



IKS – internes Kontrollsystem

Auf den 01.01.2008 wurde die Gesetzgebung geändert. IKS erhält eine gewichtigere Bedeutung.

Welchen Einfluss hat dies auf die IT?

Übersicht

- Definition IKS
 - Gesetzliche Grundlage
 - Was ist eine interne Kontrolle im Sinne der Gesetzgebung

- Zusammenhang Risikomanagement / IKS

- Einfluss der IT auf das Risikomanagement

- Wie kann die „interne Kontrolle“ einer IT-Infrastruktur stattfinden

Definition IKS – Gesetz

- OR wurde auf den 01.01.2008 angepasst.
 - Artikel 728a
 - Die Revisionsstelle prüft, ob ein internes Kontrollsystem existiert
 - Die Revisionsstelle berücksichtigt bei der Durchführung und bei der Festlegung des Umfanges der Prüfung das interne Kontrollsystem
 - Artikel 728b
 - Die Revisionsstelle erstattet dem Verwaltungsrat einen umfassenden Bericht mit Feststellungen über die Rechnungslegung, das **interne Kontrollsystem** sowie die Durchführung und das Ergebnis der Revision

- → Ein IKS ist nicht freiwillig, es ist Pflicht.

Was ist interne Kontrolle?

- Ein Internes Kontrollsystem (IKS) besteht aus systematisch gestalteten, organisatorischen Massnahmen und Kontrollen im Unternehmen zur Einhaltung von Richtlinien und zur Abwehr von Schäden, die durch das eigene Personal oder böswillige Dritte verursacht werden können.

Die Massnahmen beruhen auf technischen und organisatorischen Prinzipien. Sie umfassen Aktivitäten und Einrichtungen zur unternehmensinternen Kontrolle sowie ihre Beziehungen zueinander. Sie umfassen z.B.

- Bauliche und softwaretechnische Zutrittskontrollen
- Schriftliche Weisungen
- Massnahmen zum Schutz der materiellen und immateriellen Vermögenswerte des Unternehmens
- Massnahmen zur Abwehr von illegalen Vorgängen im Bereich der Wirtschaftskriminalität...

Quelle: wikipedia

Was ist interne Kontrolle

■ Beispiele

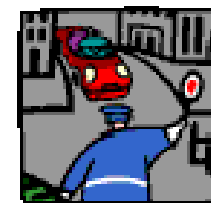
- Sicherstellung des Normalbetriebs
- Aktiver Schutz vor Notfallsituationen
- Sichern von Betriebsgeheimnissen
- Einhaltung des Soll-Zustandes
- Aktiver Schutz vor Wirtschaftskriminalität
- Aktiver Schutz vor Sabotage
- Risikobeurteilung und Berichterstattung
- Sicherstellung, dass geltende Gesetze eingehalten werden
- ...

Was ist interne Kontrolle

- → Instrumente zur Kontrolle und Steuerung des Unternehmens auf dem Weg zum Soll-Zustand schaffen



- → Die geschaffenen Instrumente nutzen um Kursabweichungen zu detektieren und die nötigen Massnahmen einzuleiten.



Wer ist betroffen (gemäss OR)

- Publikumsgesellschaften (die der ordentlichen Revision unterstehen)

 - „wirtschaftlich bedeutende Unternehmen“
 - Bilanz ≥ 10 Mio.
 - Umsatz ≥ 20 Mio.
 - MA ≥ 50
- 2 der 3 Kriterien müssen erfüllt sein

Verantwortlichkeiten

- **Verwaltungsrat**
 - Trägt die Gesamtverantwortung, dass eine IKS vorhanden ist.
 - Entscheidet, ob ein IKS eingeführt werden muss
 - Muss im Bilanzanhang Angaben über die Durchführung einer Risikobeurteilung machen.

- **Geschäftsleitung**
 - Umsetzung des IKS
 - Management der Risiken und Compliance

- **Revisionsstelle**
 - Prüfung ob ein IKS existiert
 - Umfassender Bericht mit Feststellungen zum IKS

Wie muss IKS gemacht werden?

- Der Gesetzgeber lässt offen, wie das IKS aufgebaut wird
- Umfang und Ausgestaltung des IKS sind auf die individuellen Gegebenheiten jeder Unternehmung anzupassen und von folgenden Punkten abhängig
 - Grösse
 - Komplexität der Geschäftstätigkeit
 - Art der Finanzierung
- IKS sollte
 - Überprüfbar (dokumentiert) sein
 - Den Mitarbeitern bekannt sein

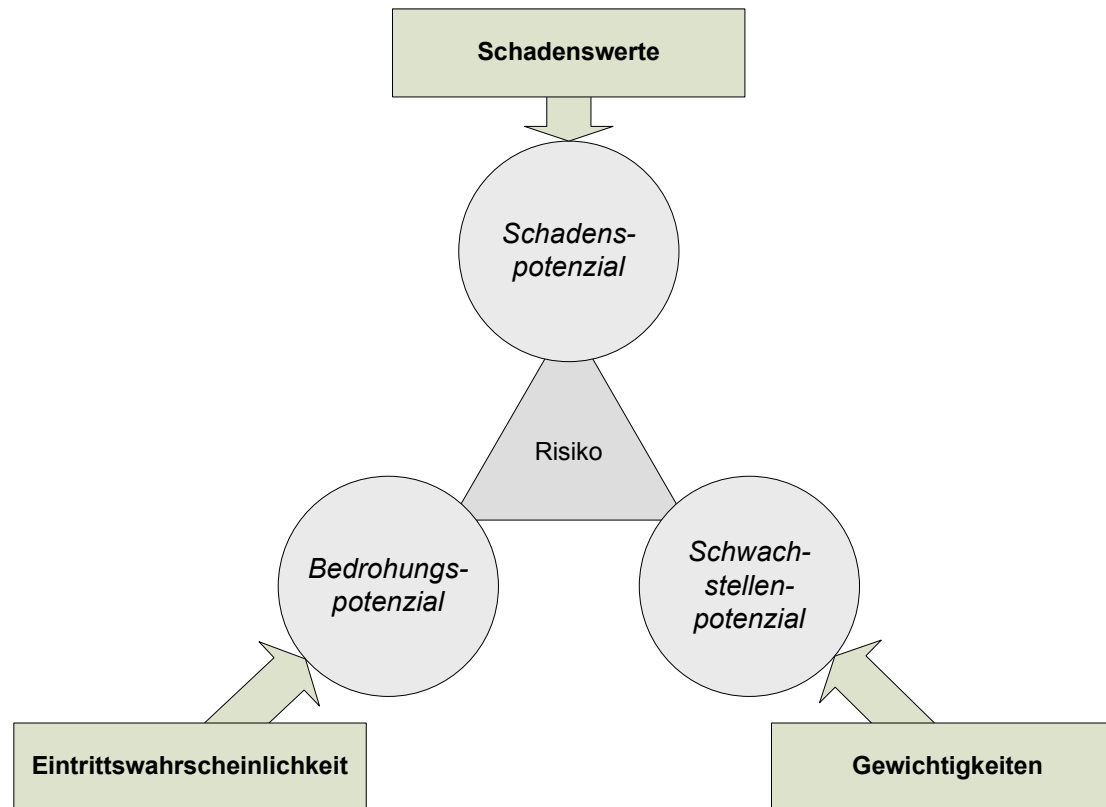
Konsequenzen bei fehlendem oder mangelhaftem IKS

- Bemerkung im Revisionsbericht an die Generalversammlung
- Ausführungen im Erläuterungsbericht der Revisionsstelle an den Verwaltungsrat
- Verletzt ein Organ der Gesellschaft seine Pflichten fahrlässig oder absichtlich, haftet dieses für allfälligen Schadenersatz
- Kann strafrechtliche Folgen haben StGB Art. 102 (Organisationsverschulden)

Zusammenhang Risikomanagement / Internes Kontrollsystem

- Ein auf das Unternehmen zugeschnittenes IKS setzt eine unternehmensspezifische Risikobeurteilung voraus
- Die Risikobeurteilung ist ein Teilaspekt eines umfassenden Risikomanagements
- Artikel 663b Ziff. 12 OR (Erfolgsrechnung)
 - Der Anhang enthält Angaben über die Durchführung einer Risikobeurteilung
 - Das bedeutet, dass **jedes** Unternehmen eine Risikobeurteilung durchführen muss.

Risikomanagement

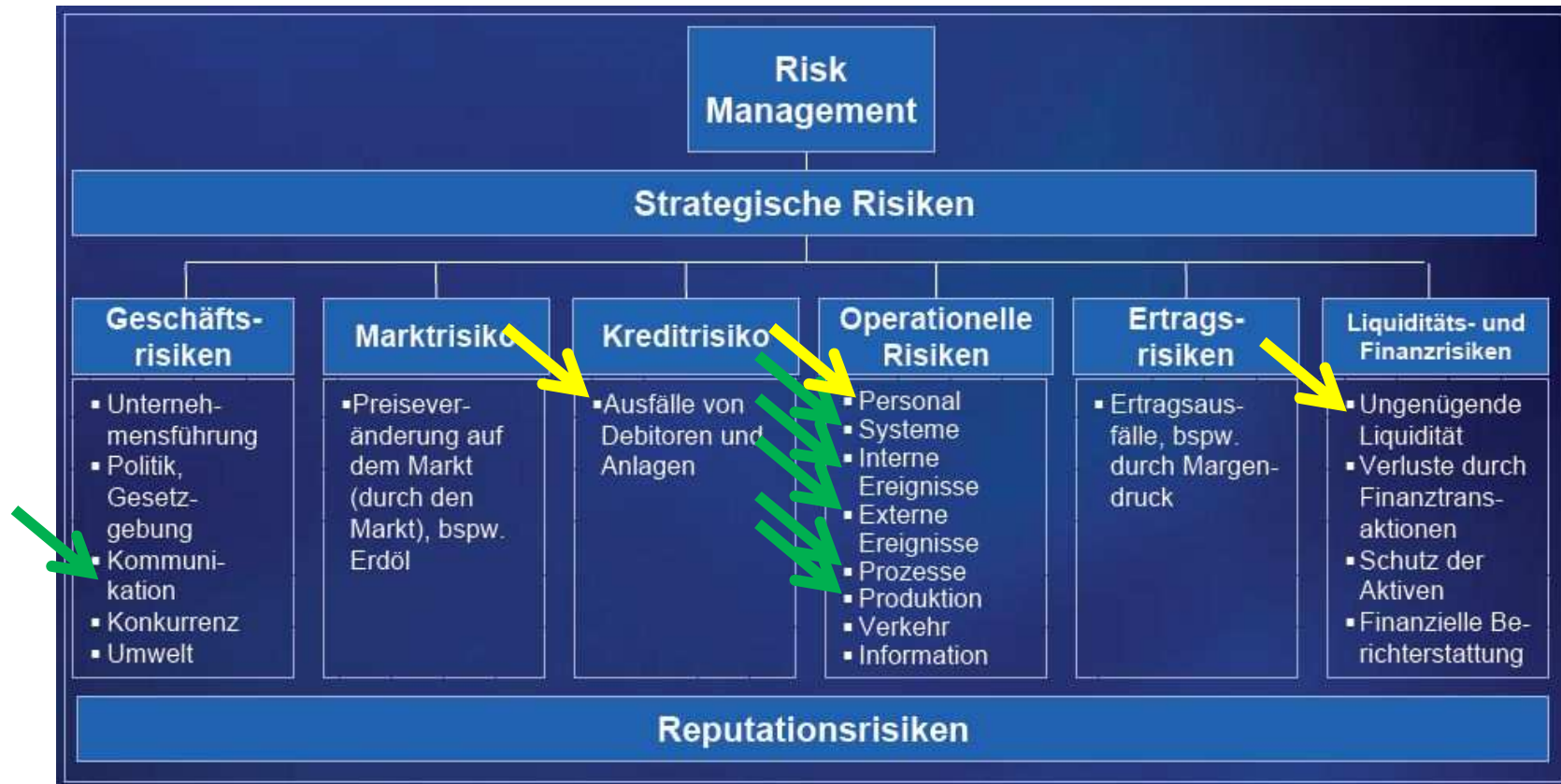


Risikomanagement

- Was muss sichergestellt werden?
 - C onfidentiality Vertraulichkeit
 - I ntegrity Integrität
 - A vailability Verfügbarkeit

- Vertraulichkeit: Nur autorisierte Personen dürfen die Daten sehen.
 - Lohn
 - Geschäftsleitung
- Integrität: Daten müssen vor Manipulation geschützt werden.
 - Strafregister / Patientendaten
 - Kundendaten
- Verfügbarkeit: Maximale Ausfallzeiten der Systeme

Risikomanagement Einfluss der IT



Quelle: KPMG

Risikomanagement Einfluss der IT

- Beispiel Kino mit Sitzplatzreservation (wichtiger Prozess)

Prozess:



- Direkt involvierte Systeme

- Webserver
- Datenbankserver
- E-Mailserver

- Indirekt involvierte Systeme

- Netzwerk
- Firewall / Router
- DNS-Server
- Internetanbindung
- ...

Risikomanagement Einfluss der IT

- Beispiel Kino mit Sitzplatzreservation (wichtiger Prozess)

Prozess:



- Direkt involvierte Systeme

- VoIP-Server
- VoIP-Telefon
- Datenbankserver
- E-Mailserver

- Indirekt involvierte Systeme

- Netzwerk
- Firewall / Router
- DNS-Server
- Internetanbindung
- ...

Risikomanagement Einfluss der IT

- Beispiel Kundenauftragsabwicklung Autoreparaturwerkstatt (vereinfacht)

Prozess



- Direkt involvierte Systeme
 - E-Mail Server
 - Auftragsabwicklung
 - Bestellsoftware
 - Buchhaltungssoftware
- Indirekt involvierte Systeme
 - Netzwerk
 - Internet-Abindung
 - Firewall / Router
 - DHCP Server
 - ...

Risikomanagement: Verfügbarkeit

- Übersicht mittels Verfügbarkeitsmatrix mit den Geschäftsprozessen und den IT-Systemen.

<i>Verfügbarkeitsmatrix</i>	Prozess 1	Prozess 2	Prozess 3	Prozess 4	Prozess 5	Prozess 6	Prozess 7
Domainkontroller	X	X	X	X	X	X	X
Exchange-Server	X		X	X	X		
File-Server	X	X	X	X	X		X
SQL-Datenbank	X			X	X		
CNC-Maschinen	X	X					X
Internetzugang	X				X		
Zugriff von aussen auf Daten	X			X			
Verbindung zu Standort	X					X	X

Grün = Maximale Ausfalldauer von 4 Stunden
 Gelb = Maximale Ausfalldauer von 6 Stunden
 rot = Maximale Ausfalldauer von 10 Stunden

Risikomanagement: Verfügbarkeit

- Verfügbarkeitsanforderungen an einzelne System müssen als Teilresultat aus dem Risikomanagement folgen.

OBJEKT	VERANTWORT- LICHKEIT	VERFÜGBARKEIT TAG/NACHT	TOLERIERBARE AUSFALLDAUER TAG/NACHT	PRIORITÄT
Domain-Kontroller	IT	Sehr hoch / hoch	4 / 6	3
Exchange-Server	IT	Hoch / gering	8 / 10	4
File-Server	IT	Sehr hoch / hoch	4 / 6	2
SQL-Datenbank	IT	Hoch / gering	8 / 10	7
CNC-Maschinen	Techniker	Sehr hoch / hoch	4 / 8	1
Internetzugang	Provider	Gering / sehr gering	8 / 10	8
Zugriff von aussen auf Daten	IT	Hoch / gering	6 / 10	6
Verbindung zu Aussenstandort	Provider	Hoch / gering	4 / 10	5

Risikomanagement: Vertraulichkeit

- Datenklassifikation in den meisten Fällen unumgänglich
 - Öffentlich
 - Unproblematische Daten bezüglich Vertraulichkeit
 - z. B. Preislisten
 - Vertraulich
 - Für den internen Gebrauch
 - Unternehmen ist durch Veröffentlichung aber nicht existenziell bedroht
 - z. B. Mitarbeiterrichtlinien zum Umgang mit den IT-Mitteln
 - Geheim
 - Unternehmen kann grossen Schaden erleiden, wenn die Information in falsch Hände gelangt. (z. B. durch das Gesetz)
 - z. B. Patientendaten

Risikomanagement: Vertraulichkeit

- Datenklassifikation in den meisten Fällen unumgänglich
 - Daten müssen klassifiziert werden.
 - Schutz vor unerlaubten Zugriff muss technisch sichergestellt werden. (Zugriffsschutz, Verschlüsselung)
 - Umgang mit sensiblen Daten muss festgehalten werden

 - **Mitarbeiter müssen im Umgang mit Firmendaten geschult werden!**

Risikomanagement: Integrität

- Die Datenintegrität stellt sicher, dass Daten auch zu einem späteren Zeitpunkt nicht verändert werden können bzw. Veränderungen erkannt werden.
- Dies kann erreicht werden durch:
 - Hash-Werte (z.B. MD5, SHA-1)
 - Digitale Signaturen
- Das Gesetz sieht vor, dass alle rechnungsrelevanten Informationen unveränderbar gespeichert werden müssen!

Risikomanagement: Handlungsbedarf

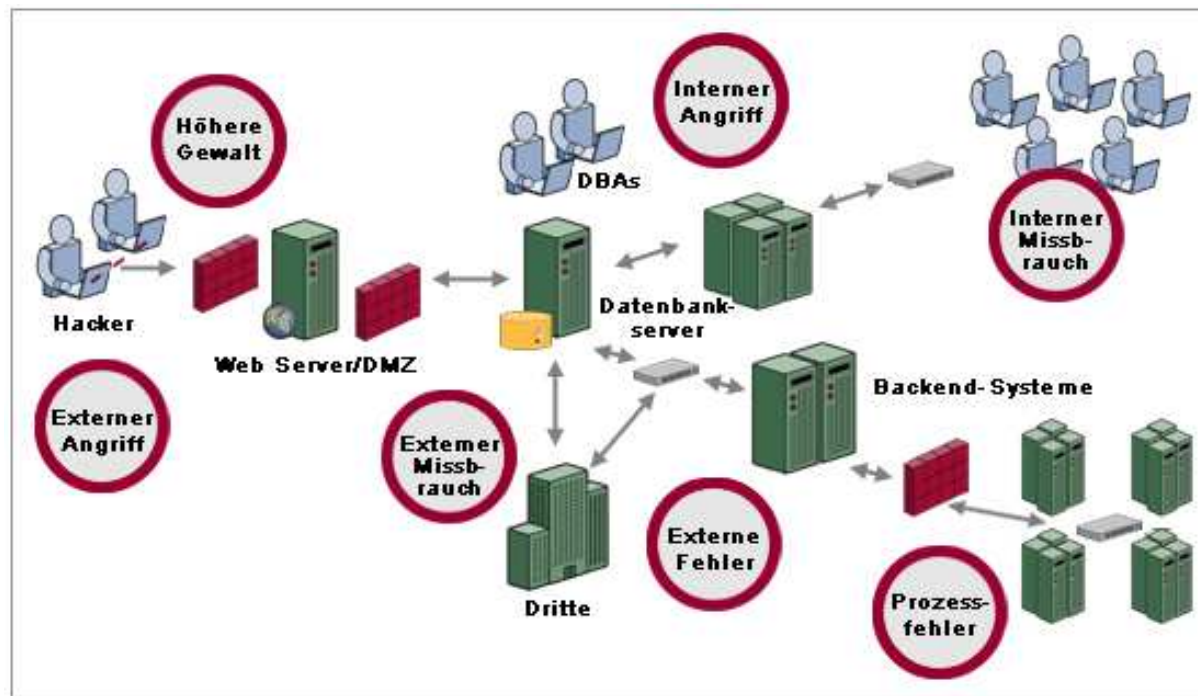
Verfügbarkeitsmatrix

	Prozess 1	Prozess 2	Prozess 3	Prozess 4	Prozess 5	Prozess 6	Prozess 7
Domainkontroller	X	X	X	X	X	X	X
Exchange-Server	X		X	X	X		

		Eintrittswahrscheinlichkeit		
		Wenig Wahrscheinlich	Wahrscheinlich	Sehr Wahrscheinlich
		1	2	3
Schaden bei Eintritt	Gering	1		
	Mittel	2		
	Schwer	3		

Risikomanagement

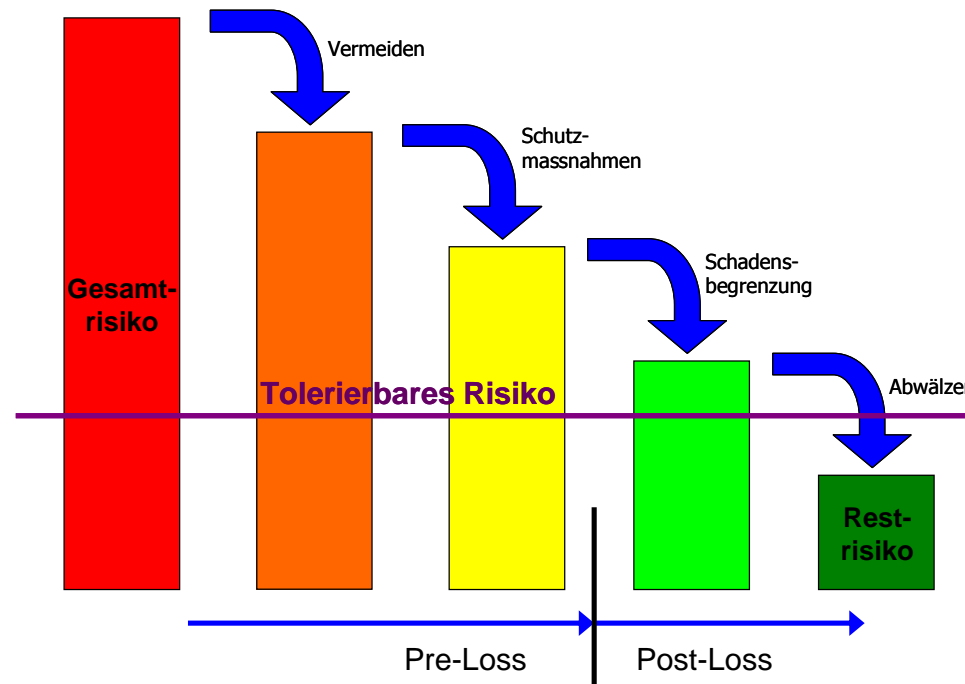
- Eine Variante für die Risikodefinition



Quelle: www.verisign.de

Risikoreduktion

- Risikoreduktion bis zum akzeptierbaren Restrisiko



Risikomanagement Fazit

- Die IT ist stark in die Geschäftsprozesse integriert
- Die IT hat dadurch einen grossen und direkten Einfluss auf die Geschäftsrisiken und muss deshalb zwingend berücksichtigt werden.
- Die Steuerung und Kontrolle der IT ist eine wichtige Aufgabe des Managements
- Risikomanagement ist Pflicht

Voraussetzungen

- Als Voraussetzung für eine optimale Steuerung und Kontrolle der IT mittels IKS müssen einige Voraussetzungen erfüllt sein. Unter Umständen bedeutet dies einen gewissen Initialaufwand.
 - Unternehmensziele und Strategie definiert
 - Geschäfts-Prozesse definiert
 - Kritische Prozesse bekannt
 - IT-Strategie definiert
 - Risikobeurteilung der Prozesse und dadurch abgeleitet Verfügbarkeitsanforderungen an die unterschiedlichen IT-Elemente bekannt.

Zusammenfassung

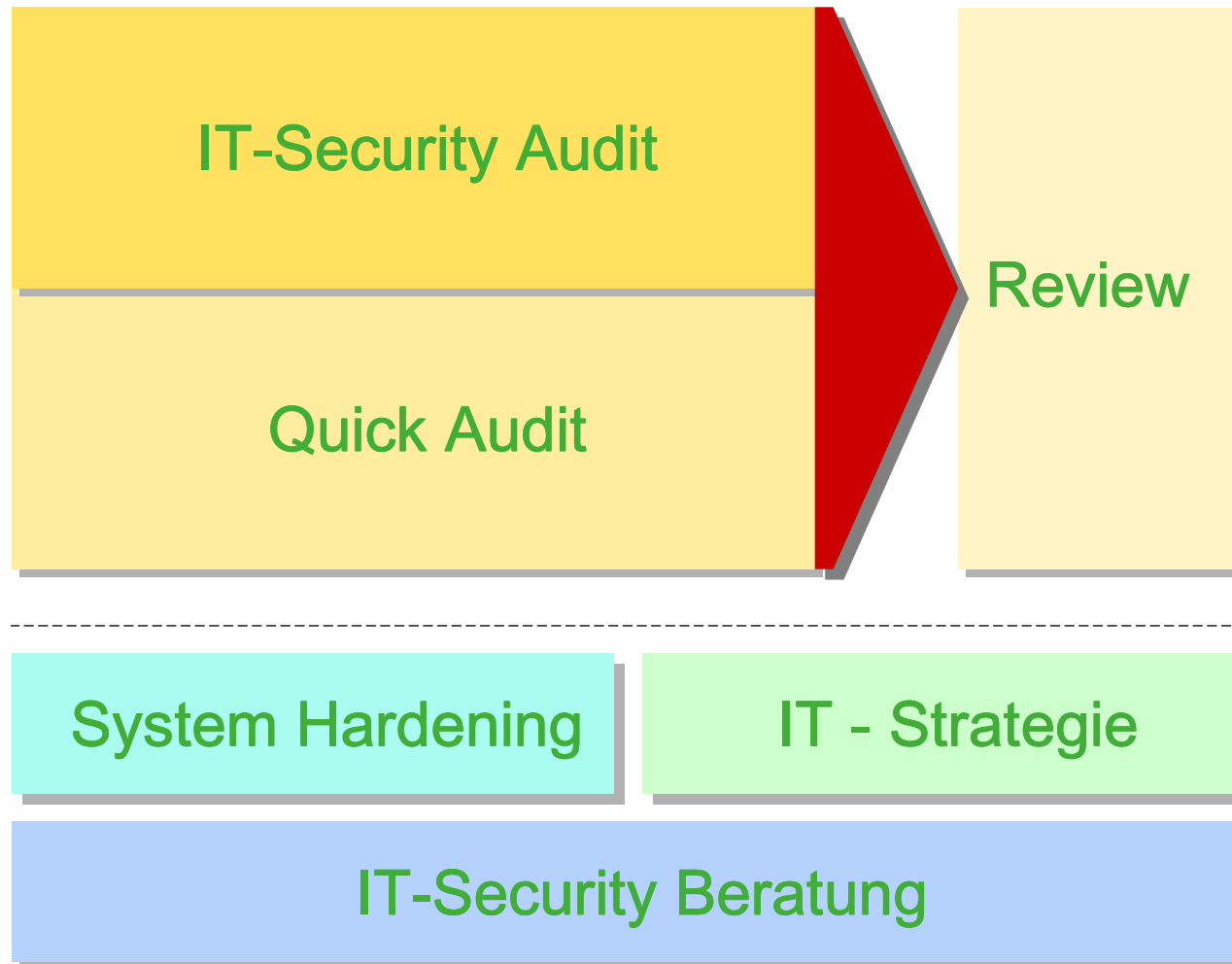
- Jedes Schweizer Unternehmen ist gesetzlich zu einem Risikomanagement gezwungen.
- Jeder der ordentlichen Revision untersehende Unternehmen ist zur Führung eines IKS verpflichtet. (Die Revision muss dies prüfen.)
- Der Gesetzgeber macht keine Vorschriften über das „wie“.
- Risikomanagement ist eine Grundlage für ein effizientes IKS.
- Steht die IT-Infrastruktur stehen die meisten Unternehmen.

Mögliches Kontrollinstrument

- IT-Security Überprüfung (Audit)
 - Technisch und organisatorisch
 - Komplett oder Teilbereiche

- Penetration Test
 - Von aussen
 - Von innen
 - Mit Benutzerlogin
 - Mit fremden Gerät
 - Kombiniert mit Social Engineering

Dienstleistungen der GO OUT





DIGICOMP



Mit uns wissen Sie,
wie es um Ihre IT-Sicherheit steht!



T. Hofmann



D. Reisacher



Ph. Hagmann



Th. Furrer



S. Müller



D. Reisacher



A. Wisler