

Comments on Paper „The internal audit function in banks“ issued by The Basel Committee on Banking Supervision as of December 2nd, 2011

German version after page 9

Mitglied des
Institute of Internal
Auditors (IIA), Inc.

Mitglied der
European Confederation
of Institutes of Internal
Auditing (ECIIA)

Dear Sir or Madam,

on December 2nd, 2011, you published the consultation paper "The internal audit function in banks" (the Paper). Thank you for the opportunity to comment on this.

The DIIR – Deutsches Institut für Interne Revision e.V., is a national non-profit association to promote and enhance the profession of internal auditing in Germany. Founded in 1958, it now represents approximately 2.500 members from all areas of the economy, science and public institutions. The DIIR is an associated organization of the global Institute of Internal Auditors (the IIA).

Our comments have been developed by the DIIR working group "Minimum requirements of the risk management of banks". This working group consists of members of all kinds of German banking groups and forms the interface of the DIIR to the respective committee of the Federal Financial Supervisory Authority (BaFin). This working group primarily deals with regulatory requirements on the internal audit function.

We highly appreciate that the internal audit function in banks, resulting by stressing and profiling the tasks and function of internal audit by a globally applicable paper, is strengthened.

Overall, we expect that the new paper will have a stronger binding character than the paper "Internal audit in banks and the supervisor's relationship with auditors" issued in 2001. Having said this, we would like to start with some general remarks before commenting on detailed principles and articles.

1. General remarks

Two-Tier System vs. One-Tier System

Whereas respective laws for stock corporations, cooperative societies and saving banks in Germany define a two-tier system (dualistic system or two-board system), this Paper is generally based on the one-tier system (monistic system) as organizational structure.

Additionally, banks in Germany have to adhere to the "Minimum Requirements on the Risk Management of Banks", which specify § 25a German Banking Law (KWG). These also substantiate the setup of a two-tier system, which can be described as follows:

The two-tier system, in contrary to the one-tier system, stipulates a reporting line of the internal audit function to "senior management" (board of managing directors, "Vorstand" or "Geschäftsleitung"), being solely in charge of the management of the organization. Consequently, in this system the internal audit function is an **"instrument of senior management"** (board of managing directors). The supervisory board is responsible to purely monitor senior management. In the two-tier system, the audit committee as a sub-committee of the supervisory board, "only" has a monitoring respective oversight-function of the internal audit function.

In the context of this oversight-function the internal audit function has to ensure appropriate communication on internal auditing performance with the audit committee. The audit committee's governance position, as a sub-committee of the supervisory board in a two-tier system, however, is not the same position as in a one-tier system.

As a result of the two-tier system incorporated in German laws a 1:1 transformation of some individual principles and articles is not possible, instead can intended objectives of the principles and articles based on given management- and governance functions be met.

Even though the introduction of the Paper (Introduction, Art. 5.) states that the principles should be applied in accordance with the applicable national corporate governance structures of each country, German financial institutions could get – especially abroad – into argumentative problems on the interpretation of the principles.

Having said this, we consider it necessary to **emphasize more clearly in Art. 5, that the Papers' precise phrasing of the individual principles is based on the (Anglo-Saxon) one-tier board system, and that the opening clause requires being specified.** It should be stressed that a global regulation may not be possible by a "one size fits all" approach and that there are different ways to reach individual objectives of the Paper.

Therefore it should be clarified how to proceed, if due to national corporate governance structures single rules cannot be adopted. **Our recommendation is to form a regulation, that in case a principle or article cannot be adopted, such implementation is considered as sufficient, which corresponds to the intended objective of the respective principle or article of the Paper.**

Critical regarding its adaptability in Germany in this context are articles: 6, 12, 23, 29, 43 – 47, 49, 50, 52, 53, 54, 59, 60, 71, 73, 80, 86, 87, 88, 90 and Annexes 1 and 2.

Role of the External Auditor

The Paper does not clarify the role of the external auditor (chartered accountant) in supervising the internal audit function. Whereas annex 1 "Internal audit function's communication channels" presents the external auditor as a central point of communication, a supervisory role is not allocated. Additionally, this part of the Paper refers to the standards of the IIA, the ISA-rules and other publications and papers by the BCBS, such as "The Relationship Between Banking Supervisors and Banks' External Auditors", "Core Principles for Effective Banking Supervision" and "Principles for enhancing corporate governance". As the latter mentioned two publications also relate to aspects of supervision, audit function, audit committee and tasks of the external auditor, there are overlapping content topics with this Paper.

Assurance After Effect vs. Forward Looking Approach

To give a fair consideration of the role of internal audit and the main current practice, we suggest to add a **further principle** clarifying that internal audit does not only perform ex post audits ("Assurance After Effect", "ex post"), but also considers future developments ("Forward Looking", "ex ante"). This approach does not only comprise ex-ante supervision of projects but also future-oriented evaluations e.g. regarding the business- and risk-strategy or the design of the risk-management system.

2. Comments on individual articles

Art./Principle	Wording	Comment/Recommendation
Art. 5	The principles set out in this document should be applied in accordance with the applicable national corporate governance structure of each country.	<p><u>See remarks above:</u></p> <ul style="list-style-type: none"> ▪ Clarify that the precise phrasing of the principles is based on the one-tier board system of corporate governance. ▪ Specification of the opening clause. ▪ Clarify that fulfilling the intended objective of the respective principle or article is considered as sufficient to meet the requirements.
Art. 15	The independence and objectivity of the internal audit function may be undermined if the staff's remuneration is linked to the financial performance of the business line for which they exercise internal audit responsibilities or to the financial performance of the bank as a whole.	<p>A certain link to the financial performance of the organization as a whole should be possible to allow equal treatment of all employees within an organization and to assure a remuneration being consistent with the economic situation of the organization. We do not consider the suggested procedure can be implemented in practice.</p> <p>Therefore, we would like to suggest cancelling the last part of the sentence.</p>

Art. 16

Professional competence depends on the auditor's capacity to collect and understand information, to examine and evaluate audit evidence and to communicate with the **stakeholders** of the internal audit function. This should be combined with suitable methodologies and tools and sufficient knowledge of auditing techniques. Consideration should also be given to ensuring the internal audit staff acquire appropriate ongoing training in order to meet the growing technical complexity of banks' activities and the increasing diversity of tasks that need to be undertaken as a result of the introduction of new products and processes within banks and other developments in the financial sector.

The constitution of the group of "stakeholders" for the internal audit function remains unclear.

As the constitution of the stakeholders has an impact on required competency of the internal audit function and on the procedures, we consider a definition of "stakeholders" as being necessary.

Art. 56

Control failings by one line of defence should, in principle, be detected by another line of defence. However, responsibility for internal control does not transfer from one line to another.

We do not encounter that vice versa controls will lead to results, as for instance no operative unit is to review the internal audit function. This would endanger the independence and standing of the internal audit function within the organization. Further there is a risk of mixed responsibilities, multiple control performances and therefore inefficient processes.

We recommend to modify the first sentence as follows:

Control failings by one line of defence should, in principle, be detected by the higher line(s) of defence.

Art. 57

Operational management has **ownership, responsibility and accountability** for identifying, assessing, controlling, mitigating and reporting on risks encountered in the course of a bank's business activities.

The terms "ownership", "accountability" and "responsibility" should be clearly defined.

Especially the translation and transformation to national jurisdiction could result in an allocation of tasks and responsibilities, which is not intended by the Basel Committee, leading to divergency of legislations, which would contradict the Paper's objective of harmonization.

Art. 58

The risk management function facilitates and monitors the implementation of effective risk management practices by operational management. It assists operational management in defining risk exposures and reporting through the organisation. The compliance function monitors the risk of non-compliance with laws, regulations and standards. These functions are also **control functions** which ensure that policies and procedures with regard to risk-taking are enforced. Other **monitoring functions** may include human resources and the legal department.

The terms "control functions" and "monitoring functions" should be clearly defined, as the term "control" has a very broad meaning in the English language.

Especially the translation and transformation to national jurisdiction could result in an allocation of tasks and responsibilities, which is not intended by the Basel Committee, leading to divergency of legislations, which would contradict the Paper's objective of harmonization.

Art. 62

Principle 6 ("Every activity [including outsourced activities] and every entity of the bank should fall within the overall scope of the internal audit function") and related paragraphs of this document are also applicable **to groups**, that is, every activity (including outsourced activities) and every entity of the group should fall within the overall scope of the internal audit function.

This wording might be interpreted in a way that in addition to the internal audit function of an entity, the internal audit function of the parent company (group level) has to audit all processes and activities of every entity of the group, which would make double audits necessary.

Therefore, we recommend clarifying that the audit function of the parent company has to complement the audit function of an entity with respect to the risk management on group level and, doing this, can consider the results of the audit function of an entity.

Principle 15

Principle 15: Regardless of whether internal audit activities are outsourced, the **board of directors** remains ultimately responsible for ensuring that the system of internal control and the internal audit function are adequate and operating effectively.

Principle 9: The bank's board of directors has the ultimate responsibility for ensuring that **senior management** establishes and maintains an adequate, effective and efficient internal control framework and internal audit function.

In Principle 15 "Senior Management" should be used in analogy to Principle 9, to avoid potential contradictions in interpreting the Paper.

Art. 64

The head of internal audit should ensure that outsourcing **suppliers comply with the principles in the bank's internal audit charter**. To preserve independence, it is important to ensure that the supplier has not been previously engaged in a consulting engagement in the same area within the bank unless a reasonably long "cooling-off" period has elapsed. Similarly, as a best practice banks should not outsource internal audit activities to their own external audit firm.

In our opinion it is not sufficient just to comply with the internal audit charter. Rather should the overall audit standards (as for instance the IIA standards) be mentioned.

Recommendation:

The head of internal audit [...] internal audit charter and internal auditing standards, such as The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing (as far as not covered by the charter).

Art. 68

The relationship between the supervisor and the internal audit function should be established in a structured and transparent way. In principle, the supervisor will initiate this relationship.

We assume that the phrase "in a structured and transparent way" means, embedding the organs of the organization and internal audit.

DIIR

Deutsches Institut für
Interne Revision e.V.

Ohmstraße 59
60486 Frankfurt am Main
Telefon (069) 71 37 69 - 0
Fax (069) 71 37 69 - 69
www.diir.de
info@diir.de

Geschäftsführer:
Wilfried Fischenich
Volker Hampel
USt-ID DE 114235123
Vereinsregisternummer:
Amtsgericht Frankfurt
am Main VR 5326

Stellungnahme zum Papier „The internal audit function in banks“ des Baseler Ausschusses vom 2. Dezember 2011

Mitglied des
Institute of Internal
Auditors (IIA), Inc.

Mitglied der
European Confederation
of Institutes of Internal
Auditing (ECIIA)

Sehr geehrte Damen und Herren,

am 2. Dezember 2011 hatten Sie Ihr Konsultationspapier „The internal audit function in banks“ veröffentlicht. Wir bedanken uns für die Möglichkeit einer Stellungnahme.

Das DIIR – Deutsches Institut für Interne Revision e.V. ist ein gemeinnütziges Institut zur Förderung und Weiterentwicklung der Internen Revision in Deutschland. Es wurde 1958 gegründet und hat mittlerweile über 2.500 Mitglieder aus allen Bereichen der Wirtschaft, Wissenschaft und Verwaltung. Das DIIR ist Mitglied des The Institute of Internal Auditors (IIA). Unsere Stellungnahme wurde von dem Arbeitskreis „Mindestanforderungen an das Risikomanagement“ (AK MaRisk) erstellt. Der Arbeitskreis ist mit Vertretern aus allen deutschen Kreditinstitutgruppen besetzt und stellt die Schnittstelle des DIIR zum MaRisk-Fachgremium der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) dar. Er beschäftigt sich insbesondere mit den regulatorischen Anforderungen an die Interne Revision.

Grundsätzlich begrüßen wir die aus der Herausarbeitung sowie der Konkretisierung der Aufgaben und der Funktion der Internen Revision im Rahmen eines weltweit gültigen Papiers resultierende Stärkung der Internen Revisionsfunktion.

Insgesamt erwarten wir gegenüber dem im Jahre 2001 veröffentlichten Papier „Internal audit in banks and the supervisor's relationship with auditors“ einen stärker verbindlichen Charakter. Vor diesem Hintergrund möchten wir zunächst einige grundsätzliche Anmerkungen machen und in der Folge einzelne Detailregelungen kommentieren.

1. Grundsätzliche Anmerkungen

Dualistisches System vs. Monistisches System

Dem Papier wird grundsätzlich das monistische System (One-Board- oder One-Tier-System) der Unternehmensleitung zugrunde gelegt, wohingegen in Deutschland das dualistische System (Two-Board- oder Two-Tier-System) aktien-, genossenschafts- und sparkassenrechtlich verankert ist. Im deutschen Bankensektor sind zusätzlich noch die den § 25a KWG präzisierenden „Mindestanforderungen an das Risikomanagement“ (MaRisk), zu berücksichtigen. Diese konkretisieren ebenfalls die Ausgestaltung des dualistischen Systems, welches sich wie folgt darstellt:

Das dualistische System sieht – im Gegensatz zum monistischen System – die Zuordnung („reporting line“) der Internen Revision zum Vorstand bzw. der Geschäftsleitung („Senior Management“), welcher die alleinige operative Verantwortung trägt, vor. Die Interne Revision ist in diesem System somit ein **„Instrument des Vorstandes“**. Dem Aufsichts- bzw. Verwaltungsrat kommt alleine die Überwachung des Vorstandes zu. Der Prüfungsausschuss (Audit Committee), ein Unterausschuss des Aufsichts- bzw. Verwaltungsrates, hat im dualistischen System „lediglich“ eine Überwachungsfunktion („Monitoring“ bzw. „Oversight“) hinsichtlich der Internen Revision. Im Rahmen dieser Überwachung erfolgt eine angemessene Berichterstattung („Information“) über die Tätigkeit der Internen Revision an den Prüfungsausschuss, dessen Stellung in der Corporate Governance eine andere ist, als die des Audit Committees im monistischen System.

Das in Deutschland verankerte dualistische System führt dazu, dass für einzelne Principles bzw. deren Textziffern die Umsetzung nicht 1:1, sondern lediglich im Sinne der Zielsetzung der jeweiligen Principles und auf Basis der gegebenen Geschäftsleitungs- und Überwachungsfunktionen erfolgen kann.

Zwar werden in der Einführung dieses Papiers (Introduction, Tz. 5.) nationale Gestaltungsfreiheiten eingeräumt, um den gegebenen Corporate Governance Strukturen entsprechen zu können, die deutschen Finanzinstitute können jedoch bei der Interpretation der Principles – insbesondere im Ausland – in Erklärungszwang geraten.

Vor diesem Hintergrund halten wir es für notwendig, in Tz. 5 **deutlicher herauszustellen, dass das Papier sich bei der konkreten Ausformulierung der einzelnen**

Principles am (angelsächsischen) monistischen board-System orientiert und die Öffnungsklausel zu präzisieren. Es sollte herausgestellt werden, dass bei einer länderübergreifenden Regulierung ein „one size fits all“ nicht möglich ist und dass es mehrere Wege zur Erreichung der einzelnen Ziele dieses Papiers geben kann.

Folglich sollte klargestellt werden, wie bei einer durch die nationale Corporate Governance Struktur bedingten Nichtanwendbarkeit einzelner vorliegender Regeln zu verfahren ist.

Unsere Empfehlung ist eine Regelung, welche deutlich macht, dass im Falle einer Nichtanwendbarkeit einer Regel diejenige Umsetzung, welche der Zielsetzung des jeweiligen Principles des Papiers entspricht, zur Erfüllung der jeweiligen Anforderung des Papiers ausreichend ist.

Kritisch hinsichtlich der Anwendbarkeit in Deutschland sind in diesem Zusammenhang die Tzn.: 6, 12, 23, 29, 43 – 47, 49, 50, 52, 53, 54, 59, 60, 71, 73, 80, 86, 87, 88, 90 sowie Annex 1 und 2.

Rolle des externen Prüfers (Abschlussprüfer)

Das vorliegende Papier lässt unklar, welche Funktion dem Abschlussprüfer (External Auditor/Chartered Accountant) bei der Überwachung der Revisionsfunktion zukommen soll. Zwar wird der Abschlussprüfer in Annex 1 „Internal audit function's communication channels“ als zentrale Anlaufstelle dargestellt, eine Überwachungsfunktion wird ihm hierbei jedoch nicht zugewiesen. Zudem erfolgt an dieser Stelle des Papiers ein Verweis auf die IIA-Standards, die ISA-Regeln und andere BCBS-Veröffentlichungen wie z. B. „The Relationship Between Banking Supervisors and Banks' External Auditors“, „Core Principles for Effective Banking Supervision“ und „Principles for enhancing corporate governance“. Da sich die beiden letztgenannten Veröffentlichungen ebenfalls auf Aspekte der Aufsicht, Revisionsfunktion, des Audit Committee sowie auf die Aufgaben des Abschlussprüfers beziehen, ergeben sich zu dieser Veröffentlichung thematische Überschneidungen.

After effect vs. Forward looking approach

Um der Rolle der Internen Revision bzw. der zumeist bereits gelebten Praxis gerecht zu werden, schlagen wir ein **weiteres Principle** vor, welches klarstellt, dass die Interne

Revision nicht nur nachträgliche Prüfungen vornimmt („Assurance After Effect“, „ex post“), sondern auch im Hinblick auf zukünftige Entwicklungen („Forward Looking“, „ex ante“) tätig wird. Dieser Ansatz umfasst nicht nur eine ex-ante Begleitung von Projekten, sondern durchaus auch zukunftsgerichtete Evaluierungen beispielsweise hinsichtlich der Geschäfts- und Risikostrategie oder der Ausgestaltung des Risikomanagement-Systems.

2. Anmerkungen zu einzelnen Textziffern

Tz./Principle	Wortlaut	Anmerkung/Empfehlung
Tz. 5	The principles set out in this document should be applied in accordance with the applicable national corporate governance structure of each country.	<p><u>Siehe grundsätzliche Anmerkungen oben:</u></p> <ul style="list-style-type: none"> ▪ Klarstellung, dass sich die konkrete Ausformulierung der Principles am monistischen System orientiert. ▪ Detaillierung der Öffnungsklausel. ▪ Klarstellung, dass Umsetzung entsprechend der Zielsetzung der Principles für Erfüllung ausreichend ist.
Tz. 15	The independence and objectivity of the internal audit function may be undermined if the staff's remuneration is linked to the financial performance of the business line for which they exercise internal audit responsibilities or to the financial performance of the bank as a whole.	<p>Eine gewisse Verbindung zum Unternehmenserfolg im Ganzen sollte möglich sein, um einerseits eine Gleichbehandlung aller Mitarbeiter des Unternehmens und andererseits eine im Einklang mit der wirtschaftlichen Situation des Unternehmens stehende Vergütung sicherzustellen. Die vorgeschlagene Vorgehensweise halten wir nicht für realisierbar.</p> <p>Wir empfehlen daher, den letzten Halbsatz zu streichen.</p>

Tz. 16

Professional competence depends on the auditor's capacity to collect and understand information, to examine and evaluate audit evidence and to communicate with the **stakeholders** of the internal audit function. This should be combined with suitable methodologies and tools and sufficient knowledge of auditing techniques. Consideration should also be given to ensuring the internal audit staff acquire appropriate ongoing training in order to meet the growing technical complexity of banks' activities and the increasing diversity of tasks that need to be undertaken as a result of the introduction of new products and processes within banks and other developments in the financial sector.

Hier bleibt unklar, wie weit der Kreis der „Stakeholder“ der Internen Revision zu fassen ist.

Da der Umfang der Stakeholder Auswirkungen auf die in einer Internen Revision benötigten Kompetenzen sowie die anzuwendenden Vorgehensweisen hat, erachten wir hier eine Definition des Kreises der „Stakeholder“ der Internen Revision als notwendig.

Tz. 56

Control failings by one line of defence should, in principle, be detected by another line of defence. However, responsibility for internal control does not transfer from one line to another.

Wir halten eine gegenseitige Kontrolle für nicht zielführend, da es beispielsweise keine Aufgabe der operativen Einheiten ist, die Interne Revision zu kontrollieren. Dies würde sowohl die Unabhängigkeit als auch das Ansehen der Internen Revisionsfunktion innerhalb des Unternehmens beeinträchtigen. Ferner besteht das Risiko der Vermischung von Zuständigkeiten sowie Mehrfachkontrollen und somit von unwirtschaftlichen Abläufen.

Wir empfehlen, den ersten Satz wie folgt zu modifizieren: Control failings by one line of defence should, in principle, be detected by the higher line(s) of defence.

Tz. 57

Operational management has **ownership, responsibility and accountability** for identifying, assessing, controlling, mitigating and reporting on risks encountered in the course of a bank's business activities.

Die Begriffe „ownership“, „accountability“ und „responsibility“ sollten eindeutig voneinander abgegrenzt werden.

Insbesondere bei der Übersetzung bzw. der darauf folgenden Umsetzung in nationales Recht könnten hier neben einer vom Baseler Ausschuss nicht beabsichtigen Zuordnung von Verantwortlichkeiten, Divergenzen zwischen einzelnen Legislativen entstehen, welche dem Harmonisierungsgedanken dieses Papiers widersprechen.

Tz. 58

The risk management function facilitates and monitors the implementation of effective risk management practices by operational management. It assists operational management in defining risk exposures and reporting through the organisation. The compliance function monitors the risk of non-compliance with laws, regulations and standards. These functions are also **control functions** which ensure that policies and procedures with regard to risk-taking are enforced. Other **monitoring functions** may include human resources and the legal department.

Die Begriffe „control functions“ und „monitoring functions“ sollten eindeutig voneinander abgegrenzt werden, da der Begriff „control“ im Englischen sehr weit gefasst ist.

Insbesondere bei der Übersetzung bzw. der darauf folgenden Umsetzung in nationales Recht könnten hier neben einer vom Baseler Ausschuss nicht beabsichtigen Zuordnung von Aufgaben und Verantwortlichkeiten, Divergenzen zwischen einzelnen Legislativen entstehen, welche dem Harmonisierungsgedanken dieses Papiers widersprechen.

Art. 62

Principle 6 ("Every activity [including outsourced activities] and every entity of the bank should fall within the overall scope of the internal audit function") and related paragraphs of this document are also applicable **to groups**, that is, every activity (including outsourced activities) and every entity of the group should fall within the overall scope of the internal audit function.

Diese Formulierung könnte derart ausgelegt werden, dass die Interne Revision des Mutterunternehmens zusätzlich zur Internen Revision des Tochterunternehmens alle Prozesse und Aktivitäten des Tochterunternehmens zu prüfen hat und somit eine Doppel-Prüfung notwendig ist.

Wir empfehlen daher eine Klarstellung, dass die Revision des Mutterunternehmens im Rahmen des Risikomanagements auf Gruppenebene ergänzend zur Revision des Tochterunternehmens tätig werden muss und hierbei Prüfungsergebnisse der Internen Revision des Tochterunternehmens berücksichtigen kann.

Principle 15

Principle 15: Regardless of whether internal audit activities are outsourced, the **board of directors** remains ultimately responsible for ensuring that the system of internal control and the internal audit function are adequate and operating effectively.

Principle 9: The bank's board of directors has the ultimate responsibility for ensuring that **senior management** establishes and maintains an adequate, effective and efficient internal control framework and internal audit function.

In Principle 15 sollte der Begriff „Senior Management“ analog zu Principle 9 Berücksichtigung finden, um potentielle Widersprüche bei der Auslegung des Papiers zu vermeiden.

Tz. 64

The head of internal audit should ensure that outsourcing **suppliers comply with the principles in the bank's internal audit charter**. To preserve independence, it is important to ensure that the supplier has not been previously engaged in a consulting engagement in the same area within the bank unless a reasonably long "cooling-off" period has elapsed. Similarly, as a best practice banks should not outsource internal audit activities to their own external audit firm.

Unserer Meinung nach genügt es nicht, lediglich die Charter der Internen Revision einzuhalten. Vielmehr sollten hier auch ein Verweis auf allgemeine Revisionsstandards (z. B. die IIA-Standards) Erwähnung finden.

Text-Vorschlag: The head of internal audit [...] internal audit charter and internal auditing standards, such as The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing (as far as not covered by the charter).

Tz. 68

The relationship between the supervisor and the internal audit function should be established in a structured and transparent way. In principle, the supervisor will initiate this relationship.

Wir gehen davon aus, dass mit der Formulierung „in a structured and transparent way“ die Einbindung der Organe sowie der Internen Revision gemeint ist.