LALIVE

THE DISPUTES POWERHOUSE

Internationale Entwicklungen in Governance, Risiko- und Compliance-Management

Vortrag Netzwerk Risikomanagement
Bern, 27. März 2019

Dr. Daniel Lucien Bühr
Partner, LALIVE

Agenda

1. Einleitung
2. Internationale GRC Trends
3. Internationale Best Practice im Risiko und Compliance Management
4. Exkurs: Besondere Aspekte der öffentlichen Hand
5. Anregungen

1. Einleitung

«Governance»-Vorfälle sind omnipräsent, auch in der Schweiz :

RAIFFEISEN

DIE POST

bls

PILATUS

Universität St.Gallen

UBS

1. Einleitung

Die Medien berichten intensiv über Governance-Vorfälle und Gräben zwischen ethischer Erwartungshaltung und Realität:

Beispiel:

«Die Wirtschaft sieht die Warnzeichen nicht»*;* NZZ, 10.1.2019:

Die vom Bundesrat geplante Lockerung für Waffenexporte oder auch die Versenkung des CO2-Gesetzes waren wenig angetan, das Vertrauen der Schweizer in die Moral der Wirtschaftsvertreter zu stärken. […] Dem offenbar wachsenden Bedürfnis der Schweizerinnen und Schweizer nach mehr Ethik und Nachhaltigkeit in der Wirtschaft Rechnung zu tragen, ist für die Bürgerlichen offenbar keine Option.

1. Einleitung

Gräben zwischen ethischer Erwartung und faktischer Governance - Beispiel:

Kein Bericht zum Ausmass der Steuerhinterziehung

Der Nationalrat will nicht wissen, in welchem Ausmass in der Schweiz Steuern hinterzogen werden. Er hat es am Mittwoch mit 135 zu 57 Stimmen abgelehnt, vom Bundesrat einen Bericht zu verlangen. SP-Nationalrätin Mattea Meyer (ZH) hatte in ihrem Postulat vorgeschlagen, zur Analyse die Daten aus den straflosen Selbstanzeigen einzubeziehen – mitsamt den Daten aus den «Panama Papers» und den «Paradise Papers». Steuerhinterziehung sei kein Kavaliersdelikt, sagte Meyer. Es sei unerlässlich, mehr über Ausmass und Merkmale der Steuerhinterzieher zu kennen. (sda)

Quelle: https://www.srf.ch/news/schweiz/maurer-warnt-vor-neuer-liste-nationalrat-schuetzt-bestehende-inhaberaktien

1. Einleitung

Gräben zwischen ethischer Erwartung und faktischer Governance - Beispiel:

Basel Institute on Governance: Anti-Money Laundering Index 2018

Erläuterung:
Bestplatziertes Land: Finnland
Rang: 129
Score: 2.57
Schlechtest platziertes Land: Tadjikistan
Rang: 1
Score: 8.30

59	EL SALVADOR	5.43	+0.06
60	BOTSWANA	5.40	+0.10
61	MOLDOVA	5.37	-0.06
62	EGYPT	5.35	-0.21
63	SOUTH AFRICA	5.34	+0.75
64	SWITZERLAND	5.33	+0.48
65	BAHRAIN	5.33	-0.10
66	GHANA	5.32	-1.01
67	GEORGIA	5.31	+0.03
68	INDIA	5.28	+0.38

https://index.baselgovernance.org/sites/collective.localhost/files/aml-index/basel_aml_index_10_09_2018.pdf

2. Internationale GRC Trends

- Weltweite Einigkeit unter GRC Fachleuten: Erhalt der License to Operate, Wettbewerbsfähigkeit und langfristiger Erfolg von Organisationen setzt Best Practice GRC Management voraus.

- Best Practice wird primär in internationalen Standards konsolidiert: ISO 31000 – Risk management; ISO 19600/ISO 37301 – Compliance management, ISO 37001 – Anti-bribery management etc. – CN, BR, neben USA, UK, DE, FR starke Treiber (CH seit vielen Jahren aktiv involviert).

- Risiko Management und Compliance Management sind heute je eigene Berufsfelder und schnell wachsende wissenschaftliche Disziplinen.

2. Internationale GRC Trends

- Die Welt wird immer transparenter: AIA, globaler Wettbewerb im Whistleblowing, neue Medien, Journalisten-Netzwerke etc.
- Rasant zunehmende internationale Zusammenarbeit im Enforcement
- Digitalisierung der Compliance (Regulatory Technology/Reg Tech).

2. Internationale GRC Trends

Beispiel für die Anforderungen an das Compliance Management (Feb. 2017):

1

U.S. Department of Justice
Criminal Division
Fraud Section

Evaluation of Corporate Compliance Programs

Introduction

The Principles of Federal Prosecution of Business Organizations in the United States Attorney's Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporate entity, determining whether to bring charges, and negotiating plea or other agreements. These factors, commonly known as the "Filip Factors," include "the existence and effectiveness of the corporation's pre-existing compliance program" and the corporation's remedial efforts "to implement an effective corporate compliance program or to improve an existing one."

Quelle: https://www.justice.gov/criminal-fraud/page/file/937501/download

2. Internationale GRC Trends

Das DOJ prüft das Compliance Management von Unternehmen in:

- **11 Haupt-Bereichen**, bspw. *Senior and Middle Management, Autonomy and Resources* oder *Risk Assessment*, und

- **46 Unter-Bereichen**, bspw. *Conduct at the Top*, *Funding and Resources* oder *Risk Management Process*.

2. Internationale GRC Trends

Beispiele für die Prüffragen des DOJ:

2. Senior and Middle Management

- *Conduct at the Top – How have senior leaders, through their words and actions, encouraged or discouraged the type of misconduct in question? What concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts? How does the company monitor its senior leadership's behavior? How has senior leadership modelled proper behavior to subordinates?*

2. Internationale GRC Trends

Beispiele für die Prüffragen des DOJ:

5. Risk Assessment

- *Risk Management Process – What methodology has the company used to identify, analyze, and address the particular risks it faced?*

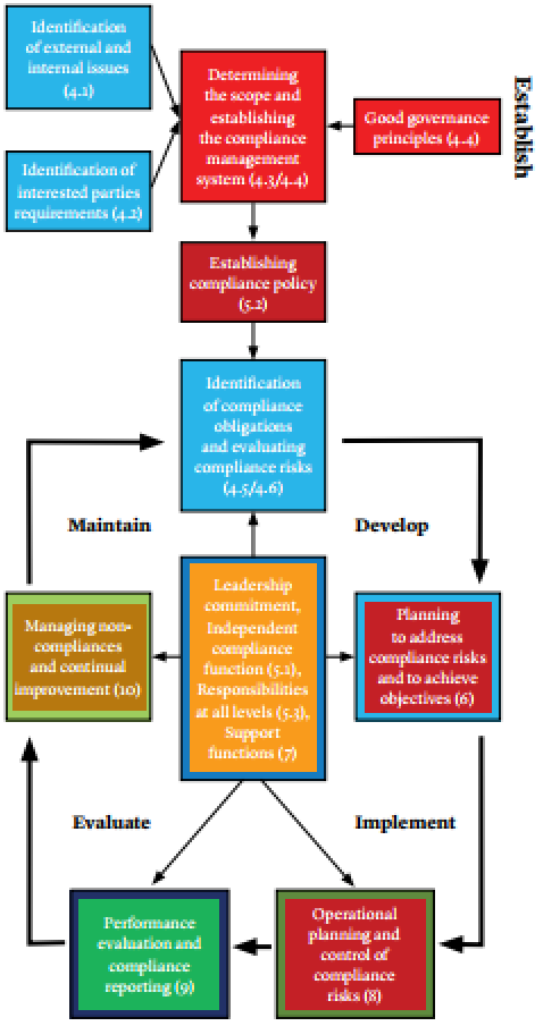
Es gibt weltweit zwei anerkannte Methoden für Risikomanagement: ISO 31000 und das COSO Enterprise Risk Management/ERM Framework.

2. Internationale GRC Trends

Konsolidierung der internationalen Best Practice DOJ ≙ ISO :

No.	DOJ document topic	ISO 19600, sections	Overlap?
1	Analysis of underlying misconduct	Introduction; 10.1	Yes[3]
2	Senior and middle management	Introduction; 4.4; 5.1; 7.3.2.3	Yes
3	Autonomy and resources	4.4; 5.3; 5.3.4	Yes
4	Policies and procedures	5.1; 5.2; 5.2.1; 5.3.4; 6.2; 8.1; 8.2; 9; 9.1; 9.1.6	Yes
5	Risk assessment	4.6; 6.1	Yes
6	Training and communications	5.3.4; 7.2.2; 7.3.2.3; 9.1.6;	Yes
7	Confidential reporting and investigation	5.3.3; 9.1.7; 9.2; 10.1.2	Yes
8	Incentives and disciplinary measures	5.3.4; 7.3.2.2; 7.3.2.3; 10	Yes
9	Continuous improvement, testing and review	9.2, 9.3 and 10.2	Yes (principles)
10	Third-party management	8.3	Yes (principles)[4]
11	Mergers and acquisitions	N/A	N/A

The Flowchart of a compliance management system taken from ISO 19600:2014 is reproduced with the permission of the International Organization for Standardization, ISO. The numbers in the chart cells refer to the relevant sections of the Standard, which can be obtained from any ISO member and from the website of the ISO Central Secretariat at the following address: www.iso.org. Copyright remains with ISO.



3. Internationale Best Practice im Risiko und Compliance Management

Internationale Best Practice wird in erster Linie in internationalen Standards festgehalten: Dies schafft Transparenz bezüglich der Regeln der Kunst, erhöhte Wirksamkeit, Kosteneffizienz und Reduktion des Haftungsrisikos.

- *ISO 31000 – Risk management:* «ISO 31000 has *de facto* become the world standard» (OECD – Risk Management and Corporate Governance, 2014).
- *ISO 19600 – Compliance management systems:* erster internationaler Standard für Compliance Management; = Schweizer Norm SN ISO 19600.
- *Weitere zentrale Governance Standards:*
  - ISO 27000 – Information security management systems
  - ISO 37001 – Anti-bribery management systems
  - Künftige Standards Governance of Organisations, Whistleblowing etc.

3. Internationale Best Practice im Risiko und Compliance Management

Beispiel: ISO 37001 – Umsetzer des Standards:

Alstom, Takeda Pharma, Bosch und ENI sind ISO 37001 zertifiziert.

Microsoft, Walmart etc. haben ISO 37001 implementiert und sind in Zertifizierung bzw. zertifiziert.

Singapur, Peru, Nigeria führen ISO 37001 in der Verwaltung und bei den Staatsunternehmen ein. Die Provinz Québec, die Stadt Montreal oder bspw. Palau (Ship Registry) sind in Zertifizierung.

3. Internationale Best Practice im Risiko und Compliance Management

Compliance-Managementsystem nach SN ISO 19600

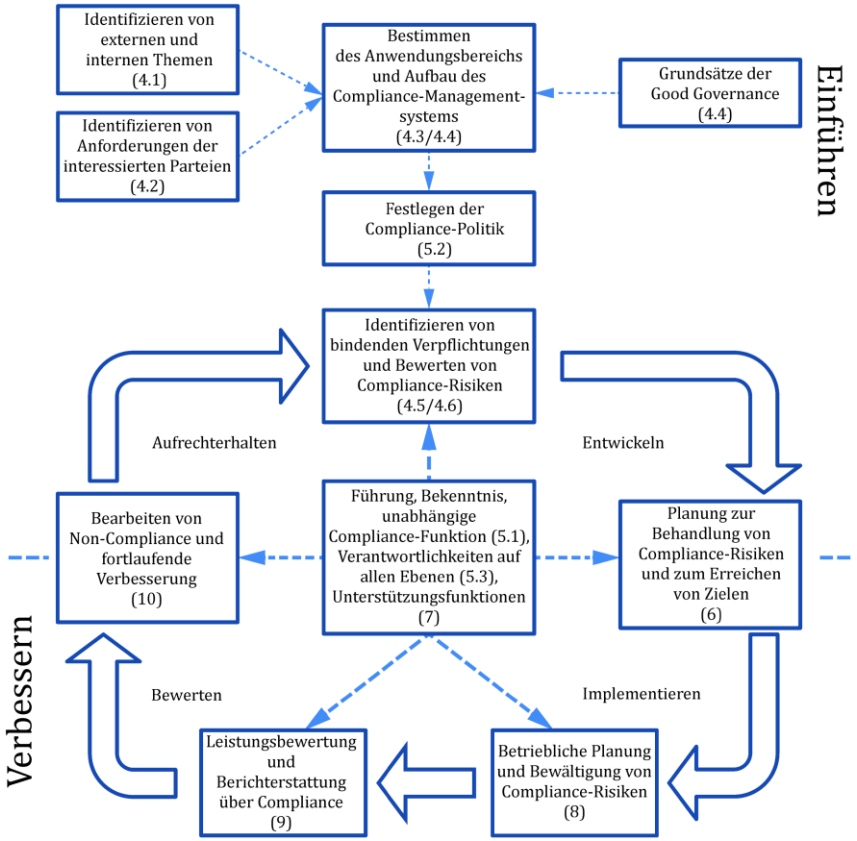


Bild 1 — Ablaufdiagramm eines Compliance-Managementsystems
Quelle: SN ISO 19600:2016-11 (Seite 6)

3. Internationale Best Practice im Risiko und Compliance Management

Bsp.: Auszug SN ISO 19600:

Einführung:

«Die Verankerung von Compliance im Verhalten der Personen, die für eine Organisation arbeiten, hängt in erster Linie von der Führung auf allen Ebenen und von klar definierten Werten einer Organisation sowie von der Anerkennung und der Verwirklichung von Massnahmen zur Förderung regelkonformen Verhaltens ab. Sind diese Voraussetzungen nicht auf allen Ebenen der Organisation erfüllt, besteht das Risiko von Regelverstössen.»

3. Internationale Best Practice im Risiko und Compliance Management

Bsp.: Auszug SN ISO 19600, Ziffer 7.3.2.3 – Compliance Kultur:

«Die Entwicklung einer Compliance-Kultur erfordert ein aktives, sichtbares, konsistentes und nachhaltiges Bekenntnis des obersten Organs, der obersten Leitung und der Führungskräfte zu einem gemeinsamen, bekannt gegebenen Verhaltensstandard, der in jedem Bereich der Organisation gefordert wird.»

4. Exkurs: Besondere Aspekte der öffentlichen Hand

GRC Besonderheiten beim Bund:

Die öffentliche Hand ist in viele Einheiten gegliedert: Gesamtregierung, Kanzlei, Departemente, Ämter, Aufsichtsbehörden, öffentliche Anstalten, Parlament und Kommissionen, Bundesbetriebe, öffentliche Unternehmen etc. Eine stringente GRC-Gesamtführung besteht (noch) nicht.

Die Mittel der öffentlichen Hand sind begrenzt und wirksames GRC-Management hat (noch) nicht höchste Priorität.

Die Vertreter der öffentlichen Hand stehen unter besonderer Beobachtung von Medien, NGOs, ausländischen Staaten, internationalen Organisationen und … natürlich der Bürger. Die ethische und rechtliche Erwartungshaltung ist sehr hoch.

4. Exkurs: Besondere Aspekte der öffentlichen Hand

GRC Management beim Bund:

Die Managementsystem-Standards der ISO richten sich an alle Organisationen und sind auch in kleinen Organisationseinheiten einfach umsetzbar.

Ein uneinheitlicher Ansatz im Governance, Risiko und Compliance Management ist aufwändig, teuer und wenig wirksam.

Der Bund, unter der Leitung der EFV, betreibt das Risikomanagment einheitlich nach ISO 31000.

Der Bund hat (noch) keinen Ansatz für wirksame Kontrollsysteme nach internationaler Best Practice. Die grösste Lücke besteht im Compliance Management.

5. Anregungen

Die obersten Führungspersonen sollten das GRC Managements stärken, indem sie:

- **Global anerkannte Standards** für das Risiko- und für das Compliance-Managementsystem festlegen und zeitnah umsetzen.
- **Unabhängige externe Prüfungen** durchführen (Vollständigkeit, Wirksamkeit).
- Ein **internes Kontroll-Konzept** genehmigen und implementieren (IKS = Dreieck Risiko-Managementsystem/Compliance-Managementsystem/ Finanzkontrolle, überwacht durch Interne Revision [wo vorhanden]).

Die **Einsparungen** durch Transparenz und Reduktion der Komplexität, Auditierbarkeit und höhere Wirksamkeit und dürften sich bei grossen Organisationen schnell im hohen Millionenbereich bewegen.

Es gibt viel zu tun, packen wir es an …

Danke für Ihr Interesse und Ihre Aufmerksamkeit.
Bei Fragen stehe ich Ihnen gerne zur Verfügung.

Daniel Lucien Bühr
dbuhr@lalive.law