Wirksame Aufsicht und Kontrolle durch den Verwaltungsrat

Dr. Daniel Lucien Bühr, Partner, LALIVE (Zürich)

Der Verwaltungsrat ist das oberste Kontrollorgan der Aktiengesellschaft. Seine Kontrollfunktion ist genau gleich zu gewichten wie seine Leitungsfunktion. Er muss mit seismografischem Gespür Leistungsmängel bei der Umsetzung der Governance, der Ethik und der Gesetzestreue erfassen und Korrekturmassnahmen ergreifen. Zentral sind das Interne Kontrollsystem und die Assurance des Verwaltungsrats.

Eine wirksame Aufsicht und Kontrolle durch den Verwaltungsrat (VR) ist keine Astrophysik. Trotzdem lassen sich existenzielle Risiken und schwere Krisen in Unternehmen regelmässig auf elementare und offenkundige Mängel in der Kontroll-Governance zurückführen.

Die Unternehmen sind heute mehr denn je zu grosser Transparenz verpflichtet und sie werden unablässig durch ihre Stakeholder und die Medien nach ihrer Governance, ihrem Zweck und ihrer Leistung gefragt. Wird Fehlverhalten im Unternehmen vermutet oder festgestellt, so wird unmittelbar die Frage nach Kontrollversagen und Verantwortlichkeit gestellt.

Die Mitglieder des VR müssen ihre Aufsichts- und Kontrollaufgabe mit *aller Sorgfalt* wahrnehmen. Dieser gesetzliche Sorgfaltsmassstab ist der höchste im Schweizer Recht und verlangt sozusagen nach einem seismografischen Gespür bei allen VR für mögliche Verfehlungen im Unternehmen sowie nach konsequenter Untersuchung, Transparenz und griffigen Korrekturmassnahmen.

In diesem Beitrag wird die gesetzliche Regelung der Aufsicht und Kontrolle der Aktiengesellschaft durch den VR dargestellt, für das Grundverständnis auf die Entwicklungen der letzten drei Jahrzehnte eingegangen und die heutige Best Practice mit einem Fokus auf das Interne Kontrollsystem (IKS) und die Assurance des VR aufgezeigt.

Einleitung

Die moderne Corporate Governance beruht auf dem Cadbury Report vom 1. Dezember 1992. Dieser Bericht wurde von der London Stock Exchange im Nachgang der Überschuldung der Maxwell Communications Group und des Konkurses der Bank of Credit and Commerce International in Auftrag gegeben. Eine Expertenkommission unter dem Vorsitz von Sir Adrian Cadbury (damals Chairman von Cadbury Schweppes) erarbeitete den Bericht. Er gilt als Basis und Startpunkt der modernen Corporate Governance.

Der Cadbury Report befasste sich primär mit der Kontroll- und Berichtsfunktion des Board of Directors und der Rolle der Revisoren. Der Bericht hatte aber auch zum Ziel, die Corporate Governance in Unternehmen insgesamt zu verbessern (Good Corporate Governance).

Nach dem Cadbury Report ist Corporate Governance das System der Leitung und Kontrolle von Unternehmen. Die oberste Leitung und die oberste Kontrolle sind also die beiden gleichbedeutend zentralen Aufgaben aller Mitglieder oberster Leitungsorgane. Die VR sollten also grundsätzlich gleich viel Zeit für Aufsicht und Kontrolle aufwenden, wie sie den strategische Führungsthemen widmen. Nur wenn die Mitglieder oberster Leitungsorgane diese Balance einhalten, können die ansonsten unvermeidlichen Kosten mangelnder Kontrolle vermieden werden.

Im Cadbury Report wurde zur Aufsichts- und Kontrollfunktion der obersten Leitung festgehalten: «*Directors are responsible [...] for maintaining adequate accounting records. To meet these responsibilities directors need in practice to maintain a system of internal control over the financial management of the company, including procedures designed to minimise the risk of fraud. There is, therefore, already an implicit requirement on directors to ensure that a proper system of internal control is in place.*»

Mit Bezug auf das IKS führte der Cadbury Report weiter aus: «*The Committee is convinced that an effective internal control system is an essential part of the efficient management of a company. We have already recommended that directors should report on the effectiveness of their system of internal control, and that the auditors should report on their statement. A great deal of detailed work is now necessary to develop these proposals [...]*»

Zusammengefasst verlangte der Cadbury Report, dass das Board ein IKS verwirklichen und sich zu dessen Wirksamkeit äussern muss und dass die Revisoren über die Aussage des Boards Bericht erstatten müssen.

Die Empfehlungen des Cadbury Report wurden bis heute weltweit nicht bzw. nur in Ansätzen umgesetzt. Zur Wirksamkeit des IKS müssen weder die obersten Leitungsorgane noch die Revisoren

eine Aussage machen, womit die Anleger, Gläubiger und Behörden noch heute nicht wissen, wie das IKS ausgestaltet ist und ob es wirksam ist.

Aktuelle Regelung von Aufsicht und Kontrolle in der Schweiz

Seit der Revision des Obligationenrechts (OR) per 1. Januar 2008 (Neugestaltung des Revisionsrechts) ist das IKS im Gesetz explizit erwähnt. Es gibt im OR jedoch keine Regelung der Governance von Aufsicht und Kontrolle durch den VR und keine Definition des IKS und der Assurance, also der Vergewisserung des VR über die Einhaltung seiner Vorgaben. Das OR verlangt bei der ordentlichen Revision bloss (und von der Politik explizit gewünscht), dass die Revisionsstelle prüft, ob ein IKS existiert. Das IKS wird dabei als rein finanzielles IKS verstanden.

Da sich das OR *nicht* zum Inhalt des IKS äussert, fordert der Gesetzgeber von der Revisionsstelle somit, dass sie die Existenz eines Systems prüft, das es als definiertes, transparentes und auditierbares Institut nach dem Gesetz gar nicht gibt. Er verlässt sich also stillschweigend darauf, dass Standards (sog. *Soft Law*) die gesetzliche Lücke schliessen.

Soft Law zur Schliessung der Governance-Lücken des OR

Entwicklungen seit dem Cadbury Report

1992 veröffentlichten das COSO (Committee of Sponsoring Organizations of the Treadway Commission) und die internationale Revisionsstelle PwC die Leitlinie «Internal Control – Integrated Framework» (das COSO-Kontrollmodell). Diese private «Standesleitlinie» verfolgt das Ziel, Unternehmen bei der Einführung und Weiterentwicklung ihrer IKS zu unterstützen.

Das COSO-Kontrollmodell umfasst drei Dimensionen. Die erste Dimension statuiert die drei Zielsetzungen «Effektivität und Effizienz der Tätigkeiten», «Verlässlichkeit der finanziellen Berichterstattung» und «Gesetzes- und Normenkonformität». Die zweite Dimension ist in fünf Komponenten gegliedert und dient dazu, die genannten Ziele zu erreichen. Die dritte Dimension beinhaltet die einzelnen Unternehmenseinheiten und -prozesse, die bei der IKS-Planung und -Verwirklichung berücksichtigt werden sollen.

Die Schwächen des im Kern 30 Jahre alten COSO-Modells sind (1) die fehlende Governance der Kontrolle im Unternehmen, also die Umschreibung der Governance-Grundsätze und der Rollen und Verantwortlichkeiten auf allen Ebenen, (2) die fehlende Definition des IKS als Kontroll-Managementsystem, (3) die teilweise unklare oder fehlende Einbindung der Risikomanagementmethodik, (4) das Fehlen einer Compliance-Managementmethodik und (5) die unklare Schnittstelle und Abgrenzung zwischen IKS und Assurance-Prozessen.

Das «Three Lines Model»

Das «Three Lines Model» ist ein Praktiker-Governance-Modell, das auf drei «Linien» beruht: den operativ tätigen Mitarbeitenden (1. Linie), den Kontrollfunktionen (2. Linie, insb. Risikofunktion und Compliance-Funktion) und der Internen Revision (3. Linie). Es wurde im Jahr 2013 vom Institute of Internal Auditors (IIA) publiziert. Das Modell (damals «Three Lines of Defense» genannt) wurde ab Mitte der 1990er-Jahre als Antwort auf den Cadbury Report entwickelt.

Seit seiner Einführung hat es weite Verbreitung als Rahmenwerk für eine einfache Praktiker-Kontroll-Governance gefunden. Die einfache Erklärbarkeit mit den drei Linien ist der grosse Vorteil des Modells. In der Praxis zeigen sich aber die Schwächen des Modells: Die 1. Linie, die «Front», kann nicht Teil eines unabhängigen Kontrollsystems sein, da sie sich in einem strukturellen Interessenkonflikt befindet und an die Geschäftsleitung berichtet. Die 2. Linie berichtet ebenso an die Geschäftsleitung und ist damit strukturell ebenfalls nicht unabhängig und der Gefahr des Overruling ausgesetzt. Und die 3. Linie, die Interne Revision (die nur ca. 4% der Unternehmen aufweisen), ist zwar aufgrund der Berichtslinie an den VR strukturell unabhängig, hat aber in der Regel die kleinsten Ressourcen und wird in der Praxis oft vom CFO und nicht vom VR gelenkt.

Das Three Lines Model basiert also nicht auf einem IKS, sondern letztlich auf einer einzigen unabhängigen Kontrollfunktion, der Internen Revision, sofern vorhanden.

ISO-Standards zu Aufsicht und Kontrolle

Seit 2009 hat die ISO Standards für Risikomanagement (ISO 31000), Compliance-Management (ISO 37301), Anti-Korruptions-Management (ISO 37001), Whistleblowing (ISO 37002) und die Governance von Organisationen (ISO 37000) publiziert. Diese Standards werden von den ca. 160 Mitgliedsorganisationen der ISO, inkl. der Schweizerischen Normenvereinigung, in einem transparenten, unabhängigen und inklusiven Prozess erarbeitet. Sie sind der State of the Art und ihre Anwendung führt zur natürlichen Vermutung sorgfältigen Handelns. Im Bereich der Aufsicht und Kontrolle von Organisationen sind sie die weltweit aktuellsten Standards und widerspiegeln die internationale Best Practice.

Für die Aufsicht und Kontrolle von Organisationen ist der ISO-Standard 37000 – Governance of organizations von zentraler Bedeutung. Der Standard wurde von 90 Staaten und internationalen Organisationen, darunter massgebend auch dem IIA, während 4 Jahren erarbeitet und 2021 veröffentlicht. In Ziffer 6.4 – «Oversight» wird das Governance-Prinzip der «Aufsicht und Kontrolle» beschrieben: Das oberste Leitungsorgan überwacht

die Leistung der Organisation, um sicherzustellen, dass sie seine Absichten und Erwartungen an die Organisation, ihr ethisches Verhalten und ihre Compliance-Verpflichtungen erfüllt. ISO 37000 erläutert sodann, dass eine wirksame Aufsicht und Kontrolle sicherstellt, dass der Unternehmenszweck und die strategischen Ziele wie beabsichtigt und gefordert erreicht werden.

Die wichtigsten Elemente der Best Practice des obersten Leitungsorgans sind die folgenden:

(1) Manager, an die Aufgaben delegiert werden, müssen *zeitgerecht und genau Bericht* erstatten
(2) Ein *IKS*, bestehend aus einem *Risikomanagementsystem*, einem *Compliance-Managementsystem* und einem *System der Finanzkontrolle*, muss verwirklicht werden
(3) Das oberste Organ muss *korrigierend eingreifen*
(4) Das oberste Organ muss sich der *Korrektheit der Berichte des Managements und der Wirksamkeit des IKS vergewissern* (Assurance)

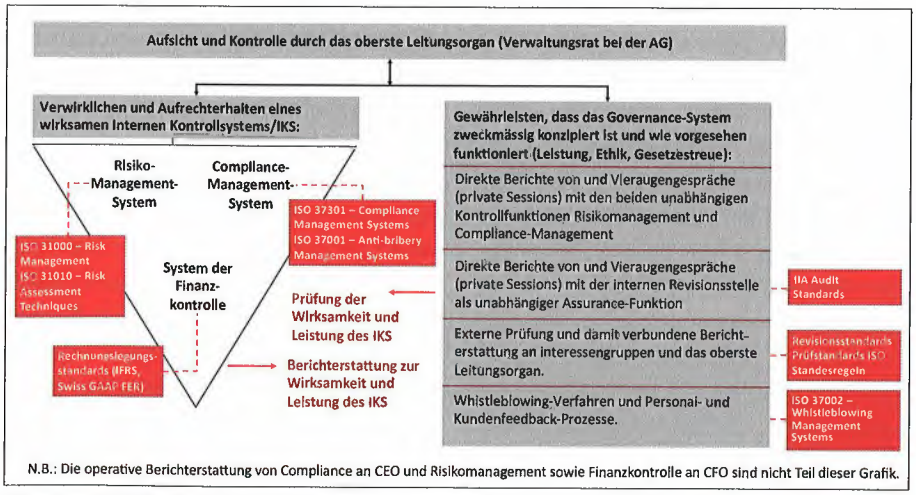
ISO 37000 erläutert dann im Detail, wie das oberste Leitungsorgan die Leistung der Organisation überwacht und kontrolliert sowie korrigierend eingreift, bspw. durch eine Prüfung, ob Werte und Governance die Organisation und deren Kultur und die Compliance effektiv leiten und ob die Risikobeurteilung und -bewältigung sowie das Compliance-Management gestützt auf Informationen, die das oberste Organ direkt von der Risikofunktion und der Compliance-Funktion erhält, wirksam und im Einklang mit der Unternehmenskultur sind.

Die Assurance ist in ISO 37000 ebenfalls klar definiert, nämlich als Vergewisserung des obersten Organs, dass das Governance-System zweckmässig geplant wurde und wie beabsichtigt funktioniert. Der wichtigste Assurance-Prozess ist die Prüfung der Berichterstattung durch das Management sowie – dort wo das oberste Leitungsorgan nicht direkt prüfen kann – die unabhängige Berichterstattung im Rahmen von Vieraugengesprächen des VR mit den Leitungspersonen der unabhängigen separaten Kontrollfunktionen Risikomanagement und Compliance-Management sowie der Internen Revision (als unabhängiger Assurance-Funktion). Weiter sind externe Prüfungen (bspw. der Wirksamkeit des IKS und der Assurance) sowie Berichte, die über die Whistleblowing-Meldestelle eingehen, zentrale Assurance-Instrumente.

ISO 37000 hat somit fast 30 Jahre nach dem Cadbury Report dessen Forderungen umgesetzt: Das IKS wird erstmals klar und umfassend – als finanzielles und nichtfinanzielles IKS – definiert. Sodann wird (1) die Prüfung der Wirksamkeit des IKS durch das oberste Leitungsorgan statuiert, (2) die Assurance erstmals klar definiert und vom IKS unterschieden und (3) die Interne Revision erstmals in einem ISO-Standard ausdrücklich als unabhängige Assurance-Funktion erwähnt und darin eingebunden.

Diese Konzeption von Aufsicht und Kontrolle nach ISO 37000 wurde im Jahr 2023 vom revidierten Swiss Code of Best Practice for Corporate Governance übernommen, insbes. die Definition des IKS und der Assurance durch den VR, inkl. Vieraugengespräche mit den Kontrollfunktionen des Risikomanagements und des Compliance-Managements sowie mit der Internen Revision als unabhängiger Assurance-Funktion.

Die Grafik auf S. 7 stellt das internationale Best-Practice-Modell von Aufsicht und Kontrolle nach ISO 37000 dar.



Internationale Best Practice Governance von Aufsicht und Kontrolle durch den VR mittels IKS und Assurance nach ISO 37000 – Governance of organizations.

Key Takeaways

Alle VR sollten 50% ihrer Zeit für die «seismografische» Aufsicht und Kontrolle der Leistung des Managements aufwenden, das IKS der Gesellschaft verwirklichen und dessen Wirksamkeit durch seine Assurance prüfen und durch Korrekturmassnahmen gewährleisten.

Wo durch das IKS und die Assurance des VR Schwächen bezüglich der Leistung der Gesellschaft, des Erreichens der Governance-Anforderungen, der Werte, der ethischen Ziele oder der Gesetzestreue zutage treten, müssen die VR im Sinne der sorgfältigen Wahrnehmung ihrer Aufgaben zeitnah korrigierend eingreifen, unter Einschluss des Instruments der externen Prüfung.

ÜBER DEN AUTOR

Daniel Lucien Bühr ist Partner bei LALIVE. Er berät Unternehmen in Governance-Fragen, bei komplexen internen und externen Untersuchungen sowie zur Nachhaltigkeitsberichterstattung.