

Eidgenössische Bankenkommission
Herren
Dr. K. Hauri, Präsident
D. Zuberbühler, Direktor
Schwanengasse 12
Postfach
3001 Bern

Zürich, 26. Juli 2005

Vernehmlassung zum Entwurf des EBK-RS Interne Überwachung und Kontrolle
Ihre Referenz: 432/2004/02575-0020

Sehr geehrter Herr Präsident
Sehr geehrter Herr Direktor

Mit Schreiben vom 3. Mai 2005 haben Sie uns um Stellungnahme zum Entwurf für ein EBK-Rundschreiben Interne Überwachung und Kontrolle („Rundschreiben“) gebeten. Gerne kommen wir Ihrer Einladung nach und unterbreite Ihnen folgenden Kommentar.

Allgemein

Als Vereinigung der Schweizer Compliance Officers begrüssen wir zwar grundsätzlich, dass in einem Regelwerk Aussagen zum Berufsstand der Compliance Officers gemacht werden. Trotzdem erlauben wir uns die folgenden kritischen Bemerkungen:

Es ist nicht nachvollziehbar, wieso vom bewährten System der Selbstregulierung abgewichen werden soll: Die grundlegenden Prinzipien der internen Überwachung und Kontrolle sind in den Richtlinien zur Internen Kontrolle der Schweizerischen Bankiervereinigung vom Juni 2002 enthalten. Es kann sinnvoll sein, diese Richtlinien, insbesondere mit Blick auf die Empfehlungen des Basel Committee on Banking Supervision (compliance and the compliance function in banks), den neuesten Gegebenheiten anzupassen. Der Bedarf, diese Richtlinien durch das vorgeschlagene Rundschreiben gänzlich zu ersetzen, ist aber nicht ausgewiesen.

Vom Rundschreiben ist auch deshalb abzusehen, weil kein Anlass für den Erlass einer *staatlichen* Regulierung besteht; jedenfalls macht Ihr Begleitschreiben vom 3. Mai 2005 diesbezüglich keine Angaben. Ebenso vermissen wir im Begleitschreiben eine Aussage zu den Kosten-/Nutzenüberlegungen.

Dem Rundschreiben fehlt darüber hinaus ein Zweckartikel mit der Aussage, was mit der internen Überwachung und Kontrolle erreicht werden soll.

Das Rundschreiben enthält Eingriffe in das Aktienrecht (z.B. mit Aussagen zur Unabhängigkeit des Verwaltungsrats) und in das Privatrecht (z.B. mit Aussagen zum Schutz der Persönlichkeit eines "Whistleblowers"). Falls an diesen Eingriffen festgehalten werden soll, stellt sich die Frage, ob die Form des Rundschreibens dazu qualifiziert.

Das Rundschreiben hält nicht nur Grundsätze der internen Überwachung und Kontrolle fest, sondern greift sehr stark in die interne Organisations-Autonomie der einzelnen Institute ein. Es ist nicht erwiesen, dass es solche Detailregelungen überhaupt braucht, weshalb das Rundschreiben allgemeiner formuliert werden sollte. Damit kann der Grosse, Geschäftstätigkeit und den Bedürfnissen der betroffenen Institute besser Rechnung getragen werden.

Unsere nachfolgenden spezifischen Bemerkungen zu den einzelnen Bestimmungen sind im Kontext mit unserem grundsätzlichen Vorbehalt zum Erlass einer staatlichen Regelung zu verstehen.

Bemerkungen zu den einzelnen Bestimmungen

In Rz 2 werden die verschiedenen Stufen einer wirksamen internen Kontrolle bestimmt:

- Basis-Stufe: Risikomanagement und Prozesse zur Sicherstellung der Compliance
- Übergeordnete Stufe: Risikokontrolle und Compliance Funktion
- Oberste Stufe: Interne Revision

Diese Aufteilung der stufengerechten Kontrolle wird im Rundschreiben aber nicht überall konsequent umgesetzt. Für die oberste Stufe ist die Zuordnung der Verantwortungen und Aufgaben noch klar: Verantwortlich ist der Verwaltungsrat, als Instrument dazu dient ihm die interne Revision. Auf der mittleren Stufe liegt die Verantwortung bei der Geschäftsführung, unterstützt durch die Compliance Funktion. Nicht erwähnt wird jedoch die Risikokontrolle, die ebenfalls eine Unterstützungsfunktion für die Geschäftsleitung wahrnimmt.

Um die Beschreibung der mittleren Stufe analog der obersten Stufe zu strukturieren, sollte die Kapiteleinteilung wie folgt gestaltet werden:

Ziff 5: Geschäftsführung

- Setzt die Vorgaben des Verwaltungsrats bezüglich interner Kontrollen um;
- Verantwortlich für Compliance (Ziff. 5.1) und andere Risiken (d.h. Risiken die von der Risikokontrolle erfasst werden; ein solcher Abschnitt fehlt).

Ziff. 6: Compliance Funktion

Unter dieser Ziffer ist die bisherige Ziff. 5.2 einzuordnen.

Ziff. 7: Risikokontrolle

Unter dieser Ziffer ist die bisherige Ziff. 5.3 einzuordnen.

Gänzlich unerwähnt bleibt die Basis-Stufe (Risikomanagement und die Prozesse zur Sicherstellung der Compliance). Diese Stufe müsste konsequenterweise und der Vollständigkeit halber in einer weiteren Ziff. 8 beschrieben werden.

Verwaltungsrat

Es muss dem Verwaltungsrat möglich sein, sich so zu organisieren, dass gewisse Fachkenntnisse (Rz 11) delegiert werden können. Dies gilt insbesondere auch für die Privatbankiers, da sonst die Partner gezwungen werden könnten, zusätzliches know how nicht nur in der Geschäftsführung oder im Kontrollsystem sicherzustellen, sondern auch personell in die Partnerschaft aufzunehmen.

Die Formulierung, "dass Interessenkonflikte mit dem Institut möglichst vermieden werden" (Rz 12) lässt zwar einen gewissen Spielraum, ist aber möglicherweise für die Praxis wenig glücklich. Eine alternative Formulierung wäre: "Die Mitglieder des Verwaltungsrats ordnen deshalb ihre persönlichen und geschäftlichen Verhältnisse so, dass Interessenkonflikte mit dem Institut vermieden werden; lässt sich ein Interessenkonflikt im Einzelfall nicht vermeiden, ergreifen sie geeignete Massnahmen zur Lösung des Interessenkonflikts."

Es ist ungenügend geregelt, in welcher „Art“ und welchem „Umfang“ ein Verwaltungsrat in „geschäftlichen Beziehungen“ zum Institut stehen darf (Rz 16). Die Formulierung „welche zu einem Interessenkonflikt führen könnte“ ist zu weit gefasst. Eine Alternative wäre eine Formulierung wonach ein Interessenkonflikt nur vorliegt, wenn der Konflikt unvereinbar wird, d.h. wenn der Konflikt durch keine vernünftigen Massnahmen gelöst werden kann.

Die 10-%-Schwelle in Rz 17 überzeugt nicht. Die Unvereinbarkeit sollte nur bei einer *signifikanten* Beteiligung und nicht bereits bei 10 % eintreten. Die 10-%-Schwelle entspricht nicht internationalen Standards. Zudem ist nicht ersichtlich, ob damit auch in einem Poolvertrag zusammengefasste Aktien sowie solche von nahe stehenden Personen und Gesellschaften einbezogen werden. Diese Bestimmung verkennt zudem die Situation der Kantonalbanken. (Gemäss Art. 3a BankG ist eine Kantonalkantonalbank eine Bank, an welcher der Kanton mindestens 1/3 des Kapitals hält.) Rz 17 ist deshalb ersatzlos zu streichen.

Audit Committee

Das dem angelsächsischen Recht entnommene Institut des Audit Committee ist für Schweizer Banken *unnötig*, weil die notwendige Unabhängigkeit zwischen Oberleitung, Aufsicht und Kontrolle einerseits und der Geschäftsführung andererseits bereits im BankG bzw. in der BankV stipuliert ist. Der zweite Satz in Rz 18 ist daher ersatzlos zu streichen.

Sollte auf die ersatzlose Streichung verzichtet werden, erlauben wir uns folgende kritischen Bemerkungen zum Thema Audit Committee:

- Es ist nicht einsehbar, weshalb die *Anzahl* Verwaltungsräte eine konkrete Bedeutung für die Errichtung eines Audit Committee haben soll (Rz 25). Diese Bestimmung ist deshalb ersatzlos zu streichen.
- Die Formulierung "angemessene Kenntnisse und Erfahrung im Finanz- und Rechnungswesen" (Rz 29) erscheint als sehr vage bzw. breit und gleichzeitig als übermässig einschränkend. Wie verhält es sich z.B. mit einem Anwalt, der viel von interner Kontrolle versteht, aber keine Erfahrung im Rechnungswesen hat? Wird die Bestimmung grosszügig interpretiert, ist sie bedeutungslos, wird sie eng ausgelegt, schliesst sie einen grösseren Kreis fähiger Personen aus.

- Gemäss Rz 34 soll das Audit Committee die Revisionsberichte der internen Revision kritisch analysieren und diese mit dem Leiter der internen Revision besprechen. In einer grösseren Bank ist es nicht möglich, jeden einzelnen Revisionsbericht zu analysieren und zu besprechen. Eine allgemeinere Formulierung wäre auch hier angezeigt.
- Sodann erscheint die Berichterstattung der internen Revision uneinheitlich geregelt: Nach Rz 57 berichtet sie in erster Linie dem Verwaltungsrat (nicht dem Audit Committee), nach Rz 65 informiert sie Verwaltungsrat und Geschäftsführung und nach Rz 67 schliesslich erstattet sie dem Verwaltungsrat bzw. dem Audit Committee und der Geschäftsführung Bericht. Eine weniger detaillierte Regelung wäre auch hier vorzuziehen.

Verfahren zur Meldung vermuteter Unregelmässigkeiten im Institut (Rz 44 „whistleblowing“)

Es liegt im Interesse jedes Institutes, ein Verfahren zur Meldung von Unregelmässigkeiten vorzusehen. Die Bestimmung ist daher als Ganzes *unnötig* oder müsste zumindest anders formuliert werden:

- Der Begriff „whistleblowing“ ist unglücklich gewählt, da dieser auf etablierte und klar geregelte Rechtsinstitute im angelsächsischen Raum Bezug nimmt.
- Die Regelung des Verfahrens sollte den einzelnen Instituten überlassen werden, insbesondere sollte es möglich sein, andere Stellen, als den Verwaltungsrat oder das Audit Committee, zu bezeichnen (z.B. Compliance Funktion, Rechts- oder Personaldienst), an welche sich die meldenden Mitarbeiter wenden können. Diese Stellen hätten die Fälle zu bearbeiten, aber nicht alle dem Verwaltungsrat bzw. seinem Audit Committee zu rapportieren.
- Die Formulierung "vermutete Unregelmässigkeiten in der Rechnungslegung oder bei der Einhaltung gesetzlicher, regulatorischer und interner Vorschriften" ist sehr breit und gleichzeitig sehr technisch-einschränkend. "Vermutet" öffnet missbräuchlichem Denunziantentum Tür und Tor. "Einhaltung interner Vorschriften" kann eine individuelle Spesenabrechnung oder das Nichtausschalten eines Geräts am Feierabend sein. Andererseits sind auch Missstände ausserhalb eines Verstosses gegen konkrete Vorschriften denkbar.
- Eine meldewürdige Verletzung interner Vorschriften dürfte stets auch gegen externe rechtliche und regulatorische Normen verstossen. Besser wäre deshalb eine Formulierung wie: „Der Verwaltungsrat stellt sicher und bringt allen Mitarbeitenden zur Kenntnis, dass festgestellte erhebliche Missstände, insbesondere hinsichtlich der Rechnungslegung oder der Einhaltung rechtlicher und regulatorischer Vorschriften, unternehmensintern gemeldet werden können.“

Unklar ist auch, was mit der Sicherstellung des Schutzes der Persönlichkeit des meldenden Mitarbeiters gemeint ist. Bedeutet dies, dass anonyme Meldungen möglich sein müssen? Das könnte wiederum *nicht* sichergestellt werden, da der meldende Mitarbeiter z.B. in einem nachfolgenden Straf- oder Aufsichtsverfahren bekannt werden könnte. Es sollte ferner zumindest heissen: "Der Schutz der Persönlichkeit eines in guten Treuen meldenden Mitarbeiters ist zu wahren".

Geschäftsführung

In diesem Abschnitt sind zwecks Vermeidung von Redundanzen noch Präzisierungen vorzunehmen. So bestehen z.B. Überschneidungen im Reporting:

- Die Compliance Funktion muss mindestens einmal jährlich das Compliance Risiko einschätzen und die Geschäftsführung darüber informieren.
- Die Risikokontrolle hat mindestens halbjährlich einen Bericht über die Risiken zuhanden der Geschäftsführung zu verfassen.

Bedeutet dies, dass einmal im Jahr die Compliance Funktion direkt einen Bericht an die Geschäftsführung abzuliefern hat und halbjährlich einen Bericht an die Risikokontrolle, damit diese Einheit ebenfalls ihren Berichterstattungsverpflichtungen gegenüber der Geschäftsführung nachkommen kann? Um Redundanzen zu vermeiden sind die Aufgaben der Compliance Funktion und der Risikokontrolle entsprechend zu präzisieren. Dabei ist insbesondere der Begriff „Risikokontrolle“ (Rz 87) zu definieren.

Verschiedene Banken unterscheiden zwischen rechtlichen und regulatorischen Risiken, welche je nach Institutsgrosse vom Rechtsdienst bzw. von der Compliance Abteilung bearbeitet werden. Aus der Formulierung „Als compliance gilt das Einhalten von gesetzlichen, regulatorischen und internen Vorschriften ...“ ist abzuleiten, dass die Compliance Funktion auch n/cM-regulatorische Risiken zu bearbeiten hat, was für die Mehrheit der betroffenen Institute eine Erweiterung des Aufgabengebietes der Compliance Abteilung bedeuten würde. Der Begriff „gesetzlich“ ist zu streichen.

Das Rundschreiben erwähnt in Rz 74 (und Rz 85) die zeitgerechte Berichterstattung an die Geschäftsführung. Wieso darüber hinaus eine jährliche Berichterstattung an den Verwaltungsrat bzw. an das Audit Committee erfolgen soll, ist nicht nachvollziehbar. Rz 86 ist ersatzlos zu streichen.

Erklärungsbedürftig ist, wie eine organisatorische Eingliederung "von ertragsorientierten Geschäftsaktivitäten unabhängig" zu erfolgen hat (Rz 75), da auch die Geschäftsführung, an welche die Compliance Funktion berichten soll, ertragsorientiert ist. Die Bedingung von Rz 75 ist kaum zu erfüllen.

Die übermässige Einschränkung der erfolgsabhängigen Entschädigung führt de facto zu einem Verbot von variablen Gehaltskomponenten, was nicht wünschenswert ist. Es sollte möglich sein, die Entschädigung von Institutsbereichen (anderer Begriff: Sparte, Abteilung odergemäss BIZ: „business line“; z.B. Private Banking, Investment Banking) abhängig zu machen. Rz 78 ist deshalb ersatzlos zu streichen.

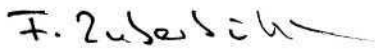
Bereits heute wird durch die interne Revision eine periodische Risikobeurteilung durchgeführt (vergl. Rz 62) und es sollte den Instituten überlassen werden, ob sie die Einschätzung des Compliance Risikos als Bestandteil dieser Risikobeurteilung durchführen möchten. Welche Bedeutung dem „risikoorientierten Tätigkeitsplan“ (Rz 83) zukommt, ist zudem völlig offen gelassen. Sollte darunter das angelsächsische Institut des „Surveillance Programme“ bzw. „Compliance Monitoring Programme (CMP)“ verstanden werden, so wäre dies mit Zusatzaufwand für die Institute verbunden. Bei der Einführung eines CMPs müsste es den betroffenen Instituten überlassen sein, ein ihrer Grosse und Geschäftstätigkeit angepasstes Vorgehen zu wählen.

Wie gewünscht, lassen wir Ihnen die vorliegende Stellungnahme auch in elektronischer Form zukommen und sind mit der Publikation auf Ihrer Homepage selbstverständlich einverstanden.

Wir danken Ihnen bestens, dass Sie SACO als Zusammenschluss der Schweizer Compliance Officers Gelegenheit zur Stellungnahme gegeben haben. Das vom vorgeschlagenen Rundschreiben behandelte Gebiet der internen Überwachung und Kontrolle stellt für uns ein zentrales Thema dar und wir bitten Sie, unsere kritischen Bemerkungen als konstruktiven Beitrag zu verstehen. Für Fragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüsse

SACO - Swiss Association of Compliance Officers



Fredy Urs Zuberbühler
Präsident



Thomas Steinebrunner
Aktuar