

IT-Security in KMU

IWI Institut für Wirtschaftsinformatik

Ursula Sury

Rechtsanwältin

Professorin Informatikrecht

ursula.sury@hslu.ch

6. Mai 2008

Revision des Obligationenrechtes, seit 01.01.08

Wer, was, wann

- Muss der Verwaltungsrat ein **I**nternes **K**ontrollsystem (IKS) betreiben
- Die Revisionsstelle überprüft das Vorhandensein des IKS
- gilt erstmals für das Kalenderjahr 2008

Art. 716a¹

2. Unübertragbare Aufgaben

¹ Der Verwaltungsrat hat folgende unübertragbare und unentziehbare Aufgaben:

1. die **Oberleitung der Gesellschaft** und die Erteilung der nötigen Weisungen;
2. die **Festlegung der Organisation**;
3. die **Ausgestaltung des Rechnungswesens, der Finanzkontrolle** sowie der Finanzplanung, sofern diese für die Führung der Gesellschaft notwendig ist;
4. die Ernennung und Abberufung der mit der Geschäftsführung und der Vertretung betrauten Personen;
5. die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten, Reglemente und Weisungen;
6. die Erstellung des Geschäftsberichtes² sowie die Vorbereitung der Generalversammlung und die Ausführung ihrer Beschlüsse;
7. die Benachrichtigung des Richters im Falle der Überschuldung.

² Der Verwaltungsrat kann die Vorbereitung und die Ausführung seiner Beschlüsse oder die Überwachung von Geschäften Ausschüssen oder einzelnen Mitgliedern zuweisen. Er hat für eine angemessene Berichterstattung an seine Mitglieder zu sorgen.

Art. 662¹ OR

B. Geschäftsbericht

I. Im Allgemeinen

1. Inhalt

- ¹ Der **Verwaltungsrat erstellt** für jedes Geschäftsjahr einen Geschäftsbericht, der sich aus der **Jahresrechnung**, dem Jahresbericht und einer Konzernrechnung zusammensetzt, soweit das Gesetz eine solche verlangt.
- ² **Die Jahresrechnung besteht aus** der Erfolgsrechnung, der Bilanz und **dem Anhang.**

Art. 728a OR

2. Aufgaben der Revisionsstelle

a. Gegenstand und Umfang der Prüfung

1 Die Revisionsstelle prüft, ob:

1. die Jahresrechnung und gegebenenfalls die Konzernrechnung den gesetzlichen Vorschriften, den Statuten und dem gewählten Regelwerk entsprechen;
2. der Antrag des Verwaltungsrats an die Generalversammlung über die Verwendung des Bilanzgewinnes den gesetzlichen Vorschriften und den Statuten entspricht;
3. **ein internes Kontrollsystem existiert.**

2 Die Revisionsstelle berücksichtigt bei der Durchführung und bei der Festlegung des Umfangs der Prüfung das interne Kontrollsystem.

3 Die Geschäftsführung des Verwaltungsrats ist nicht Gegenstand der Prüfung durch die Revisionsstelle.

Art. 728b OR

b. Revisionsbericht

- ¹ Die Revisionsstelle erstattet dem Verwaltungsrat einen umfassenden Bericht mit Feststellungen über die Rechnungslegung, das interne Kontrollsystem sowie die Durchführung und das Ergebnis der Revision.**
- ² Die Revisionsstelle erstattet der Generalversammlung schriftlich einen zusammenfassenden Bericht über das Ergebnis der Revision. Dieser Bericht enthält:
 1. eine Stellungnahme zum Ergebnis der Prüfung;
 2. Angaben zur Unabhängigkeit;
 3. Angaben zu der Person, welche die Revision geleitet hat, und zu deren fachlicher Befähigung;
 4. eine Empfehlung, ob die Jahresrechnung und die Konzernrechnung mit oder ohne Einschränkung zu genehmigen oder zurückzuweisen ist.
- ³ Beide Berichte müssen von der Person unterzeichnet werden, die die Revision geleitet hat.

Art. 663b1 OR

IV. Anhang 1. Im Allgemeinen²

Der Anhang enthält:

- 12.3 Angaben über die Durchführung einer Risikobeurteilung;

Aufgaben des Verwaltungsrates

- Der Verwaltungsrat hat im Rahmen seiner unübertragbaren Kompetenzen und Verantwortlichkeiten sorgfältig zu handeln
- Sorgfältiges Handeln impliziert Risikobeurteilung
- über diese Risikobeurteilung hat der Verwaltungsrat im Anhang der Jahresrechnung Angaben zu machen

Aufgabe der Revisionsstelle

- Die Revisionsstelle prüft, **ob** ein internes Kontrollsystem existiert
- Die Geschäftsführung des Verwaltungsrates ist aber nicht Gegenstand der Prüfung der Revisionsstelle
- Die Revisionsstelle erstattet einen umfassenden Bericht zu Handen des Verwaltungsrates mit Feststellungen über das interne Kontrollsystem

Unklarheiten der gesetzlichen Regelung: Was überprüft die Revisionsstelle

- Überprüft die Revisionsstelle nur, ob ein IKS vorliegt
- Worin liegt der Zusammenhang resp. die Differenz der Begriffe IKS (Art. 728a und Art. 728b OR) und Risikobeurteilung (663b OR) und welche Konsequenzen hat dies auf die Prüfung durch die Revisionsstelle?

Hinweise zur Revision

- Die Bestimmungen über IKS und Risikobeurteilung gelten auch für die GmbH (Art. 801 und 818 OR)
- Für die Kommandit AG (Art. 764 Abs. 2 OR)
- Für die Genossenschaft (Art. 906 und Art. 908 OR)
- Für den Revisionspflichtigen Verein (Art. 69b Abs. 3 ZGB)
- Für die Stiftung (Art. 83a Abs. 2 und 83b Abs. 3 ZGB)

Hinweise zur Revision

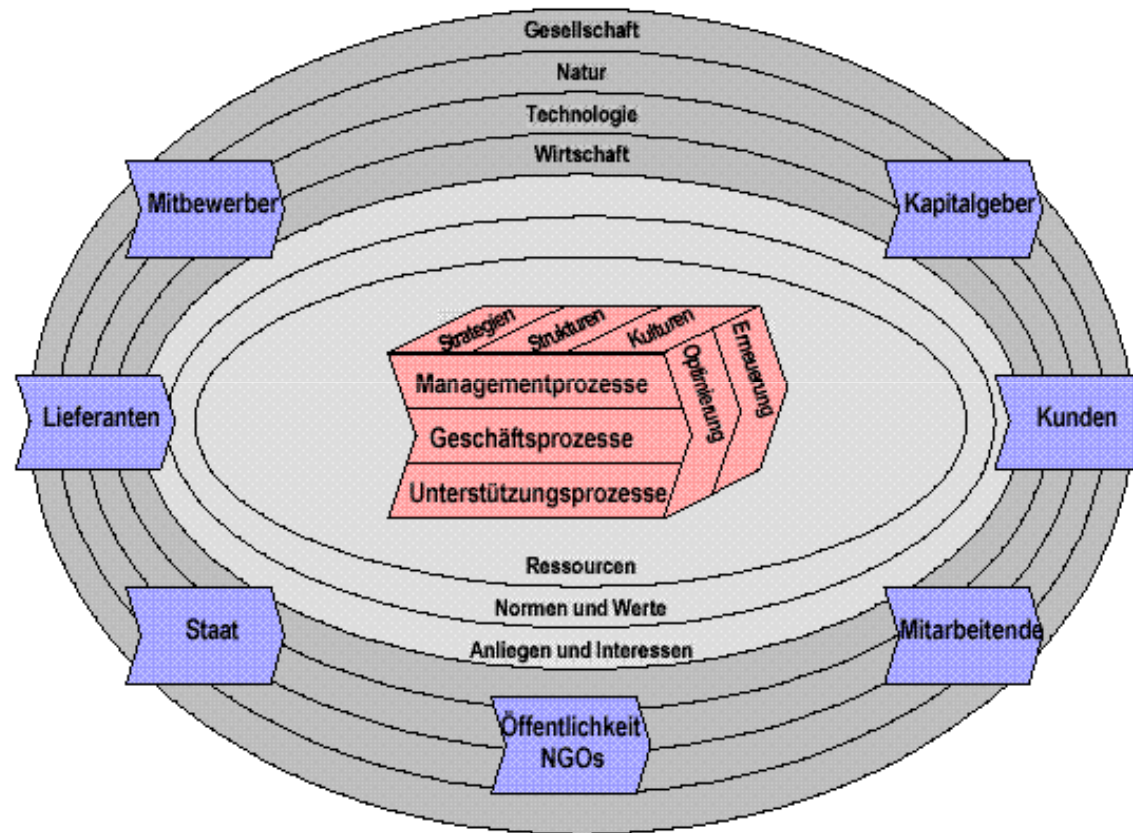
- Für Aktiengesellschaften, welche auf eine Revision verzichten (Opting-out, Art. 727a Abs. 2 OR) wird die Durchführung der Risikobeurteilung logischerweise durch die Revisionsstelle nicht kontrolliert

Opt-out heisst, dass mit Zustimmung sämtlicher Aktionäre auch auf die eingeschränkte Revision verzichten werden kann, wenn die Gesellschaft nicht mehr als zehn Vollzeitstellen im Jahresdurchschnitt hat (Art. 727a Abs. 2 OR)

Auswirkungen auf die Informatiksicherheit

- Der Verwaltungsrat ist für die Oberleitung der Gesellschaft, der damit verbundenen und dafür notwendigen Organisation in sämtlichen Unternehmerischen Bereichen verantwortlich
- Führungsverantwortung impliziert Auswahl, Instruktion und Kontrolle von Personen im Hinblick auf optimale Erreichung unternehmerischer Ziele
- Diese sorgfältige Unternehmensführung impliziert auch, dass Gesetze eingehalten werden und sämtliche unternehmerischen Risiken minimiert werden
- Damit unternehmerische Risiken minimiert werden können, müssen sie erkannt (verstanden!) und bewertet werden

St.Galler Management Konzept : Die Unternehmung als dynamisches System



nach Prof. Johannes Rüegg-Stürm, Hochschule St. Gallen

© B.R.Waser

- Sicher funktionierende IT ist das zentrale Element jedes unternehmerischen Unterstützungsprozesses
- Sicher funktionierende IT ermöglicht in vielen Betrieben erst die Erfüllung/Erstellung des Geschäftsprozesses
- Sicher funktionierende IT liefert die für die Geschäftsführung notwendigen Managementinformationen

IKS und IT-Sicherheit

Management IT-Sicherheit IT-Governance	–	prozess
Geschäfts IT-Sicherheit IT-Governance	–	prozess
Unterstützungs IT-Sicherheit IT-Governance	–	prozess

IKS und IT-Sicherheit

- Die (in der Literatur vielfach diskutierten und bekannten) Risiken der IT und insbesondere der IT-Sicherheit müssen folglich im Rahmen eines IKS festgestellt (verstanden!) und bewertet werden
- Es sind Massnahmen zur Minimierung der Risiken aufzuzeigen oder zu erläutern, warum man mit gewissen Risiken bewusst leben kann

IKS gemäss Schweizerprüfungsstandart PS890

- IKS wird im PS890 inhaltlich eingegrenzt verwendet, unter IKS werden hier Vorgänge und Massnahmen einer Unternehmung verstanden, welche die ordnungsmässige Buchführung und finanzielle Berichterstattung sicherstellen
- Es betrifft somit alles was implizit oder explizit Einfluss auf wahre und klare Buchführung haben kann

Gemäss PS890 ist in der Verantwortung des Verwaltungsrates

- Die Entscheidung betreffend Ausgestaltung des IKS unter Berücksichtigung der Zweckmässigkeit und dessen periodische Überprüfung
- sicherzustellen, dass die von der Geschäftsleitung zu treffenden Massnahmen zur Umsetzung der IKS implementiert werden, sowie
- sicherzustellen, dass die Wirksamkeit des IKS einer angemessenen Kontrolle unterliegt

Bestandteil eines IKS ist gemäss PS890

- Kontollumfeld
- Risikobeurteilungsprozess des Unternehmens
- Rechnungslegungrelevante Informationssysteme, damit verbundene Geschäftsprozesse und Kommunikation
- Kontrollaktivitäten
- Überwachung der Kontrollen

IKS, Risikomanagement, IT und IT-Sicherheit

Sicherheitsanforderungen an IT-Produkte als solche

- IT-Produkte/Software muss inhaltlich so angelegt sein
- dass sie kein Risiko bilden
- keine Falses generieren
- korrekte Managementinformationen liefern
- korrekten Geschäftserstellungoutput liefern
- keine Gesetze verletzen
- etc.

Risiken beim Einsatz von ganzen IT-Systemen

- Ausfallrisiken
- zu weit gehendes Monitoring (Datenschutzverletzung!)
- Unsichere Transaktionen
- Nicht beweisbare Transaktionen
- falsche Zustellungen
- etc.

Zusammenfassung

- Der Verwaltungsrat ist zu sorgfältiger Geschäftsführung persönlich verpflichtet
- sorgfältige Geschäftsführung impliziert Kontrolle, die Durchführung von systematischen Kontrollen muss im Rahmen einer Risikobeurteilung der Revisionsstelle nachgewiesen werden
- welche Konkreten Anforderungen der Gesetzgeber ans IKS stellt ist noch weitgehend unklar
- was die Revisionsstelle alles prüft, ist noch weitgehend unklar, Hinweise ergibt der PS890
- IT und IT-Sicherheit sind wesentliche und exestentielle Elemente des Management-, Geschäfts- und Unterstützungsprozesses einer Unternehmung und sind somit mit den entsprechenden Risiken behaftet
- IT und IT-Sicherheit bildet sowohl betreffend der verwendeten Produkte als auch ganzer Systeme und Verfahren Bestandteil des IKS

Ich danke für Ihre Aufmerksamkeit

HINWEISE AUF PUBLIKATIONEN

www.dieadvokatur.ch

www.itandlaw.ch

WEITERBILDUNGSMÖGLICHKEITEN
AUCH IT-RECHT

www.hslu.ch

Prof. Ursula Sury

Rechtsanwältin

Alpenquai 4

6005 Luzern