Dr. Mark Lawrence
Managing Director, Mark Lawrence Group

Mr. Harrison Young

January 16, 2015

Mr. William Coen
Secretary General
Basel Committee on Banking Supervision
Centralbahnplatz 2
CH-4051 Basel
Switzerland

RE: Response to BCBS Consultative Document: *Guidelines Corporate Governance Principles for Banks*

Dear Mr. Coen,

The authors[1][2] appreciate the opportunity to comment on the Basel Committee on Banking Supervision (BCBS) October 2014 consultation paper: Guidelines - Corporate Governance Principles for Banks (the *"Guidelines"*).

We congratulate the committee on the high quality and comprehensive and detailed nature of the *Guidelines*. We believe the *Guidelines* will be seen in years to come as an important document – a compendium of good and emerging best practices in risk management and governance for banks which reflects the substantial evolution in those areas following the Global Financial Crisis. There is little in the document we disagree with. While there are some gaps we would like to see filled, it is admirably comprehensive. Every chief executive, chief risk officer, board chairman and director should have a copy on the corner of his or her desk and read it through a couple of times a year.

---

[1] Dr. Lawrence has been working in the field of risk management since becoming a foundation member of the market risk group at Merrill Lynch in New York in 1987. He received a PhD in mathematics from the University of Wisconsin. He was Chief Risk Officer of ANZ Banking Group in Melbourne from 1999 to 2004. In recent years he has worked extensively with a variety of financial institutions in both developed and emerging markets on various risk management matters, with particular emphasis on implementing risk appetite and strengthening risk culture. He was co-chairman of the Institute of International Finance's Risk Management Working Group in 2009 and its Working Group on Risk Appetite in 2010-2011. The comments that follow represent his personal views and not those of any organization. He can be reached at mark@marklawrencegroup.com

[2] Mr. Young has been a corporate lending officer, an investment banker specializing in banks, a senior officer of the Federal Deposit Insurance Corporation in Washington, a member of the Court of Directors of the Bank of England and a non-executive member or chairman of various corporate and not-for-profit boards. He helped establish financial institutions in Bahrain and Beijing and has advised twelve governments on financial system matters. He has been a director, and chairman of the risk committee, of Commonwealth Bank of Australia for seven years, but the opinions expressed herein are his own. He can be reached at harrison.h.young@gmail.com

In this response we have chosen to focus our comments primarily in the areas of risk governance and risk management and control. Certainly, the *Guidelines* are closely aligned with various best-practice recommendations from industry on these topics, post-crisis[3]; in general, they are also quite well-aligned with our own views on these topics.

We begin our response with some general comments. Subsequently, we offer some detailed comments and suggested amendments to selected elements of the *Guidelines*.

General comments on the *Guidelines*

The *Guidelines* are aspirational. This is true at two levels. From an organizational perspective, the risk management framework depicted will take a long time to put in place. It is dangerous to generalize, because banks differ so much in their complexity, how deep their problems are and how much work they have done already, but to make our point, the journey the *Guidelines* send the industry on will take most banks another five to ten years, not two or three. We believe the document should provide a warning to this effect. You invest differently – in software, in people, in process development – depending on the time scale of a project.

At the level of individual non-executive directors, the *Guidelines* will look to many like a new job description. It tells directors they should be "actively engaging in the major matters of the bank and keeping up with material changes in the bank's business and the external environment as well as acting in a timely manner to protect the long-term interests of the bank."[4] Paragraph 23 explains what this entails. It uses the word, "oversee" several times, but at least some directors will feel that what is described is awfully close to management – that the *Guidelines* represent a change from the governance model they signed up for.

It would be possible for directors and supervisors to have an unproductive argument about this – starting with definitions and moving on to workload. Officials would no doubt assert that the *Guidelines* mandate nothing fundamentally new. Directors would respond that their to-do list has gotten a lot longer. Suffice it to say that the *Guidelines* advocate a way of running a bank that involves a lot of homework for directors – especially new ones – and an on-going dialogue between board and management regarding every form of risk-taking the institution engages in.

We support this approach, believing that effective bank governance requires an engaged board. But there is bound to be debate regarding the number of days per month "engagement" should entail. Workaholics aren't always good directors. Many of the best believe they have a duty to remain objective, which is to say, not *too* engaged – and in any event have other commitments.

Boards will deal with the *Guidelines* the way all successful executives cope. They will prioritize, digging into some matters and waving others through without much discussion. As an

---

[3] See for example: Institute of International Finance (2008) *"Final Report of the IIF Committee on Market Best Practices: Principles of Conduct and Best Practice Recommendations",* https://www.iif.com/file/7102/download?token=zVgadpJM, Institute of International Finance (2009) *"Reforms in the Financial Services Industry: Strengthening Industry Practices for a More Stable System",* https://www.iif.com/file/7071/download?token=w6PvaJA3, and Institute of International Finance (2011) *"Implementing Robust Risk Appetite Frameworks to Strengthen Financial Institutions"* https://www.iif.com/publication/regulatory-report/strengthening-approaches-risk-appetite-and-risk-it-should-be-key-risk & https://www.iif.com/file/7075/download?token=NOwe4NwK

[4] *Guidelines,* paragraph 22.

aspirational document, the *Guidelines* have nothing to say about priorities. Arguably they should, however. Banks are commercial entities and have to make choices. The *Guidelines* risk having diminished impact if they are seen as too distant from commercial realities.

In the wake of the Global Financial Crisis, supervisors have increasingly focused on the performance of boards. Why, it is asked, were some boards able to sidestep catastrophe while others – often with similar business models and operating in the same markets – did not? Perhaps their boards made the difference, and if so, how? What should all boards therefore be doing?[5] The answers in the *Guidelines* are primarily administrative – determinations boards must make, organizational arrangements that must exist, *papers* that must exist. A casual reader of the *Guidelines* could get the impression that with *enough* governance, risk management will take care of itself. In our experience, this is not the case. When banks make the right choices regarding risk, more is going on than procedural obedience. Good *judgments* are being made. The industry and the official sector both would benefit from a conversation about how that can be caused to happen.

Prioritization is a matter of judgment, of course. So as a conversation-starter about how good judgments get made – and to address the question of how busy boards should prioritize – we offer the following road map:

1. Gather the board or the risk committee and some of senior management – the group should be as small as possible – somewhere away from the office.
2. Write or adopt descriptions of the business models of the major divisions and of the group as a whole. Limit the number of businesses you look at. Make the descriptions concrete and simple. Make sure everyone in the room understands the business models.
3. Identify the risks inherent in those business models. Express surprise that there are some you hadn't thought about recently.
4. Describe how those risks are measured and assessed, including both quantitative and qualitative factors. Are your risk reports complete, accurate, timely, understandable and actually used? Describe in laymen's terms your most important quantitative risk models. Do they seem to work – *i.e.*, how good are their predictions?
5. Describe how risks are currently managed. Who makes transaction decisions? What policies guide them? What role does technology play? What role does culture play? How do you decide at budget time how much to spend on risk management capabilities?
6. Talk about remote but plausible contingencies. When was the last time this business got hammered? What stress tests have been done and what insights did they deliver?
7. Decide which businesses you are comfortable with and which ones worry you. Investigate the latter. Look for hidden correlations throughout the group. What parts of the bank's risk appetite statement, limit structure or policy framework may need review?

We wish to make three points. The first – illustrated by this imaginary off-site agenda – is that you should start with specifics, not with an abstract risk appetite statement. A sensible risk management framework, in all its aspects, flows from deep understanding of your business. The answers to these diagnostic questions – and the quality of the discussion – tell a board or risk committee a great deal about what its priorities should be.

---

[5] See for example the speech *"The Importance of Good Governance"* delivered in February of 2013 by John Laker, chairman of the Australian Prudential Regulatory Authority
http://apra.gov.au/Speeches/Pages/The-importance-of-good-governance.aspx

The second point should be obvious – that *conversation* is an essential risk management tool. It's the way to make judgments. Good conversations are both disciplined and open-ended. The evidence needs to be in the room. The right people need to be in the room. Challenge is constructive. There needs to be enough time.

Supervisors are increasing their engagement with boards, committees and chairs – a trend the *Guidelines* support and we applaud. Our third point is that directors themselves have work to do on understanding boardroom dynamics.

The whole notion of board oversight is premised on a belief, which we share, that small, diverse but cohesive groups best harness human intuition to make important judgments. Unfortunately, such groups can also make very *bad* judgments. Some brilliant, highly accessible books have been published in the past few years that help explain these phenomena.[6] Behavioral psychology offers insights about group decision-making as important to directors as a working knowledge of finance, accounting and corporate law. The *Guidelines* need not explore this topic but they should flag it.

Specific comments and suggested amendments to the *Guidelines*

We offer the following additional comments and suggest some specific amendments to the *Guidelines* text.

Glossary

- **Risk capacity:** we suggest replacing the word "measures" with the word "capabilities"

Principle 1

- Paragraph 33: In practice, while the process of developing the risk appetite framework and statement is often led by management, our experience and that of the industry[7], has shown that active engagement by the board is essential. Hence it may be clearer to commence the paragraph with the following text: "The board should take an active role in the risk appetite development process, which may be led by management, and ensuring its alignment…"

Principle 3

- Paragraph 68, 7th bullet: It is stated that the Audit Committee is responsible for reviewing "third-party opinions on the design and effectiveness of the risk governance framework and internal control system." We believe that more commonly the Risk Committee

[6] For example, Daniel Kahneman's *Thinking, Fast and Slow (2011),* and especially Cass Sunstein and Reid Hastie's *Wiser: Getting Beyond Groupthink to Make Groups Smarter* (2015)

[7] See for example: Institute of International Finance, (2011), *"Implementing robust risk appetite frameworks to strengthen financial institutions",* pp 12-13 https://www.iif.com/file/7075/download?token=NOwe4NwK

would have this responsibility, in some cases both committees may wish to review such third party opinions. Some flexibility is needed here with respect to the boundary and potential overlap between the responsibilities of these committees, in the spirit of paragraph 74. Similarly, it is common for the Risk Committee to have oversight of compliance, especially in those banks where compliance function is part of the risk management function within management (as is common), and where no separate Compliance or Ethics Committee exists (paragraph 76).

- *Responsibilities of the Risk Committee for oversight of quantitative risk models and internal rating systems:* Paragraphs 70 – 74 of the *Guidelines* are well-written, however we are surprised that they are silent regarding the Risk Committee's responsibility for oversight of statistical risk models and quantitative measures. These are used in an essential way by bankers to understand the performance and risk characteristics of products and asset portfolios, to decide which transactions to originate, in stress testing and scenario analysis, and in the process of assessing capital adequacy.

  While recognizing that different banks have greater or lesser reliance on analytical models within their risk management frameworks and processes, reflecting their different business models and levels of sophistication, our view is that it is generally neither necessary nor appropriate for directors to personally grapple with the detailed underpinnings of statistical risk models from quantitative finance. Nevertheless, we believe that members of the risk committee should have an intelligent laymen's understanding of the most important quantitative risk models – including what they are used for, and how they work. As a guide, we suggest that this understanding should include the following points, in a manner which is proportional and takes account of the business model and complexity of the risk-taking activities:

  - Which statistical risk models and internal rating systems are most important and central to the processes of transaction approval, portfolio monitoring, risk reporting and control, and provisioning, for each major business line
  - Which models are used to generate the risk numbers and forecasts that are contained in the risk reports which are presented to the committee
  - The main design features and material assumptions embedded in the most important models – for example, are credit models providing "Through the cycle" or "Point in time" estimates (and what do these terms mean[8])?
  - Material model constraints and weaknesses
  - How well the models are performing – i.e., how closely the realized risk outcomes are aligned with the estimates that were produced by the models, and how effectively management is able to use the models to forecast risk outcomes in each business line
  - How management monitors the performance of the models, to ensure that they are performing as intended, and the steps that are taken by management when risk models lose their predictive power

  We believe that the *Guidelines* would be enhanced by the inclusion of some guidance regarding the responsibilities of the Risk Committee in this area, to complement the guidance to management which is contained in paragraph 117.

[8] See for example, Institute of International Finance (2009) *"Reforms in the Financial Services Industry: Strengthening Industry Practices for a More Stable System",* Appendix V
https://www.iif.com/file/7071/download?token=w6PvaJA3

Principle 6

- Paragraph 107: The second sentence of paragraph 107 suggests that the board takes the lead in developing the bank's risk appetite and RAS – however it is also common for this process to be led by management (see the earlier comment for paragraph 33). Additionally, the first sentence should be expanded to provide extra clarity regarding the CRO's lead responsibility for ongoing strengthening of the bank's risk management capabilities. Accordingly, we suggest commencing the paragraph with the following text: "The CRO has primary responsibility for overseeing the development and implementation of the bank's risk management function. This includes the ongoing strengthening of staff skills and enhancements to risk management systems, policies, processes, quantitative models, and reports as necessary to ensure that the bank's risk management capabilities are sufficiently robust and effective to fully support its strategic and growth objectives, and all of its risk-taking activities. The CRO is responsible for supporting the board in its engagement with and oversight of the development of the bank's risk appetite and RAS and for translating the risk appetite into a risk limits structure."

- *Responsibilities of the CRO:* Paragraph 107 provides a thoughtful discussion of the responsibilities of the CRO. However, the CRO usually has a number of other important responsibilities, in addition to those listed in paragraph 107. These typically include, for example:

    - Lead responsibility for ongoing strengthening of the bank's risk management capabilities (see discussion above)
    - Staying abreast of key developments in the evolution of industry best practices in risk management, and of regulatory requirements regarding specific risk management practices and related mandatory reporting requirements
    - Organizing education sessions for the board and Risk Committee about risk management matters, including specialist or technical topics (e.g., risk appetite, risk culture, models)
    - Providing specialist risk management expertise to board and senior management, as necessary
    - Leading the ongoing development and evolution of the RAS
    - A defined role in the independent oversight and approval of internal risk rating systems and other risk models
    - A clearly defined role - usually as either member or chair - on all relevant internal, senior management risk committees (for credit, market, liquidity, operational and compliance risks, etc.)
    - A clearly defined role and authority with regard to the evolution and approval of new or changed risk policies, and new products
    - A special responsibility to identify and communicate with senior management and the Board regarding new or emerging risks, including risk concentrations and any risks which are growing rapidly or changing

    We believe that the *Guidelines* should be augmented to include these examples of typical additional CRO responsibilities, possibly in a footnote similar in spirit to footnote 19, which we support. Additional detailed discussion and recommendations regarding the

responsibilities of the CRO may be found in the July 2008 report of the IIF Committee on Market Best Practices[9].

Principle 7

We appreciate the very high quality of the thorough and detailed discussion of this principle in paragraphs 110 – 124 relating to risk identification, monitoring and controlling.

- Paragraph 113: The first sentence of this paragraph regarding internal controls is not fully clear. We propose the following revision: "For each key risk, there is an applicable policy framework including limits, clearly defined approval authorities for staff and approved processes which must be followed, a set of specified measurement tools and models which are approved for use in prescribed circumstances, and appropriate reporting requirements to ensure adequate transparency and understanding of risks. Internal controls are designed, among other things, to ensure that these elements exist and are being applied effectively and work as intended. As such, internal controls help ensure process integrity…"

Principle 9

- Paragraph 136: The text at the start of the paragraph should be amended to read as follows: "The compliance function is independent from business or line management and provides separate reporting…"

As noted in paragraph 40, the compliance function is part of the "second line of defence". Depending upon the organizational structure, it may either be part of the risk management function, or separate from it. In any case, since 100% compliance with all laws, regulations and internal policies is in practice very difficult to achieve, it is crucially important for banks to understand very well the various specific risks associated with non-compliance in these areas, i.e. "compliance risks". In our experience, risk management disciplines can be effectively applied in this area. As noted in paragraph 72, the Risk Committee should have oversight of these risks, which – as recent experience has demonstrated - can be substantial.

Principle 11

- Paragraph 149: We strongly support this paragraph and propose to add the following additional sentence at the end: "In particular, it is important to ensure that incentives embedded within compensation structures do not incentivize staff to take excessive risks, i.e. risks outside the boundaries of approved risk appetite."

- Paragraph 150: In a similar spirit, we suggest to slightly extend the list of examples at the end of the penultimate sentence of this paragraph as follows: "Banks should ensure that variable compensation is adjusted to take into account the full range of current and

9 Institute of International Finance (2008) *"Final Report of the IIF Committee on Market Best Practices: Principles of Conduct and Best Practice Recommendations",* pp 36 – 38
https://www.iif.com/file/7102/download?token=zVgadpJM

potential risks an employee takes as well as realized risks, including breaches of risk appetite, limits, internal procedures or legal requirements."

Principle 13

- Paragraph 163: This paragraph begins with the sentence "As part of their evaluation of the overall corporate governance in a bank, supervisors should also endeavor to assess the governance effectiveness of the board and senior management, especially with respect to the risk culture of the bank", and continues with further explanation and guidance. We welcome the intent of this paragraph, but note the special difficulties and challenges involved. Further detailed discussion of the difficulties and challenges for supervisors to assess risk culture (including a number of specific recommendations in this regard) is contained in the final report of a training workshop for major bank supervisors in APEC economies that was held in Shanghai in May 2013[10].

Conclusion

The draft *Guidelines* articulate a high standard, to which all banks should aspire. As reflected in our comments above, we recommend the document include an acknowledgment that approaching that standard will require a sustained commitment over a number of years. Indeed, building a strong risk governance and management framework is a task that is never really finished. It will be important for boards to set realistic targets for management and to prioritize their own efforts.

It is hoped that these comments will be helpful to the Committee's further deliberations on this topic.

Sincerely,

Dr. Mark Lawrence

Mr. Harrison Young

Managing Director,
Mark Lawrence Group

[10] Final report of APEC training workshop: *"Enhancing Supervision of Financial Institutions' Risk Appetite Frameworks"* (2013) http://publications.apec.org/publication-detail.php?pub_id=1472