische und organisatorische Einzelmaßnahmen (Datensicherung, Virenscanner, Firewall, ...)

Vielen Dank
für Ihre Aufmerksamkeit!



consequa

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