Risikomanagement und Compliance

Compliance Management in einem KMU einführen

Die Pflicht zur Einhaltung von Gesetzen, Vorschriften und freiwilligen Selbstverpflichtungen gilt für alle Unternehmen, unabhängig von ihrer Grösse, Rechtsform oder Geschäftstätigkeit. So müssen sich KMU mit wenigen Mitarbeitern nach dem risikobasierten Ansatz oft mit den gleichen Compliance-Themen auseinandersetzen wie Grossunternehmen mit mehreren tausend Mitarbeitern.

Von Claude Bollinger, Dr. Christian Zipper und Dr. Daniel Lucien Bühr

Wegen ihrer vermeintlichen Komplexität und dem befürchteten Aufwand haben Compliance-Managementsysteme bei vielen KMU noch nicht ihren festen Platz gefunden. Dies obwohl sich das Umfeld durch verstärkte Rechtsdurchsetzung gegen Unternehmen und die Mitglieder der obersten Leitung deutlich verändert hat und Compliance-Verstösse zu erheblichen Haftungsrisiken für die Unternehmen und ihre Leitung führen und die Reputation sowie die Existenz eines Unternehmens bedrohen können.

Compliance-Hilfestellung auch für KMU

Der im Dezember 2014 erschienene internationale Standard ISO 19600 «Compliance management systems – Guidelines» unterstützt KMU bei der Implementierung und Aufrechterhaltung eines wirksamen und erfolgreichen Compliance Management Systems (CMS). Die ISO 19600:2014 (bei DIN jetzt auch auf Deutsch erschienen) ist für alle Organisationen anwendbar und gemäss dem Grundsatz von Angemessenheit und Verhältnismässigkeit unabhängig von Grösse, Struktur, Art und Komplexität des Unternehmens ein passender Leitfaden. So kann ein CMS nach ISO 19600:2014 ohne grosse zusätzliche Bürokratie, massgeschneidert auf das Unternehmen zugeschnitten werden. Praktische Erfahrungen zeigen, dass es nur wenige organisatorische Massnahmen und Verfahren und ca. 15 Seiten originäre Texte (VR-Entscheid zu Werten und Governance, Compliance-Policy, Weisungen zu Kern-Risiken, Trainingsplan, Audit- und Berichtsplan) braucht, um ein einfaches, robustes CMS aufzubauen, das, wenn die richtigen Massnahmen getroffen werden, manchem CMS eines internationalen Grosskonzerns in seiner Stimmigkeit als System und in seiner Wirksamkeit überlegen sein dürfte.

Mittels eines wirksamen CMS nach ISO 19600:2014 kann ein Unternehmen mit hoher Wirksamkeit sicherstellen, dass die bindenden Verpflichtungen eingehalten werden. Dadurch werden Compliance-Risiken beseitigt oder minimiert und die Rechtssicherheit erhöht.

Anwendungsbeispiel eines CMS nach ISO 19600:2014

An der ZHAW School of Engineering in Winterthur wurde im Rahmen einer Masterarbeit in integriertem Risikomanagement (MAS IRM) der Aufbau, die Entwicklung, die Verwirklichung, die Bewertung, die Aufrechterhaltung und die Verbesserung eines CMS nach ISO 19600:2014 am Beispiel eines international agierenden Unternehmens mit weniger als 20 Mitarbeitern untersucht.

Das Managementsystem des Unternehmens basierte bereits auf der ISO 9001:2015. So war der Aufbau der Normstruktur (High Level Structure) der Standards einheitlich und die Integration des neuen ISO-Standards in das integrierte Managementsystem (IMS) war dadurch vereinfacht.

Vorgehensweise bei der Implementierung von ISO 19600:2014

ISO 19600:2014 besteht aus 7 Hauptelementen und ist grundsätzlich in zwei Hauptphasen aufgebaut, den Aufbau und den Betrieb des CMS. Dabei muss beachtet werden, dass alle Elemente der ISO 19600:2014 konsequent umgesetzt werden müssen, damit ein effektives und effizientes CMS entsteht. Ebenfalls soll das CMS auf den Grundsätzen einer guten und verantwortungsvollen Unternehmensführung basieren (z. B. dass Führungsentscheidungen auf nachhaltige Wertschöpfung ausgerichtet sind, eine transparente und offene Unternehmenskommunikation gefördert wird, Interessen von interessierten Parteien gewahrt werden, angemessener Umgang mit Risiken usw.).

Die **Aufbauphase** enthält vor allem das Element «Kontext der Organisation», bei dem die strategische Ausrichtung des CMS festgelegt wird. Es wurden klare Compliance-Ziele definiert und mit den übrigen Zielen des Unternehmens abgeglichen. Ebenfalls wurde der Anwendungsbereich des CMS bestimmt und dokumentiert. Danach konnte der organisatorische Rahmen definiert werden. Dazu wurden die wichtigen internen und externen Einflussfaktoren bestimmt, welche einen Einfluss auf die Leistungsfähigkeit des CMS haben. Dabei wurde das äussere Umfeld mittels einer systematischen Umfeldanalyse analysiert. Ebenfalls wurden auch die Anforderungen von relevanten internen oder externen Parteien (Personen oder Organisationen) berücksichtigt, welche mittels einer Stakeholder-Analyse in Erfahrung gebracht werden konnten. Aus den ermittelten Grundlagen der Aufbauphase wurden auch die Compliance-Strategie bzw. die Compliance-Politik definiert.

Im **Übergang zwischen Aufbau- und Betriebsphase** wurden Verfahren eingerichtet, um sämtliche gesetzlichen und freiwilligen bindenden Verpflichtungen systematisch zu ermitteln und deren Auswirkungen mit den Aktivitäten, Produkten und Dienstleistungen des Unternehmens zu überprüfen. Dadurch konnten die Risiken aus einer Ver-

letzung der bindenden Verpflichtungen identifiziert werden. Da es sich bei der ISO 19600:2014 um einen risikobasierten Standard handelt, kam der Risikobeurteilung und der Risikobewältigung eine besondere Stellung zu.

Wie die gemeinsame Struktur der ISO-Normen, so ist auch der risikobasierte Ansatz zu einer übergreifenden und zentralen Schnittstelle in der ISO-Welt geworden. Bei einem integrierten Managementsystem, bei dem Risiken aus verschiedenen Bereichen zu beurteilen sind, ist es daher sinnvoll, eine systematische Vorgehensweise nach ISO 31000:2009 Risk-Management anzuwenden. Damit konnten die compliance-relevanten Risiken optimal identifiziert, analysiert, bewertet und bewältigt werden.

In der **Betriebsphase** werden der Aufbau, die Entwicklung, die Verwirklichung, die Bewertung, die Aufrechterhaltung und die Verbesserung eines wirksamen und effektiven CMS behandelt. Mit Hilfe des PDCA Management-Zyklus (Plan-Do-Check-Act) werden hierbei die Compliance-Prozesse fortlaufend verbessert. Zuerst wurde im Element «Planung» das CMS strategisch geplant, um sicherzustellen, dass die Zielsetzungen des CMS erreicht werden und dass ungeplante Effekte verhindert, entdeckt oder reduziert werden. Dazu wurden Konzepte, Massnahmen und Aktionen festgelegt, um die in der Aufbauphase identifizierten Compliance-Risiken zu bewältigen. Auch wurden klare, mess- und überprüfbare Compliance-Ziele für relevante Funktionen und Bereiche festgelegt. Diese wurden unter anderem von der Compliance-Politik abgeleitet.

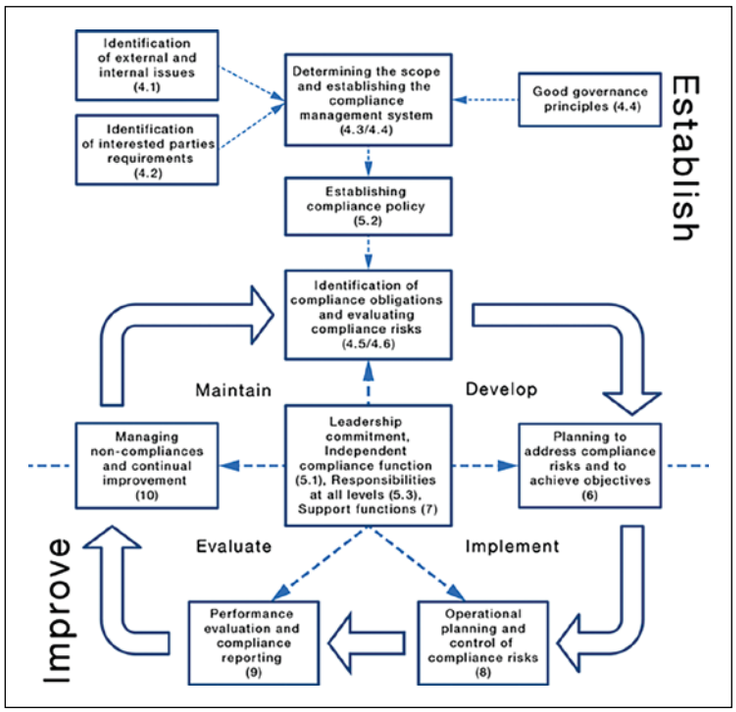
Mittels des Elements «Führung und Engagement» konnte aufgezeigt werden, wie die Führungsorgane mit ihrem Handeln die Bedeutung und die Leistungsfähigkeit des CMS wesentlich beeinflussen können: ISO 19600:2014 betont die zentrale Bedeutung guter Führung (leadership) und einer werteorientierten Kultur (values, culture) für die Wirksamkeit eines CMS. Dies widerspiegelt empirische Erkenntnisse, wonach ohne das Vorbild der obersten Leitung («tone at the top»), ohne Werte und gute Governance eine Kultur der Ethik und Compliance nicht entstehen kann und – auch wenn ein Verhaltenskodex und ein «Compliance-Programm» vorhanden sind – kein wirksames Compliance Management möglich ist.

Für die Verantwortlichkeiten und Zuständigkeiten von Compliance konnte die gleiche Führungsstruktur wie beim bestehenden Managementsystem verwendet werden. Eine eigenständige Struktur hätte die Möglichkeiten des Unternehmens überschritten und das Management und die Mitarbeiter mit Verwaltungsaufgaben beschäftigen, anstatt die Ressourcen für das CMS aufzuwenden. Es wurde jedoch darauf geachtet, dass die Compliance-Funktion unabhängig ist und genügend Befugnisse und direkten Zugang zum Aufsichtsorgan hat (Prinzipien der guten Unternehmensführung).

Im Element «Unterstützung» wurden die erforderlichen internen und externen Ressourcen für ein wirksames CMS ermittelt, damit sie vom Unternehmen zur Verfügung gestellt und effektiv eingesetzt werden können. Ebenfalls wurden Schulungen, Aus- und Weiterbildungen geplant, damit die Mitarbeiter die erforderlichen Kompetenzen besitzen und den von ihnen unter dem Standard geforderten Beitrag für ein wirksames CMS leisten können. Auch wurde ein Kommunikationskonzept ausgearbeitet, damit eine aktive interne und externe Compliance-Kommunikation betrieben werden kann. Danach konnten im Element «Betrieb» Prozesse, Richtlinien, Verfahren und deren Kontroll- und Steuerungsmassnahmen, welche zur Erfüllung des CMS nötig sind, implementiert werden. Dabei wurden ebenfalls externe Prozesse und Drittparteien berücksichtigt.

Um die Wirksamkeit des CMS sicherzustellen, wurden im Element «Leistungsbewertung» Verfahren eingerichtet, um das CMS selbst und dessen Leistung regelmässig zu überwachen, zu analysieren und zu bewerten. Zu diesem Zweck wurden messbare Indikatoren bestimmt, mit deren Hilfe die Compliance-Leistung des Unternehmens quantifiziert werden konnte. Dies waren Effizienz der Schulungen, bewertete Korrekturmassnahmen (Tätigkeitsindikatoren), Anzahl gemeldeter Compliance-Verstösse, finanzielle Auswirkungen der Compliance-Verstösse (Rückwirkende Indikatoren) Auswirkungen von Compliance-Risiken (Vorausschauender Indikator).

Ebenfalls wurde ein Berichtswesen vorgesehen, um die Geschäftsleitung über die Wirksamkeit und Angemessenheit des CMS zu informieren. Dabei konnten die Ergebnis-



Grafische Darstellung des PDCA Managementzyklus nach ISO 19600:2014.

se der laufenden Überwachungen in die bereits beim Unternehmen vorhandenen Berichte eingearbeitet werden. Für Ereignisse, welche zeitnah berichtet werden müssen, wie z.B. Compliance-Verstösse, wurde ein Ausnahmeberichtsystem eingerichtet, damit diese an die notwendigen Stellen, Funktionen und Behörden gemeldet werden.

Um das CMS zu verbessern und Schwachstellen aufzudecken, wurde im Element «**Verbesserung**» der Umgang des Unternehmens mit Compliance-Verstössen aufgezeigt. So sollen Massnahmen zur Beseitigung der Ursachen ermittelt und ein Wiederauftreten möglichst verhindert werden. Die Sanktionierung von Mitarbeitern aller Stufen bei willentlichen oder fahrlässigen Compliance-Verstössen ist ein zentrales Element eines funktionierenden CMS. Viele Unternehmen scheuen sich davor, Verantwortung einzufordern und Sanktionen auszusprechen. Ohne Kultur der Verantwortung und ohne Sanktionen bleibt die Forderung der Achtung der Werte und der Einhaltung der bindenden Verpflichtungen aber ein leerer Buchstabe («paper compliance»). Die Grafik zeigt, wie der PDCA-Managementzyklus im Standard abgebildet wird.

Die ISO 19600:2014 eignet sich auch für KMU

Die Untersuchungen der oben erwähnten Masterarbeit führten zum Schluss, dass ein CMS nach ISO 19600:2014 auch optimal für ein KMU mit weniger als 20 Mitarbeitenden geeignet ist und Voraussetzungen schafft, um die jetzigen und zukünftigen Anforderungen an ein wirksames CMS nach den Regeln der Kunst (lege artis) zu erfüllen.

- Eine Integration des CMS nach ISO 19600:2014 in bestehende Managementsysteme nach ISO gestaltet sich aufgrund der einheitlichen Struktur aller ISO-Managementsysteme, der einheitlich definierten Begriffe und der Effizienzen durch vorbestehende Grundkenntnisse des Managements von PDCA-Managementzyklen und der einfacheren Prüfung durch interne und externe Revisoren einfach und praktikabel. Es entsteht ein starkes Führungsinstrument und ein effizienteres Managementsystem, da vor allem mehr Teilaspekte betrachtet werden und das Managementsystem sich vermehrt nach der Gesamtzielsetzung des Unternehmens ausrichtet. So können die Unternehmensprozesse effizienter und wirksamer gestaltet, gelenkt und kontrolliert werden. Dies wirkt sich, wie jedes gute, professionelle Management positiv auf die Bewältigung von Risiken und damit auf den Unternehmenserfolg aus.
- Bei der Integration des CMS ist es entscheidend, die Schnittstellen zu den anderen Managementsystemen der Organisation zu analysieren und proaktiv zu pflegen: zum Qualitätsmanagement (ISO 9001:2015), Risikomanagement (ISO 31000:2009), Umweltmanagement (ISO 14001:2015), Informationssicherheits-Management (ISO 27001: 2013), Arbeits- und Gesundheitsschutz-Management (ISO 45001:2016) und zum Business Continuity Management (BCM, ISO 22301: 2010). Nur wenn diese Herausforderung gemeistert wird, kann ein effektives und effizientes Integriertes Managementsystem (IMS) entstehen, welches der Organisation maximalen Nutzen bringt.
- Die Elemente der ISO 19600:2014 folgen dem bekannten PDCA-Managementzyklus. In dieser logischen Abfolge kann das CMS methodisch optimal und wirksam umgesetzt und verbessert werden. Dies führt zu einer nachhaltigen und wirksamen Compliance-Lösung.
- Compliance-Risiken oder Aktivitäten, bei denen es zur Nichteinhaltung von Compliance-Verpflichtungen kommen kann, können durch das Zusammenspiel mit der ISO 31000:2009 optimal identifiziert, analysiert, bewertet und bewältigt werden (Risikobasierter Ansatz nach ISO 31000:2009).
- Im Falle von Regelverstössen kann ein Unternehmen den Nachweis erbringen, dass kein Organisationsverschulden (Unternehmensstrafrecht, Artikel 102 Strafgesetzbuch) vorliegt, und damit auch das Management vor Haftungsrisiken schützen und im Falle eines Einzelverstosses entlasten. Darüber hinaus fördert ein wirksames CMS auch das Vertrauen der interessierten Parteien, insbesondere von Mitarbeitern und Kunden. ■

Claude Bollinger ist Quality Manager und Head of Engineering bei Ecodyne UET Schweiz AG.

Dr. Christian Zipper ist Studienleiter MAS Integrated Risk Management an der ZHAW School of Engineering, Institut für Nachhaltige Entwicklung.
E-Mail: christian.zipper@zhaw.ch.

Dr. Daniel Lucien Bühr ist Partner bei LALIVE Rechtsanwälte in Zürich/Genf, Mitglied der Arbeitsgruppe, die ISO 19600 erarbeitet hat, sowie Vize-Präsident von Ethics and Compliance Switzerland.
www.ethics-compliance.ch