

Zusammenfassung – Security Management

5. Semester Wirtschaftsinformatik

Institution: Hochschule Luzern

Studiengang: Bachelor in Wirtschaftsinformatik

Datum: 16.01.2017

Status: Veröffentlicht

Autor:

Janik von Rotz

<http://janikvonrotz.ch>

I'm not scared of a computer passing the turing test... I'm terrified of one that intentionally fails it.



Inhaltsverzeichnis

1	Begriffe	4
2	Einführung	5
2.1	Risikoberechnung	5
2.2	Risikobestimmungsmatrix.....	6
2.3	Risiko-Portfolio.....	7
2.4	Risiko-Assessment.....	7
2.5	Risikoidentifikation	8
2.6	Management-Systeme im Unternehmen	9
2.7	PDCA	10
2.8	ISO 27002:2013.....	11
2.8.1	Statement of Applicability	11
2.8.2	Schwachstellenanalyse	12
2.9	Rollen Informationssicherheit	12
3	Zertifikatsbasierende Anwendungen und PKI.....	13
3.1	Gesetzliche Vorschriften	13
3.1.1	Signatur Unterscheidung	15
3.1.2	Anforderungen	16
3.2	System für die Anerkennung von Zertifizierungsstellen.....	18
3.3	Gegenüberstellung der Zertifikatstypen.....	19
3.4	Erstellung von qualifizierten Signaturen.....	21
3.5	Demonstration Kaufvertrag	21
3.6	Einbettung von Gültigkeitsinformationen	22
3.7	Signature as a Service	23
4	Trustketten und Prüfung der Zertifikate	24
4.1	Prüfung von Zertifikaten	24
4.2	Zertifikatstypen	26
4.3	Kreuzzertifizierung	27
4.4	Zertifikatsketten.....	28
4.5	Trustmodelle	30
4.5.1	Hierarchisches Modell	30
4.5.2	Verteiltes Modell	31
4.5.3	Verteiltes Modell	32
4.5.4	Flaches Modell.....	33
4.5.5	Benutzer Trustmodell	34
4.6	Zertifikatsüberprüfung.....	35

Zusammenfassung – Security Management

5	Governance, Risk and Compliance	36
5.1	Definitionen GRC.....	36
5.2	Corporate Governance	37
5.3	IT Governance	38
5.3.1	Ziele IT Governance	39
5.4	Compliance	40
5.4.1	Ziele Compliance	40
5.4.2	Modelle und Referenzen Compliance	41
5.5	GRC Anwendungsfall.....	42
5.5.1	Audit and Assurance.....	42
5.6	Nutzen GRC	43
5.6.1	Umsetzung GRC	43
5.7	Frameworks	44
5.7.1	Open Compliance and Ethics Group (OCEG)	44
5.7.2	ISO / IEC 38500:2008	45
5.7.3	Committee of Sponsoring Organizations (COSO)	46
5.7.4	COBIT 5	47
5.8	Zusammenfassung GRC	49
6	Stichwortverzeichnis	50

1 Begriffe

Was verstehen wir unter «Risiko» ?

- **Generelle Risiko-Definition der ISO:**
„Wirkung von Ungewissheit auf Ziele“
(ISO Guidle 73 2009)
- **Risiko-Definition im betriebswirtschaftlichen Praxiseinsatz:**
„Ein Risiko ist eine nach Wahrscheinlichkeit (Eintritts-Häufigkeit) und Auswirkung bewertete Bedrohung eines zielorientierten Systems.“
Das Risiko betrachtet dabei die unerwünschte und ungeplante Abweichung von erwarteten Systemzielen.“
Dem Risiko kann auch eine positive Abweichung, d.h. eine Chance, gegenüberstehen.

Begriffe

- **Bedrohungen**
- Unerwünschte **Zielabweichungen**
- **Folgen** der Ziel-Abweichungen (z.B. Abweichungen von Geschäftszielen)
- **Wahrscheinlichkeit** des Eintretens von möglichen Folgen
- **Eintritts-Häufigkeit**
- Geschätzte **Schadenshöhe**
- Keine Möglichkeiten von Zielabweichungen = «**sicher**»
- In Informationssicherheit: «**System-Ziel**» => «**Sicherheits-Ziel**»

Bedrohung ist extern und Schwachstelle intern

Anmerkung: Unter «System» wird in diesem Zusammenhang ein allgemeines System verstanden, das beispielsweise ein ökonomisches, ein gesellschaftliches oder ein technisches System mit zielorientierten Werten sein kann. Systeme mit ihren Untersystemen interagieren untereinander und werden für eine Risikobetrachtung entsprechend definiert und abgegrenzt.

Praktisches Risiko-Modell



- **«Objekte» (Assets):** sind Unternehmenswerte. materiell (z.B. Gebäude, Hardware) oder immateriell (z.B. Informationen, Service-Prozesse)
- Bei Risiko Objekten «primäre» Systemziele:
 - «Vertraulichkeit»,
 - «Integrität» und
 - «Verfügbarkeit»
 bei Informationen oder
 - „Qualität“
 - „Termin“ und
 - „Kosten“
 bei Projekten.
- **«Massnahmen»:** sämtliche Vorehrungen, Anordnungen und Eigenschaften, die ein Schutzobjekt zu schützen vermögen.
- **«Schwachstellen»:** ungenügende oder fehlende Massnahmen

ISO Begriff	Begriff im deutschsprachigen Raum
Asset	Schutzobjekt (=alles was für ein Unternehmen von Wert ist, z.B. Information, Software, physische Einrichtungen wie Computer, Services, Personen, nichtgreifbare Werte wie Reputation)
Threat	Bedrohung (=potentielle Ursache für ein ungewolltes Ereignis das dem Unternehmen schaden könnte)
Control (Safeguard)	Massnahme (=Mittel zur Behandlung von Risiken, einschl. Policies, Prozeduren, Richtlinien etc.)
Vulnerability	Verletzlichkeit oder Schwachstelle (=durch Bedrohungen ausnutzbare Schwäche)
Impact	Auswirkung eines Schadensereignisses (=negativer Einfluss auf die Erreichung von Geschäftszielen)
Probability	Wahrscheinlichkeit eines Ereignisses (=mathematische Variable mit numerischen Werten zwischen 0 und 1) oder in %
Likelihood, Frequency	Häufigkeit des Auftretens innerhalb einer <u>Zeitperiode</u>
Residual Risk	Restrisiko (=Risiko nach der Behandlung mit Massnahmen)

2 Einführung

2.1 Risikoberechnung

Vorsicht bei der Anwendung der einfachen Risikoformel und «quantitativen» Berechnung

$$R = p_E * S_E$$

R: Risiko;

p_E : Wahrscheinlichkeit, dass ein Schadensereignis mit dem Schaden S_E eintritt;

S_E : Ausmass des Schadensereignisses (auch Tragweite oder Verlust).

$$R_T = H_T * S$$

Vorausgesetzt ist dass man die Häufigkeit kennt.

R_T : in der **Zeitperiode T**, „erwarteter“ Schaden;

H_T : in der Zeitperiode T erwartete Anzahl (Häufigkeit) der Schadenseintritte;

S: erwartete (durchschnittliche) Schadenshöhe der eintretenden Schadensereignisse.

Anm.: Vorsichtigerweise wird in ISO Guide 73 und ISO/IEC 27000 „Risiko“ lediglich als „Kombination“ von „Wahrscheinlichkeit“ und „Konsequenzen“ eines Ereignisses definiert.

2.2 Risikobestimmungsmatrix

Risikobestimmung mittels Risiko-Matrix

Monetarisierte Risiko-Werte in Mio. €					
bis 0,1	0,1 - 0,3	0,3 - 1	1 - 3	3 - 10	über 10
sehr klein	klein	mittel	gross	sehr gross	katastrophal
Schadenshöhe pro Fall	E klein	D mittel	C gross	B sehr gross	A katastrophal
Häufigkeit der Fälle					
sehr oft (mehrmals pro Jahr)	mittel	gross	sehr gross	irreal	irreal
oft (1 mal in 1 – 3 Jahren)	klein	mittel	gross	sehr gross	irreal
seltene (1 mal in 3 – 10 Jahren)	sehr klein	klein	mittel	gross	katastrophal
sehr selten (1 mal in 10 – 30 Jahren)	sehr klein	klein	klein	mittel	katastrophal
unwahrscheinlich (1 mal in mehr als 30 Jahren)	sehr klein	sehr klein	klein	mittel	katastrophal (*)

Für seltene Fälle mit katastrophalen Schäden wird das Risiko mit der Höhe des Schadens gleichgesetzt.

- Instrument zur pragmatischen Einschätzung und Bewertung der Risiken
- „Semiquantitative“ Darstellung
- Risiko-Wahrnehmung des Managements „vorprogrammieren“

Schadensmetrik in einem Unternehmen

Impacts	Direkter finanzieller Verlust [€] (Barwert der Ersatzkosten + Opportunitäts-Kosten)	Sonstige firmentypische Schadensauswirkungen		
		Schädigung der geschäftlichen und wirtschaftlichen Interessen	Nichteinhaltung gesetzlicher und regulatorischer Verpflichtungen (*)	Beeinträchtigung der Gesundheit, Sicherheit und des Schutzes anderer Personen
Stufe				
A katastrophal	Über 15 Mio. € (z.B. Verlust einer wichtigen Lizenz, so dass Geschäftstätigkeit aufgegeben werden muss)	z.B. Grossabnehmer kündigen Verträge aufgrund bekannt gewordener negativer Produkteigenschaften (z.B. krankmachendes Stoffumwelt)	-	Systematische Schädigung von Leib und Leben anderer Personen
B sehr gross	5-15 Mio. € (z.B. aufgrund lang anhaltender Produktions-Ausfälle)	z.B. Einige Abnehmer stellen auf Alternativprodukte um, infolge preisgegebener Produktionssecrenisse	Strafe infolge Verstoss gegen Kartellrecht	Schädigung von Leib und Leben anderer Personen im Einzelfall

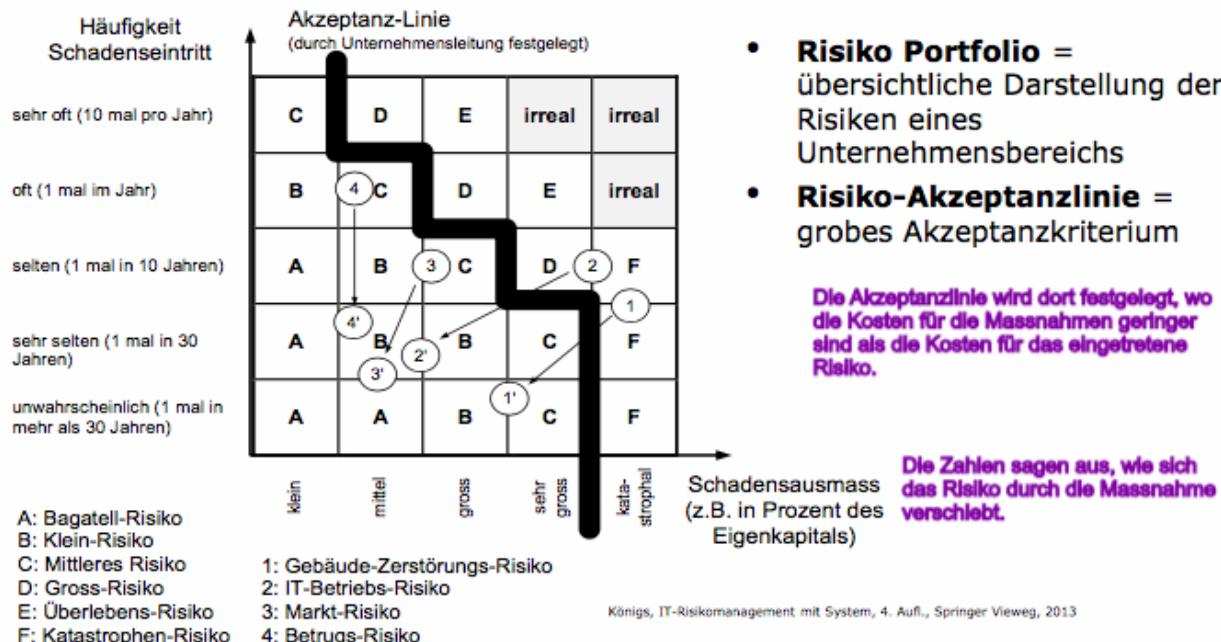
- Einstufungs-Kriterien
- Einheitliche Schadens-Metrik
- Monetäre Höhe
- Bewilligung und Inkraftsetzung Schadenseinstufungstabelle durch Geschäftsleitung

Nicht monetäre Schaden:

- Image
- Ausfälle

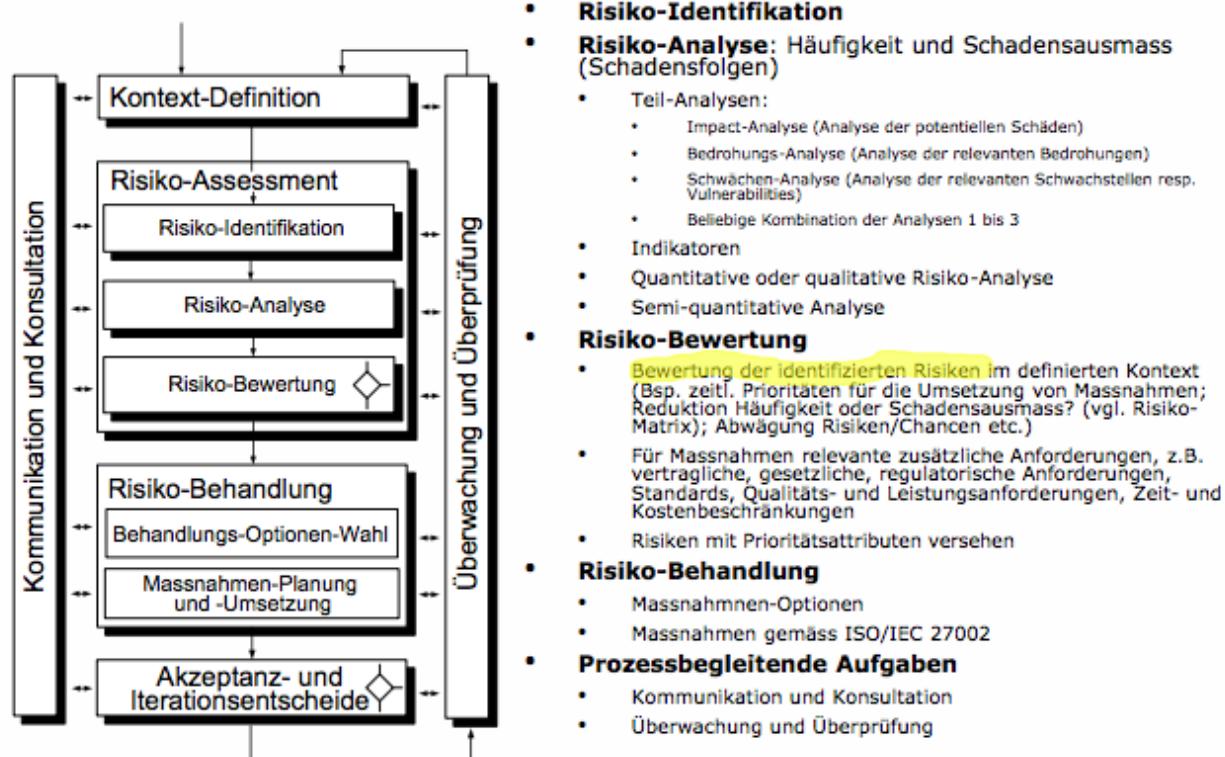
2.3 Risiko-Portfolio

Risiko-Portfolio in Risk-Map mit Akzeptanzlinie

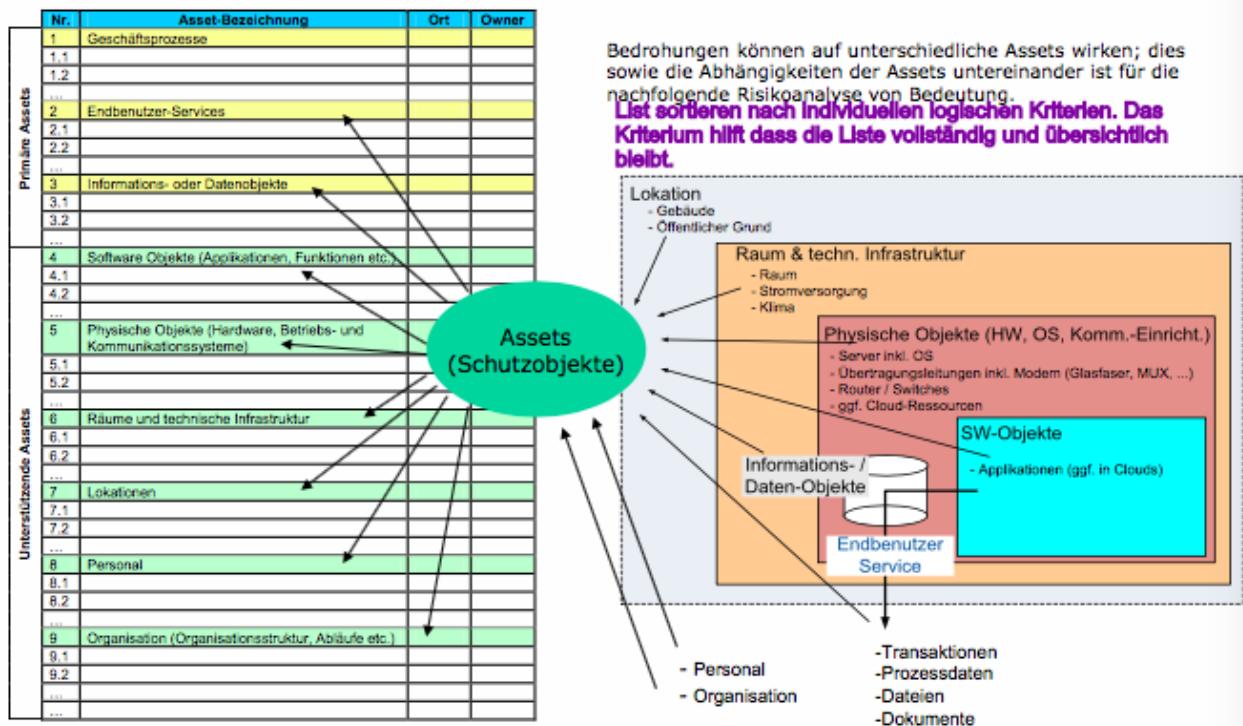


2.4 Risiko-Assessment

Risiko-Assessment im «fusionierten» Standard-Prozess (Fusion aus ISO 31000, ISO/IEC 27005, BS31100 und ONR 49001)



2.5 Risikoidentifikation



Beispiel IT-Risikokatalog (Risk-Register) mit Risikobewertung

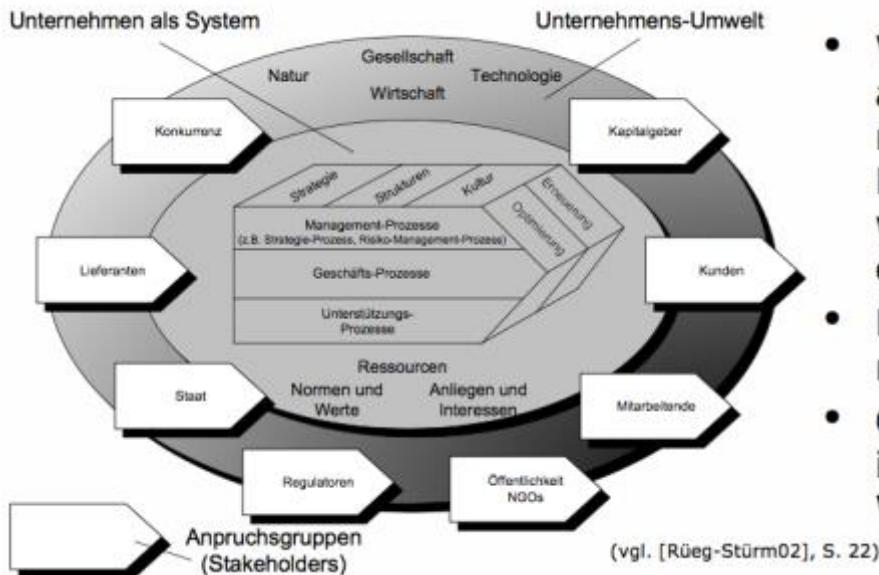
Nr.	Primärer Asset	Unterstützende Assets	Risiko-Assessment				Bewertung																							
			Identifikation		Analyse																									
			Risiko-Bezeichnung	Spezifische Bedrohung	Schwachstellen (& Abhängigkeiten)	Schadensszenario																								
1.1	Hardware Software Personal	Betrug an Kundenvermögen	Maskerade einer Benutzer-Identität	Unachtsamkeit Benutzer	Diebstahl Kunden-Credentials mittels Phishing-Attacke	<table border="1"> <tr> <td>s. klein (1)</td> <td>klein (2)</td> <td>mittel (3)</td> <td>gross (4)</td> <td>s. gross (5)</td> </tr> </table>	s. klein (1)	klein (2)	mittel (3)	gross (4)	s. gross (5)	<table border="1"> <tr> <td>Wiederherstellbarkeit</td> <td>Imageverlust</td> <td>Unerlaubter finanzieller Schaden</td> <td>Vertraulichkeitsverlust</td> <td>Informations-Kriterium</td> </tr> </table>	Wiederherstellbarkeit	Imageverlust	Unerlaubter finanzieller Schaden	Vertraulichkeitsverlust	Informations-Kriterium	<table border="1"> <tr> <td>Häufigkeit</td> <td>Akzeptanz-Vorgaben:</td> </tr> <tr> <td>> 5 Mal pro Jahr (5)</td> <td>a = vermeiden oder reduzieren;</td> </tr> <tr> <td>1-5 Mal pro Jahr (4)</td> <td>b = bewältigen nach wirtsch. Aspekten</td> </tr> <tr> <td>1 Mal in 1-3 Jahren (3)</td> <td>c = tragen unter Beobachtung,</td> </tr> <tr> <td>1-10 Jahre (2)</td> <td>Zeitprioritäten für Umsetzung:</td> </tr> <tr> <td>> 10 Jahre (1)</td> <td>1 = hoch; sofort; 2 = mittel; im Rahmen Budget; 3 = tief; in nächster Strategie-/ Budget-Periode einplanen.</td> </tr> </table>	Häufigkeit	Akzeptanz-Vorgaben:	> 5 Mal pro Jahr (5)	a = vermeiden oder reduzieren;	1-5 Mal pro Jahr (4)	b = bewältigen nach wirtsch. Aspekten	1 Mal in 1-3 Jahren (3)	c = tragen unter Beobachtung,	1-10 Jahre (2)	Zeitprioritäten für Umsetzung:	> 10 Jahre (1)	1 = hoch; sofort; 2 = mittel; im Rahmen Budget; 3 = tief; in nächster Strategie-/ Budget-Periode einplanen.
s. klein (1)	klein (2)	mittel (3)	gross (4)	s. gross (5)																										
Wiederherstellbarkeit	Imageverlust	Unerlaubter finanzieller Schaden	Vertraulichkeitsverlust	Informations-Kriterium																										
Häufigkeit	Akzeptanz-Vorgaben:																													
> 5 Mal pro Jahr (5)	a = vermeiden oder reduzieren;																													
1-5 Mal pro Jahr (4)	b = bewältigen nach wirtsch. Aspekten																													
1 Mal in 1-3 Jahren (3)	c = tragen unter Beobachtung,																													
1-10 Jahre (2)	Zeitprioritäten für Umsetzung:																													
> 10 Jahre (1)	1 = hoch; sofort; 2 = mittel; im Rahmen Budget; 3 = tief; in nächster Strategie-/ Budget-Periode einplanen.																													
1.2	Zahlungswesen E-Banking	Authentisierungs- system Hardware Software	Ausspielen Bankdaten	Schwaches Authentisierungs- verfahren		<table border="1"> <tr> <td>4</td> <td>3</td> <td>2</td> <td>1</td> <td>x</td> </tr> </table>	4	3	2	1	x	<table border="1"> <tr> <td>Wiederherstellbarkeit</td> <td>Imageverlust</td> <td>Unerlaubter finanzieller Schaden</td> <td>Vertraulichkeitsverlust</td> <td>Informations-Kriterium</td> </tr> </table>	Wiederherstellbarkeit	Imageverlust	Unerlaubter finanzieller Schaden	Vertraulichkeitsverlust	Informations-Kriterium	<table border="1"> <tr> <td>Häufigkeit</td> <td>Akzeptanz-Vorgaben:</td> </tr> <tr> <td>> 5 Mal pro Jahr (5)</td> <td>a = vermeiden oder reduzieren;</td> </tr> <tr> <td>1-5 Mal pro Jahr (4)</td> <td>b = bewältigen nach wirtsch. Aspekten</td> </tr> <tr> <td>1 Mal in 1-3 Jahren (3)</td> <td>c = tragen unter Beobachtung,</td> </tr> <tr> <td>1-10 Jahre (2)</td> <td>Zeitprioritäten für Umsetzung:</td> </tr> <tr> <td>> 10 Jahre (1)</td> <td>1 = hoch; sofort; 2 = mittel; im Rahmen Budget; 3 = tief; in nächster Strategie-/ Budget-Periode einplanen.</td> </tr> </table>	Häufigkeit	Akzeptanz-Vorgaben:	> 5 Mal pro Jahr (5)	a = vermeiden oder reduzieren;	1-5 Mal pro Jahr (4)	b = bewältigen nach wirtsch. Aspekten	1 Mal in 1-3 Jahren (3)	c = tragen unter Beobachtung,	1-10 Jahre (2)	Zeitprioritäten für Umsetzung:	> 10 Jahre (1)	1 = hoch; sofort; 2 = mittel; im Rahmen Budget; 3 = tief; in nächster Strategie-/ Budget-Periode einplanen.
4	3	2	1	x																										
Wiederherstellbarkeit	Imageverlust	Unerlaubter finanzieller Schaden	Vertraulichkeitsverlust	Informations-Kriterium																										
Häufigkeit	Akzeptanz-Vorgaben:																													
> 5 Mal pro Jahr (5)	a = vermeiden oder reduzieren;																													
1-5 Mal pro Jahr (4)	b = bewältigen nach wirtsch. Aspekten																													
1 Mal in 1-3 Jahren (3)	c = tragen unter Beobachtung,																													
1-10 Jahre (2)	Zeitprioritäten für Umsetzung:																													
> 10 Jahre (1)	1 = hoch; sofort; 2 = mittel; im Rahmen Budget; 3 = tief; in nächster Strategie-/ Budget-Periode einplanen.																													
1.3	Internet Portal Netzwerk Hardware Sicherheitssoftware	Lahmlegen E-Banking	Denial of Service- Attacke	keine technischen und vorrangigen Massnahmen	gezielte Blockade des Internet-Zugangs mittels Distributed-Denial-of-Service-Attacke	<table border="1"> <tr> <td>2</td> <td>3</td> <td>2</td> <td>x</td> <td></td> </tr> </table>	2	3	2	x		<table border="1"> <tr> <td>Wiederherstellbarkeit</td> <td>Imageverlust</td> <td>Unerlaubter finanzieller Schaden</td> <td>Vertraulichkeitsverlust</td> <td>Informations-Kriterium</td> </tr> </table>	Wiederherstellbarkeit	Imageverlust	Unerlaubter finanzieller Schaden	Vertraulichkeitsverlust	Informations-Kriterium	<table border="1"> <tr> <td>Häufigkeit</td> <td>Akzeptanz-Vorgaben:</td> </tr> <tr> <td>> 5 Mal pro Jahr (5)</td> <td>a = vermeiden oder reduzieren;</td> </tr> <tr> <td>1-5 Mal pro Jahr (4)</td> <td>b = bewältigen nach wirtsch. Aspekten</td> </tr> <tr> <td>1 Mal in 1-3 Jahren (3)</td> <td>c = tragen unter Beobachtung,</td> </tr> <tr> <td>1-10 Jahre (2)</td> <td>Zeitprioritäten für Umsetzung:</td> </tr> <tr> <td>> 10 Jahre (1)</td> <td>1 = hoch; sofort; 2 = mittel; im Rahmen Budget; 3 = tief; in nächster Strategie-/ Budget-Periode einplanen.</td> </tr> </table>	Häufigkeit	Akzeptanz-Vorgaben:	> 5 Mal pro Jahr (5)	a = vermeiden oder reduzieren;	1-5 Mal pro Jahr (4)	b = bewältigen nach wirtsch. Aspekten	1 Mal in 1-3 Jahren (3)	c = tragen unter Beobachtung,	1-10 Jahre (2)	Zeitprioritäten für Umsetzung:	> 10 Jahre (1)	1 = hoch; sofort; 2 = mittel; im Rahmen Budget; 3 = tief; in nächster Strategie-/ Budget-Periode einplanen.
2	3	2	x																											
Wiederherstellbarkeit	Imageverlust	Unerlaubter finanzieller Schaden	Vertraulichkeitsverlust	Informations-Kriterium																										
Häufigkeit	Akzeptanz-Vorgaben:																													
> 5 Mal pro Jahr (5)	a = vermeiden oder reduzieren;																													
1-5 Mal pro Jahr (4)	b = bewältigen nach wirtsch. Aspekten																													
1 Mal in 1-3 Jahren (3)	c = tragen unter Beobachtung,																													
1-10 Jahre (2)	Zeitprioritäten für Umsetzung:																													
> 10 Jahre (1)	1 = hoch; sofort; 2 = mittel; im Rahmen Budget; 3 = tief; in nächster Strategie-/ Budget-Periode einplanen.																													
...																						

Risiko-Bewertung sowohl nach "Wichtigkeit" als auch nach "Dringlichkeit" der Massnahmen

Risiko-Bewertung der "Wichtigkeit" der Massnahmen anhand Risiko-Matrix:

Häufigkeit	Schaden				
	4	3	2	1	0
4	b	b	a	a	a
3	b	b	a	a	a
2	c	b	b	b	b
1	c	c	b	b	b
0	c	c	c	b	b
	0	1	2	3	4
	Schaden				

2.6 Management-Systeme im Unternehmen



- Wertschöpfungsaktivitäten und dazu notwendige Führungsarbeiten werden in Prozessen erbracht
- Erneuerung = radikaler Wandel
- Optimierung = inkrementaler Wandel

- Jedes Unternehmen wird mittels eines mehr oder weniger gut entwickelten Management-Systems (auch Führungssystem) geführt
- **Managementsysteme** beschreiben die Aufgaben des Managements und definieren Methoden, um die Management-Aufgaben (Ziele setzen, steuern und kontrollieren) erfolgreich zu bewältigen (Wikipedia).
- Einige Einzel-Management-Systeme sind stark ausgebaut
 - Vorgabe «Strukturen», «Prozesse», «Mittel» und «Methoden»
- Ein Unternehmens-Management-System kann aus einem oder mehreren Einzel-Management-Systemen bestehen, z.B. :
 - Risikomanagement-System (ISO 31000)
 - Business-Continuity-Management-System (ISO 22301, BS 25999-2)
 - Qualitäts-System (ISO 9001),
 - Umwelt-Management-System (ISO 14001),
 - Informations-Sicherheits-Management-System (ISO/IEC 27001)
 - Service-Management-System (ITIL oder ISO/IEC 20000-x)

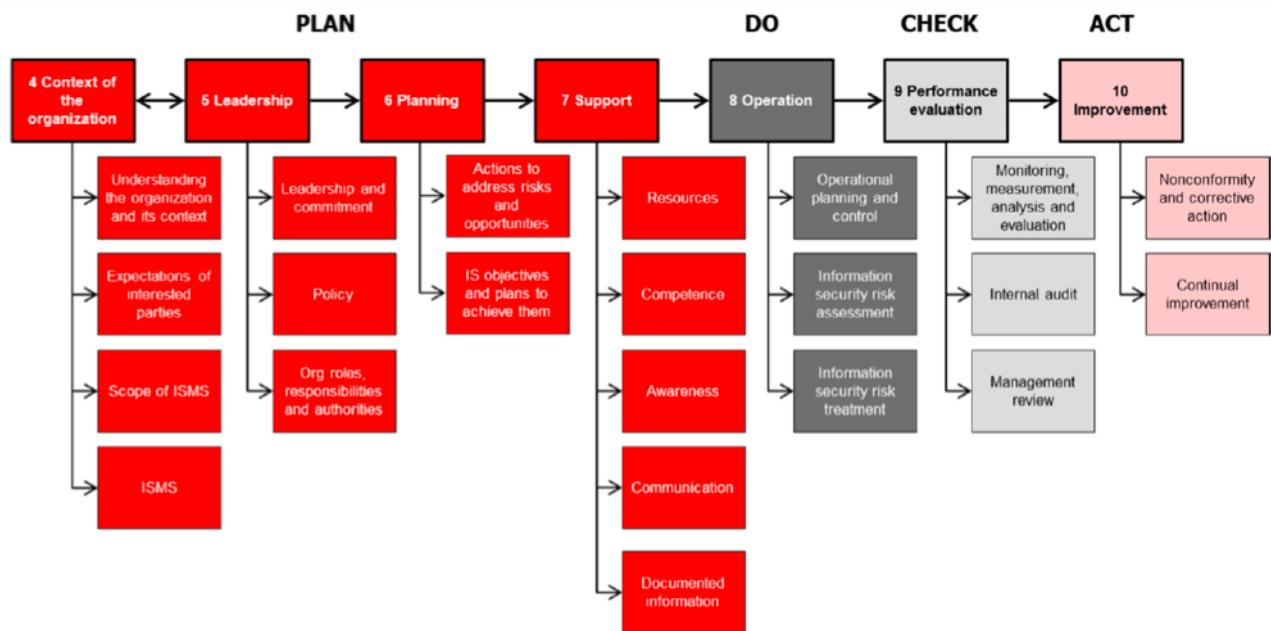
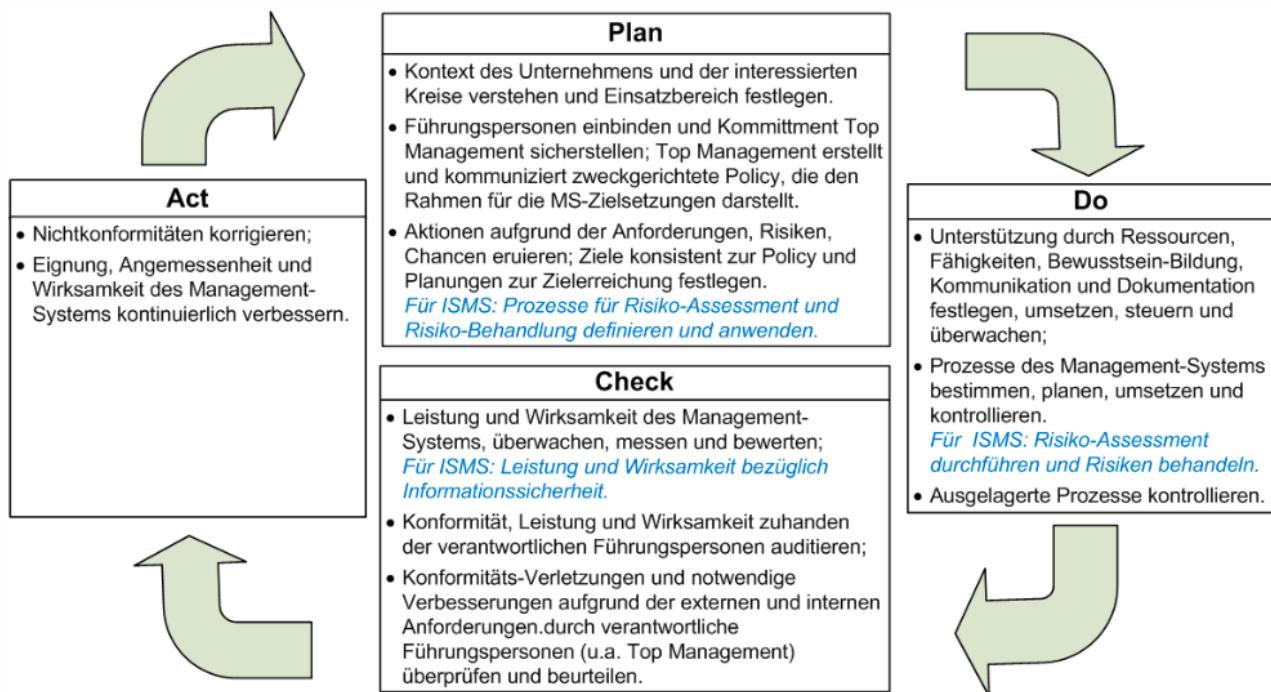
Eigenschaften neuerer Management-Systeme

- Als **Prozesse** aufgebaut; diese zielen auf
 - Anpassung hinsichtlich zukünftiger Veränderungen und
 - laufende Verbesserung und Optimierung
- **Plan-Do-Check-Act-Zyklus**
 - ursprünglich Shewhart*-Cycle und später als Deming**-cycle bekannt gewordenes Qualitäts-Management-Modell

* Walter A. Shewhart; **W. Edwards Deming
- **Unternehmenskultur** (u.a. Management-Commitment und Mitarbeiterverhalten) ist wesentlicher Bestandteil dieser Systeme.
- **Vereinheitlichung** der Vielzahl von ISO/IEC-Standards über Managementsysteme (z.B. 27001 oder 9001) in neueren Releases. Der PDCA-Zyklus ist dabei nur noch implizit enthalten (z.B. in ISO 27001).

2.7 PDCA

Vereinheitlichter Aufbau von Managementsystemen im Hinblick auf ISO/IEC 27001:2013 „Information security management system“ (ISMS)



2.8 ISO 27002:2013

9 Access control ← Eine von 14 Domänen

Eines von 35 Kontrollzielen
(engl. Control Objectives)

9.1 Business requirements of access control

Objective: To limit access to information and information processing facilities.

9.1.1 Access control policy

Control ← Eine von 114 Kontrollen (Massnahmen, Prüfpunkte)

An access control policy should be established, documented and reviewed based on business and information security requirements.

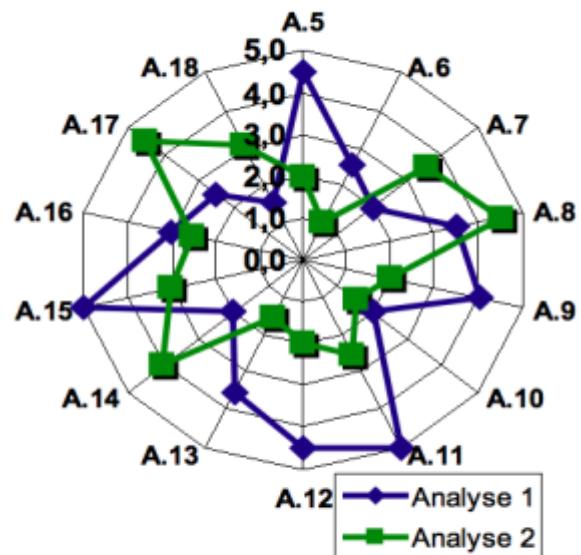
2.8.1 Statement of Applicability

Paragraph	Massnahmenziel (Control Objective 27002)	Massnahme (Control 27002)	Anwendbar ja/nein	Bemerkungen:
				1) Begründung Massnahmenwahl 2) Bereits bestehende Massnahmen 3) Nichtverwendung von Massnahmen aus Anhang A und Begründung 4) Referenz-Dokumente (Beispiele)
A.5	Information security policies			
A.5.1	Management direction for information security	A.5.1.1 Policies for information security	ja	Dokumente Nr. 001 „Informationssicherheits- Politik“ Nr. 002 bis Nr. 013 „Information security policies“ für spezifische Sicherheitsgebiete (Policies =Weisungen, Richtlinien, Standards etc.)
		A.5.1.2 Review of policies for information security	ja	Vorgehen (Prozess, Frequenz, Adressaten etc.) in Dokument 001 festgelegt.
A.6	Organisation of information security			
A.6.1	Internal Organisation	A.6.1.1 Information security roles and	ja	In Dokument Nr. 001 „Informationssicherheits- Politik“

2.8.2 Schwachstellenanalyse

Sicherheitskapitel und Unterkapitel ISO/IEC 27002:2013		
A.5	Informationssicherheits-Policies ▪ Management-Vorgaben	A.12 Betriebssicherheit ▪ Betriebsverfahren und -Verantwortlichkeiten ▪ Schutz vor Schadsoftware ▪ Datensicherung ▪ Aufzeichnungen und Überwachung ▪ Schutz des Systembetriebs ▪ Management technischer Schwachstellen ▪ Rücksichtnahme bei Audit-Aktivitäten
A.6	Organisation der Informationssicherheit ▪ Interne Organisation ▪ Mobile Geräte und Telearbeit	A.13 Kommunikationsicherheit ▪ Management der Netzwerksicherheit ▪ Informationstransfer
A.7	Personalsicherheit ▪ Vor der Anstellung ▪ Während der Anstellung ▪ Bei Austritt und Veränderung	A.14 Beschaffung, Entwicklung und Wartung von Informationssystemen ▪ Sicherheitsanforderungen an Informationssysteme ▪ Sicherheit bei Entwicklung und Support ▪ Testdaten
A.8	Management von organisationseligen Werten ▪ Verantwortlichkeiten für Vermögenswerte ▪ Klassifizierung der Information ▪ Handhabung von Medien	A.15 Lieferantenbeziehungen ▪ Informationssicherheit in Lieferantenbeziehungen ▪ Service-Lieferungs-Management mit Lieferanten
A.9	Zugriffskontrolle ▪ Geschäftsanforderungen für die Zugriffskontrolle ▪ Management Benutzer-Zugriffe ▪ Benutzer-Verantwortlichkeiten ▪ System- und Applikations-Zugriffskontrolle	A.16 Management von Informations-Sicherheitsvorfällen ▪ Management der Informations-Sicherheits-Vorfälle und -Verbesserungen
A.10	Kryptographie ▪ Kryptographische Massnahmen	A.17 Informationssicherheits-Aspekte beim Management der Geschäfts-Kontinuität ▪ Informationssicherheits-Kontinuität ▪ Redundanzen
A.11	Physische und umgebungsbezogene Sicherheit ▪ Sicherheitsbereiche ▪ Ausstattungen und Einrichtungen	A.18 Einhaltung von Vorgaben und Verpflichtungen ▪ Einhaltung von gesetzlichen und vertraglichen Anforderungen ▪ Informationssicherheits-Überprüfungen

Beispiel:



Noten für Zielerreichung pro Kapitel:
sehr gut = 5; keine = 0.

Königs, IT-Risikomanagement mit System, 5. Aufl., Springer Vieweg, 2015

2.9 Rollen Informationssicherheit

- Verwaltungsrat mit Präsident
- Geschäftleitung mit CEO
- CSO oder CISO
- Prüfungsausschuss
- Interne Kontrolle (Interne Revision oder Inspektorat)
- Informatik mit CIO
- Linien-Vorgesetzte
- (Prozess)-Owner mit Sicherheitsverantwortung für abgrenzten Bereich
- Sicherheitsadministratoren
- Benutzer

3 Zertifikatsbasierende Anwendungen und PKI

3.1 Gesetzliche Vorschriften

- **Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES)¹**
- **Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (VZertES)**
- Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur (TAV)
- OR (Art. 14 Abs. 2^{bis})

Gleichstellung mit der eigenhändigen Unterschrift

- OR Art. 14 Abs. 2^{bis}

Der eigenhändigen Unterschrift gleichgestellt ist die qualifizierte elektronische Signatur, die auf einem qualifizierten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom 19. Dezember 2003 über die elektronische Signatur beruht. (...)

Formfreiheit

- Vertragsparteien können selber bestimmen, in welcher Form sie Verträge miteinander abschliessen wollen (mündlich, schriftlich etc.)
- Die Form muss nur dort eingehalten werden, wo sie explizit vom Gesetzgeber gefordert wird (OR Art. 11)
- Nur dort wo die *schriftliche Form* – also eine *eigenhändige Unterschrift* – gefordert wird (z. B. bei einem Lehrvertrag oder bei Grundstücksgeschäften), muss eine *qualifizierte elektronische Signatur* auf der Basis eines *qualifizierten Zertifikats* einer *anerkannten Anbieterin von Zertifizierungsdiensten* gesetzt werden
- In den übrigen Fällen können sich die Vertragsparteien auf das zu verwendende Zertifikat einigen (fortgeschrittenes Zertifikat oder sonst ein Zertifikat)
- In der Regel werden fortgeschrittene Zertifikate verwendet, wenn keine qualifizierten Zertifikate notwendig sind (sie sind je nach Herausgeber günstiger, bieten auch ein hohes Mass an Sicherheit und können in den verschiedensten Bereichen angewendet werden)

Haftung nach OR

Art. 59a²¹

¹ Der Inhaber eines Signaturschlüssels haftet Drittpersonen für Schäden, die diese erleiden, weil sie sich auf das qualifizierte gültige Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom 19. Dezember 2003²² über die elektronische Signatur verlassen haben.

² Die Haftung entfällt, wenn der Inhaber des Signaturschlüssels glaubhaft darlegen kann, dass er die nach den Umständen notwendigen und zumutbaren Sicherheitsvorkehrungen getroffen hat, um den Missbrauch des Signaturschlüssels zu verhindern.

Haftung nach ZertES

Art. 16 Haftung der Anbieterin von Zertifizierungsdiensten

¹ Die Anbieterin von Zertifizierungsdiensten haftet der Inhaberin oder dem Inhaber des Signaturschlüssels und Drittpersonen, die sich auf ein gültiges qualifiziertes Zertifikat verlassen haben, für Schäden, die diese erleiden, weil die Anbieterin den Pflichten aus diesem Gesetz und den entsprechenden Ausführungsvorschriften nicht nachgekommen ist.

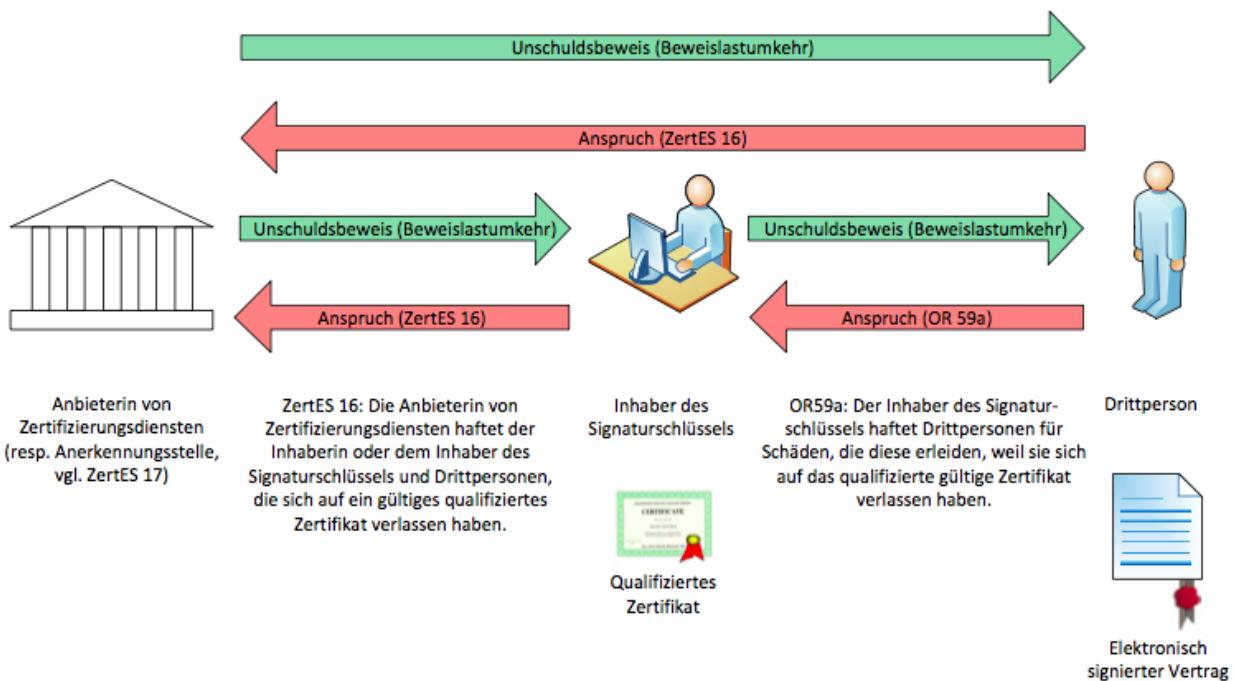
² Sie trägt die Beweislast dafür, den Pflichten aus diesem Gesetz und den Ausführungsvorschriften nachgekommen zu sein.

³ Sie kann ihre Haftung aus diesem Gesetz weder für sich noch für Hilfspersonen wegbedingen. Sie haftet jedoch nicht für Schäden, die sich aus der Nichtbeachtung oder Überschreitung einer Nutzungsbeschränkung (Art. 7 Abs. 2) ergeben.

Art. 17 Haftung der Anerkennungsstelle

Die Anerkennungsstelle nach Artikel 2 Buchstabe h haftet der Inhaberin oder dem Inhaber des Signaturschlüssels und Drittpersonen, die sich auf ein gültiges qualifiziertes Zertifikat verlassen haben, für Schäden, die diese erleiden, weil die Anerkennungsstelle ihren Pflichten aus diesem Gesetz und den Ausführungsvorschriften nicht nachgekommen ist. Artikel 16 Absätze 2 und 3 gilt sinngemäß.

Haftung – Beweislastumkehr



- Die **Beweislastumkehr** wirkt sich zum Nachteil der beklagten Partei aus, da es in der Regel schwierig ist, seine **Unschuld** zu beweisen
- Dies erhöht den Druck auf die Anerkennungsstelle, die Anbieterin von Zertifizierungsdiensten resp. den **Inhaber des Signaturschlüssels** alle Anforderungen zu erfüllen

3.1.1 Signatur Unterscheidung

- Digitale Signatur:** kryptografische Verfahren (technischer Begriff)
- Elektronische Signatur:** wie eigenhändig unterschr. (rechtlicher Begriff)

Elektronische Signatur	Fortgeschrittenes Signatur	Qualifizierte Signatur
Sicherheit: niedrig	Sicherheit: hoch	Sicherheit: sehr hoch
Bsp: private / geschäftliche E-Mail mit Signatur From: Max Mustermann To: Lisa Mustermann Subject: Testmail Liebe Lisa, hier der Text. LG Max ----- Max Mustermann John-Doe-Str. 1 99999 Musterstadt	Bsp: PGP/SMIME-signierte E-Mail From: Max Mustermann To: Lisa Mustermann Subject: Testmail -----BEGIN PGP MESSAGE----- Version: GnuPG v2 Liebe Lisa, hier der Text. LG Max -----BEGIN PGP SIGNATURE----- Version: GnuPG v2 iQEcBAEBCAAGBQJWOIv4AAoJE [...] M4PXLmzSiGD1QxzN3ve6/Sd1Uwo -----END PGP SIGNATURE-----	Zertifikat wird nach Identitätsprüfung ausgestellt. Eine sichere Signaturerstellungseinheit (SEE) - zum Beispiel ein spezielles Kartenlesegerät - ist erforderlich.

Fortgeschrittene elektronische Signatur

Gemäss Art. 2, lit. b, ZertES

- Ist ausschliesslich dem Inhaber zugeordnet
- Ermöglicht die Identifizierung des Inhabers
- Wird mit Mitteln erzeugt, welche der Inhaber unter seiner alleinigen Kontrolle hat
- Ermöglicht zu erkennen, wenn die Daten, auf die sie sich bezieht, nachträglich verändert wurden

Qualifizierte elektronische Signatur

Gemäss Art. 2, lit. c, ZertES

- Ist eine fortgeschrittene elektronische Signatur, die auf einer sicheren Signaturerstellungseinheit nach Art. 6, Abs. 1 und 2 und auf einem qualifizierten und zum Zeitpunkt der Erzeugung gültigen Zertifikat beruht

3.1.2 Anforderungen

Anforderungen an die Signaturerstellungseinheit

Sinngemäß nach Art. 6, Abs. 2, ZertES

- Die Signaturerstellungseinheit stellt sicher, dass der Signaturschlüssel nicht mehrfach auftreten kann («Geheimhaltung») ...
- ... und dass er nicht missbräuchlich durch unberechtigte Personen verwendet werden kann (nur autorisierte Verwendung)

Gemäss TAV (auszugsweise)

- Signaturerstellungseinheit ist nach Common Criteria EAL 4+ zertifiziert oder nach ITSEC Stufe E3



Beispiel: Aladdin eToken PRO 32K, 4.2B

Gemäss TAV (auszugsweise)

- Schlüsselpaar muss auf der Signaturerstellungseinheit berechnet werden
- Signaturschlüssel darf nicht verwendet werden können, bevor er aktiviert wurde (→ Transport-PIN und Token werden mit separater Post ausgeliefert)
- Signaturerstellungseinheit muss in einer sicheren Umgebung und unter der Kontrolle des Zertifikatsinhabers betrieben werden (vgl. den später beschriebenen Angriff auf die SuisseID)

Anforderungen an qualifizierte Zertifikate

Gemäss TAV zwingende Zertifikatsfelder (Auswahl)

- Key Usage (Schlüsselverwendungszweck): Nur Non Repudiation^{1 2} ist erlaubt
- Issuer Alternative Name (Name der Anerkennungsstelle), Bsp. QuoVadis-Zertifikat:

O=ZertES Recognition Body: KPMG AG

C=CH

Gemäss TAV zwingende Zertifikatsfelder (Auswahl)

- qcStatements (OID 1.3.6.1.5.5.7.1.3, «Anweisungen für qualifiziertes Zertifikat»^{1 4}), Bsp. QuoVadis-Zert.:

Dieses Zertifikat wurde in Übereinstimmung mit RFC3039² erzeugt

Qualifiziertes Zertifikat entsprechend der Umsetzung der EU-Direktive 1999/93/EC im Staat des Herausgebers

Monetäre Beschränkung³ = 100000 CHF

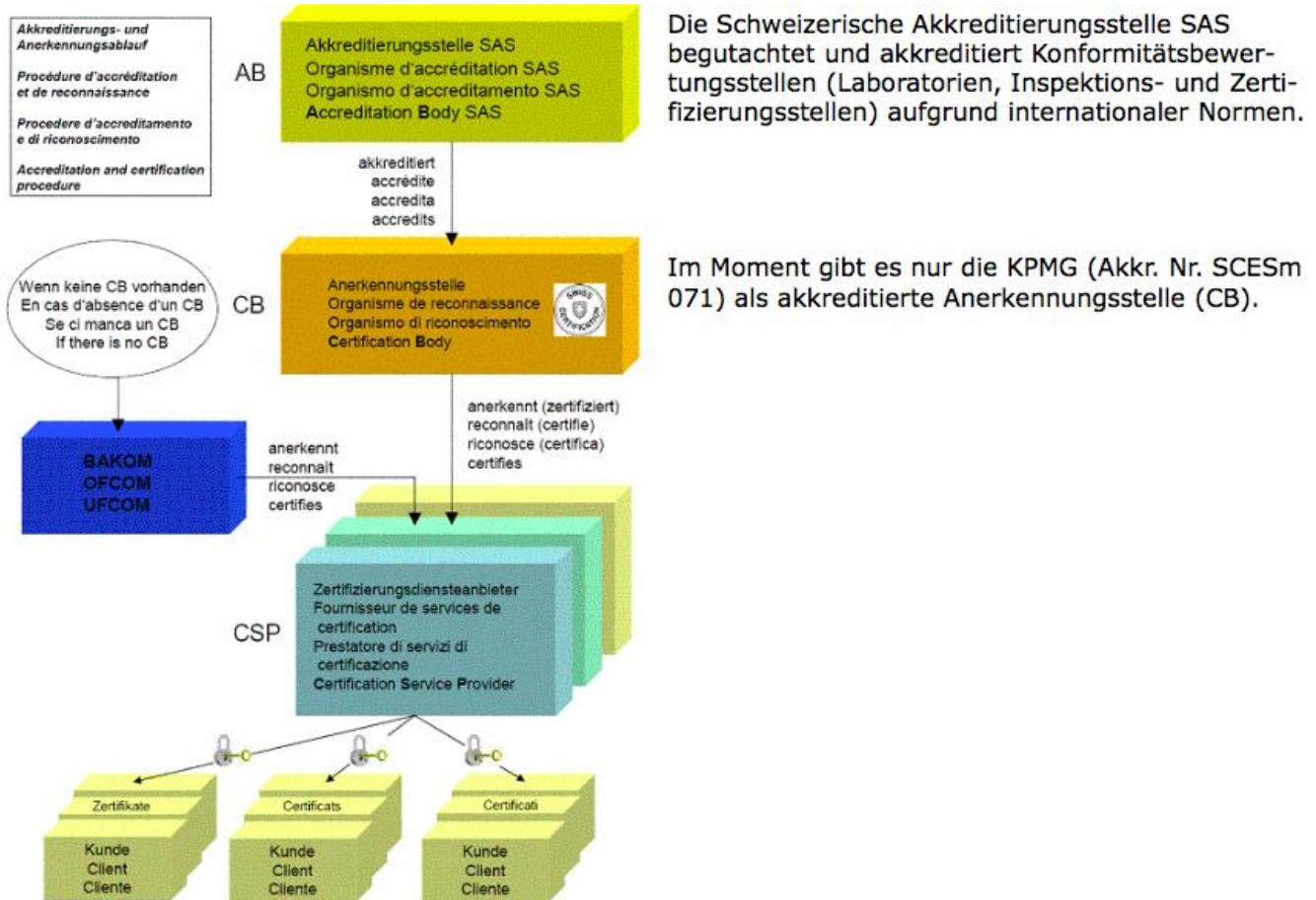
Gemäss Art. 8, ZertES

- Der Antragssteller muss persönlich bei der anerkannten Anbieterin von Zertifizierungsdiensten vorsprechen und den Nachweis seiner Identität erbringen
- Die Anbieterin von Zertifizierungsdiensten muss sich vergewissern, dass der Antragssteller im Besitze des entsprechenden Signaturschlüssels ist
- Sie darf die Aufgabe zur Identifikation von Antragsstellern delegieren (Registrierungsstellen, s.u.)

Wichtig:

- Da eine Firma in der Regel keine anerkannte Anbieterin von Zertifizierungsdiensten ist, können auf deren eigenen Zertifizierungsstelle auch keine qualifizierten Zertifikate ausgestellt werden
- In der Schweiz anerkannte Anbieterinnen von Zertifizierungsdiensten (Stand Anfang 2013)
 - Swisscom (Schweiz) AG
 - QuoVadis Trustlink Schweiz AG
 - SwissSign AG
 - Bundesamt für Informatik und Telekommunikation (BIT)

3.2 System für die Anerkennung von Zertifizierungsstellen



- Der Bundesrat bezeichnet die für die Akkreditierung der Anerkennungsstellen zuständige Stelle (SAS)
 - Vgl. Art. 1, VZertES
- Um sich als Anerkennungsstelle akkreditieren zu lassen (z.B. KPMG), müssen die Kriterien der europäischen Norm EN 45012 erfüllt werden
 - EN 45012: Allgemeine Anforderungen an Stellen, die Qualitätsmanagementsysteme begutachten und zertifizieren
- Anerkannte Zertifizierungsstellen müssen jedes Jahr Audits durchführen, um die Konformität ihrer Aktivitäten mit den relevanten Gesetzestexten und technischen Normen nachzuweisen

3.3 Gegenüberstellung der Zertifikatstypen

Gegenüberstellung Fortgeschrittenes vs. qualifiziertes Zertifikat (Hrsg. QuoVadis)

Zertifikatsfeld	Fortgeschrittenes Zertifikat	Qualifiziertes Zertifikat
Issuer	CN = QV Schweiz ICA OU = Issuing Certificate Authority O = QuoVadis Trustlink Schweiz AG C = CH	CN = QuoVadis Qualified Issuing Certification Authority 1 OU = Issuing Certification Authority O = QuoVadis Limited, Bermuda C = CH
Subject	E = hans.muster@bluewin.ch CN = Hans Muster OU = Standard Personal Certificate L = Luzern S = LU C = CH	E = hans.muster@bluewin.ch CN = Hans Muster SN = Muster G = Hans OU = Qualified Certificate L = Luzern S = LU C = CH
Issuer Alternative Name		Verzeichnisadresse: O=ZertES Recognition Body: KPMG AG C=CH
Key Usage	Digitale Signatur Nicht Abstreitbarkeit Schlüsselverschlüsselung Datenverschlüsselung Schlüsselvereinbarung	Nicht Abstreitbarkeit
Extended Key Usage	Serverauthentifizierung Clientauthentifizierung Sichere E-Mail Smartcard-Anmeldung	

- Das qualifizierte Zertifikat ist aus zwei Gründen nicht geeignet zum Verschlüsseln von Daten
 - Key Usage = Nicht-Abstreitbarkeit
 - Es gibt kein Backup vom privaten Schlüssel
- Da der Schlüsselverwendungszweck *Digitale Signatur* fehlt, kann es auch nicht zum Authentifizieren verwendet werden
- Fortgeschrittene Zertifikate sind im Gegensatz dazu in der Regel für unterschiedlichste Verwendungszwecke geeignet (und es gibt ein Backup)

SuisseID-Zertifikate

- Zur SuisseID gehören 2 Zertifikate (vgl. [1])
 - Ein qualifiziertes Zertifikat zum rechtsgültigen Signieren: *Qualified Certificate (QC)*
 - Ein nicht qualifiziertes Zertifikat zum Authentifizieren: *Identification and Authentication Certificate (IAC)*
- Beide Zertifikate und ihre privaten Schlüssel sind auf dem gleichen physischen Token abgelegt
- Für Ausstellung und Management kommen bei beiden Zertifikaten die gleichen organisatorischen und operationellen Abläufe zur Anwendung

- Neu: Jeder SuisseID-Besitzer wird über eine eindeutige, zertifikatsunabhängige Nummer identifiziert (sog. *SuisseID Number*, zu finden im Subject-Feld)
- Revokation macht diese Nummer nicht ungültig
- Anstelle des richtigen Namens kann im Zertifikat auch ein Pseudonym vermerkt werden
- Auch Berufsbezeichnungen (z.B. «Notar») können aufgenommen werden
- Wichtig: Zur SuisseID gehören standardmäßig keine Zertifikate zum Verschlüsseln (Begründung: Datenverlustrisiko/Key-Backup-Problematik)

Gegenüberstellung SuisseID IAC vs. SuisseID QC (Hrsg. SwissSign)

Zertifikatsfeld	SuisseID IAC	SuisseID QC
Issuer	CN = SwissSign SuisseID Platinum CA 2010 - G2 O = SwissSign AG C = CH	CN = SwissSign Qualified Platinum CA 2010 - G2 O = SwissSign AG C = CH
Subject	SERIALNUMBER = 1300-0010-9394-9155 E = hans.muster@bluewin.ch CN = Hans Muster (Authentication)	SERIALNUMBER = 1300-0010-9394-9155 E = hans.muster@bluewin.ch CN = Hans Muster (Qualified Signature)
Issuer Alternative Name		Verzeichnisadresse: O=ZertES Recognition Body: KPMG AG C=CH
Key Usage	Digitale Signatur	Nicht Abstreitbarkeit
Extended Key Usage	Clientauthentifizierung Sichere E-Mail Smartcard-Anmeldung	

3.4 Erstellung von qualifizierten Signaturen

Qualifizierte Signaturen können mit unterschiedlichen Produkten erstellt und verifiziert werden, z. B.

- Adobe Acrobat
- SwissSigner (für Privatgebrauch kostenlos, www.postsuisseid.ch, Produkt von Firma ABACUS)
- Sign! (kostenlos, www.quovadisglobal.ch, Produkt von Firma Intarsys)
- SecSigner (kostenlos, www.secommerce.de)
- OPENLiMiT Reader/CC Sign (Reader kostenlos, www.openlimit.com)
- In der Schweiz gibt es im Gegensatz zu Deutschland keine konkreten Sicherheitsanforderungen an die Software für die Erstellung und Verifikation von qualifizierten Signaturen (z.B. in Form einer Zertifizierung)
- Der Gesetzgeber schreibt auch nicht die Verwendung von Kartenlesern mit Key-Pad vor (Leser der Klasse 2 oder höher) zum Schutz der PIN vor Ausspionage durch Malware
- Diese Infrastruktur würde den im September 2010 demonstrierten Angriff gegen die SuisseID verhindern (vgl. <http://www.vimeo.com/15155073>)

3.5 Demonstration Kaufvertrag



- Unterschriftenvorschau-Modus: Modus, der verhindert, dass dynamische Dokumentinhalte das Erscheinungsbild des Dokuments ändern können (→ statische, sichere Anzeige)
- PDF/SigQ Level A: Standard für Dokumente, die keinen dynamischen Inhalt aufweisen (primär für Langzeit-Archivierung vorgesehen)

Digital unterschrieben von Armand
Claude Portmann
DN: c=CH, st=LU, l=Luzern,
ou=Qualified Certificate,
givenName=Armand Claude,
sn=Portmann, cn=Armand Claude
Portmann, email=███████████

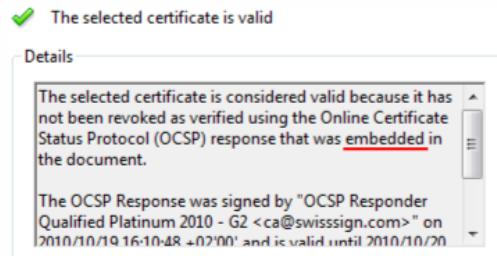
Grund: Ich akzeptiere durch meine
Unterschrift die definierten Bedingungen
Ort:Luzern
Datum: 2008.07.25 10:39:17 +02'00'

3.6 Einbettung von Gültigkeitsinformationen

- Informationen zur Zertifikatsgültigkeit können bei der Signaturerstellung in das signierte Dokument eingebettet werden → Zum Signaturprüfzeitpunkt findet keine Revokationsprüfung statt
- Entsprechende Ausgabe bei Adobe Acrobat:

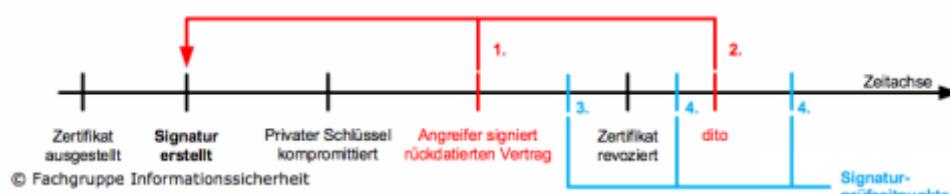


Ergebnis der Signaturprüfung ohne eingebettete Gültigkeitsinformationen (Adobe Acrobat Professional)



Ergebnis der Signaturprüfung mit eingebetteten Gültigkeitsinformationen (Adobe Acrobat Professional)

- In Adobe Acrobat lässt sich konfigurieren, ob Revokationsinformationen eingebettet werden sollen oder nicht (QuoVadis empfiehlt die Einbettung)
- SwissSigner von SwissSignbettet Revokationsinformationen immer ein
- Warum ist es zulässig, den Revokationsstatus des Zertifikats zum Signaturprüfzeitpunkt nicht mehr zu ermitteln? (Das Zertifikat könnte ja seit der Signatur revoziert worden sein!)



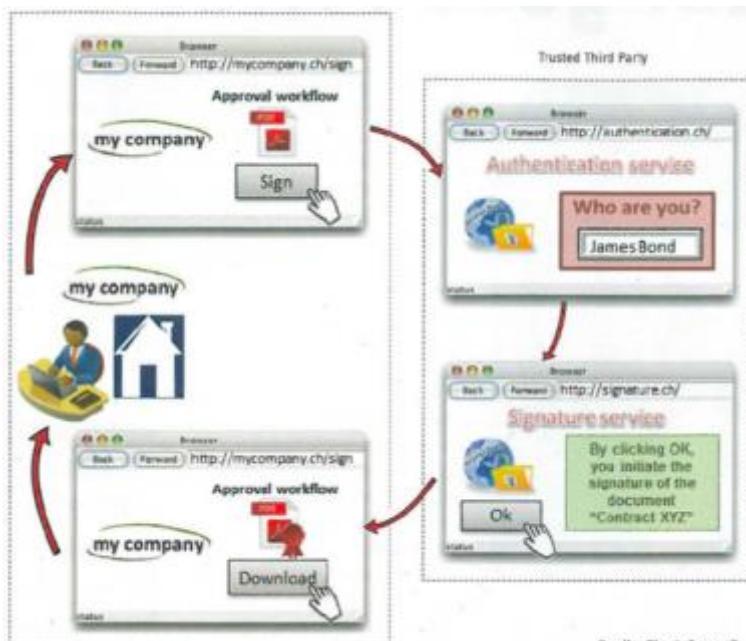
- Welcher Nachteil ergibt sich aus der Ermittlung des Gültigkeitsstatus des Zertifikats zum Signaturprüfzeitpunkt?

Antwort: Wenn ein Zertifikat revoziert wurde, dann werden alle Signaturen als ungültig angezeigt, falls zum Signaturprüfzeitpunkt der Gültigkeitsstatus des Zertifikats ermittelt wird. Dies beeinträchtigt die Anwendbarkeit der elektronischen Signatur stark. Aus diesem Grund wird in der Regel mit eingebetteten Revokationsinformationen gearbeitet.

- Adobe Acrobat 8 zeigt Signaturen nach Ablauf des Zertifikatsgültigkeitsdatums als **ungültig** an
 - Technisch gesehen korrekt: Dokument ist nicht mehr beweiskräftig
 - SwissSigner zeigt Signaturen nach Ablauf des Zertifikatsgültigkeitsdatums als **gültig** an
 - Rechtlich gesehen korrekt: Willenserklärung bleibt gültig
- Diese Diskrepanzen erschweren die korrekte Handhabung respektive die Einführung von elektronischen Signaturen
- In jedem Fall sind spezielle Massnahmen notwendig, um die Beweiskraft eines Dokuments über die Zertifikatsgültigkeit hinaus zu erhalten

3.7 Signature as a Service

- **Signaturerstellung in der Cloud**
- Änderung in der Verordnung zum ZertES ermöglicht dies seit Aug. 2011 (vgl. Art. 11): Schlüsselmaterial muss nicht mehr zwingend im Besitz, sondern nur noch unter der vollständigen Kontrolle des Benutzers sein
- **Vollständige Abwicklung über das Web ist möglich** – ohne Transfer des Dokuments zum Dienstleister. Wie funktioniert das?
- Nutzung auch auf Tablets ohne USB-Schnittstelle
- Lancierung des Service durch die Post im Jahr 2013

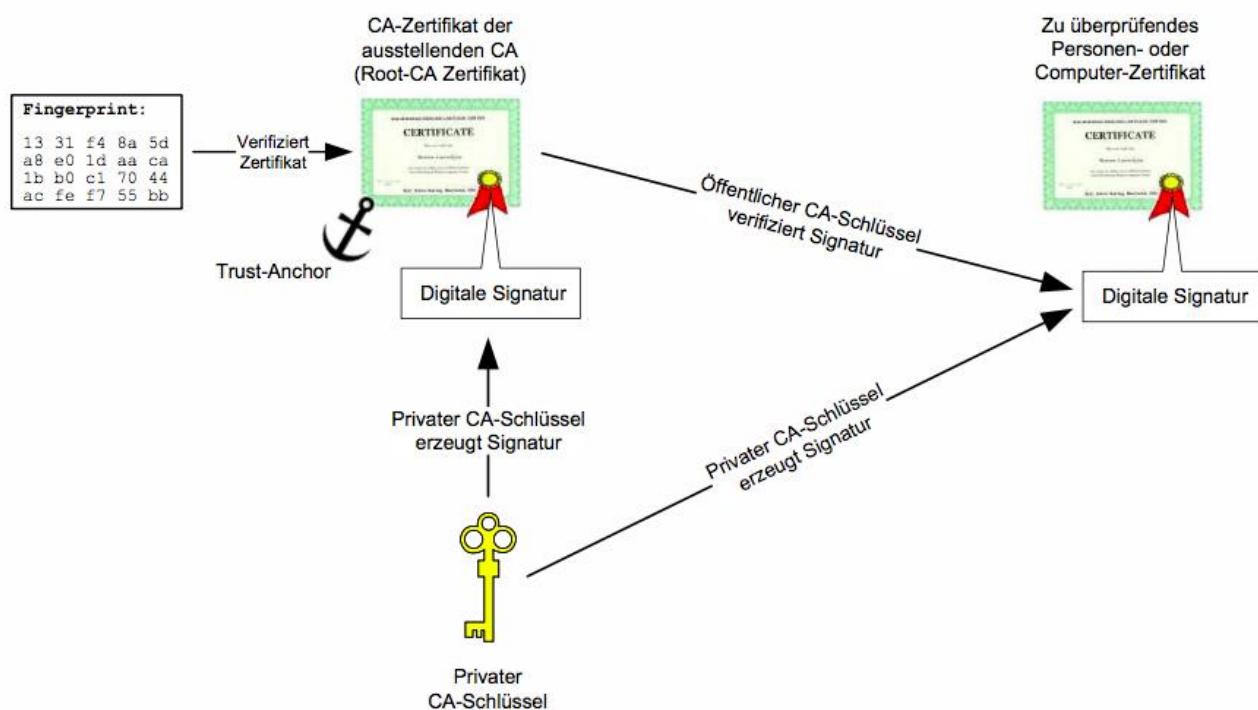


Quelle: Elca Informatik

4 Trustketten und Prüfung der Zertifikate

4.1 Prüfung von Zertifikaten

- Ein Zertifikat stellt einen Zusammenhang zwischen der Identität einer Person (od. eines Computers) und einem öffentlichen Schlüssel her
- Wird das Zertifikat von einer vertrauenswürdigen Institution (Zertifizierungsstelle, Trust-Center) herausgegeben, so spricht man auch von einem beglaubigten Zusammenhang zwischen Person (Computer) und öffentlichem Schlüssel



- CA-Zertifikate, die nicht von einer übergeordneten CA ausgestellt worden sind, werden als **Root-CA-Zertifikate** bezeichnet
- Sie sind der Aufhänger der Sicherheit und werden deshalb oft auch als **Trust-Anchor** bezeichnet
- Root-CA-Zertifikate können nicht über die Signatur überprüft werden, sondern nur mithilfe des Fingerprints (Warum?)
- Personen- oder Computer-Zertifikate lassen sich mithilfe des Zertifikats der ausstellenden CA überprüfen (Signaturverifikation) oder mithilfe des Fingerprints **Antwort: Weil das Zertifikat selbstsigniert ist, d. h. es gibt keine weitere vertrauenswürdige Instanz, die die Echtheit des Zertifikats mithilfe ihrer Signatur bestätigen könnte.**

- Generell kann die Echtheit eines jeden Zertifikats durch einen Vergleich von dessen Fingerprint mit dem **Fingerprint des Original-Zertifikats** überprüft werden
- Wie muss eine korrekte Überprüfung des Fingerprints ablaufen?
- Was fällt Ihnen bei der Betrachtung des folgenden von Windows ausgegebenen Zertifikatsinhalts auf?

Feld	Wert
Alternativer Ausstellername	Verzeichnisadresse:O=ZertES...
Stellenschlüsselkennung	Schlüssel-ID = 21 f0 05 b5 fb ...
Sperrlisten-Verteilungspunkte	[1] Sperrlisten-Verteilungspunkt...
Schlüsselkennung des Antrags...	75 24 9d 6f 5c 5b ff 00 1a 1e ...
Schlüsselverwendung	Digitale Signatur, Zugelassen, ...
Fingerabdruckalgorithmus	sha1
Fingerabdruck	31 11 66 3d 5b 10 31 9a 81 cd ...

© Fachgruppe Info 31 11 66 3d 5b 10 31 9a 81 cd 5b 58 6d 93 6f
01 2f 16 9a 9b Folie 51

Prüfung von Root-CA Zertifikaten

- Die **automatische Prüfung von Personen- oder Computer-Zertifikaten über die Signatur** setzt das **Vorhandensein von echten** (d.h. überprüften) Root-CA Zertifikaten voraus
- Betriebssystem- und Browser-Hersteller liefern mit ihren Produkten vorinstallierte Root-CA Zertifikate mit (Vertrauensfrage!)
- Nicht installierte Root-CA Zertifikate können manuell **nachinstalliert** werden (oder werden z.T. automatisch nachinstalliert)
- Durch die Installation wird dem Zertifikat **Echtheit attestiert** (heikler Vorgang! Warum?) **Point of Trust**

Prüfung von Root-CA Zertifikaten – VeriSign

- Öffentliche Zertifizierungsstellen wie VeriSign publizieren die Fingerprints ihrer Root-CA Zertifikate im Web
- Selbstverständlich muss die Authentizität von Webseiten, die Fingerprints publizieren, absolut gewährleistet sein

Serial Number: 00 9b 7e 06 49 a3 3e 62 b9 d5 ee 90 48 71 29 ef 57
Operational Period: Fri October 1, 1999 to Wed July 16, 2036
Certificate SHA1 Fingerprint: 132d 0d45 534b 6997 cdb2 d5c3 39e2 5576 6096 5c66

VeriSign Class 4 Primary CA - G3
Country = US
Organization = VeriSign, Inc.
Organizational Unit = VeriSign Trust Network
Organizational Unit = (c) 1999 VeriSign, Inc. - For authorized use only
Common Name = VeriSign Class 4 Public Primary Certification Authority - G3

Serial Number: 00 ec a0 a7 8b 6e 75 6a 01 cf c4 7c cc 2f 94 5e d7
Operational Period: Fri October 1, 1999 to Wed July 16, 2036
Certificate SHA1 Fingerprint: c0ec 8c87 9269 cb4b ab39 e9bd 7e57 67f3 1495 7394

VeriSign Class 3 Primary CA - G5
Country = US
Organization = VeriSign, Inc.
Organizational Unit = VeriSign Trust Network
Organizational Unit = (c) 2006 VeriSign, Inc. - For authorized use only
Common Name = VeriSign Class 3 Public Primary Certification Authority - G5

Serial Number: 18 da 19 9e 26 7d e8 4a 4a 21 58 cd cc 6b 3b 4a
Operational Period: Tue, November 07, 2006 to Wed, July 16, 2036
Certificate SHA1 Fingerprint: 4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

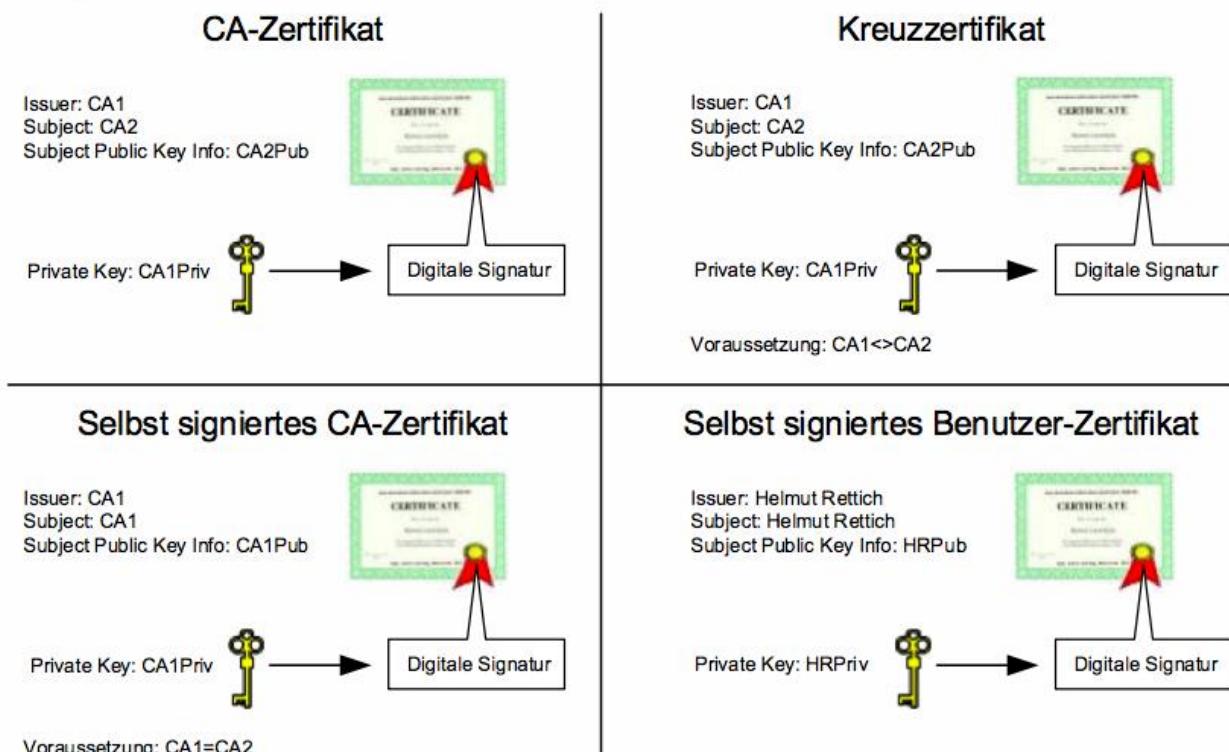
Basis einschränkungen	Typ des Antragstellers = Zertifi...
Schlüsselverwendung	Zertifikatsignatur, Offline Signi...
Fingerabdruckalgorithmus	sha1
Fingerabdruck	4e b6 d5 78 49 9b 1c cf 5f 58 ...
Anneinteuer Name	VeriSign

4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

Eigenschaften bearbeiten... In Datei kopieren... Weitere Informationen über [Zertifikatdetails](#)

- Viele Banken publizieren die Fingerprints der SSL-Zertifikate, welche für das e-Banking verwendet werden
- Der Kunde soll also dazu angehalten werden, die SSL-Zertifikate manuell zu überprüfen. Warum?
Rechtliche belangen.

4.2 Zertifikatstypen



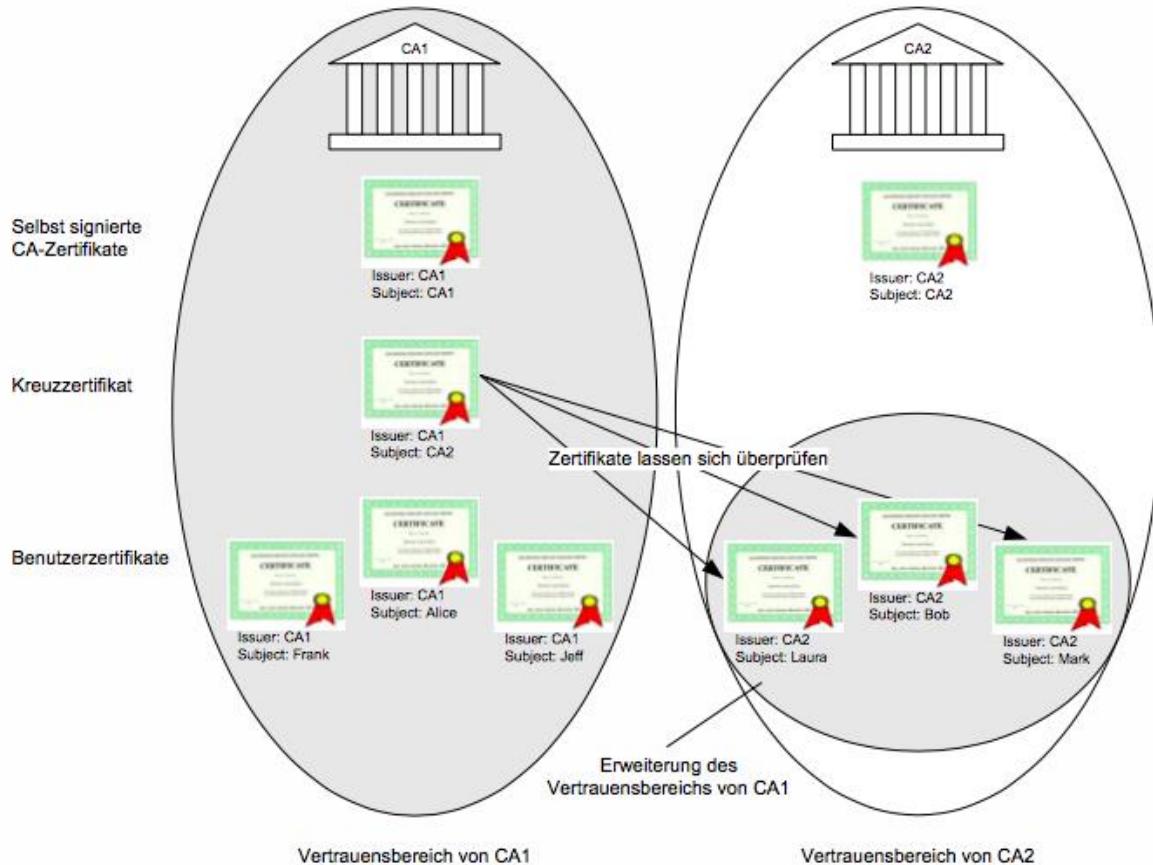
- **CA-Zertifikat:** Zertifikat, das eine CA für eine CA (gleiche oder andere) ausstellt
- **Kreuzzertifikat:** CA-Zertifikat, das eine CA für eine andere CA ausstellt (Nennen Sie ein Beispiel!)
- **Selbst signiertes CA-Zertifikat:** CA-Zertifikat, das eine CA für sich selber ausstellt, wobei der private Schlüssel den zugehörigen öffentlichen Schlüssel signiert (Nennen Sie ein Beispiel!)
- **Selbst signiertes Benutzer-Zertifikat:** Zertifikat, das ein Benutzer für sich selber ausstellt, wobei der private Schlüssel den zugehörigen öffentlichen Schlüssel signiert (Nennen Sie ein Beispiel!)
Selbstsignierung mit PGP und SMIME

Beispiel für ein Kreuzzertifikat: Intermediate-Zertifikat, Issuing-CA Zertifikat (die andere CA muss also nicht notwendigerweise zu einer anderen Organisation gehören)

Beispiel für selbst signiertes CA-Zertifikat: Root-CA Zertifikat

Beispiel für selbst signiertes Zertifikat: PGP-Zertifikat

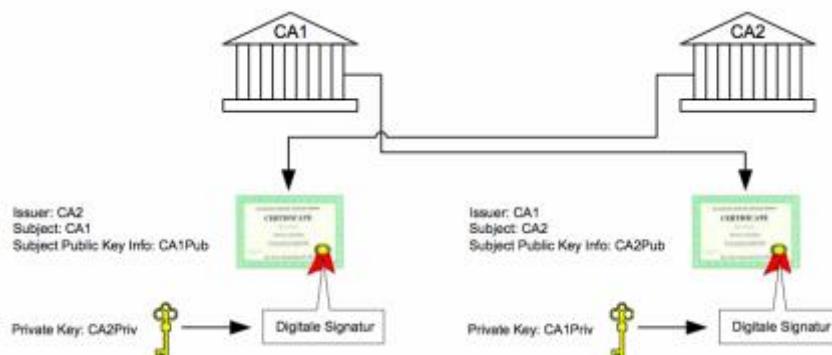
4.3 Kreuzzertifizierung



- Durch Kreuzzertifizierung wird einer anderen CA explizit Vertrauen ausgesprochen (man geht dabei davon aus, dass die CA ihren Aufgaben korrekt nachkommt)
- Kreuzzertifizierung ermöglicht es, von einer anderen CA herausgegebene Zertifikate zu überprüfen, ohne das Root-CA Zertifikat dieser CA importieren zu müssen
- Die Überprüfung der Zertifikate erfolgt über eine so genannte Zertifikatskette (s.u.)

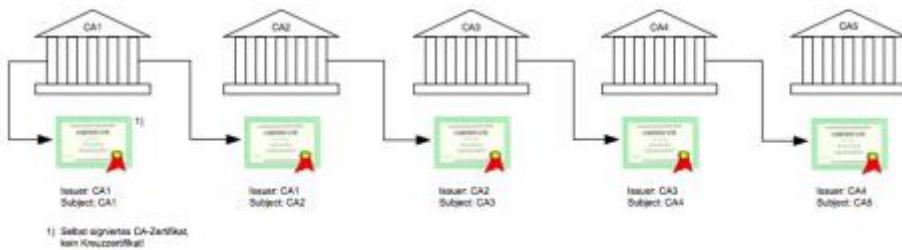
Gegenseitiges Kreuzzertifikatpaar

- Zertifikatpaar, das entsteht, wenn zwei CAs sich gegenseitig ein Kreuzzertifikat ausstellen

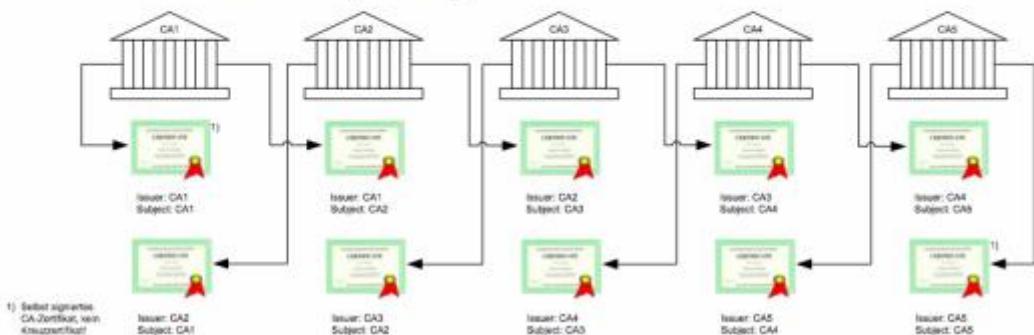


4.4 Zertifikatsketten

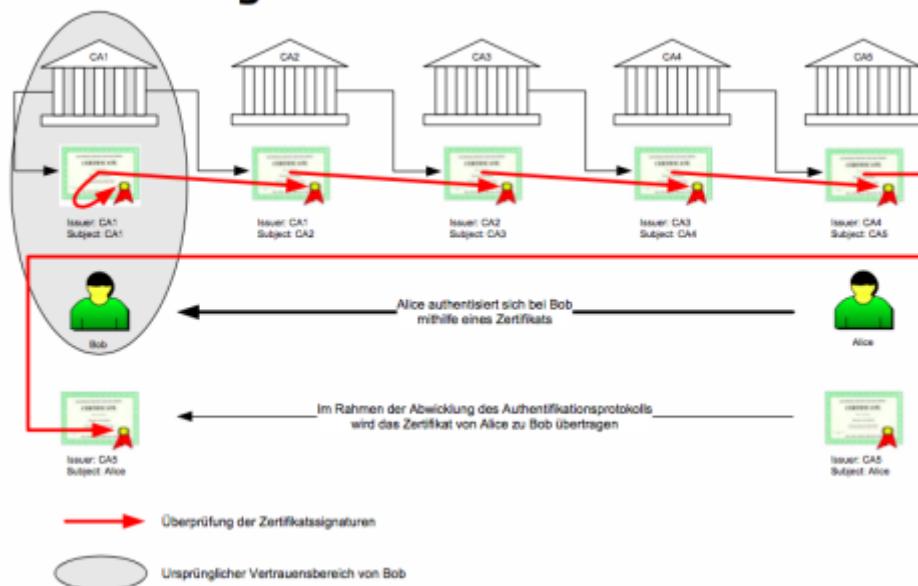
- **Unidirektionale Zertifikatskette:** Lückenlose Kette von CA-Zertifikaten, wobei jede CA der nächstfolgenden ein Kreuzzertifikat ausstellt



- **Symmetrische (reversible) Zertifikatskette:** Lückenlose Kette von CA-Zertifikaten, wobei jede CA der nächstfolgenden und der vorangehenden CA ein Kreuzzertifikat ausstellt (dabei entstehen gegenseitige Kreuzzertifikatspaare)



Anwendung einer Zertifikatskette

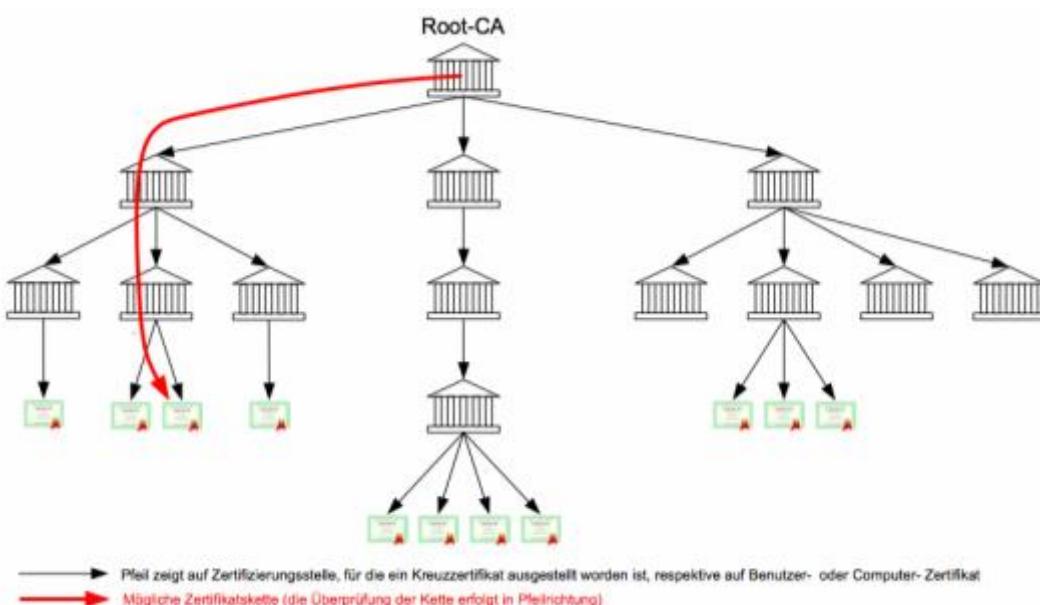


- Alice möchte sich bei Bob authentifizieren. Alice vertraut CA5 und liess sich dort ihr Zertifikat ausstellen. Bob vertraut CA1 und liess sich dort sein Zertifikat ausstellen (Bobs Zertifikat ist für die Aufgabe nicht relevant).
- Damit Bob das Zertifikat von Alice überprüfen kann, muss es eine Zertifikatskette von CA1 zu CA5 geben
- Ausgehend vom CA-Zertifikat von CA1 kann jedes nachfolgende CA-Zertifikat und schliesslich das Zertifikat von Alice überprüft werden
- Fragen
 - Angenommen Bob möchte sich in gleicher Weise bei Alice authentifizieren. Könnte dies mithilfe der Neine dargestellten Zertifikatskette bewerkstelligt werden?
 - Wie könnte man konkret eine zertifikatsbasierende Authentifikation implementieren? Welchen Mechanismus könnte man dem Protokoll zugrunde legen?
Challenge-Response-Verfahren.

4.5 Trustmodelle

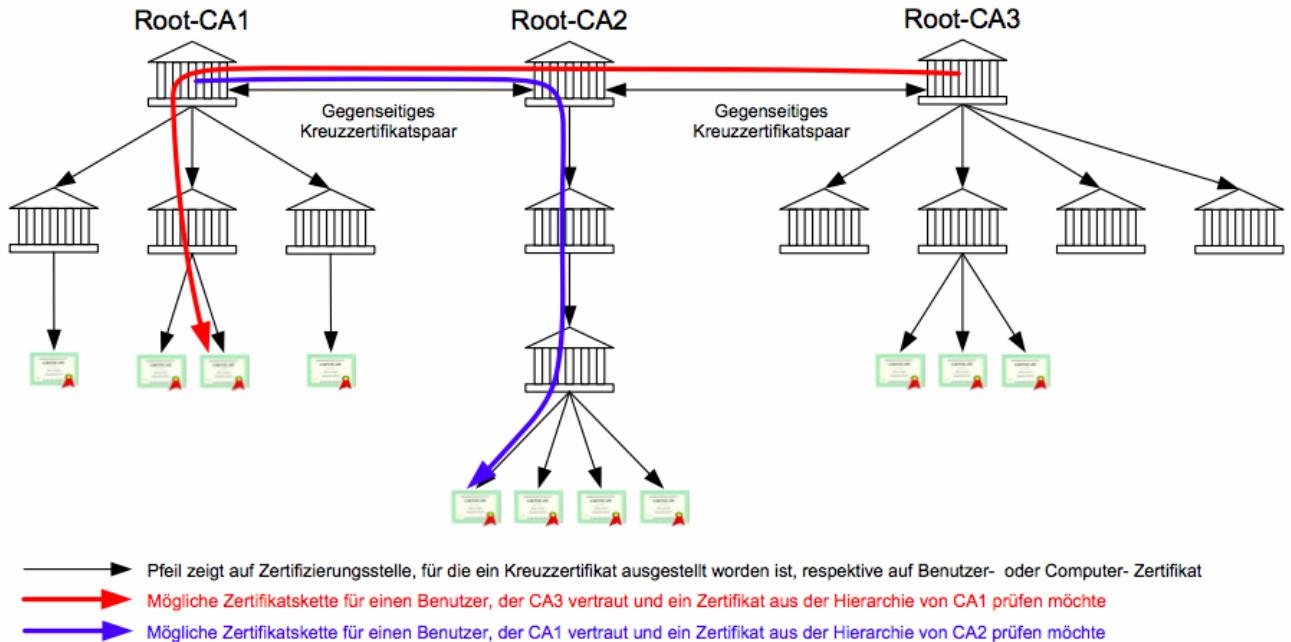
- Trustmodelle beschreiben die Art und Weise, wie Zertifikatsketten zwischen verschiedenen CAs aufgebaut werden können
- Trustmodelle charakterisieren also die Vernetzung von mehreren CAs resp. definieren die zugrunde liegenden Netztopologien
- Folgende Modelle werden i.d.R. unterschieden
 - Hierarchisches Modell
 - Verteiltes Modell (Distributed Trust Model)
 - Hub Modell (Bridge Model) → wird nicht im Detail erklärt
 - Flaches Modell (Web Model)
 - Benutzer-Trustmodell (User-Centric Trust Model)

4.5.1 Hierarchisches Modell



- Jede CA stellt ein Zertifikat (genauer ein Kreuzzertifikat) für die darunterliegende CA aus
- Dadurch entstehen Zertifikatsketten, die bei der Root-CA beginnen und bei den Benutzer- oder Computer-Zertifikaten enden
- Damit das Modell funktioniert müssen alle Benutzer der Root-CA vertrauen (Trust-Anchor)

4.5.2 Verteiltes Modell



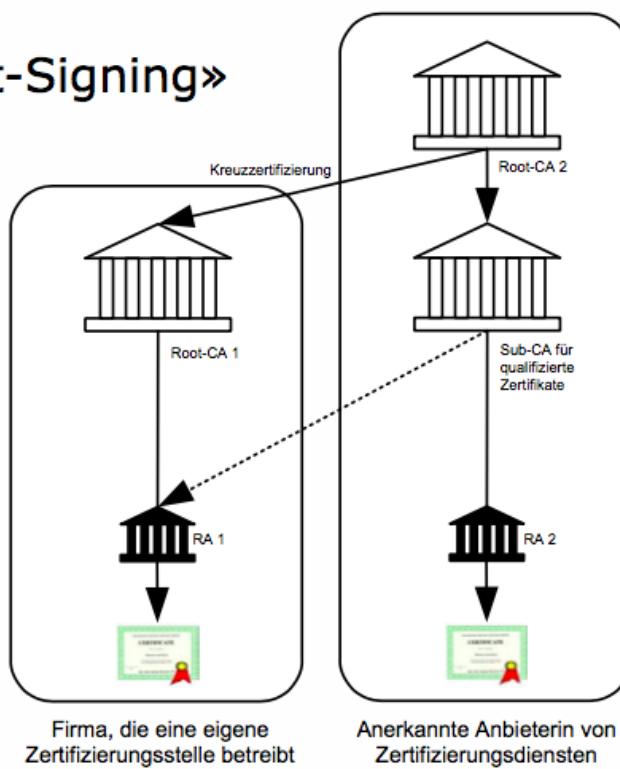
- Das verteilte Trustmodell kommt zur Anwendung, wenn mehrere bereits vorhandene hierarchische Modelle miteinander verbunden werden sollen (Zusammenschlüsse von Firmen oder öffentlichen Zertifizierungsstellen)
- Für den Aufbau stellen sich die beteiligten Root-CAs gegenseitige Kreuzzertifikatspaare aus
- Damit das Modell funktioniert müssen alle Benutzer einer Hierarchie «ihrer» Root-CA vertrauen
- Frage 1: Warum werden gegenseitige Kreuzzertifikatspaare ausgestellt?
- Frage 2: Warum könnte es sinnvoll sein, auch noch zwischen CA1 und CA3 ein gegenseitiges Kreuzzertifikatspaar auszustellen?

Antwort 1: Bei einfacher Kreuzzertifizierung wäre es nicht möglich, dass Benutzer aus beliebigen CA-Hierarchien Zertifikate aus beliebigen anderen Hierarchien überprüfen könnten.

Antwort 2: Dadurch kann die Zertifikatskette zwischen CA1 und CA3 verkürzt werden, da die Zwischenstation CA2 ausgelassen werden kann.

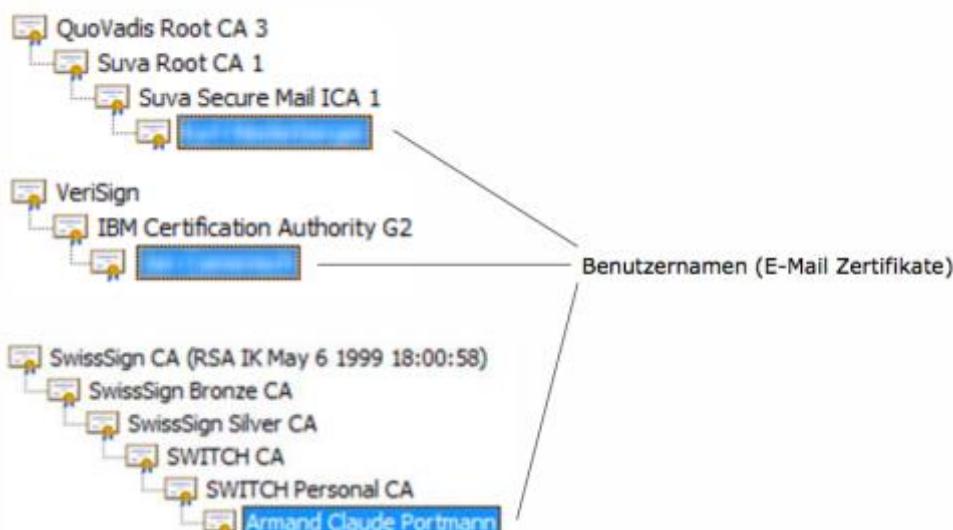
4.5.3 Verteiltes Modell

Beispiel «Root-Signing»



- Eine Firma betreibt eine eigene Zertifizierungsstelle, die der Root-CA einer anerkannten Anbieterin von Zertifizierungsdiensten durch Kreuzzertifizierung untergeordnet wird
- Motivation
 - Zertifikatskette endet bei einem vorinstallierten Root-CA-Zertifikat (dies gilt bei anerkannten CAs) → zertifikatsbasierende Anwendungen laufen «pop-up-frei!» (d.h. ohne Fehlermeldung)
 - Von der anerkannten CA können auch gerade benötigte qualifizierte oder fortgeschrittene Zertifikate bezogen werden (evtl. sogar über eine eigene RA)

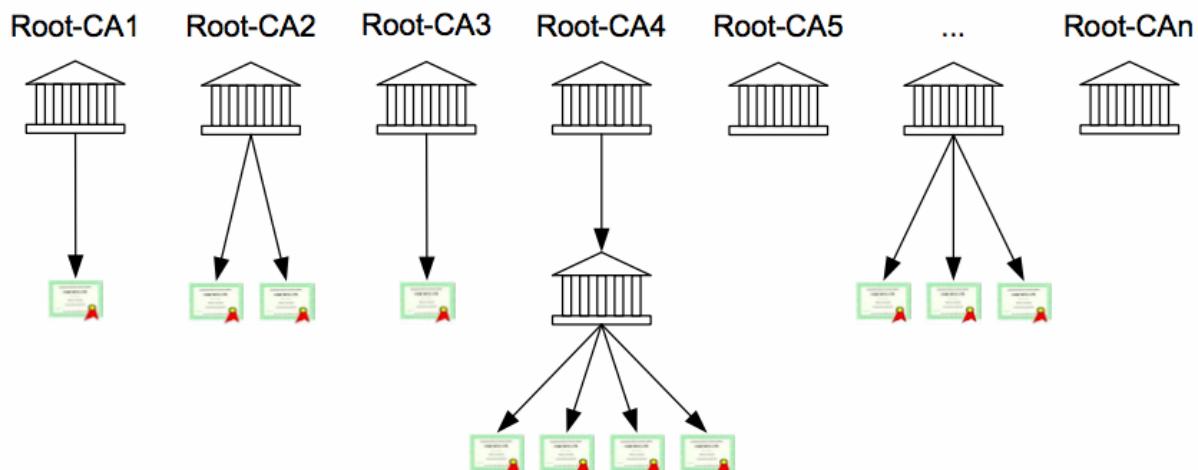
«Root Signing» - Konkrete Beispiele



4.5.4 Flaches Modell

Flaches Modell

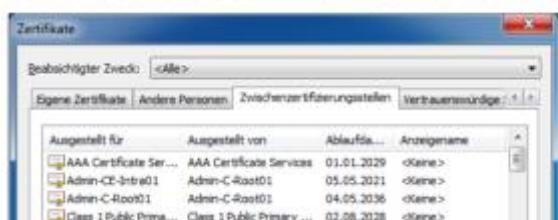
Speicher für vertrauenswürdige Stammzertifizierungsstellen
 • ...
 • TC TrustCenter Class 1 CA
 • Thawte Premium Server CA
 • VeriSign Class 1 Public Primary CA
 • ...



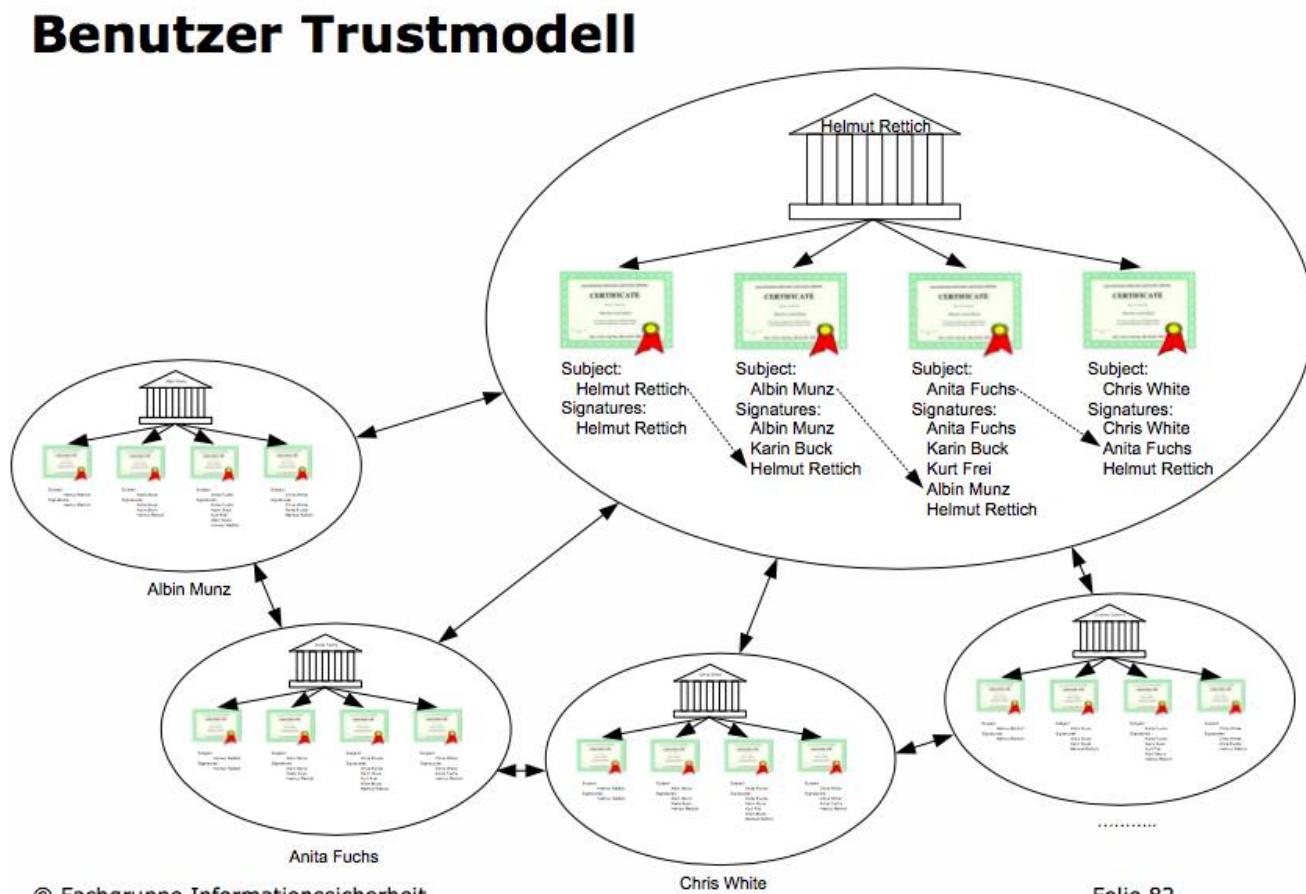
→ Pfeil zeigt auf Zertifizierungsstelle, für die ein Kreuzzertifikat ausgestellt worden ist, resp. auf Benutzer- oder Computer- Zertifikat

- Beim flachen Modell gibt es **keinerlei Assoziationen zwischen den beteiligten Root-CAs**
- Damit **beliebige Benutzer- oder Computer-Zertifikate** überprüft werden können, müssen **alle** beteiligten Root-CAs als **vertrauenswürdig** erklärt werden
- Es muss deshalb ein **umfassender Speicher für vertrauenswürdige Root-CAs angelegt** werden (auf Ebene Betriebssystem oder auf Ebene Sicherheitsapplikation)

Browser nutzen in der Regel das flache Modell; es heisst deshalb auch **Browser- oder Web-Modell**



4.5.5 Benutzer Trustmodell



© Fachgruppe Informationssicherheit

Folie 87

- Jeder Teilnehmer betreibt seine eigene «Zertifizierungsstelle»
 - Er stellt eines oder mehrere Zertifikate für sich selber aus, erzeugt also selbst-signierte Zertifikate
 - Er signiert die Zertifikate anderer Benutzer und attestiert ihnen dadurch Echtheit (Authentizität)
- Für die Überprüfung der Zertifikate anderer Benutzer ist der Teilnehmer selber verantwortlich
- Grundlagen für die Echtheitsprüfung
 - Fingerprints, die direkt abgefragt werden
 - Vorhandene Signaturen von vertrauenswürdigen Personen
 - Indirektes (transitives) Vertrauen (vgl. gestrichelte Pfeile in der Abbildung)
- Das Benutzer Trustmodell kommt bei PGP zur Anwendung und wird auch als Web of Trust bezeichnet

4.6 Zertifikatsüberprüfung

Wenn Zertifikate zwecks Benutzer-Authentifikation ausgetauscht werden, dann haben die folgenden Zertifikatsüberprüfungen zu erfolgen:

1. Gültigkeitsdauer: Aktuelles Datum liegt im Gültigkeitsbereich des Zertifikats
2. Schlüsselpaar: Privater Schlüssel passt zum öffentlichen Schlüssel im Zertifikat
 - Frage 1: Was wird mit dieser Überprüfung bezweckt?
 - Frage 2: Wie könnte die Überprüfung erfolgen?

Antwort 1: Mithilfe dieser Überprüfung beweist der Benutzer, dass er im Besitze des privaten Schlüssels ist. Unter der Annahme, dass nur der rechtmässige Besitzer auf den privaten Schlüssel zugreifen kann, wird dadurch die Identität des Benutzers unter Beweis gestellt. Diese Argumentation ist allerdings nur richtig, wenn die Echtheit des Zertifikats garantiert ist (Zuordnung öffentlicher Schlüssel <-> Benutzername).

Antwort 2: Der Benutzer könnte zum Beispiel aufgefordert werden einen Wert zu signieren (Challenge-Response-Verfahren).

3. Verwendungszweck: Vorgesehener Verwendungszweck stimmt mit dem im Zertifikat angegebenen Verwendungszweck überein
 - Wie heisst das Flag, mit dem ein Verwendungszweck als «zwingend» markiert werden kann critical
4. Zertifikatssignatur: Zertifikat ist gültig signiert (Überprüfung setzt eine gültige Zertifikatskette voraus)
5. Ungültigerklärung: Zertifikat ist nicht in der CRL aufgelistet resp. OCSP (Online Certificate Status Protocol) liefert den Zustand «gültig»

5 Governance, Risk and Compliance

5.1 Definitionen GRC

Governance

- Ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives
- Scope Notes: Conditions can include the cost of capital, foreign exchange rates, etc. Options can include shifting manufacturing to other locations, subcontracting portions of the enterprise to thirdparties, selecting a product mix from many available choices, etc.

[Quelle: <http://www.isaca.org/Pages/Glossary.aspx>]

Kontrolle durch Richtlinien.

Risk

Eintrittswahrscheinlichkeit x Schadenhöhe

- The combination of the probability of an event and its consequence.

Risk management

- The coordinated activities to direct and control an enterprise with regard to risk
- One of the governance objectives. Entails recognizing risk; assessing the impact and likelihood of that risk; and developing strategies, such as avoiding the risk, reducing the negative effect of the risk and/or transferring the risk, to manage it within the context of the enterprise's risk appetite.

Compliance

- Adherence to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies

5.2 Corporate Governance

Corporate Governance ist die Gesamtheit der auf das nachhaltige Unternehmensinteresse ausgerichteten Grundsätze, die unter Wahrung von Entscheidungsfähigkeit und Effizienz auf der obersten Unternehmensebene Transparenz und ein ausgewogenes Verhältnis von Führung und Kontrolle anstreben.

[Quelle: economiesuisse, swiss code of best practice for corporate governance, 2014]

Organization for economic cooperation and development

OECD Grundsätze der Corporate Governance

- I. Ensuring the basis for an effective corporate governance framework
- II. The rights and equitable treatment of shareholders and key ownership functions
- III. Institutional investors, stock markets and other intermediaries
- IV. The role of stakeholders in corporate governance
- V. Disclosure and transparency
- VI. The responsibilities of the board

[Quelle: G20/OECD, Principles of Corporate Governance, 2015]

Sehr abstrakt definiert.

«Code of Conduct» Verhaltenskodex der Migros



- In all unseren Handlungen sind wir verantwortungsbewusst, ehrlich und zuverlässig.
- Wir respektieren die Gesetze und die internen Richtlinien.
- Wir bestechen nicht und lassen uns nicht bestechen.
- Wir bekennen uns zum freien und fairen Wettbewerb.
- Wir vermeiden Interessenkonflikte oder legen diese rechtzeitig offen.
- Wir gehen gewissenhaft mit vertraulichen Informationen um.
- Wir tragen Sorge zu den Vermögenswerten der Migros-Gruppe.
- Innerhalb der Migros-Gruppe gehen wir wertschätzend und respektvoll miteinander um.
- Im Umgang mit unseren Kunden, unseren Geschäftspartnern und den Behörden handeln wir verlässlich, fair und verantwortungsbewusst.
- In unserer Kommunikation sind wir offen, ehrlich und klar.
- In unseren Aktivitäten und Entscheidungen verfolgen wir das Prinzip der Nachhaltigkeit.

Wir => Alle sind eingeschlossen. Inkludierend. [Quelle: Verhaltenskodex der Migros-Gruppe]

5.3 IT Governance

Teil der Corporate Governance

IT Governance liegt in der **Verantwortung des Vorstands und des Managements** und ist ein wesentlicher Bestandteil der Unternehmensführung. IT Governance besteht aus **Führung, Organisationsstrukturen und Prozessen**, die sicherstellen, dass die IT¹ die Unternehmensstrategie und -ziele unterstützt.

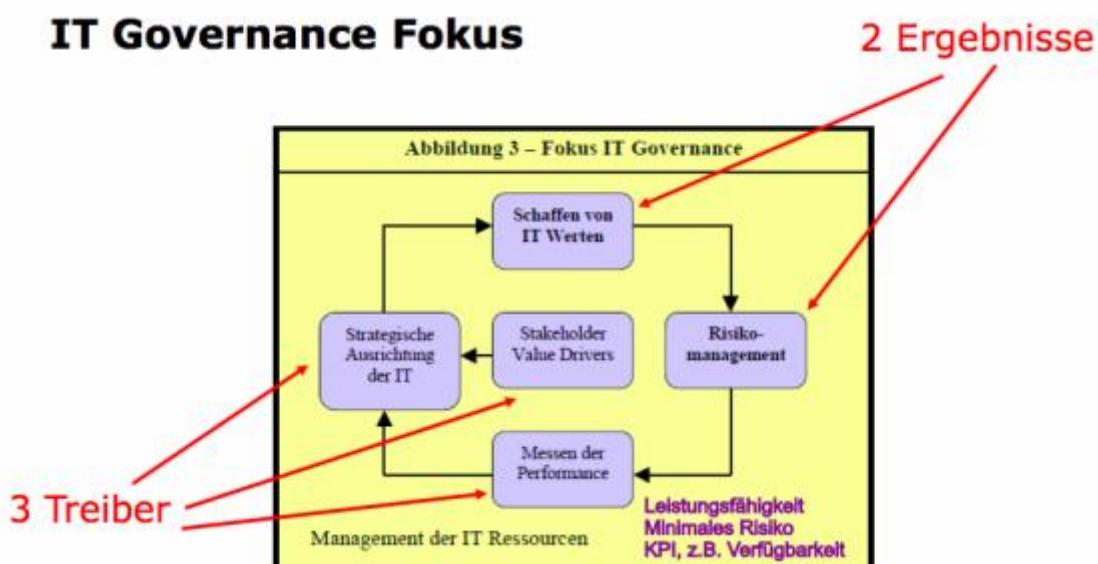
¹ unter IT wird die gesamte Infrastruktur verstanden, aber auch die Fähigkeiten und die Organisation, die die IT unterstützen und begründen.

IT so betreiben zum Nutzen der Unternehmung.

Warum IT Governance?

Umsetzung der Unternehmensstrategie unter Beachtung von gesetzlichen Vorgaben.

- Der Einsatz von IT hat das Potential, der **Haupttreiber für ökonomisches Wachstum** im 21sten Jahrhundert zu werden.
- Während sich IT schon jetzt **kritisch zum Unternehmenserfolg** verhält, ungeahnte Möglichkeiten bietet, **Wettbewerbsvorteile erzielt** und Produktivitätssteigerung bedeutet, so wird dies in Zukunft noch verstärkt.
- Die IT erfolgreich einzusetzen, ist zu einem allgemeinen **Wettbewerbsfaktor** geworden, denn damit gelingt es, das Unternehmen an den zukünftigen Anforderungen auszurichten und wertsteigernde Produkte und Services zu gestalten.



5.3.1 Ziele IT Governance

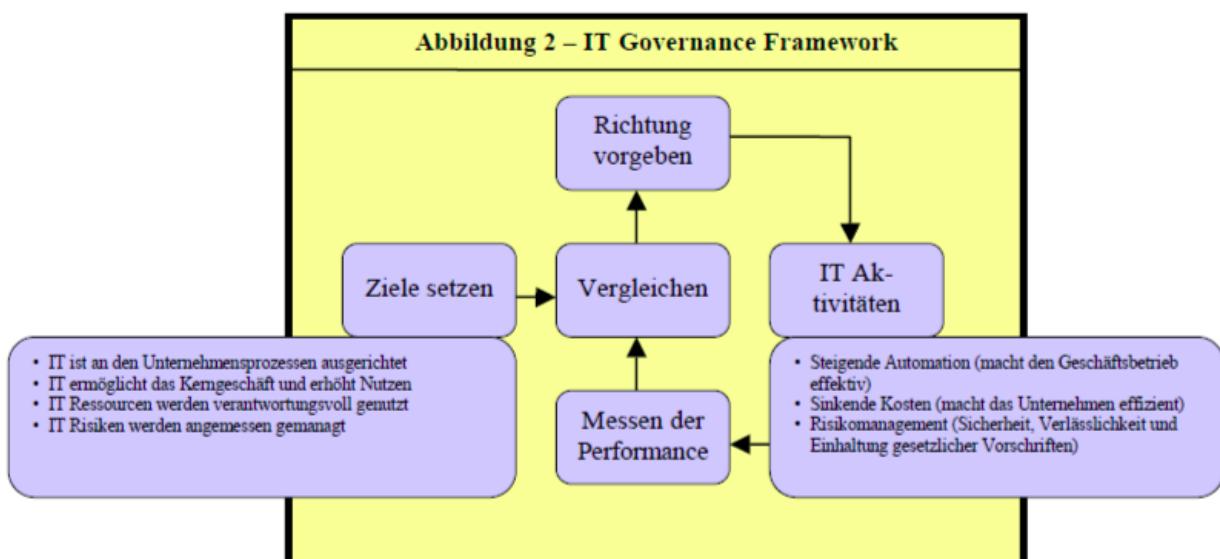
Das Hauptziel von IT Governance ist es, die **Anforderungen an die IT sowie die strategische Bedeutung von IT zu verstehen**, um den optimalen Betrieb der Unternehmensziele sicherzustellen und Strategien für die zukünftige Erweiterung des Geschäftsbetriebes zu schaffen.

- **Strategische Ausrichtung** mit Fokus auf Unternehmenslösungen
- **Nutzengenerierung** mit Fokus auf die Optimierung der Ausgaben und Bewertung des Nutzens der IT
- **Risikomanagement**, das sich auf den Schutz des IT Assets bezieht, unter Berücksichtigung von Disaster Recovery (Wiederanlauf nach Katastrophen) und Fortführung der Unternehmensprozesse im Krisenfall
- **Management** von Ressourcen, Optimierung von Wissen und IT Infrastruktur

Keines dieser Ziele kann erreicht werden, ohne dass die **Performance** regelmässig **gemessen wird**.

IT Governance Framework

Regelkreis



Schritte für die Einführung und den Betrieb der IT Governance

- ähnlich ISMS
1. Einrichtung eines IT Governance Frameworks
 2. Abgleichen der IT Strategie mit den Unternehmenszielen
 3. Risikoverständnis **Nicht nur Messung des IST-Zustands, sondern auch der Einflüsse auf die Wertschöpfung**
 4. Definition von Zielbereichen
 5. Analyse der aktuellen Ressourcen; Identifikation von Lücken
 6. Entwicklung von Verbesserungsstrategien
 7. Messen von Resultaten
 8. Regelmässiges Wiederholen der Schritte 2-7

5.4 Compliance

«Compliance handelt von **Rechts- und Reputationsrisiken** und bildet so ein Moment des Risk Management»

[...]

«Compliance ist Teil des Internen Kontrollsystems (IKS)¹ und wird als Begriff für ein **Verhaltenskonzept** verwendet»

Compliance ist eine Konzept.

Warum Compliance?

PAT generiert eine Zielkonflikt für Compliance und Wertschöpfung.

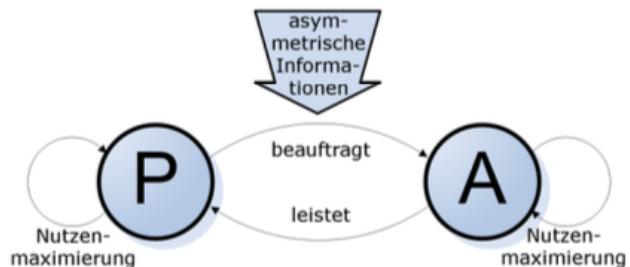
- Principal Agent Theory

Ungleicher Informationsstand und deren Konflikte.

Es geht um Verschleierung und Anreize.

Prinzipal -> im Nachteil.

Agent -> Ist im Informationsvorteil.



- Es gibt immer eine **Informationslücke** und einen **Interessenskonflikt** zwischen z.B. **Produzent und Kunde** oder zwischen **Management und Aktionären**.

5.4.1 Ziele Compliance

- **Gesetze, Verordnungen, Reglemente**, Rundschreiben und Standardregeln sowie allgemein anerkannte bzw. anerkennungswürdige Geschäftsgrundsätze müssen von der Unternehmung, vom Management und von allen Mitarbeitenden eingehalten werden.
- **Ethische Standards** wie Ehrlichkeit, Fairness, Transparenz, Anstand und Vertrauen sollen das Verhältnis zum Kunden und zu weiteren Stakeholdern auszeichnen.
- **Interessenkonflikte** sollen vermieden werden; sind sie vorhanden, so müssen sie offengelegt werden, um Transparenz zu schaffen, und fair beigelegt werden.

5.4.2 Modelle und Referenzen Compliance

Compliance-Pyramide



Compliance-Funktion Chief Compliance Officer

Unterstützung der Geschäftsleitung.

Zugriff auf Performance Kriterien -> KPI Sichtbarkeit

(Zugriff Rechtsabteilung)

Ressourcen -> Budget und Mitarbeiter (können direkt unterstellt sein)

Konsequenzen für «Non Compliance»

Imageschäden

Sanktionen

Kein nachhaltiges Betriebsergebnis -> Indirekte Folgen für Wettbewerb

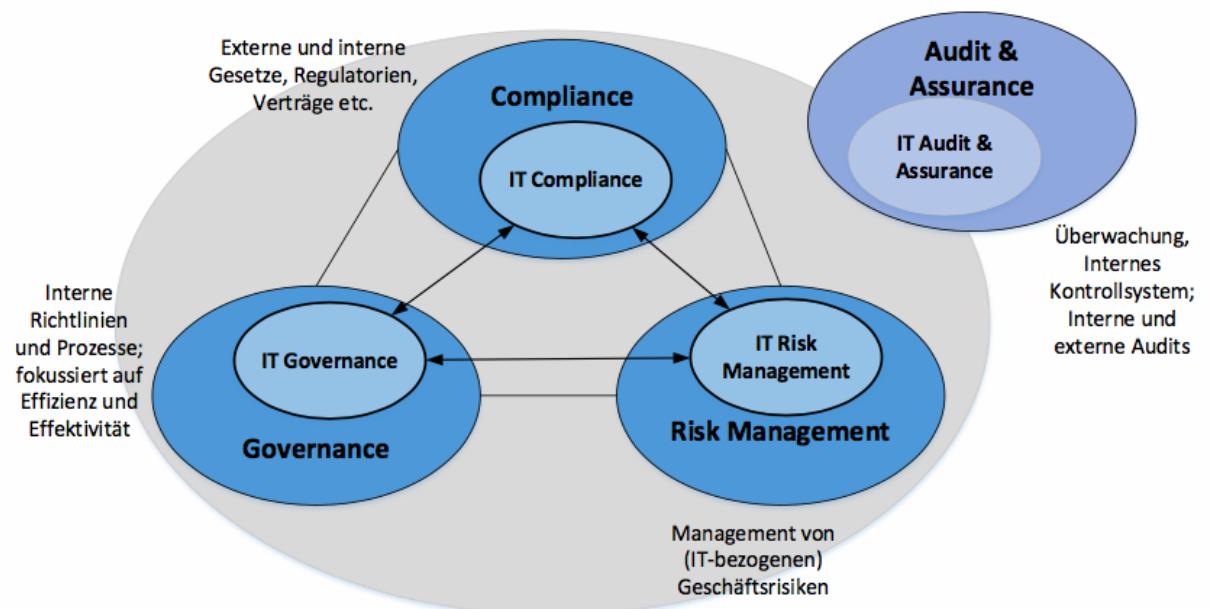
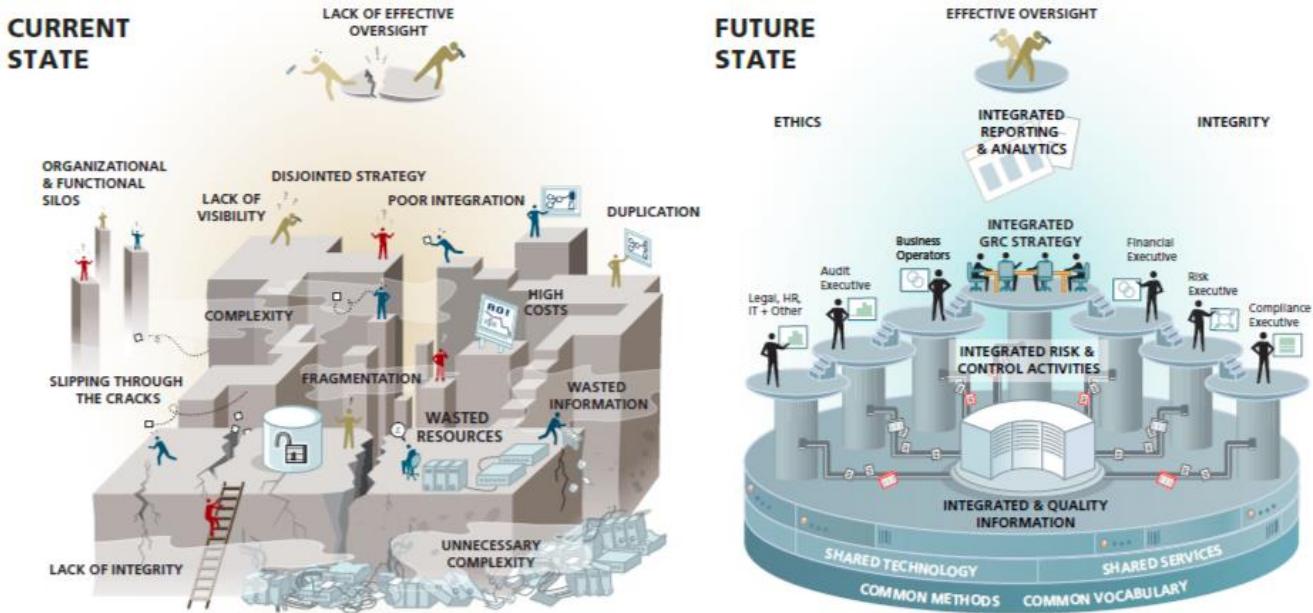
Direkt

Geldstrafen, Ausschlüsse, Verlieren von Investoren, Verminderte Bewertung

Indirekt

Verlieren von Marktanteilen, Reputationsschäden, Vertrauensverlust

5.5 GRC Anwendungsfall



5.5.1 Audit and Assurance

Audit

- Formal inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, or efficiency and effectiveness targets are being met.
- Scope Notes: May be carried out by internal or external groups.

Assurance

- Pursuant to an accountable relationship between two or more parties, an IT audit and assurance professional is engaged to issue a written communication expressing a conclusion about the subject matters for which the accountable party is responsible. Assurance refers to a number of related activities designed to provide the reader or user of the report with a level of assurance or comfort over the subject matter.

5.6 Nutzen GRC



5.6.1 Umsetzung GRC

1. IT Principles & Strategy

Get GRC practitioners at the table with IT professionals to discuss how IT can support GRC needs:

- Information needs
- Process / transaction needs
- Control / monitoring needs
- Documentation / system of record needs

2. "As-Is" Situation

Inventory all of the existing processes and the technology that supports these processes:

- What do we already have in place?
- Who owns and maintains these systems?
- Who operates them?
- What do they really do?

3. "To-Be" Vision

Define, enhance, evolve an enterprise architecture that supports GRC needs. Leverage existing technology investments where possible and look for ways to consolidate technology to serve multiple GRC areas. Integrate technology into core business processes to serve GRC needs.

4. Priorities, Projects, Budgets & Ownership

GRC and IT professionals work together to define priorities and specific

- Try to start in a specific area and expand
- Try to avoid "big bang" solutions
- Consider parallel operation of "high stakes" systems
- Involve business leaders in prioritization
- Assign ownership and accountability

5.7 Frameworks

5.7.1 Open Compliance and Ethics Group (OCEG)

OCEG is a global, nonprofit think tank and community. We inform, empower, and help advance nearly 50,000 members on governance, risk management, and compliance (GRC). Independent of specific professions, we provide content, best practices, education, and certifications to drive leadership and business strategy through the application of the OCEG GRC Capability Model and Principled Performance.

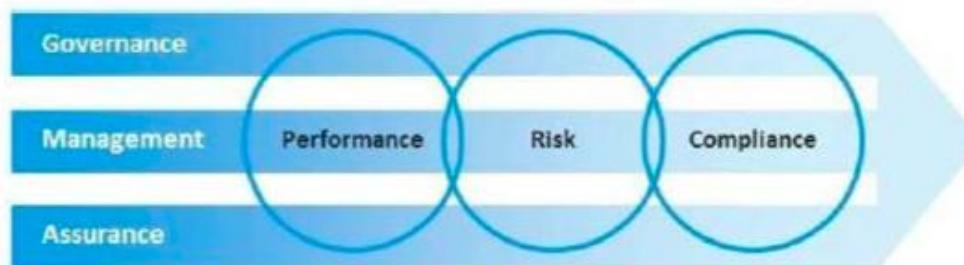
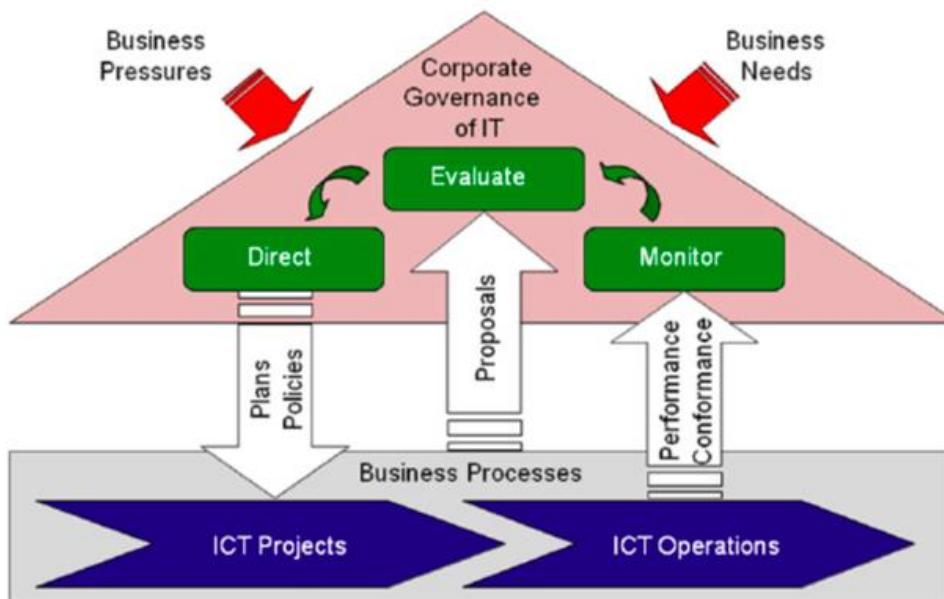


Figure 1 – The Principled Performance View of Integration



5.7.2 ISO / IEC 38500:2008

Figure 1—ISO/IEC 38500:2008 Model for Corporate Governance of IT



Sechs Prinzipien

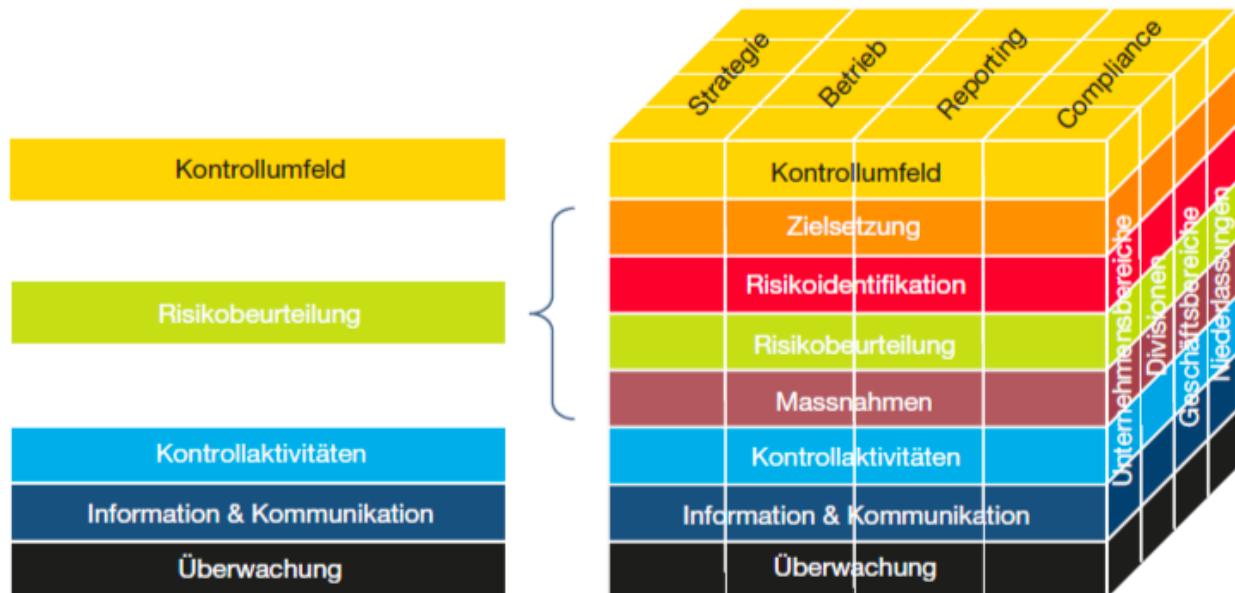
1. **Responsibility** (Verantwortung): Das Topmanagement sollte die **IT-Belange adäquat wahrnehmen**.
2. **Strategy** (Strategie): Es gilt, die **unternehmensstrategische Planung mit Blick auf die IT-Potenziale zu erweitern** und die **IT-Strategie aus den Unternehmensstrategien abzuleiten**.
3. **Acquisition** (Beschaffung): Die **Gestaltung der IT-Budgets muss sich im Rahmen transparenter Entscheidungsprozesse konsequent am Bedarf orientieren**.
4. **Performance** (Leistung): Die **IT-Services sind in Anlehnung an die Anforderungen der Fach- und Organisationsbereiche zu gestalten**.
5. **Conformance** (Konformität): Die **IT hat mit allen rechtlichen Vorgaben, Normen, internen Standards etc. konform zu gehen**.
6. **Human Behaviour** (der menschliche Faktor): Die **IT-Konzepte müssen den Bedürfnissen der internen und externen IT-Nutzer hohe Aufmerksamkeit beimessen..**

Drei Funktionen

- **Evaluate** (Bewertung): **Kontinuierliche Beurteilung des IT-Einsatzes**.
- **Direct** (Leitung): **Steuerung einer Business-gerechten Fokussierung** der IT-Massnahmen.
- **Monitor** (Kontrolle): **Systematische Überwachung von Regelkonformität (Compliance)** und Leistungsfähigkeit der IT.

5.7.3 Committee of Sponsoring Organizations (COSO)

- The Committee of Sponsoring Organizations' (COSO) mission is to provide thought leadership through the development of **comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence** designed to improve organizational performance and governance and to reduce the extent of fraud in organizations.
- US-amerikanische Organisation



Kontrollumfeld

- Das Kontrollumfeld wird durch das Leitbild des Unternehmens und die individuellen Eigenschaften der Mitarbeiter bestimmt. Z.B. Führungsstil («tone at the top») oder Verhaltensregeln wie der «code of ethics» oder der «code of conduct»

Risikobeurteilung

- Risikoidentifikation, Risikobeurteilung und Massnahmen

Kontrollaktivitäten

- Kontrollaktivitäten stellen sicher, dass die Massnahmen, welche die Geschäftsleitung zur Steuerung der Risiken und zur Zielerreichung getroffen hat, tatsächlich umgesetzt werden.

Information & Kommunikation

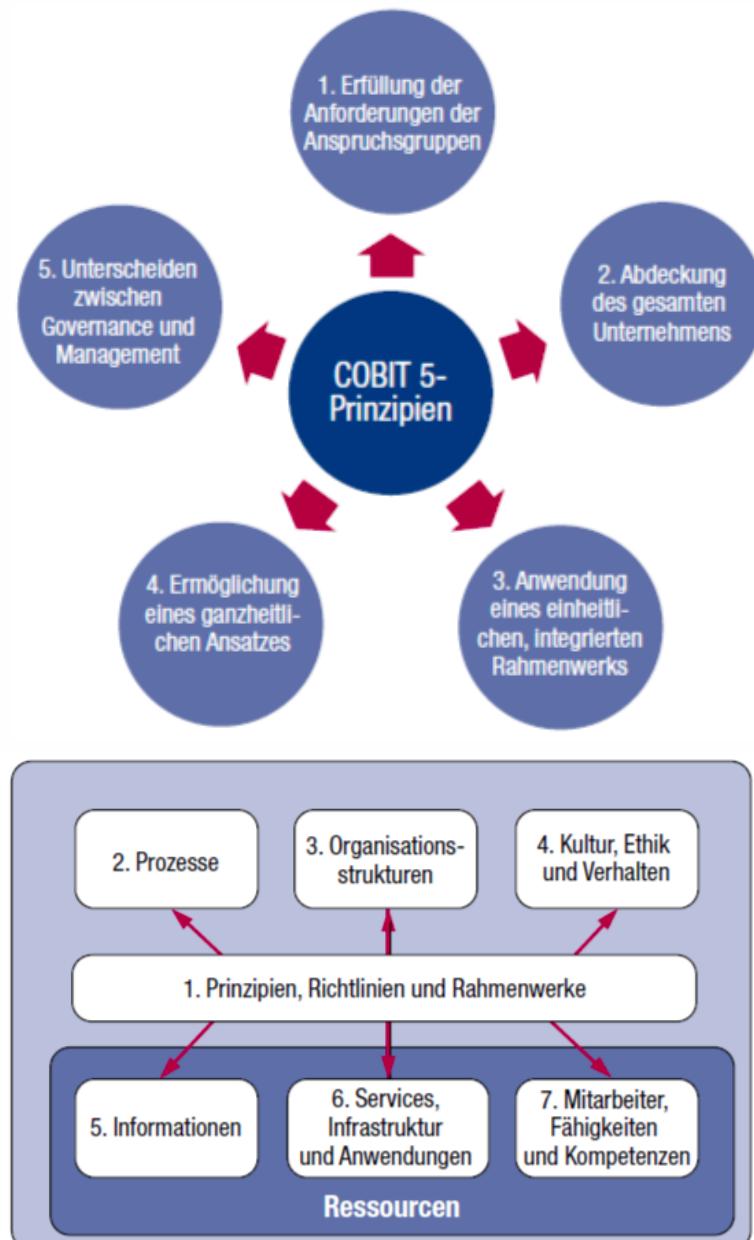
- Informations- und Kommunikationswege müssen definiert werden, damit die Mitarbeiter über jene Informationen verfügen, die sie benötigen, um die erforderlichen Kontrollen auszuführen.

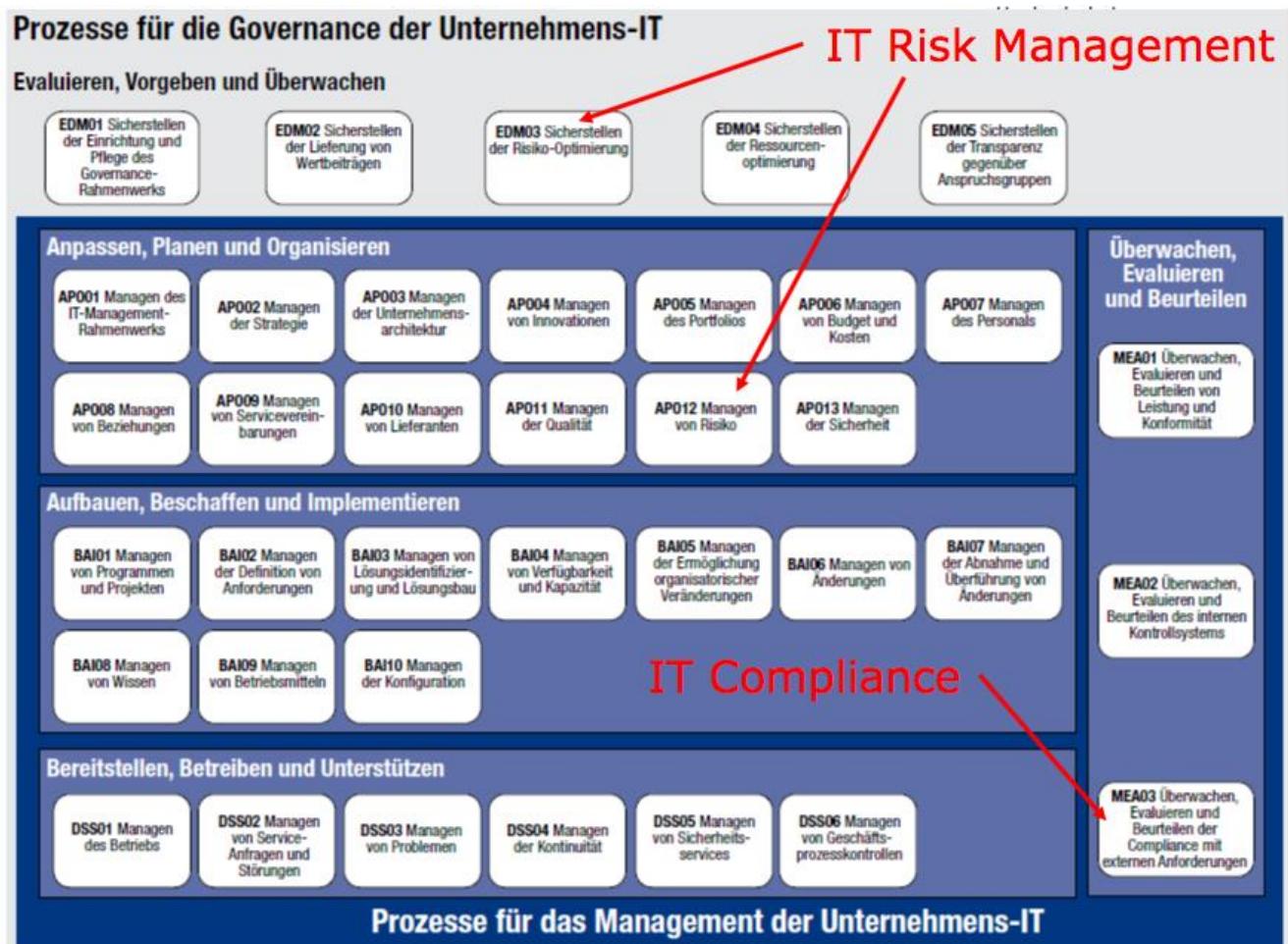
Überwachung

- Die Praxis zeigt, dass unterschiedliche Ursachen – etwa neue Produkte und Märkte, Restrukturierungen, Personalfluktuationen, neue Informationssysteme oder auch Veränderungen im regulatorischen Umfeld – dazu führen können, dass die einmal definierten Kontrollmassnahmen eine neue Risikosituation nicht mehr abdecken und Kontrollen nicht oder nur in einer sich verschlechternden Qualität durchgeführt werden.

5.7.4 COBIT 5

- ISACA-Leitlinien für die unternehmensweite Governance und Management der IT
- ISACA ist seit 1969 der internationale Verband für Spezialisten aus den Fachbereichen (IT-) Governance, Sicherheit, Risikomanagement und Revision





MEA03 Überwachen, Evaluieren und Beurteilen der Compliance mit externen Anforderungen

- Bewertung, inwieweit **IT-Prozesse und IT-gestützte Geschäftsprozesse Gesetzen, Bestimmungen und vertraglichen Anforderungen** gerecht werden. Sicherstellung, dass die Anforderungen identifiziert und eingehalten wurden, sowie Integration der IT-Compliance in die gesamte Unternehmens-Compliance.

EDM03 Sicherstellen der Risiko-Optimierung

- Sicherstellung, dass die Risikobereitschaft und Risikotoleranz **des Unternehmens verstanden, formuliert und kommuniziert werden**; Sicherstellung, dass das Risiko für den Unternehmenswert in Verbindung mit der IT-Nutzung identifiziert wurde und gemanagt wird.

APO12 Managen des Risikos

- Kontinuierliche Identifizierung, Beurteilung und Reduzierung **des IT-bezogenen Risikos innerhalb der von der Geschäftsführung festgelegten Toleranzwerte**.

5.8 Zusammenfassung GRC

Was wird unter (IT) Governance und Compliance verstanden?

- Was sind die Treiber? **Gesetzliche Vorgaben, Ziele, Strategie**
- Was sind die Zielsetzungen?
- Welche Aufgaben gibt es?
Teilschritte Framework aussuchen, Ziele definieren, Organisation definieren, Geld und Ressourcen haben, ...

Welche Abhängigkeiten/Schnittstellen zwischen (IT) Governance, Compliance und Risk Management gibt es?

ITG ist abgeleitet der Corporate Governance
Governance -> Steuert den Prozess
Compliance -> Kontrolliert den Prozess
Riskmanagement -> Ist das Hilfsmittel
ISMS -> Riskmanagement für Informationssicherheit

6 Stichwortverzeichnis

A

Anforderungen, 16
Audit and Assurance, 42

B

Begriffe, 4
Benutzer Trustmodell, 34

C

COBIT 5, 47
Committee of Sponsoring Organizations (COSO), 46
Compliance, 40
Corporate Governance, 37

D

Definitionen GRC, 36
Demonstration Kaufvertrag, 21

E

Einbettung von Gültigkeitsinformationen, 22
Einführung, 5
Erstellung von qualifizierten Signaturen, 21

F

Flaches Modell, 33
Frameworks, 44

G

Gegenüberstellung der Zertifikatstypen, 19
Gesetzliche Vorschriften, 13
Governance, Risk and Compliance, 36
GRC Anwendungsfall, 42

I

ISO / IEC 38500:2008, 45
ISO 27002:2013, 11
IT Governance, 38

K

Kreuzzertifizierung, 27

M

Management-Systeme im Unternehmen, 9
Modelle und Referenzen Compliance, 41

N

Nutzen GRC, 43

O

Open Compliance and Ethics Group (OCEG), 44

P

PDCA, 10
Prüfung von Zertifikaten, 24

R

Risiko-Assessment, 7
Risikoberechnung, 5
Risikobestimmungsmatrix, 6
Risikoidentifikation, 8
Risiko-Portfolio, 7
Rollen Informationssicherheit, 12

S

Schwachstellenanalyse, 12
Signatur Unterscheidung, 15
Signature as a Service, 23
Statement of Applicability, 11
System für die Anerkennung von Zertifizierungsstellen, 18

T

Trustketten und Prüfung der Zertifikate, 24
Trustmodelle, 30

U

Umsetzung GRC, 43

V

Verteiltes Modell, 31, 32

Z

Zertifikatsbasierende Anwendungen und PKI, 13
Zertifikatsketten, 28
Zertifikatstypen, 26
Zertifikatsüberprüfung, 35
Ziele Compliance, 40
Ziele IT Governance, 39
Zusammenfassung GRC, 49