CAS Information-Security und Risk-Management

Rechtliche Aspekte

Lukas Fässler
Rechtsanwalt & Informatikexperte
FSDZ Rechtsanwälte & Notariat AG Zug
www.fsdz.ch faessler@fsdz.ch

Lukas Fässler

Rechtsanwalt und Informatikexperte

faessler@fsdz.ch
+41 41 727 60 80
+41 79 209 24 32

Profil

1975 – 1980	Studium an der Universität Fribourg/CH
1982	Anwaltspatent des Kantons Luzern
1982 – 1984	Gerichtsschreiber am Amtsgericht Hochdorf
1984 - 1987	Gerichtsschreiber am Verwaltungsgericht Luzern
1987 - 1992	EDV-Beauftragter im Gerichtswesen Kanton Luzern
1992 - 1997	Informatikchef des Kantons Luzern
1997	Selbständiger Spezialanwalt seit September 1997
1999 - 2000	Universität Zürich, Nachdiplomstudium, Internationales Wirtschaftsrecht (Spezialisierungskurs Immaterialgüterrecht, Technologie- und Informationsrecht)

Rechtsanwalt Lukas Fässler gilt als einer der bekanntesten und renommiertesten Informatik-Experten der Schweiz mit langjähriger Praxiserfahrung. Seit 1982 befasst er sich hauptberuflich mit Informatik und Telekommunikation,Governance und Compliance von Unternehmen, insbesondere auch im Bezug auf das Informations-Management (Information Governance - Records Management und digitale Langzeitarchivierung).
Von 1992 bis 1997 leitete er als Informatikchef des Kantons Luzern die Organisations- und Informatik-Dienste (OID) des Kantons.

Dozententätigkeit

Universität Bern, Master of Advanced Studies (MAS) for Archival an Information Management

Fachhochschule Nordwestschweiz in Basel; Hochschule für Wirtschaft, CAS eCommerce und Online-Marketing: Online-Marketing, Webshop, Social Media & Co.

Fachhochschule Nordwestschweiz in Olten; Hochschule für Wirtschaft: CAS Informations- und Records-Management

Fachhochschule Nordwestschweiz in Basel, Hochschule für Wirtschaft: CAS Information Security & Risk Management (CISSP/BSI): Professionelles Security & Risk Management mit BSI-Zertifizierung und Vorbereitung auf die CISSP-Prüfung.

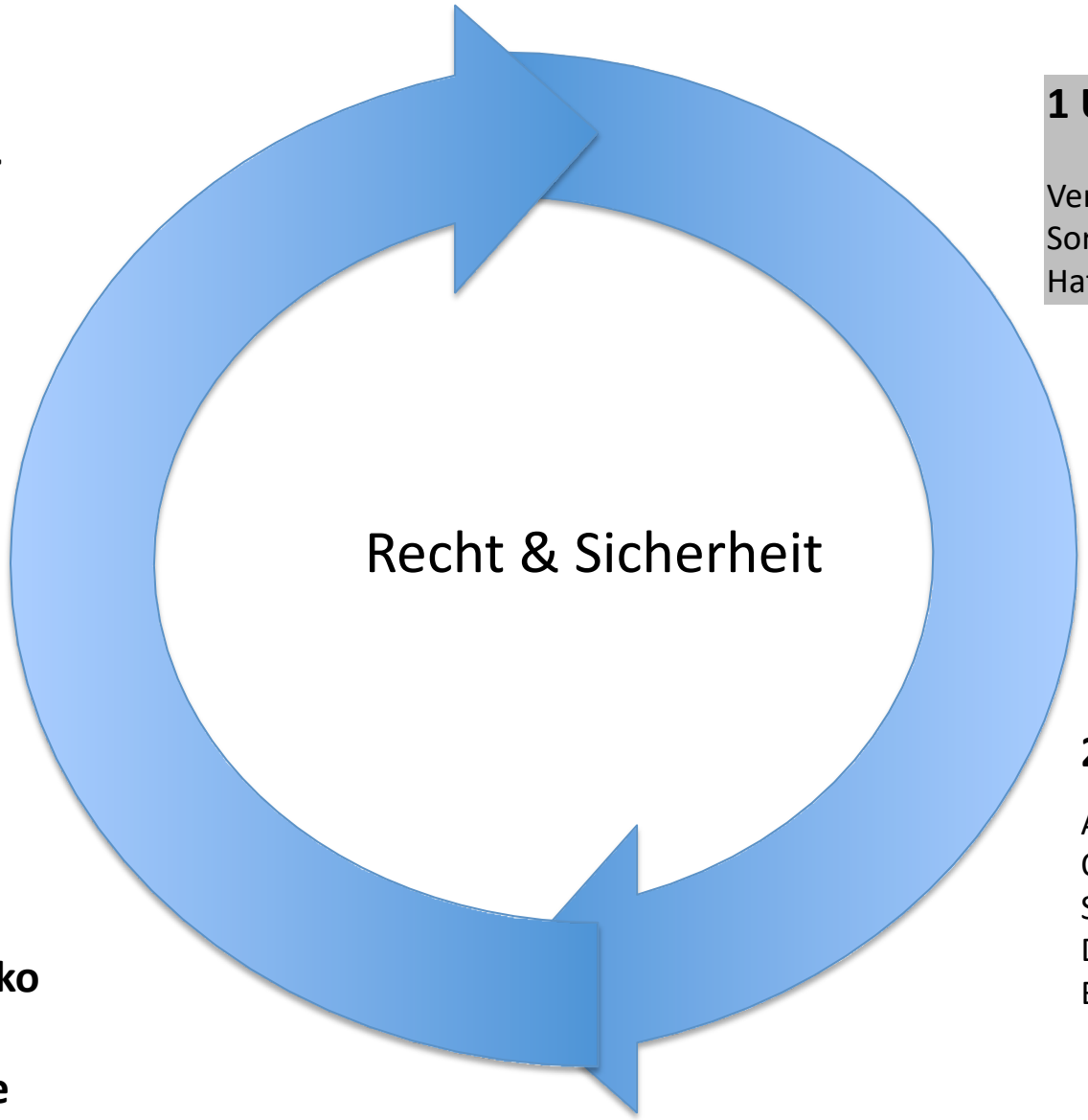
Fachhochschule Nordwestschweiz in Basel, Hochschule für Wirtschaft: CAS IT Service Management & IT Controlling (ITIL V3, COBIT):

Fachhochschule Nordwestschweiz in Basel, Hochschule für Wirtschaft: CAS Operational Risk Management:

Hochschule für Wirtschaft HSW in Luzern, Fachkurs Gemeindefinanzen (Submissionsrecht)

Inhaltsverzeichnis

1 Unternehmen & Sorgfalt
2 Standards & Normen
3 Branchenrisiken
4 Das neue EU-Datenschutzrecht
5 Grundsätze der Datensicherheit
6 Beurteilung & Verbesserung
7 Kontrolle & Durchsetzung



1 Unternehmen

Verantwortung
Sorgfaltspflichten
Haftung

2 Gesetze

Allgemeines Obligationenrecht
StGB
DSG /DSVO
BÜPF Überwachung

3 Standards & Normen

4 Branchenrisiko & Technologie

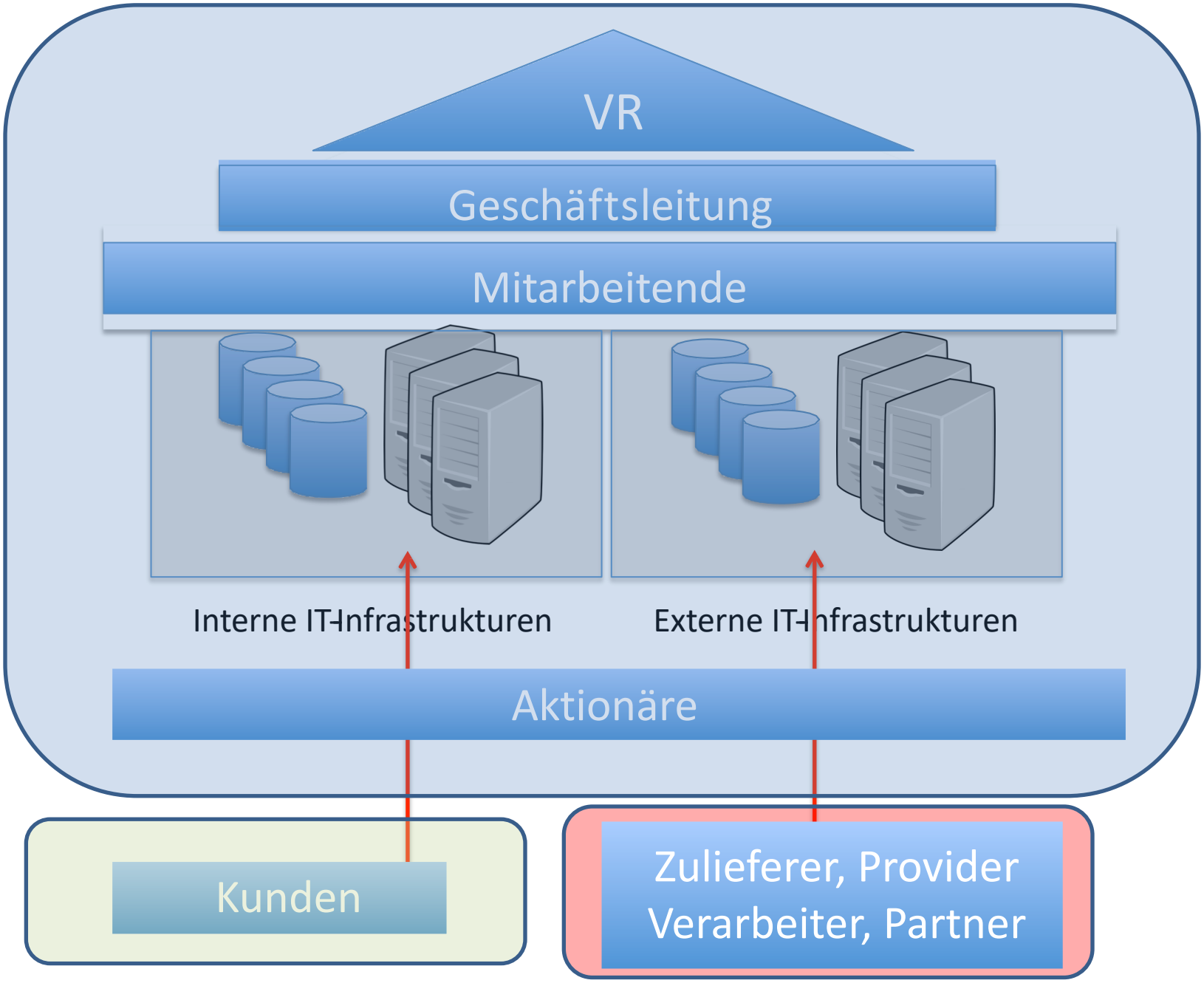
5 Beurteilung & Verbesserung

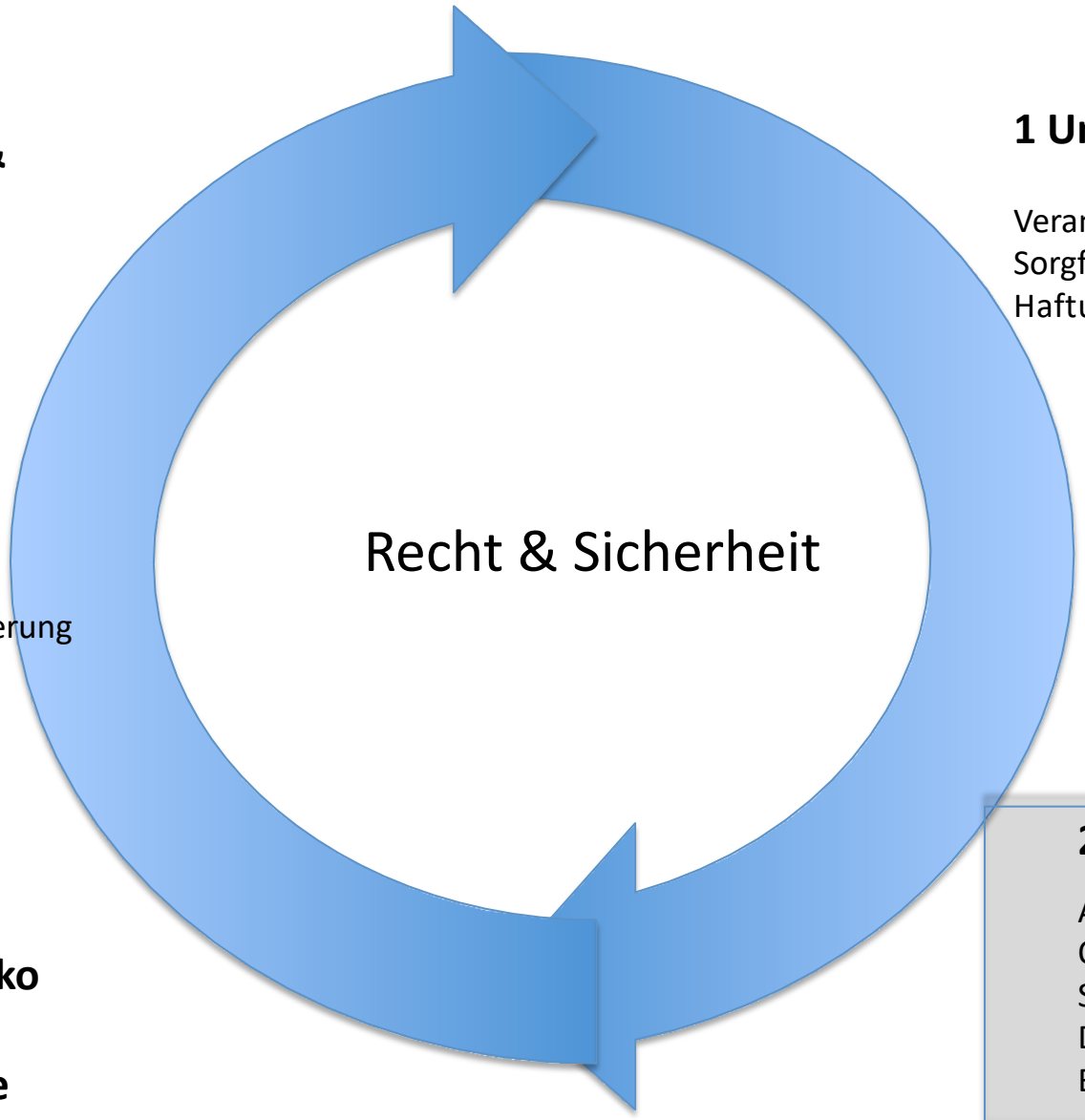
Kontinuierliche Verbesserung
Haftungsreduktion

6 Massnahmen & Durchsetzung

Abwehr
Verteidigung

1. Unternehmen und Sorgfalt


VR
Geschäftsleitung
Mitarbeitende
Interne IT-Infrastrukturen
Externe IT-Infrastrukturen
Aktionäre
Kunden
Zulieferer, Provider
Verarbeiter, Partner



1 Unternehmen

Verantwortung
Sorgfaltspflichten
Haftung

2 Gesetze

Allgemeines Obligationenrecht
StGB
DSG /DSVO
BÜPF Überwachung

3 Standards & Normen

4 Branchenrisiko & Technologie

5 Beurteilung & Verbesserung

Kontinuierliche Verbesserung
Haftungsreduktion

6 Massnahmen & Durchsetzung

Abwehr
Verteidigung

Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht)

vom 30. März 1911 (Stand am 1. Juli 2015)

Art. 716[441]

III. Aufgaben
1. Im Allgemeinen

[1] Der Verwaltungsrat kann in allen Angelegenheiten Beschluss fassen, die nicht nach Gesetz oder Statuten der Generalversammlung zugeteilt sind.

[2] Der Verwaltungsrat führt die Geschäfte der Gesellschaft, soweit er die Geschäftsführung nicht übertragen hat.

Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht)

vom 30. März 1911 (Stand am 1. Juli 2015)

Art. 716*a*[442]

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 Geschäftsberichtes[443] sowie die Vorbereitung der Generalversammlung und die Ausführung ihrer Beschlüsse;
7. die Benachrichtigung des Richters im Falle der Überschuldung.

Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht)

vom 30. März 1911 (Stand am 1. Juli 2015)

IV. Sorgfalts- und Treuepflicht

Art. 717[445]

[1] Die Mitglieder des Verwaltungsrates sowie Dritte, die mit der Geschäftsführung befasst sind, müssen ihre Aufgaben mit aller Sorgfalt erfüllen und die Interessen der Gesellschaft in guten Treuen wahren.

[2] Sie haben die Aktionäre unter gleichen Voraussetzungen gleich zu behandeln.

Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht)

vom 30. März 1911 (Stand am 1. Juli 2015)

III. Haftung für Verwaltung, Geschäftsführung und Liquidation

Art. 754[488]

[1] Die Mitglieder des Verwaltungsrates und alle mit der Geschäftsführung oder mit der Liquidation befassten Personen sind sowohl der Gesellschaft als den einzelnen Aktionären und Gesellschaftsgläubigern für den Schaden verantwortlich, den sie durch absichtliche oder fahrlässige Verletzung ihrer Pflichten verursachen.

[2] Wer die Erfüllung einer Aufgabe befugterweise einem anderen Organ überträgt, haftet für den von diesem verursachten Schaden, sofern er nicht nachweist, dass er bei der Auswahl, Unterrichtung und Überwachung die nach den Umständen gebotene Sorgfalt angewendet hat.

Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

Urteilskopf

139 III 24

4. Auszug aus dem Urteil der I. zivilrechtlichen Abteilung i.S. A. und Mitb. gegen X. AG (Beschwerde in Zivilsachen)
4A_375/2012 vom 20. November 2012

Regeste a

Art. 754 OR; aktienrechtliche Verantwortlichkeit.
Haftung des Verwaltungsrats für die Kosten eines erfolglos geführten Prozesses über die Eintragung von Namenaktien im Aktienbuch der Gesellschaft, in dem erkannt wurde, die Verweigerung der Eintragung sei nicht im Interesse der Gesellschaft erfolgt und habe gegen das Gleichbehandlungsgebot der Aktionäre sowie gegen das Rechtsmissbrauchsverbot verstossen (E. 3).

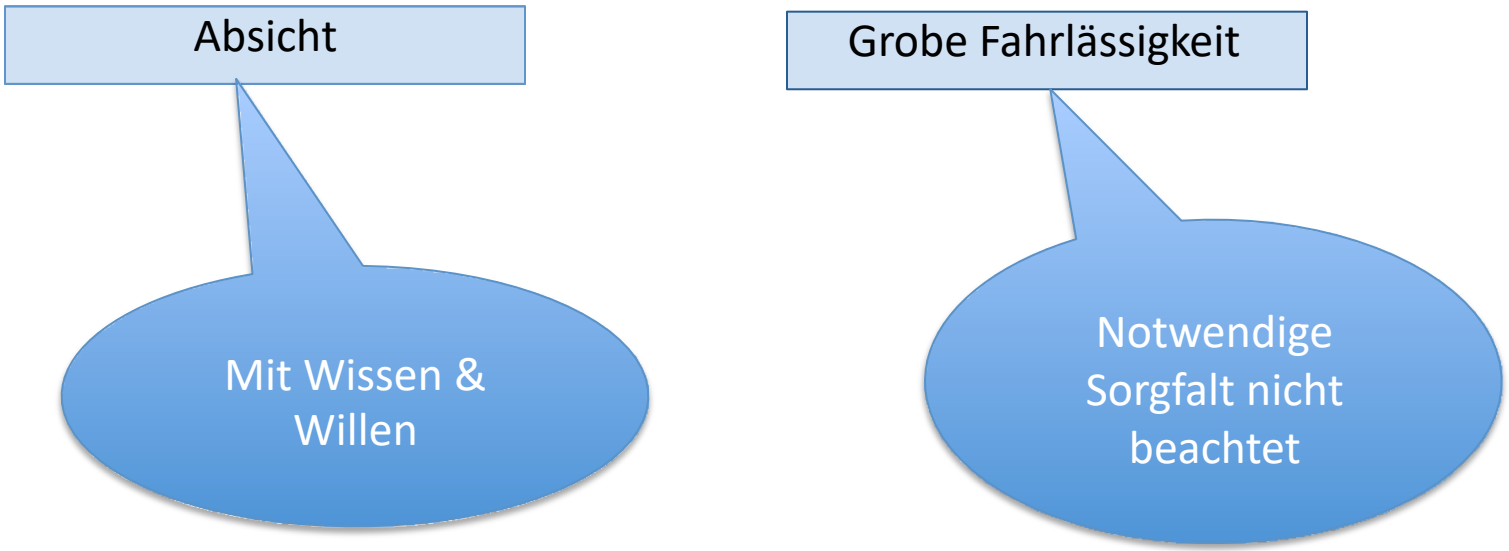
3.2 Nach **Art. 717 Abs. 1 OR** müssen die Mitglieder des Verwaltungsrats, sowie Dritte, die mit der Geschäftsführung befasst sind, ihre Aufgaben mit aller Sorgfalt erfüllen und die Interessen der Gesellschaft in guten Treuen wahren. Die gesetzlich normierte Treuepflicht verlangt, dass die Mitglieder des Verwaltungsrats ihr Verhalten am Gesellschaftsinteresse ausrichten. Für die Sorgfalt, die der Verwaltungsrat bei der Führung der Geschäfte der Gesellschaft aufzuwenden hat, gilt ein objektiver Massstab. Die Verwaltungsräte sind zu aller Sorgfalt verpflichtet und nicht nur zur Vorsicht, die sie in eigenen Geschäften anzuwenden pflegen (**BGE 122 III 195** E. 3a S. 198; **BGE 113 II 52** E. 3a S. 56). Das Verhalten eines Verwaltungsratsmitglieds wird deshalb mit demjenigen verglichen, das billigerweise von einer abstrakt vorgestellten, ordnungsgemäss handelnden Person in einer vergleichbaren Situation erwartet werden kann (PETER BÖCKLI, Schweizer Aktienrecht, 4. Aufl. 2009, § 13 N. 575).

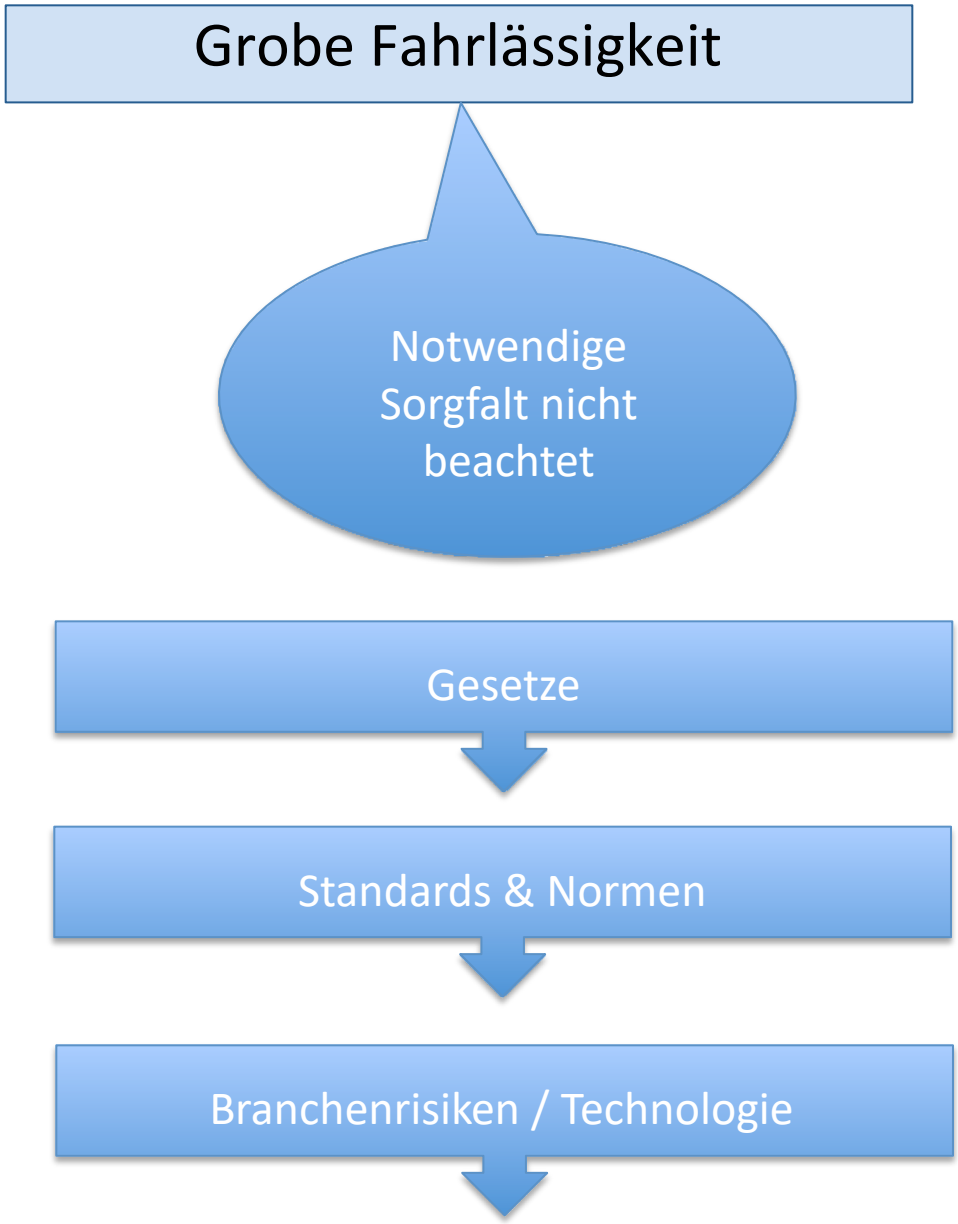
Die Sorgfalt richtet sich nach dem Recht, Wissensstand und den Massstäben im Zeitpunkt der fraglichen Handlung oder Unterlassung. Bei der Beurteilung von Sorgfaltspflichtverletzungen hat mithin eine ex ante Betrachtung stattzufinden (vgl. Urteile 4A_74/2012 vom 18. Juni 2012 E. 5.1; 4A_467/2010 vom 5. Januar 2011 E. 3.3; BERNARD CORBOZ, in: Commentaire romand, Code des obligations, Bd. II, 2008, N. 22 zu **Art. 754 OR**; GERICKE/WALLER, in: Basler Kommentar, Obligationenrecht, Bd. II, 4. Aufl. 2012, N. 31c zu **Art. 754 OR**; WATTER/PELLANDA, in: Basler Kommentar, Obligationenrecht, Bd. II, 4. Aufl. 2012, N. 6 zu **Art. 717 OR**).

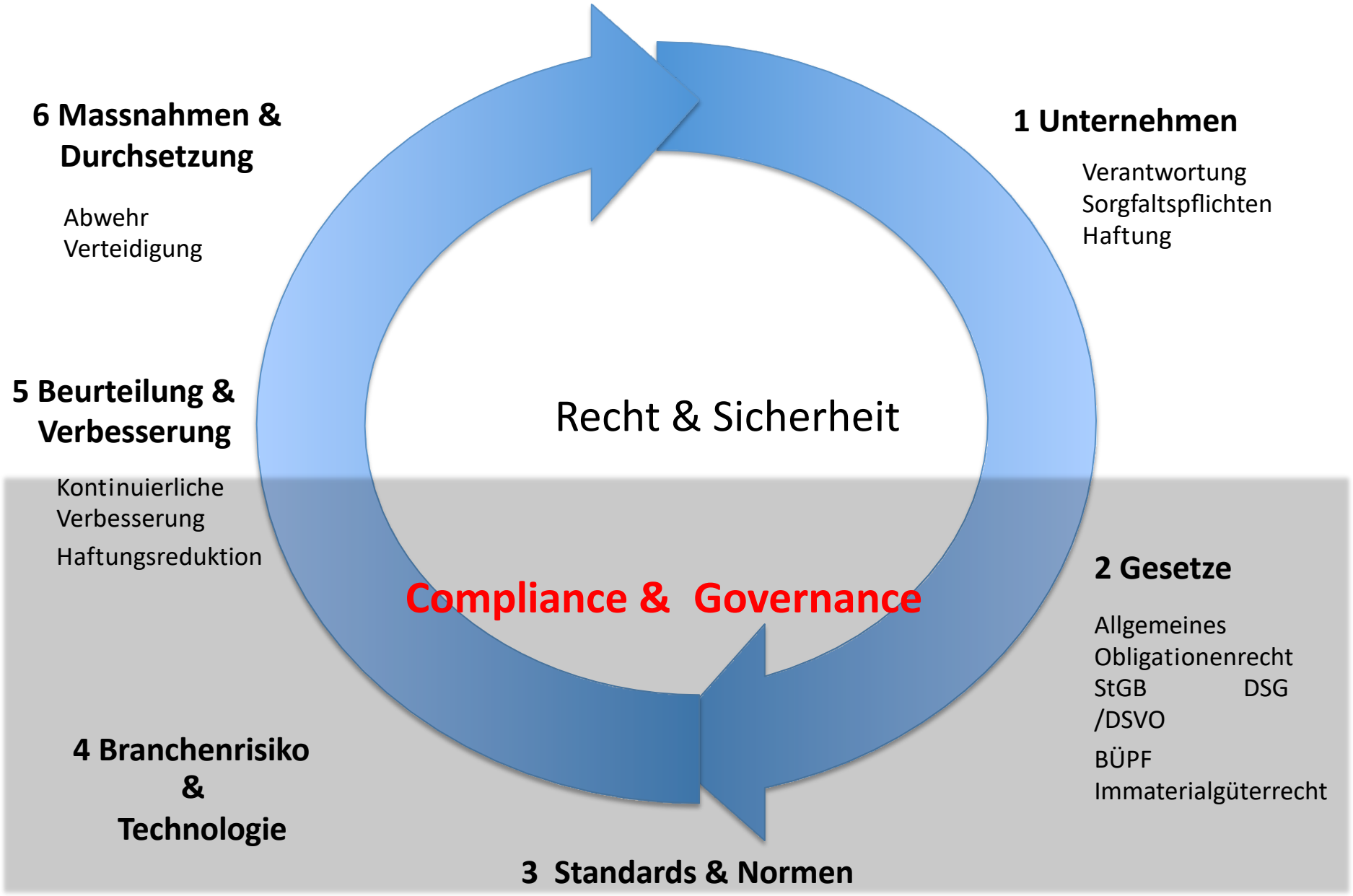
Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

Die Sorgfalt richtet sich nach dem Recht, Wissensstand und den Massstäben im Zeitpunkt der fraglichen Handlung oder Unterlassung.

für den Schaden verantwortlich, den sie durch absichtliche oder fahrlässige Verletzung ihrer Pflichten verursachen.




Grobe Fahrlässigkeit
Notwendige Sorgfalt nicht beachtet
Gesetze
Standards & Normen
Branchenrisiken / Technologie


6 Massnahmen & Durchsetzung
Abwehr
Verteidigung
1 Unternehmen
Verantwortung
Sorgfaltspflichten
Haftung
5 Beurteilung & Verbesserung
Kontinuierliche Verbesserung
Haftungsreduktion
Recht & Sicherheit
Compliance & Governance
2 Gesetze
Allgemeines Obligationenrecht
StGB DSG /DSVO
BÜPF
Immaterialgüterrecht
4 Branchenrisiko & Technologie
3 Standards & Normen

Strafrecht / Cybercrime

- **Straftatbestände**
  - **Computerdelikte/Cybercrime**
    - Unbefugte Datenbeschaffung Art. 143 StGB
    - Unbefugtes Eindringen in ein Datenverarbeitungssystem Art. 143bis StGB
    - Datenbeschädigung Art. 144bis StGB
    - Betrügerischer Missbrauch einer Datenverarbeitungsanlage Art. 147 StGB
    - Check- und Kreditkartenmissbrauch Art. 148 StGB
    - Zeitdiebstahl (Art. 150 StGB)
    - Herstellen und in Verkehrbringen von Materialien zur unbefugten Entschlüsselung codierter Angebote (Art. 150bis StGB)
    - Spamverbot (Art. 45a FMG/ 83 FDV)

Art. 143

Unbefugte Daten beschaflhng

1 Wer in der Absicht, sich oder einen anderen unrechtmässig zu bereichern, sich oder einem anderen elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

2 Die unbefugte Datenbeschaffung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

Bundesgerichtshof Deutschland BGH: **WLAN-Schlüssel im Privatbereich**
Urteil vom 24.11.2016 – I ZR 220/16

Der Inhaber eines Internetanschlusses mit WLAN-Funktion ist nach den **Grundsätzen der Störerhaftung** zur Prüfung verpflichtet, ob der verwendete Router über die im Zeitpunkt seines Kaufs für den privaten Bereich marktüblichen Sicherungen verfügt.

Hierzu zählt der im Kaufzeitpunkt aktuelle Verschlüsselungsstandard sowie die Verwendung eines individuellen, ausreichend langen und sicheren Passworten (Festhalten an BGH, Urteil vom 12. Mai 2010, I ZR 121/08, BGHZ 185, 330 Rn. 34).

Ein aus einer zufälligen 16-stelligen Ziffernfolge bestehendes, werkseitig für das Gerät individuell voreingestelltes Passwort genügt den Anforderungen an die Passwortsicherheit.

Sofern keine Anhaltspunkte dafür bestehen, dass das Gerät schon im Kaufzeitpunkt eine Sicherheitslücke aufwies, liegt in der Beibehaltung eines solchen werkseitig eingestellten Passworts kein Verstoss gegen die den Anschlussinhaber treffende Prüfungspflicht .

Tipp: WLAN-Router müssen mit aktueller Sicherheitssoftware eingesetzt werden, ansonsten die Voraussetzung nach CH-StGB „....gegen seinen unbefugten Zugriff besonders gesichert....“ entfällt und keine Strafverfolgung mehr möglich ist gegen Cybertäter.

vom 21. Dezember 1937 (Stand am 1. Juli 2013)

Unbefhgtes Eindringen in ein Daten verarbeitungs systelll

Art. 143bis

1Wer auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Freiheits strafe bis zu drei Jahren oder Geldstrafe bestraft.

2Wer Passworter, Programme oder andere Daten, von denen er weiss oder annehmen muss, dass sie zur Begehung einer strafbaren Handlung gemäss Absatz I verwendet werden sollen, in Verkehr bringt oder zugänglich macht, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

KANTON LUZERN
Amtsgericht Luzern-Lond

106 EST01

Abteilung I
Präsident Trüeb, Amtsrichterin Unternährer, Meier und Ersatzrichter Dätwyler, Gerichtsschreiberin Wigger

Urteil vom 6. Dezember 2010

Rechtsspruch

1. M W ist schuldig der mehrfachen unbefugten Datenbeschaffung nach Art. 143 Abs. 1 StGB, begangen in mittelbarer Täterschaft vom 20.5.2008 bis 31.7.2008.

2. M W wird in Anwendung von Art. 34,Art. 42 Abs. 1. Art. 44 Abs. 1, Art. 47, Art. 49 Abs. 1 und Art. 51 StGB mlt einer Geldstrafe von Fr. 8'800.00, 80 Tagessätzen zu je Fr. 110.00 bestraft unter Anrechnung von zwei Tagessätzen erstanden aus der zweitägigen Untersuchungshaft vom 19.11.2008 bis 20.11.2008. Die Geldstrafe wird bedingt ausgesprochen bei einer Probezeit von 2 Jahren.

3. Zusätzlich wird in Anwendung von Art. 42 Abs. 4 und Art 106 StGB eine Busse von Fr. 1'750.00 ausgesprochen. Die Ersatzfreiheitsstrafe beträgt 16 Tage.

vom 21. Dezember 1937 (Stand am 1. Juli 2013)

Daten beschädigung

Art. 144bis

1. Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Hat der Täter einen grossen Schaden verursacht, so kann auf Freiheitsstrafe von einem Jahr bis zu fünf Jahren erkannt werden. Die Tat wird von Amtes wegen verfolgt.

2. Wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonst wie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Handelt der Täter gewerbsmässig, so kann auf Freiheitsstrafe von einem Jahr bis zu fünf Jahren erkannt werden.

Schweizerisches Strafgesetzbuch

311.0

vom 21. Dezember 1937 (Stand am 1. Juli 2013)

Erschleichen einer Leistung

Art. 150

Wer, ohne zu zahlen, eine Leistung erschleicht, von der er weiss, dass sie nur gegen Entgelt erbracht wird, namentlich indem er

- Ein öffentliches Verkehrsmittel benützt,
- eine Aufführung, Ausstellung oder ähnliche Veranstaltung besucht,
- eine Leistung, die eine Datenverarbeitungsanlage erbringt oder die ein Automat vermittelt, beansprucht,

wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Schweizerisches Strafgesetzbuch

vom 21. Dezember 1937 (Stand am 1. Juli 2013)

Herstellen lllld Inverkehrbringen von Mate1alien zur unbefugten Entschltisselung codierter Angebote

Art. 150bis

1Wer Geräte, deren Bestandteile oder Datenverarbeitungsprogramme, die zur unbefugten Entschlüsselung codierter Rundfunkprogramme oder Fernmeldedienste bestimmt und geeignet sind, herstellt, einführt, ausführt, durchführt, in Verkehr bringt oder installiert, wird, auf Antrag, mit Busse bestraft.

2 Versuch und Gehilfenschaft sind strafbar.

vom 21. Dezember 1937 (Stand am 1. Juli 2013)

Dritter Tell: Begriffe

Art. 110

4 *Urkunden* sind Schriften, die bestimmt und geeignet sind, oder Zeichen, die bestimmt sind, eine Tatsache von rechtlicher Bedeutung zu beweisen. Die Aufzeichnung auf Bild- und Datenträgern steht der Schriftform gleich, sofern sie demselben Zweck dient.

Schweizerisches Strafgesetzbuch

311.0

vom 21. Dezember 1937 (Stand am 1. Januar 2017)

Elfter Titel: Urkundenfälschung

Art. 251[1] Urkundenfälschung

Urkundenfälschung

1. Wer in der Absicht, jemanden am Vermögen oder an andern Rechten zu schädigen oder sich oder einem andern einen unrechtmässigen Vorteil zu verschaffen,

eine Urkunde fälscht oder verfälscht, die echte Unterschrift oder das echte Handzeichen eines andern zur Herstellung einer unechten Urkunde benützt oder eine rechtlich erhebliche Tatsache unrichtig beurkundet oder beurkunden lässt,

eine Urkunde dieser Art zur Täuschung gebraucht,

wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

2. In besonders leichten Fällen kann auf Freiheitsstrafe bis zu drei Jahren oder Geldstrafe erkannt werden.

Schweizerisches Strafgesetzbuch

vom 21. Dezember 1937 (Stand am 1. Januar 2017)

Urkundenfälschung im Amt

Art. 317[317]

1. Beamte oder Personen öffentlichen Glaubens, die vorsätzlich eine Urkunde fälschen oder verfälschen oder die echte Unterschrift oder das echte Handzeichen eines andern zur Herstellung einer unechten Urkunde benützen,

Beamte oder Personen öffentlichen Glaubens, die vorsätzlich eine rechtlich erhebliche Tatsache unrichtig beurkunden, namentlich eine falsche Unterschrift oder ein falsches Handzeichen oder eine unrichtige Abschrift beglaubigen,

werden mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

2. Handelt der Täter fahrlässig, so ist die Strafe Busse.

Bundesgericht Tribunal
federal Tribunale
federale Tribunal
federal

Urtellskopf

138 IV 209

31. Auszug aus dem Urteil der Strafrechtlichen Abteilung i.S. X. gegen Staatsanwaltschaft Basel Landschaft (Beschwerde in Strafsachen) vom 22. Oktober 2012

Regeste

Art. 110 Abs. 4 und Art. 251 Ziff. 1 StGB;
Urkundenqualität eines E-Mails.

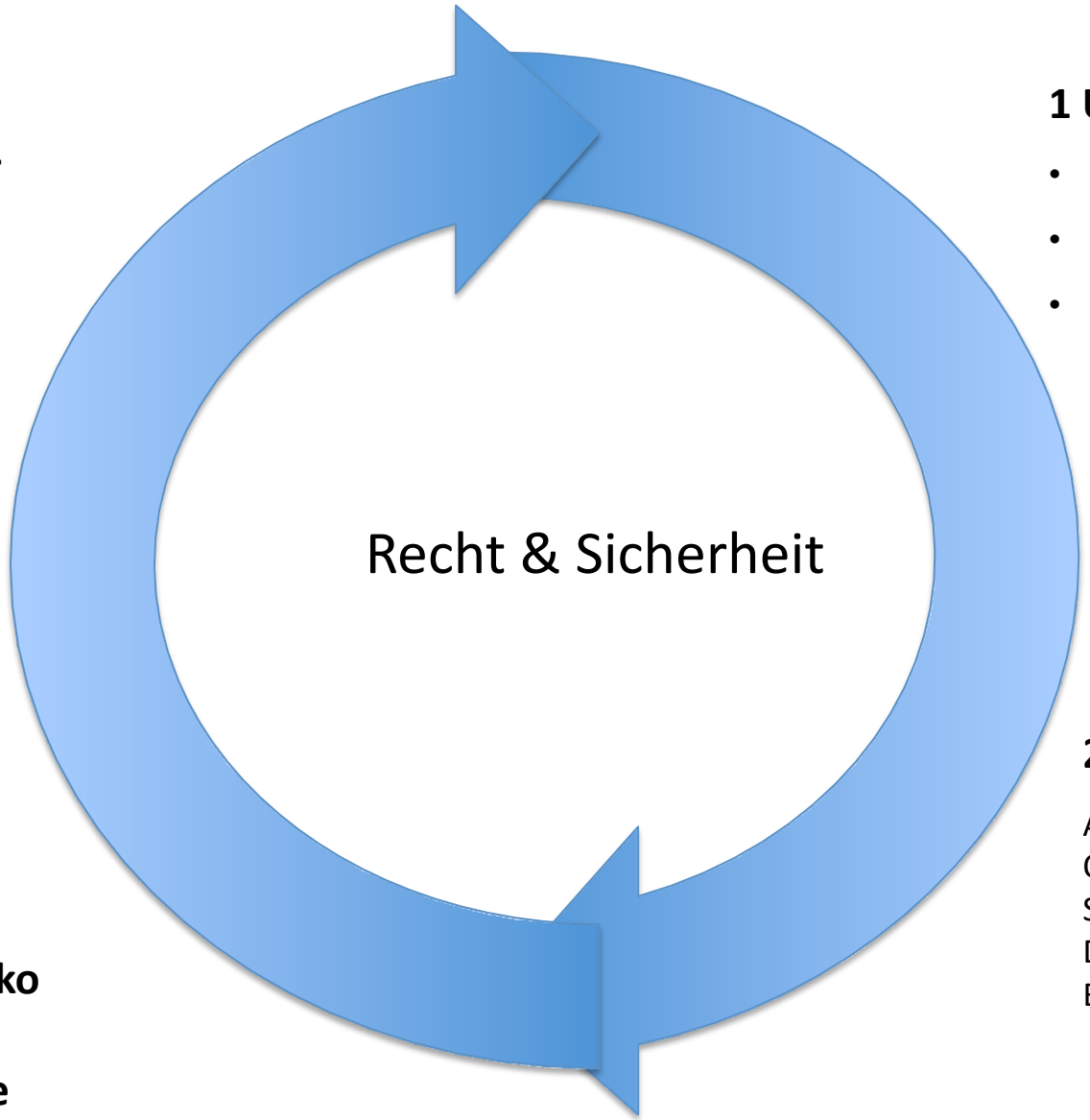
E-Mails sind Computerurkunden. Verfälscht der Täter an ihn gerichtete E-Mails und leitet sie anschliessend an Drittpersonen weiter, erfüllt er den Tatbestand der Urkundenfälschung.

5.4 Der Schuldspruch wegen Urkundenfälschung verletzt kein Bundesrecht.

Ausser Frage steht zunächst, dass E-Mails Urkunden darstellen, wenn sie beim Empfänger ausgedruckt werden, d.h. wenn die Daten sichtbar gemacht werden, sofern der Aussteller erkennbar ist (vgl. **BGE 116 IV 343** E. 3).

Wie die Vorinstanz zutreffend annimmt, kommt aber auch dem noch nicht ausgedruckten E-Mail grundsätzlich der Charakter einer (Computer-)Urkunde zu. Dabei erfüllt die Verfälschung eines E-Mails ohne weiteres den Tatbestand der Urkundenfälschung, soweit dieses nach der Manipulation weiterversendet wird und seinen Adressaten erreicht. Der Täter setzt dadurch einen Prozess in Gang, der die Speicherung der Datenurkunde zur Folge hat.

2. Standards, Normen & Richtlinien



1 Unternehmen

- Verantwortung
- Sorgfaltspflichten
- Haftung

2 Gesetze

Allgemeines Obligationenrecht
StGB
DSG /DSVO
BÜPF Überwachung

3 Standards & Normen

4 Branchenrisiko & Technologie

5 Beurteilung & Verbesserung

Kontinuierliche Verbesserung
Haftungsreduktion

6 Massnahmen & Durchsetzung

Abwehr
Verteidigung

Teil II

Corporate Governance

Die Sorgfalt richtet sich nach dem Recht, Wissensstand und den Massstäben im Zeitpunkt der fraglichen Handlung oder Unterlassung.

swiss code of best practice for corporate governance

Swiss Code of Best Practice

Seit dem 1. Juli 2002 existiert zudem der Swiss Code of Best Practice (oder *"Swiss Code"*) vom Dachverband der Schweizer Wirtschaft (economiesuisse). Dieser listet Verhaltensregeln auf, die für eine vorbildliche Corporate Governance notwendig sind. Die Anwendung des Codes basiert auf Freiwilligkeit. Dieser Swiss Code of Best Practice wurde 2007 um zehn Empfehlungen zur Vergütung von Verwaltungsräten und oberstem Management erweitert.[8]

Quelle: Wikipedia

Inhalt

Trägerschaft 4

Swiss Code of Best Practice for Corporate Governance 6

Präambel 6

«Corporate Governance» als Leitidee 6

«Swiss Code of Best Practice for Corporate Governance» als Leitlinie und Empfehlung 6

Die Aktionäre 7

Der Verwaltungsrat und die Geschäftsleitung 9
Aufgaben des Verwaltungsrats
Zusammensetzung
Unabhängigkeit
Arbeitsweise und Vorsitz des Verwaltungsrats
Umgang mit Interessenkonflikten und Wissensvorsprüngen
Vorsitz von Verwaltungsrat und Geschäftsleitung
Umgang mit Risiken und Compliance, internes Kontrollsystem
Ausschüsse des Verwaltungsrats
Besondere Verhältnisse

Die Revision 15

Die Offenlegung 15

Anhang 1 16

Einleitung 16

Empfehlungen zu den Vergütungen von Verwaltungsrat und Geschäftsleitung 16
Die Rolle der Generalversammlung
Die Rolle des Verwaltungsrats und des Vergütungsausschusses
Einzelheiten des Vergütungssystems
Vergütungsbericht und Transparenz

economiesuisse

Aufgaben des Verwaltungsrats

9

Der von den Aktionären gewählte Verwaltungsrat nimmt die Oberleitung und Oberaufsicht der Gesellschaft bzw. des Konzerns wahr.

- Der Verwaltungsrat bestimmt die strategischen Ziele, die generellen Mittel zu ihrer Erreichung und die mit der Führung der Geschäfte zu beauftragenden Personen.
- Der Verwaltungsrat prägt die Corporate Governance und setzt diese um.
- Er sorgt in der Planung für die grundsätzliche Übereinstimmung von Strategie, Risiken und Finanzen.
- Der Verwaltungsrat lässt sich vom Ziel der nachhaltigen Unternehmensentwicklung leiten.

economiesuisse

Umgang mit Risiken und Compliance, internes Kontrollsystem

20

Der Verwaltungsrat sorgt für ein dem Unternehmen angepasstes Risikomanagement und ein internes Kontrollsystem. Das Risikomanagement bezieht sich auf finanzielle, operationelle und reputationsmässige Risiken.

- Das interne Kontrollsystem ist der Grösse, der Komplexität und dem Risikoprofil der Gesellschaft anzupassen.
- Das interne Kontrollsystem deckt, je nach den Besonderheiten der Gesellschaft, auch das Risikomanagement ab.
- Die Gesellschaft richtet eine interne Revision ein. Diese erstattet dem Prüfungsausschuss («Audit Committee») und gegebenenfalls dem Präsidenten des Verwaltungsrats Bericht.

economiesuisse

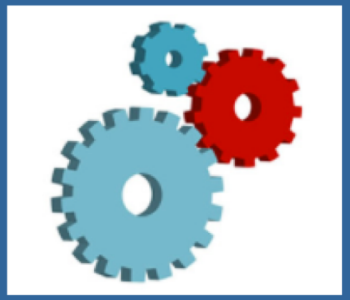
21

Der Verwaltungsrat trifft Massnahmen zur Einhaltung der anwendbaren Normen (Compliance).

- Der Verwaltungsrat ordnet die Funktion der Compliance nach den Besonderheiten des Unternehmens und erlässt geeignete Verhaltensrichtlinien.
- Er orientiert sich dabei an anerkannten Best Practice-Regeln.[3]
- Der Verwaltungsrat gibt sich mindestens einmal jährlich darüber Rechenschaft, ob die für ihn und das Unternehmen anwendbaren Compliance-Grundsätze hinreichend bekannt sind und ihnen dauernd nachgelebt wird.

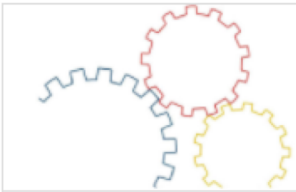
IT-Grundschutz

IT-Grundschutz - die Basis für Informationssicherheit - Der vom BSI entwickelte IT-Grundschutz ermöglicht es, notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Viele Arbeitsprozesse werden elektronisch gesteuert und große Mengen von Informationen sind digital gespeichert, werden verarbeitet und in Netzen übermittelt. Damit sind die Institutionen in Wirtschaft und Verwaltung und jeder Bürger von dem einwandfreien Funktionieren der eingesetzten IT abhängig.



IT-Grundschutz-Modernisierung

Informationen und Materialien zur derzeit durchgeführten Modernisierung des IT-Grundschutzes



IT-Grundschutz-Standards

Die BSI-Standards enthalten Empfehlungen zu Methoden, Prozessen, Vorgehensweisen und Maßnahmen zur Informationssicherheit.

IT-Grundschutz-Kataloge

Die IT-Grundschutz-Kataloge beinhalten organisatorische, technische, personelle und infrastrukturelle Empfehlungen.

IT-Grundschutz-Tools

Der Support für das GS-Tool läuft Ende 2016 aus. Anwender können auf zahlreiche Tool-Alternativen zurückgreifen, die den IT-Grundschutz unterstützen.

Zertifizierung nach ISO 27001

Informationen und Anträge zur Prüfung nach ISO 27001 auf der Basis von IT-Grundschutz

IT-Grundschutz-Schulung

Ressourcenplanung, Technik, Sicherheitskonzept: Lernen Sie den IT-Grundschutz in unserer Schulung kennen.

- Alle
  - **nach Themenbereich**
  - nach Fachgruppe
  - A bis Z
  - nach Nummer
- Standards
- Best Practice
- Hilfsmittel
- Musterlösung
- RFC's
- Eingabetermine
- Gesamtübersicht
- Verbindlichkeit
- Vorlagen

- Management
  - Strategie, Planung, Controlling, Analytik, Unternehmensarchitektur, Prozesse, Leistungen, Qualität, Archivierung, Statistik, Vertrieb, Produktion, Kommunikation
- Technologie
- Fachliche Fähigkeiten
  - Kernfähigkeiten mit Voraussetzungscharakter
    - Einwohner, Unternehmen, Objekte, Tiere, Geoinformationen, Rechtssammlung, Behörden
  - Kernfähigkeiten
    - Arbeit, Bauen, Aussenbeziehungen, Gerichtsbarkeit, Kultur, Sicherheit, Steuern, Umwelt, Gesundheit, Bildung, Wirtschaft, Landwirtschaft, Gesellschaft, Mobilität, Politische Aktivitäten, Persönliches
- Allgemeine Dienste
  - Finanzen
  - Personal
  - Beschaffung
  - Informatik
  - Logistik
  - Immobilien
  - Geschäftsabwicklung
    - Zusammenarbeiten, Informationen finden, Berechtigung prüfen, Partner bedienen, Geschäftsfall bearbeiten, Pakete austauschen, Dokument erstellen und verwalten
  - Datenschutz
  - Versicherung

Rechtsrelevanz

Standards & Normen sind keine Gesetze (= „Softlaw“ genannt)

Gesetzgeber und Branchen verweisen im Zusammenhang mit der Sorgfaltspflicht wiederholt auf Normen

Normen werden für die Beurteilung der Verantwortung der Sorgfaltspflichten zum Quasigesetz (best pracise)

Pflichtverletzung -> Verschulden (Fahrlässigkeit – Grobfahrlässigkeit) -> Haftung werden aus diesen Normen heraus abgeleitet

Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht)

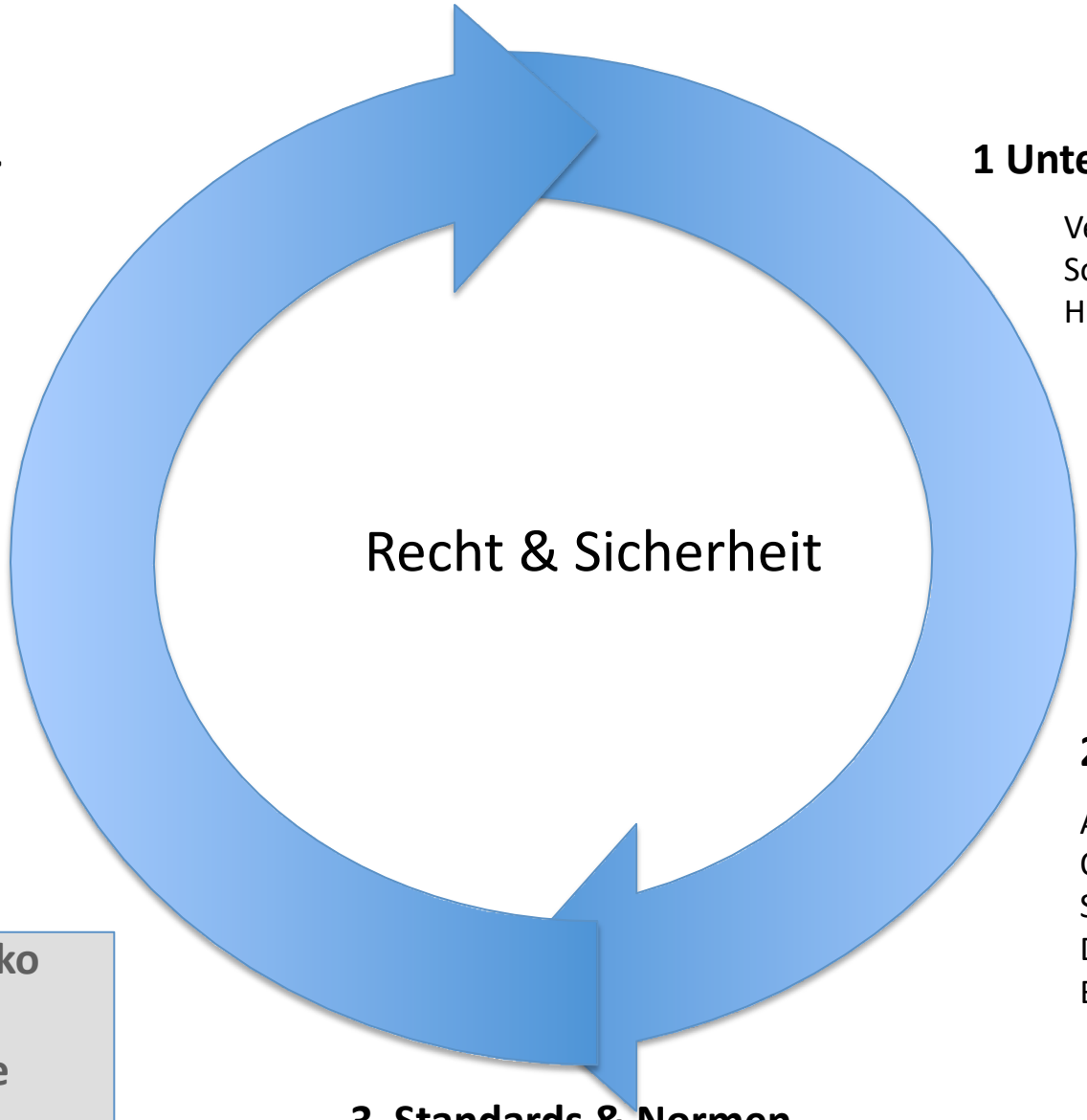
vom 30. März 1911 (Stand am 1. Januar 2016)

III. Haftung für Verwaltung, Geschäftsführung und Liquidation

sofern er nicht nachweist, dass er bei der Auswahl, Unterrichtung und Überwachung die nach den Umständen gebotene Sorgfalt angewendet hat.

Sorgfalt in der Auswahl	=	Evaluieren
Sorgfalt in der Unterrichtung	=	Kommandieren
Sorgfalt in der Überwachung	=	Kontrollieren
Sorgfalt in der Verbesserung	=	Korrigieren

3. Branchenrisiken



1 Unternehmen

Verantwortung
Sorgfaltspflichten
Haftung

2 Gesetze

Allgemeines Obligationenrecht
StGB
DSG /DSVO
BÜPF Überwachung

3 Standards & Normen

4 Branchenrisiko & Technologie

5 Beurteilung & Verbesserung

Kontinuierliche Verbesserung
Haftungsreduktion

6 Massnahmen & Durchsetzung

Abwehr
Verteidigung

Branchenrisiko

Das **Branchenrisiko** beschreibt das Risiko, welches die Unternehmen einer bestimmten Branche betrifft. Es entsteht aufgrund der Fokussierung auf bestimmte Produkte, welche im Laufe der Zeit unterschiedlichen wirtschaftlichen Entwicklungen ausgeliefert sind. Dabei kann es durch technische Innovationen außerhalb der Branche oder aber durch veränderte Konsumgewohnheiten zu Nachfrageveränderungen kommen, die sich negativ auf diesen Wirtschaftszweig auswirken und somit das Branchenrisiko begründen. Weitere Gründe für ein Branchenrisiko bestehen in der Regulierung eines Wirtschaftszweiges oder auch durch steigende Inputpreise beispielsweise für die zugrunde liegenden Rohstoffe. Besonders bei neuen Wirtschaftszweigen ist das Branchenrisiko höher, insbesondere durch den Wettbewerb mit etablierten Branchen, jedoch auch die Chancen.

221.112.944

Bundesgesetz über die Produktehaftpflicht

(Produktehaftpflichtgesetz, PrHG)

vom 18. Juni 1993 (Stand am 1. Juli 2010)

Art. 1 Grundsatz

[1] Die herstellende Person (Herstellerin)[3] haftet für den Schaden, wenn ein fehlerhaftes Produkt dazu führt, dass:

a. eine Person getötet oder verletzt wird;

b. eine Sache beschädigt oder zerstört wird, die nach ihrer Art gewöhnlich zum privaten Gebrauch oder Verbrauch bestimmt und vom Geschädigten[4] hauptsächlich privat verwendet worden ist.

[2] Die Herstellerin haftet nicht für den Schaden am fehlerhaften Produkt.

221.112.944

Bundesgesetz über die Produktehaftpflicht

(Produktehaftpflichtgesetz, PrHG)

vom 18. Juni 1993 (Stand am 1. Juli 2010)

Art. 5 Ausnahmen von der Haftung

[1] Die Herstellerin haftet nicht, wenn sie beweist, dass:

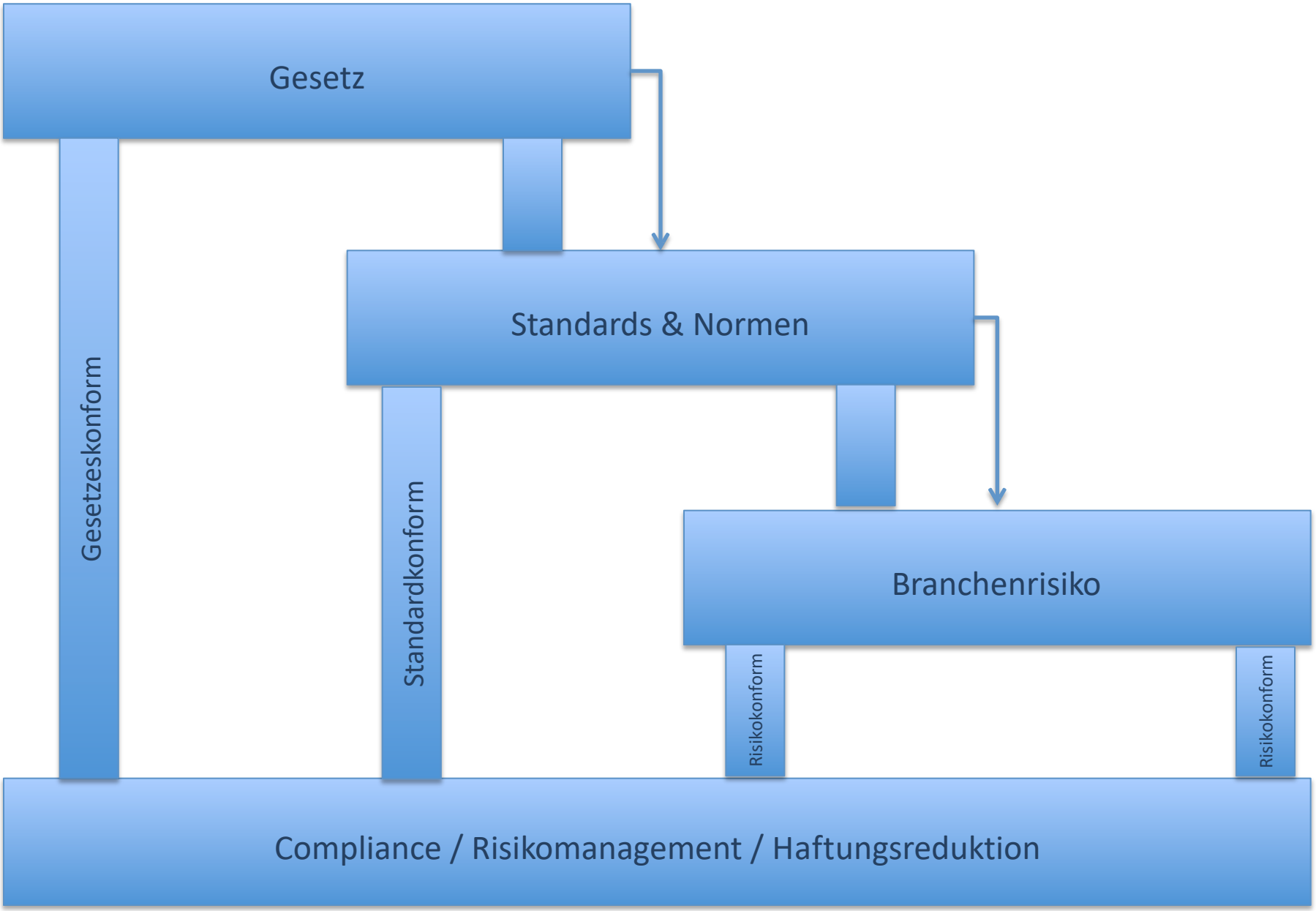
a. sie das Produkt nicht in Verkehr gebracht hat;

b. nach den Umständen davon auszugehen ist, dass der Fehler, der den Schaden verursacht hat, noch nicht vorlag, als sie das Produkt in Verkehr brachte;

c. sie das Produkt weder für den Verkauf oder eine andere Form des Vertriebs mit wirtschaftlichem Zweck hergestellt noch im Rahmen ihrer beruflichen Tätigkeit hergestellt oder vertrieben hat;

d. der Fehler darauf zurückzuführen ist, dass das Produkt verbindlichen, hoheitlich erlassenen Vorschriften entspricht;

e. der Fehler nach dem Stand der Wissenschaft und Technik im Zeitpunkt, in dem das Produkt in Verkehr gebracht wurde, nicht erkannt werden konnte.


Gesetz
Standards & Normen
Branchenrisiko
Gesetzeskonform
Standardkonform
Risikokonform
Risikokonform
Compliance / Risikomanagement / Haftungsreduktion