SNV
standards connect
the world

Fachveranstaltung Netzwerk Risikomanagement:
Reputationsrisiken – Sind diese steuerbar?

ISO 37000 – Governance of organizations

Luzern, 31. August 2021

Dr. Daniel Lucien Bühr, Co-Chairperson Normenkomitee 207 – Governance von Organisationen

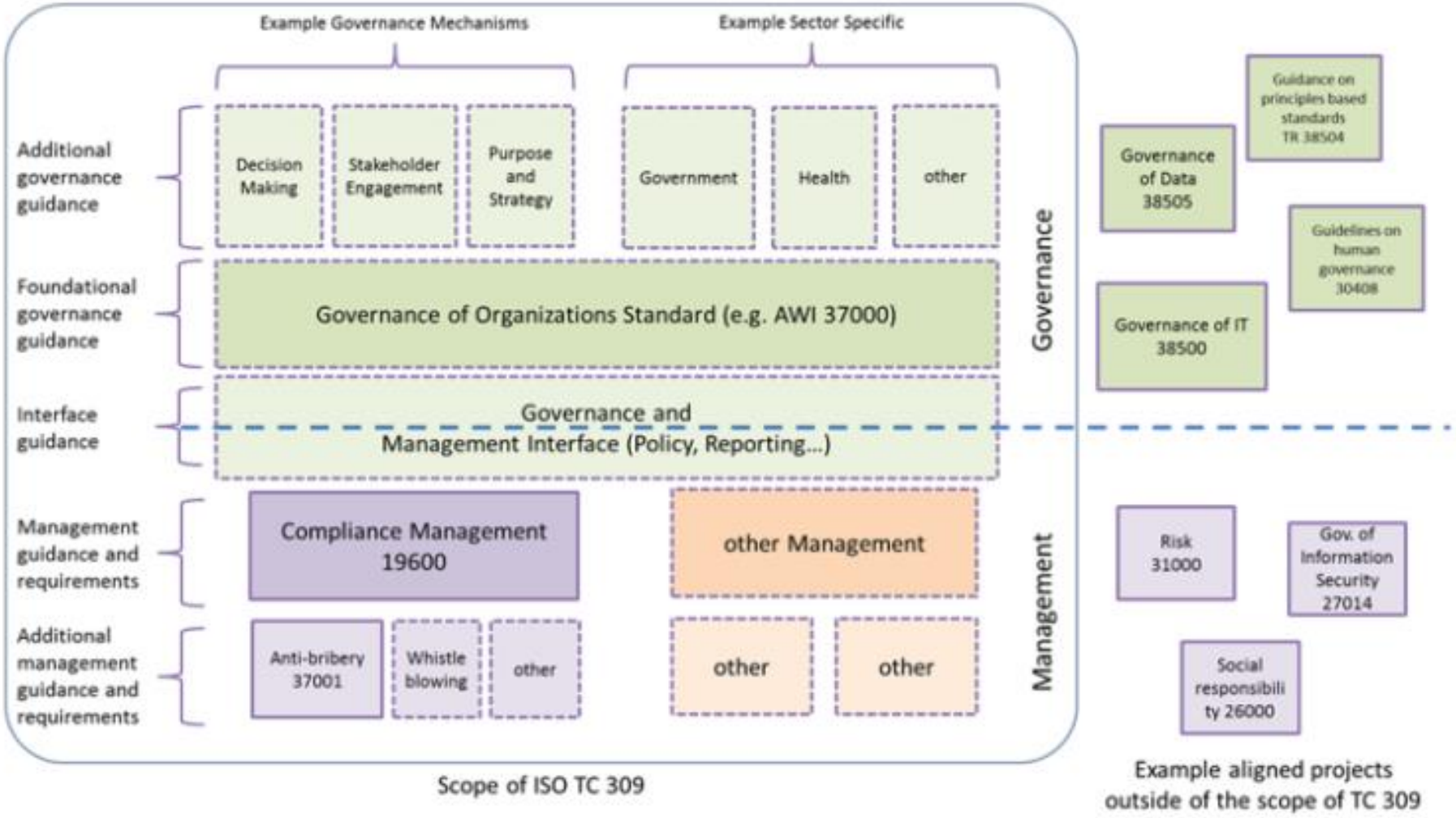
Inhaltsverzeichnis

Vorstellung ISO 37000

- Erster globaler Standard zur guten Governance von Organisationen.
- Erarbeitet von September 2017 - Juni 2021 durch Experten aus 70 Mitgliedstaaten und internationalen Organisationen (inkl. OECD, IRM, ACCA, UNCTAD, IIA etc.) – 112 Sitzungen der Experten-kommission.
- August 2021 – Einstimmige Annahme von ISO 37000.
- Publikation Mitte September 2021.
- Reduziert Komplexität und Kosten für alle Organisationen: Der Standard tritt an die Stelle einer Vielzahl privater Regelwerke.

Vorstellung ISO 37000

Zusammenspiel der ISO Standards im Bereich Governance:



Vorstellung ISO 37000

- Der Standard unterstützt das Oberste Organ (governing body) dabei, eine **integrale Governance in der ganzen Organisation** einzuführen, um wirksam, sozial verantwortlich und ethisch den Zweck zu erreichen.

- Der Standard stellt **Zweck** (purpose) und **Sozialverträglichkeit** (responsible stewardship) ins Zentrum. Er verweist auf die Social Development Goals der UNO.

- Die Erreichung des Zwecks wird durch 4 Prinzipien unterstützt: **Value Generation, Strategy, Oversight, Accountability**.

- Oversight wird durch die Regelungen zu **Risk Governance** und **Social Responsibility** unterstützt.

Oversight und Risk Governance

Die zentralen Elemente des **Governance Prinzips Oversight** sind:

- Wirksame **Aufsicht und Kontrolle** beruhen auf:

- Zeitgerechter und genauer **Berichterstattung des Managements**;
- Verwirklichung eines **internen Kontrollsystems** bestehend aus **Risikomanagementsystem**, **Compliance-Managementsystem** und **System der Finanzkontrolle**;
- **Korrekturmassnahmen** (corrective action) und
- **Assurance** betreffend die **Zuverlässigkeit der Berichterstattung** und die **Wirksamkeit des internen Kontrollsystems**.

Oversight und Risk Governance

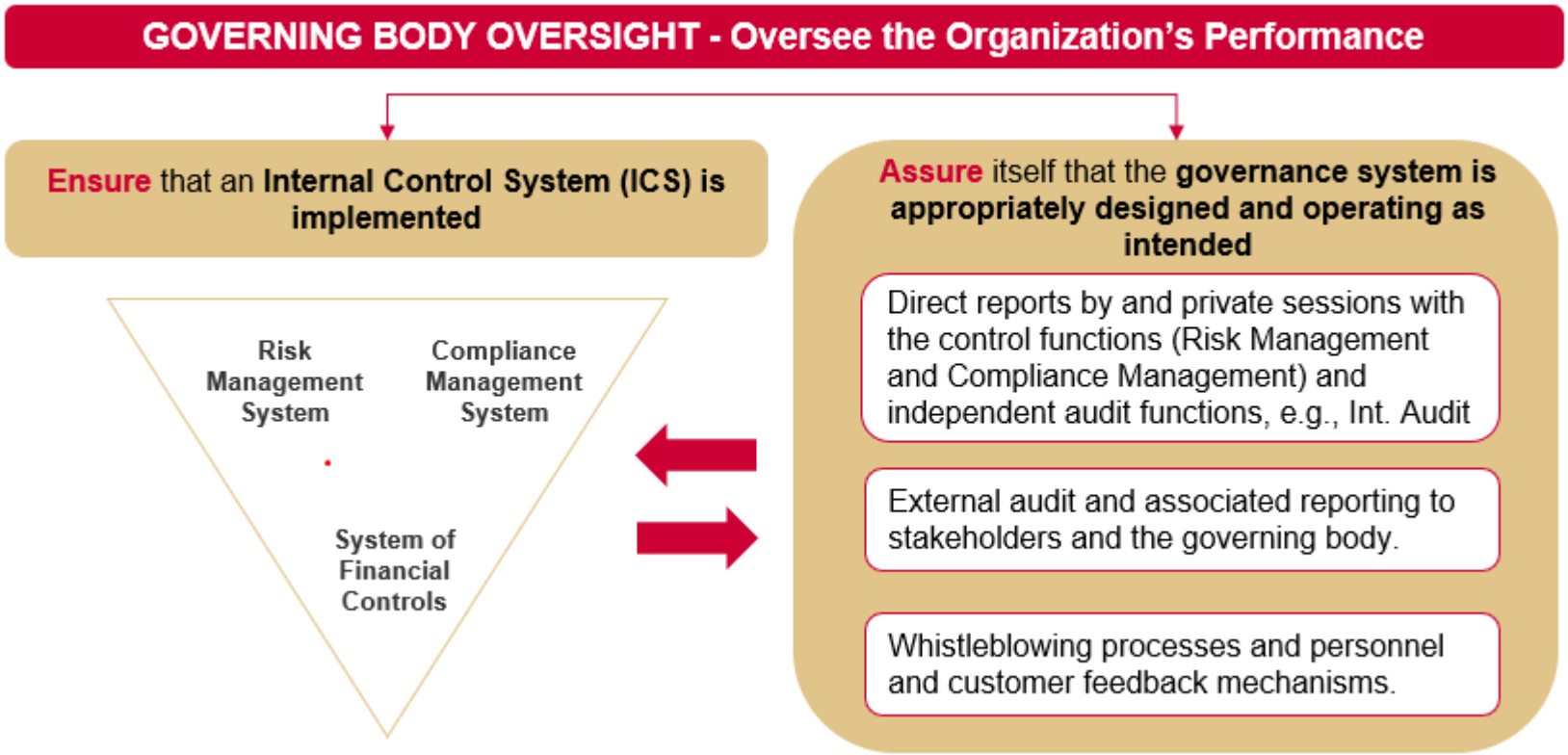
Die zentralen Elemente des **Governance Prinzips Oversight** sind:

- **Assurance** besteht aus folgenden Prozessen:

- **Direkte Prüfungen durch das Oberste Organ**;
- **Direkte Berichterstattung an** und **«Vieraugengespräche»** (private sessions) der Kontrollfunktionen **Risikomanagement** und **Compliance-Management** sowie der Assurance Funktion **Internal Audit mit dem Obersten Organ**;
- **Externe** (Abschluss-/regulatorische) **Prüfungen**;
- **Hinweisgeber-Prozesse** und Prozesse für Rückmeldungen von Mitarbeitenden und Kunden.

Oversight und Risk Governance

Oversight – Graphik:



Oversight und Risk Governance

Das Oberste Organ ist für die **Risk Governance** verantwortlich. Es

- setzt den **«tone at the top»** für die Umsetzung des Risiko-managements durch Verwirklichung des **Risikomanagement-systems**, die Festlegung der **Ressourcen,** des **Risikoappetits**, der **Risikokriterien** und der **Risikolimiten**;
- **beurteilt, bewältigt, überwacht und kommuniziert die Risiken** in seinen Entscheidungsprozessen; und
- verschafft sich Sicherheit (assurance), dass die **Kompetenzen, Befugnisse, Aufgaben und Verantwortlichkeiten für das Risikomanagement** zugeordnet sind.

LALIVE

THE DISPUTES POWERHOUSE

Fachveranstaltung Netzwerk Risikomanagement: Reputationsrisiken – Sind diese steuerbar?

Verschärfung der persönlichen Haftung für Führungskräfte durch ISO 37000?

Dr. Daniel Lucien Bühr

Luzern, 31. August 2021

Managerhaftung: Rechtliche Grundlage und Haftungsmassstab

Zentrale Bestimmungen zur Sorgfaltspflicht und zur Haftung (Organe von Kapitalgesellschaften und Genossenschaften):

Art. 717 OR:

Die Mitglieder des Verwaltungsrates sowie Dritte, die mit der Geschäfts-führung befasst sind, müssen ihre Aufgaben mit aller Sorgfalt erfüllen und die Interessen der Gesellschaft in guten Treuen wahren.

Art. 754 OR:

Die Mitglieder des Verwaltungsrates und alle mit der Geschäftsführung […] 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.

Pflichtverletzung durch Nichtbeachtung von ISO 37000?

ISO Standards wiederspiegeln die international allgemein anerkannten **Regeln der Kunst** (state-of-the-art).

Bei Befolgung von ISO Standards greift die **natürliche Vermutung, dass sorgfältig gehandelt wurde**.

Umgekehrt gilt, dass die **Nichtbeachtung von ISO Standards** Grundlage für den Nachweis bilden kann, dass eine **Führungsaufgabe nicht mit «aller Sorgfalt» erfüllt wurde**.

PS: Die **Business Judgement Rule findet im Bereich der Governance keine Anwendung** (fortlaufende Führung und Kontrolle ≠ Beschlussfassung).

Pflichtverletzung durch Nichtbeachtung von ISO 37000?

Beispiel:

Einem Unternehmen wird vorgeworfen, Kunden geschädigt zu haben. Die Kunden klagen die Mitglieder von VR und GL ein und weisen nach, dass das Unternehmen kein klar definiertes IKS und keine unabhängigen Kontrollfunktionen hatte (Risikomanagement und Compliance Management ohne Berichtslinie zum VR) und dass keine internen Assurance Prozesse bestanden. Der Compliance-Officer hatte zudem keine Fachausbildung im Compliance-Management.

Feststellungen unter Bezugnahme auf ISO 37000 und ISO 37301: Es liegt kein IKS vor, das internationalem Standard entspricht. Die fehlende Fachausbildung (Kompetenz) des Compliance-Managers verstösst gegen ISO 37301 und damit gegen Best Practice.

Pflichtverletzung durch Nichtbeachtung von ISO 37000? Erste Einschätzung.

Die Nichtbeachtung oder Verletzung internationaler Standards, auch im Bereich der Managementsystem-Standards und vorab von ISO 37000 – Governance of organizations, kann Grundlage für den Beweis von Verstössen gegen die Sorgfaltspflicht nach Art. 717 OR sein und damit eine Haftung von VR-/GL-Mitgliedern nach Art. 754 OR begründen.

Fazit: Die international anerkannten Prinzipien guter Governance, einschliesslich Aufsicht und Kontrolle, wie sie ab Mitte September 2021 nach ISO 37000 gelten werden, sollten unter allen Umständen durch die Mitglieder von VR und GL beachtet werden.

Q&A / Diskussion

Danke für Ihre Aufmerksamkeit und Ihr Interesse

Dr. Daniel Lucien Bühr, Partner
LALIVE
Stampfenbachplatz 4
8006 Zürich
www.lalive.law

Tel. 058 105 2100
E-Mail: dbuhr@lalive.law