International Federation of Accountants

529 Fifth Avenue, 6th Floor, New York, NY 10017
T + 1 (212) 286-9344 F +1 (212) 286-9570
www.ifac.org

January 9, 2015

Secretariat of the Basel Committee on Banking Supervision
Bank for International Settlements
CH-4002 Basel, Switzerland

Submitted via http://www.bis.org/bcbs/commentupload.htm

REVISED CORPORATE GOVERNANCE PRINCIPLES FOR BANKS (CONSULTATION PAPER) ISSUED BY THE BASEL COMMITTEE ON BANKING SUPERVISION

Dear Chair and Members of the Basel Committee,

The International Federation of Accountants (IFAC) values the opportunity to comment on the Basel Committee on Banking Supervision (BCBS)'s consultation paper, *Corporate Governance Principles for Banks*, outlining proposed enhancements to its *Principles for Enhancing Corporate Governance* ("the Principles").

Through its current membership of more than 175 professional accountancy organizations in 130 countries and jurisdictions, IFAC represents approximately 2.5 million accountants in public practice, industry and commerce, government, and education. As such, it aims to provide the perspective of the global accountancy profession.

Key matters are highlighted in this cover letter and additional, detailed comments are provided in the appendix. The members of the IFAC Professional Accountants in Business Committee[1] played a central role in the development of our response, as a large part of the constituencies the committee represents are involved in the operations of, or are stakeholders of, banks and other financial institutions.

General Comments on the Principles

IFAC believes good governance, risk management, and internal control are fundamental to the effective functioning of the world's capital markets and to organizations, including banks in particular, in creating sustainable value for their stakeholders.

Overall, IFAC welcomes enhancements to the Principles as they aim to strengthen risk governance, clarify the role of the board of directors in this regard, emphasize board competence, provide guidance for bank supervisors, and point out the influence of compensation systems.

---

[1] The Professional Accountants in Business Committee serves IFAC member bodies and professional accountants worldwide who work in commerce, industry, financial services, education, and the public and the not-for-profit sectors. Its aim is to promote and contribute to the value of professional accountants in business by increasing awareness of the important roles professional accountants play, supporting member bodies in enhancing the competence of their members, and facilitating the communication and sharing of good practices and ideas.

Focus on Desired Outcomes

However, the guidelines provided under the Principles are typically very detailed and prescriptive, which might promote a compliance culture rather than a values-based and behavioral route to better governance, risk management, and internal control across the organization. Arguably, such compliance efforts might draw attention and resources away from those areas where they should more appropriately be directed (i.e., "form over substance"). In that light we suggest that consideration be given to presenting the guidelines at a higher level, describing principles more focused on desired *outcomes* and less on detailed implementation guidance to achieve those outcomes.

Better Emphasize the First Line of Defense

The global financial crisis, and numerous corporate and organizational scandals and failures, have demonstrated the importance of having governance, risk management, and internal control fully integrated into all the facets of an organization. However, the revised Principles only provide limited information on how such integration can be achieved.

The comments in the introduction point out responsibilities of different parts of the organization and emphasize the importance of the "three lines of defense" model. However, the subsequent Principles and detailed guidelines pay little attention to the first line of defense, the business line, which is the most important line of defense. Instead, the proposed guidelines elaborate mainly on the risk management function (second line), compliance, and internal audit (third line). Illustrative in this respect is the fact that Principle 6, Risk Management, immediately jumps to the second line of defense, the risk management function, forgoing the first and more important line of defense (the business line).

Risk comes about primarily when organizations are trying to set and achieve their objectives. Risk is also best dealt with upfront—*before* a decision has been made or actions have been started—at the place and by the people where it arises, which is typically the business line. This includes the board and senior management managing risk while making strategic decisions and implementing them, as well as traders managing risk while engaging in financial transactions.

Therefore, IFAC suggests that the BCBS consider placing greater emphasis on the roles and responsibilities of the first line of defense and, where necessary, point to existing guidance (see below) that helps governing bodies, management, and staff assume and discharge their risk management duties in the most effective way.

Refer to Already Existing Standards and Frameworks

Contrary to most other governance codes—and different from, for example, the US Sarbanes-Oxley Act—the proposed Principles describe a separate and fairly detailed set of risk management and internal control terms, concepts, and guidelines rather than describing the broad outlines (or even better, the desired outcomes) and making reference to other existing international frameworks, standards, or guidelines in this area, such as the COSO frameworks or the International Organization for Standardization (ISO) Risk Management Standard. This potentially creates confusion for institutions that already have established formal risk management and internal control arrangements.

IFAC suggests either including references to these existing standards and frameworks, or at the very least ensuring that the various terms and concepts are aligned with them (see also the detailed comments in the appendix).

Manage Risk in Relation to the Objectives Where it Arises

Principles 6-8 discuss various aspects of risk management but with little reference to where risk comes about: while setting and achieving the organization's objectives. Such a disconnected approach might lead to a "siloed" form of risk management and an overemphasis on specific types of risks without a clear link how they, alone or in combination, affect the organization's objectives.

As risk is the effect of uncertainty on objectives,[2] the management of risk should primarily support an organization achieving its objectives, while being in compliance and avoiding surprises. Therefore, IFAC's view is that the focus of good governance, and thus these Principles, should primarily be on how organizations should properly set and achieve their objectives and then, from that perspective, how they should manage the risk that automatically comes with that.

Also, because most people in an organization, especially those in the first line, are primarily focused on doing their job well and achieving their objectives, establishing an explicit connection on how risk affects their jobs and their objectives makes them more inclined to also manage the related risk.

For example, subparagraph 121 rightly notes that banks should have risk management approval for new products and services, or the outsourcing of bank functions, which are often the source of governance or risk management failures. Ideally, however, the business line should be primarily responsible for managing the inherent risk and not the risk management function.

Similarly, IFAC believes that Principle 8 on risk communication might best be re-focused, as it encourages communication about risks separated from the bank's objectives and activities—which is where risk comes about—often in the form of disconnected "risk registers" and separate "risk paragraphs" in board and accountability documents. This is then often separated from the discussion on the bank's objectives and how it is envisaged that these objectives will be achieved, which can also lead to difficulties, for example, in preparing an effective integrated report.

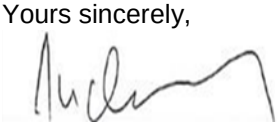
Detailed Comments

Detailed comments are included in the appendix to this response.

We hope you find our suggestions useful and constructive as you finalize the Principles.

Please do not hesitate to contact us should you wish to discuss any of the matters raised in this letter.

Yours sincerely,



Fayezul Choudhury
Chief Executive Officer

[2] See definition of risk in *ISO Standard 31000 Risk Management*.

APPENDIX

DETAILED COMMENTS ON THE REVISED CORPORATE GOVERNANCE PRINCIPLES FOR BANKS (CONSULTATION PAPER) ISSUED BY THE BASEL COMMITTEE ON BANKING SUPERVISION

Name: Fayezul Choudhury
Email: VincentTophoff@IFAC.org
Stakeholder group: Accountancy profession
Organization name: International Federation of Accountants (IFAC)
Industry sector: Not-for-profit
Geographical region: Global

Page 1 Glossary

As an overall comment on the definitions, IFAC believes that there is scope for the definitions included in the Principles to be better aligned with the definitions from COSO frameworks, the ISO 31000 Standard on Risk Management, and ISO Guide 73 Risk Management Vocabulary.

> *"Control functions: Those functions that have a responsibility independent from management to provide objective assessment, reporting and/or assurance. This includes the risk management function, the compliance function and the internal audit function."*

Risk assessment (and risk reporting) should be primarily the responsibility of the business line and, as such, should not be a separate control function.

A definition of "risk management function" should also be considered.

> *"Independent director: For the purposes of this paper, a member of the board who does not have any management responsibilities with the bank and is not under any other undue influence, internal or external, that would impede the board member's exercise of objective judgment."*

IFAC suggests that the BCBS should consider the following textual change to also exclude any significant shareholders from the definition of independent director: *"Independent director: For the purposes of this paper, a member of the board who does not have any management responsibilities with the bank, or represents a significant shareholder, and is not under any other undue influence, internal or external, that would impede the board member's exercise of objective judgment."*

> *"Internal control system: A set of rules and controls governing the bank's organisational and operational structure including reporting processes, and functions for risk management, compliance and internal audit."*

In this definition, an internal control system encompasses the functions for risk, whereas in most risk management publications—including IFAC's International Good Practice Guidance, *Evaluating and Improving Internal Control in Organizations*—internal control is a subset of risk management, as controls are used to manage risk.

Therefore, IFAC suggests that consideration be given to reversing these concepts in the definition. For example, refer to the definition of "risk capacity" where IFAC believes the order presented is correct.

Also, an internal control "*system*" implies a stand-alone system, separated from, or at least not fully integrated with, the bank's overall system of management. As the management of risk, including internal control, is an integral part of managing an organization, it would be better to speak about "internal control arrangements" or an "internal control framework" (or even better: "risk management framework" within which internal control automatically resides/is included).

> *"Risk culture: A bank's norms, attitudes and behaviours related to risk awareness, risk taking and risk management and controls that shape decisions on risks. Risk culture influences the decisions of management and employees during the day-to-day activities and has an impact on the risks they assume."*

There is debate about whether a "risk culture" exists as a separate concept, or is part of an organization's overall corporate culture, of which risk awareness or risk appetite is a part.

IFAC suggests considering making risk awareness an integral aspect of the organization's overall corporate culture, rather than aiming to define a specific/separate risk culture.

> *"Risk governance framework: As part of the overall corporate governance framework, the framework through which the board and management establish and make decisions about the bank's strategy and risk approach; articulate and monitor adherence to risk appetite and risk limits vis-à-vis the bank's strategy; and identify, measure, manage and control risks."*

Refer to the comments above on risk culture. IFAC's view is that the management of risk is an integral part of the governance framework and management of an organization, and as such, a specific/separate risk governance framework should not be defined.

> *"Risk management: The processes established to ensure that all material risks and associated risk concentrations are identified, measured, limited, controlled, mitigated and reported on a timely and comprehensive basis."*

IFAC suggests that the BCBS should consider aligning this important term with the ISO 31000 definition of risk management. In that respect, the definition would refer to "risk" (singular) rather than "risks"[3] (plural), as risk is the overall effect of uncertainty on the bank's objectives. In addition, it is not clear why risk in this definition should be limited, controlled, *and* mitigated.

IFAC suggests deleting these three words and use the word "managed" instead.

Also, the term "risk concentration" is not defined and unclear. IFAC suggests alignment with the ISO 31000 term "level of risk," defined as the "magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood."

> *"Risk profile: Point in time assessment of the bank's gross (ie before the application of any mitigants) or, as appropriate, net risk exposures (ie after taking into account mitigants) aggregated within and across each relevant risk category based on current or forward-looking assumptions."*

[3] The term "risks" is typically used to describe either the sources or the effects of risk, such as drunken driving and car crash.

It is not clear that a definition can aim to describe both gross and net risk exposures. A gross risk exposure is mainly a theoretical and often confusing concept, as a risk exposure will nearly always be partly mitigated by having certain controls in place. Therefore, it might be preferable to limit this definition to net risk exposure.

Furthermore, consideration might be given to aligning the term "net risk exposure" with the ISO term "residual risk," which is "the risk remaining after risk treatment"—often considered to be more meaningful and a better quantifiable measure.

Finally, the BCBS might consider whether it is appropriate to refer to a "risk category" as if risks are individual items (refer to previous comments). An alternative might be to use the term "sources of risk," preferably in combination with the objectives that might be affected by the risk exposure.

Other Paragraphs

> *"27. A fundamental component of good governance is a demonstrated corporate culture of reinforcing appropriate norms for responsible and ethical behaviour. These norms are especially critical in terms of a bank's risk awareness, risk-taking and risk management."*

This sentence is somewhat convoluted because it is unclear what exactly the fundamental component of good governance is—a culture of reinforcing norms?

Consideration might be given to rephrasing as "*A fundamental component of good governance is the establishment of a corporate culture in which appropriate norms for responsible and ethical behaviour are explicitly set, followed by all (including board and senior management), and reinforced. These norms are especially critical in terms of a bank's risk awareness, risk-taking, and risk management."*

> *"61. In jurisdictions where the chair is permitted to assume executive duties, the bank should have measures in place to mitigate the adverse impact on the bank's checks and balances of such a situation. These could include having a lead board member, senior independent board member or a similar position or having a larger number of non-executives on the board so as to provide effective challenge to executive board members."*

We believe that even in jurisdictions where the chair is permitted to assume executive duties, banks should voluntarily consider, or at least be encouraged to consider, the governance benefits of having the chair of the board be a non-executive and independent board member and/or not serve as the chair of any board committee.

Consideration might be given to including in paragraph 61 language explaining that for banks in such jurisdictions, having a non-executive chair is strongly recommended.

> *"68 ….receiving key audit reports and ensuring that senior management is taking necessary corrective actions in a timely manner to address control weaknesses, non-compliance with policies, laws and regulations and other problems identified by auditors and other control functions;"*

It is not clear why the guidance included in this paragraph focuses on control weaknesses and not on exposure to risk beyond the organization's risk appetite and risk limits. Furthermore, this is the only instance of the term "control weakness" being used in the Principles.

Consideration might be given to rephrasing to: *….receiving key audit reports and ensuring that senior management is taking necessary corrective actions in a timely manner to address exposures to risk beyond the organization's risk appetite and risk limits."*

> *"70. The risk committee of the board: should discuss all risk strategies on both an aggregated basis and by type of risk and make recommendations to the board thereon, and on the risk appetite.*

This paragraph introduces the undefined term "risk strategy," which in turn makes it unclear exactly what it is that the risk committee is expected to discuss. Additionally, consistent with previous comments, risk strategies should best be discussed (assessed?) in relation to the objectives or activities from where they arise rather than in isolation.

> *92. "Senior management should implement, consistent with the direction given by the board, risk management systems, processes and controls for managing the risks – both financial and non-financial – to which the bank is exposed and for complying with laws, regulations and internal policies.*
> *• This includes comprehensive and independent risk management, compliance and audit functions, as well as an effective overall system of internal controls.*
> *• Senior management should recognise and respect the independent duties of the risk management, compliance and internal audit functions and should not interfere in their exercise of such duties."*

This paragraph suggests that senior management's main responsibility with regard to risk is to implement risk management systems, processes, and controls for managing risks, especially with respect to the second and third line of defense. Arguably, this overlooks senior management's primary responsibility to actively manage the risk that arises in their decision making and subsequent execution and control.

IFAC reiterates its earlier suggestion that consideration be given to more strongly emphasizing the "first line of defense" role of senior management.

Additionally, the phrase "risk management systems, processes and controls for managing the risks" is introduced in this section, but none of the terms are defined or used elsewhere in the document (see also earlier comments regarding the use of the word system). It appears that elsewhere in the document the term "risk governance framework" is being used. In addition, "processes and controls for managing the risks" are already included in the overall management of risk.

IFAC suggests that the document should be reviewed for consistency with respect to the use of such terms.

> *Principle 6: "Risk management"*

IFAC suggests that the BCBS should consider changing the title of this section to "The risk management *function*" for greater clarity about the more limited content of this section, as risk management as a whole is a much broader concept than described here.

> *103. "The independent risk management function is a key component of the bank's second line of defence. This function is responsible for overseeing risk-taking activities across the enterprise. The independent risk management function (bank-wide and within subsidiaries) should have authority within the organisation to oversee the bank's risk management activities."*

As all activities in an organization are "risk-taking" activities, IFAC suggests deleting the sentence, "*This function is responsible for overseeing risk-taking activities across the enterprise,"* especially as the subsequent sentence appears to be making the same point.

> *103 "Key activities of the risk management function should include:*
> *• identifying material individual, aggregate and emerging risks;*
> *• assessing these risks and measuring the bank's exposure to them;"*

IFAC asserts that the activities described above are primarily the responsibility of the "first line", and not the "second line." The implication of describing the activities in this manner is that it might give the impression that those working in the front line don't have to worry about these activities, as they are supposedly the responsibility of the risk management function (i.e., the second line).

> *103 "Key activities of the risk management function should include: ongoing monitoring of the risk-taking activities and risk exposures to ensure they are in line with the board-approved risk appetite, risk limits and corresponding capital or liquidity needs (ie capital planning);"*

IFAC suggests that consideration might be given to emphasizing that monitoring risk-taking activities, as well as risk exposures, is primarily the responsibility of line management, especially as all activities in an organization—including or especially decision-making activities—are "risk-taking activities." In addition, the following textual change might be considered: *"Key activities of the risk management function should include: ongoing monitoring of the risk ~~taking~~ management activities and risk exposures to ensure they are in line with the board-approved risk appetite, risk limits, and corresponding capital or liquidity needs (i.e., capital planning)."*

> *103 "Key activities of the risk management function should include: influencing and, when necessary, challenging material risk decisions;"*

This paragraph introduces the undefined term "risk decision", which does not appear to be used elsewhere in the text of the document. This term is problematic as every decision involves risk. Consideration might be given to revising the text to say, "influencing and, when necessary, challenging decisions that give rise to material risk."

> *Principle 7: "Risks should be identified, monitored and controlled on an ongoing bank-wide and individual entity basis. The sophistication of the bank's risk management and internal control infrastructure should keep pace with changes to the bank's risk profile, to the external risk landscape and in industry practice."*

IFAC suggests that the terms used in the opening sentence of this Principle should be re-ordered to say, "*Risk~~s~~ should be identified, evaluated/assessed, ~~monitored~~ controlled (or better: "managed"), and ~~controlled~~ monitored."* As noted earlier, consideration should be given to using the singular "risk", rather than "risks".

Additionally, IFAC notes that wording used in the description of the Principle is inconsistent with how the risk management process is described in other paragraphs. For example, in paragraph 116, the term "to identify and assess risk" is used, and in paragraph 117 the term "to address and mitigate risks." IFAC

believes that the BCBS should consider ensuring greater consistency in the use of various terms throughout the document, and preferably aligning the definitions of these terms with generally accepted risk management guidelines, such as COSO or ISO.

This description of Principle 7 introduces undefined wording "risk management and internal control infrastructure" and "risk landscape" that do not appear to be used elsewhere in the document.

Finally, IFAC believes that the "how-to" risk management guidance in section 7 might be better aligned with the already existing standards and frameworks, such as COSO and ISO 31000.

> *113. "Internal controls are designed, among other things, to ensure that each key risk has a policy, process or other measure, as well as a control to ensure that such policy, process or other measure is being applied and works as intended."*

IFAC notes that "internal controls" is not a defined term in the document, and this paragraph does not seem to provide a clear description. As noted previously, IFAC suggest that consideration be given to aligning terms issued in the document to generally accepted definitions.

> *120. "In addition to identifying and measuring risk exposures, the risk management function should evaluate possible ways to mitigate these exposures. In some cases, the risk management function may direct that risk be reduced or hedged to limit exposure. In other cases, such as when there is a decision to accept or take risk that is beyond risk limits (ie on a temporary basis) or take risk that cannot be hedged or mitigated, the risk management function should report and monitor the positions to ensure that they remain within the bank's framework of limits and controls or within exception approval. Either approach may be appropriate depending on the issue at hand, provided that the independence of the risk management function is not compromised."*

As noted in previous comments, IFAC strongly believes that it should be primarily the "first line" of defense's responsibility to identify and measure risk exposures, and evaluate possible ways to mitigate these exposures, and not the risk management function ("second line"). The same applies to directing that risk be reduced or hedged, or taking risk, especially as the risk management function should then have to "report and monitor [its own] positions".

> *121 "Banks should have risk management and approval processes for new or expanded products or services, lines of business and markets, as well as for large and complex transactions that require significant use of resources or have hard-to-quantify risks. Banks should also have review and approval processes for outsourcing bank functions to third parties. The risk management function should provide input on risks as part of such processes and on the outsourcer's ability to manage risks and comply with legal and regulatory obligations. Such processes should include:*
> *• A full and frank assessment of risks under a variety of scenarios, as well as an assessment of potential shortcomings in the ability of the bank's risk management and internal controls to effectively manage associated risks.*
> *• An assessment of the extent to which the bank's risk management, legal and regulatory compliance, information technology, business line and internal control functions have adequate tools and the expertise necessary to measure and manage related risks.*

> *• If adequate risk management processes are not in place, a new product, service, business line or third-party relationship or major transaction should be delayed until the bank is able to appropriately address the activity.*
> *• There should also be a process to assess risk and performance relative to initial projections and to adapt the risk management treatment accordingly as the business matures."*

Even though IFAC agrees that, "The risk management function provides input on risks as part of such processes and on the outsourcer's ability to manage risks and comply with legal and regulatory obligations," the paragraph might be more explicit that these activities are also primarily a responsibility of the first line. This is especially true for the first bullet point ("full and frank assessment of risks") and the fourth bullet point ("process to assess risk and performance relative to initial projections and to adapt the risk management treatment accordingly").

> *Principle 8: "An effective risk governance framework requires robust communication within the bank about risk, both across the organisation and through reporting to the board and senior management."*

IFAC suggests that consideration be given to expanding the breadth of this Principle to read: "An effective risk governance framework requires robust communication and consultation with~~in the bank~~ both internal and external stakeholders about risk, (both across the organisation and through reporting to the board and senior management)."[4]

Consistent with this suggestion, the guidance under this Principle would then also need to be expanded to "communication and consultation" as well as "with internal and external stakeholders."

> *125. "Ongoing communication about risk issues, including the bank's risk strategy, throughout the bank is a key tenet of a strong risk culture. A strong risk culture should promote risk awareness and encourage open communication and challenge about risk-taking across the organisation as well as vertically to and from the board and senior management. Senior management should keep control functions informed of management's major plans and activities so that the control functions can properly assess the risks."*

This paragraph introduces an undefined term "risk issues".

IFAC suggests considering changing the text to: "Ongoing communication and consultation about the importance of the effective management of risk…" (Also refer to earlier comments about the term "risk culture.")

Furthermore, the guidance that, "*Senior management should keep control functions informed of management's major plans and activities so that the control functions can properly assess the risks,"* might inadvertently give the impression that the control functions are primarily responsible for the assessment of risk(s), and not senior management itself.

[4] The second part of this Principle is actually an example and should be better placed in the subsequent guidance, than in the principle itself.

IFAC suggests considering changing the sentence to: "*Senior management should ~~keep~~ actively communicate and consult with the control functions ~~informed of~~ on management's major plans and activities so that the control functions can appropriately ~~assess the risks~~ assume their responsibilities.*"

> *130. "Banks should avoid organisational "silos" that can impede effective sharing of information across an organisation and can result in decisions being taken in isolation from the rest of the bank."*

IFAC agrees with the notion outlined in this paragraph and notes that having various risk management functions might inadvertently create the organizational silos that one is trying to prevent. This may result in decisions being taken in isolation from the risk that is involved in those decisions, as well as risk being identified and managed in isolation from the decision where it arose, and possibly also only after the decision already has been made.

> *Principle 9: "The bank's board of directors is responsible for overseeing the management of the bank's compliance risk. The board should approve the bank's compliance approach and policies, including the establishment of a permanent compliance function."*

IFAC believes the undefined term "compliance risk" may be confusing to readers, and suggests that consideration be given to wording such as, *"The bank's board of directors is responsible for overseeing the management of the bank's compliance ~~risk~~ objectives."*

> *132. "Compliance starts at the top. It will be most effective in a corporate culture that emphasizes standards of honesty and integrity and in which the board of directors and senior management lead by example."*

This paragraph discusses "a corporate culture that emphasizes standards of honesty and integrity," whereas an earlier paragraph (paragraph 27) discusses a "corporate culture of reinforcing appropriate norms for responsible and ethical behaviour." While the two descriptions are similar, IFAC suggests that more consistency in this use of this and other such terms throughout the document would improve understanding and use.

> *135. "The compliance function should advise the board and senior management on compliance laws, rules and standards, including keeping them informed of developments in the area. It should also help educate staff about compliance issues, act as a contact point within the bank for compliance queries from staff members, and provide guidance to staff on the appropriate implementation of compliance laws, rules and standards in the form of policies and procedures and other documents such as compliance manuals, internal codes of conduct and practice guidelines."*

While IFAC broadly agrees with the responsibilities described for the compliance function, as noted in previous comments, it believes that the guidance should better emphasize that—even though there might be a compliance function active within the bank—the "first line" is still primarily responsible for ensuring overall compliance in their decision making and subsequent execution.

> *Principle 10: "The internal audit function provides independent assurance to the board and supports board and senior management in promoting an effective governance process and the long-term soundness of the bank. The internal audit function should have a clear mandate, be accountable to the*

board, be independent of the audited activities and have sufficient standing, skills, resources and authority within the bank.

IFAC suggests that the BCBS consider better aligning this chapter to, or including more references to, the International Professional Practices Framework of the Institute of Internal Auditors (IIA), especially as paragraph 142 already explicitly refers to the standards of the IIA. For example, with respect to the definition of internal audit, which is not currently included in the document, and other terms and concepts relevant to internal auditing.

In addition, IFAC believes that good governance includes both appropriate internal and external audit. Therefore, we recommend that the BCBS considers referring to its recent guidance *External Audits of Banks*, which sets out guidelines regarding the audit committee's responsibilities in overseeing the external audit function, and the prudential supervisor´s relationships with external auditors of banks and the audit oversight body.

Principle 11: "The bank's compensation structure should be effectively aligned with sound risk management and should promote long term health of the organisation and appropriate risk-taking behaviour."

IFAC suggests that consideration be given to broadening this Principle to: *"The bank's compensation structure should be effectively aligned with sound corporate governance, including risk management, and should promote long term health of the organisation and appropriate risk-taking behaviour."*

Furthermore, this appears to be the only instance that the concept of long term health is used, whereas terms such as "long-term performance" and "long-term soundness" are used in other parts of the document. IFAC suggests that the BCBS consider consistency in the use of such terms throughout the document.