Below, the detailed comments on the Basle Committee on Banking Supervision, Consultative Document Guidelines : Corporate governance principles for banks by ECIIA

Page	Text of consultation paper	Suggested version (plus rationale given)
1	**Glossary** … 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. …	**Glossary** **…** Internal control system: A set of rules and controls governing the bank's organisational and operational structure including reporting processes, and functions for e.g. risk management and~~,~~ compliance ~~and internal audit~~. The internal audit function is responsible for independently reviewing the internal control system. … **Rationale:** Clarification to make it coherent with e.g. # 104. To avoid misinterpretations the different role of internal audit in regard to risk management and compliance should be stated clearly.
3	2. Corporate governance determines the allocation of authority and responsibilities by which the business and affairs of a bank are carried out by its board and senior management, including how they: • set the bank's strategy and objectives; • select and oversee personnel; • operate the bank's business on a day-to-day basis; • protect the interests of depositors, meet shareholder obligations, and take into account the interests of other recognised stakeholders; • align corporate culture, corporate activities and behaviour with the expectation that the bank will operate in a safe and sound manner, with integrity and in compliance with applicable laws and regulations; and • establish control functions.	2. Corporate governance determines the allocation of authority and responsibilities by which the business and affairs of a bank are carried out by its board and senior management, including how they: • have been selected / elected; • set the bank's strategy and objectives; • select and oversee personnel; • operate the bank's business on a day-to-day basis; • protect the interests of depositors, meet shareholder obligations, and take into account the interests of other recognised stakeholders; • align corporate culture, corporate activities and behaviour with the expectation that the bank will operate in a safe, ~~and~~ sound and ethical manner, with integrity and in compliance with applicable laws, ~~and~~ regulations and codexes; ~~and~~ • act and communicate in a transparent manner; and • establish control functions.

		Rationale: Adding selection of board and senior mgt. to make it coherent with # 23 and Principle 2 + 12. Adding ethics to make it coherent with # 27. Adding transparency in coherence with Principle 12.
4	11. The increased focus on risk and the supporting governance framework includes identifying the responsibilities of different parts of the organisation for addressing and managing risk. Often referred to as the "three lines of defence", each of … … The compliance function is also deemed part of the second line of defence. The internal audit function …	11. The increased focus on risk and the supporting governance framework includes identifying the responsibilities of different parts of the organisation for addressing and managing risk~~,~~ o~~O~~ften referred to as the "three lines of defence", each of … … The compliance function is also ~~deemed~~ part of the second line of defence. The internal audit function … **Rationale:** - orthography - avoidance of misinterpretation.
8	28. In order to promote a sound corporate culture, the board should take the lead in establishing the » tone at the top » by : • setting and adhering to corporate values for itself, senior management and other employees that create expectations that all business should be conducted in a legal and ethical manner; • promoting risk awareness within a strong risk culture,conveying the board's expectation that it does not support excessive risk taking and that all employees are responsible for helping ensure that the bank operates within the agreed risk appetite and risk limits; • ensuring that appropriate steps are taken to communicate throughout the bank the corporate values, professional standards or codes of conduct it sets, together with supporting policies and • ensuring that employees, including senior management, are aware that appropriate disciplinary or other	28. In order to promote a sound corporate culture, the board should ~~take the lead in~~ assume overall responsibility for establishing and ensuring compliance with the » tone at the top » by : • setting and adhering to corporate values for itself, senior management and other employees that create expectations that all business should be conducted in a legal and ethical manner; • establishing the risk appetite for the organisation, giving clear limits to acceptable behaviour on risk; • promoting risk awareness within a strong risk culture, conveying the board's expectation that ~~it does not support excessive risk taking and that~~ all employees are responsible for helping ensure that the bank operates within the agreed risk appetite and risk limits; • ensuring that appropriate steps are taken to communicate throughout the bank the corporate values, professional standards or codes of

	actions will follow unacceptable behaviours and transgressions.	conduct it sets, together with supporting policies; ~~and~~ • ensuring that employees, including senior management, are aware that appropriate disciplinary or other actions will follow unacceptable behaviours and transgressions and~~.~~ • seeking objective assurance that the „tone at the top" is properly reflected in actions and decisions throughout the organisation. **Rationale** Internal audit is tasked to include in its scope three different aspects of corporate culture namely the risk and controle culture of the organisation, the customer facing culture and the design and operating effectiveness of policies and processes to ensure that they are in line with the objectives, risk appetite and values of the organisation.
8.	30. The Bank's corporate values should recognise the critical importance of timely and frank discussion and escalation of problems to higher levels within the organisation. • Employees should be encouraged and able to communicate, confidentially and without the risk of reprisal, legitimate concerns about illegal, unethical or questionable practices. This can be facilitated through a well communicated policy and adequate procedures and processes, consistent with national law, which allow employees to communicate material and bona fide concerns and observations of any violations in a confidential way (eg whistle blower policy). This includes communicating material concerns to the bank's supervisor. • There should be direct or indirect communications to the board (eg through an independent audit or compliance process or through an ombudsman independent oft he	30. The Bank's corporate values should recognise the critical importance of timely and frank discussion and escalation of problems to higher levels within the organisation. • Employees should be encouraged and able to communicate, confidentially and without the risk of reprisal, legitimate concerns about illegal, unethical or questionable practices. This ~~can~~should be facilitated through a well communicated policy and adequate procedures and processes, consistent with national law, which allow employees to communicate material and bona fide concerns and observations of any violations in a confidential way (eg via an internal wistleblower mechanism independent of management or an esternal wistleblowing service~~whistle blower policy~~). This includes communicating material concerns to the bank's regulatory supervisor. • ~~There should be direct or indirect communications to the board (eg~~

	internal „chain of command“) • The board should determine how and by whom legitimate concerns shall be investigated and addressed by an objective independent internal or external body, senior management and/or the board itself.	~~through an independent audit or compliance process or through an ombudsman independent oft he internal „chain of command“)~~ The board, ideally a named independent director, should take overall responsibility for the oversight of the whistleblowing policy and mechanisms, seeking independent assurance that they are working effectively, and ensuring that senior management address legitimate issues that are raised. • The board should determine how and by whom legitimate concerns shall be investigated and addressed, for example by an objective independent internal and external body~~, senior management and/or the board itself~~ and ensure that internal audit is informed of the results. **Rationale** To ensure that the mechanism works effectively, the responsibility of the board must be clear : seeking independent assurance, having the oversight of the process and the results (and not the Senior Management). Whistleblowing hotspots are important indicators for internal audit of potential issues and internal audit must be informed about the whistleblowing alerts.
10	39. The second line of defence includes an independent and effective risk management function…	39. The second line of defence includes, amongst others, an independent and effective risk management function… **Rationale:** Addendum necessary, as the second line of defence might comprise quite a few more functions and more than the often quoted risk management and compliance (e.g. controlling, quality control etc.).
10	41. The third line of defence consists of an independent and effective internal audit function. Among other things, it provides independent review and assurance on the	41. The third line of defence consists of an ~~independent and~~ effective internal audit function independent of executive management. Among other things, it provides

	quality and effectiveness of the bank's risk governance framework including links to organisational culture, as well as strategic and business planning, compensation and decision-making processes. Internal auditors must be competent and appropriately trained and not involved in developing, implementing or operating the risk management function (see Principle 9).	independent review and objective assurance on the quality and effectiveness of the bank's internal control system, the first and the second line of defence and the risk governance framework including links to organisational culture, as well as strategic and business planning, compensation and decision-making processes. Internal auditors must be competent and appropriately trained and not involved in developing, implementing or operating the risk management function (see Principle 9). **Rationale:** It should be clarified that the third line of defence reviews the work of the second line and gives assurance about their work. The important feature about internal audit's independence is that it is independent of executive management and can therefore give objective assurance to the board and its committee.
10.	42. The board should ensure that the risk management, compliance and audit functions are properly positioned, staffed and resourced and carry out their responsibilities independently and effectively. In the board's oversight of the risk governance framework, the board should regularly review policies and controls with senior management and with the heads of the risk management, compliance and audit functions to identify and address significant risks and issues, as well as determine areas that need improvement.	42. The board should ensure that the risk management, compliance and internal audit functions are properly positioned, staffed and resourced and carry out their responsibilities independently, objectively and effectively. In the board's oversight of the risk governance framework, the board should regularly review policies and controls with senior management and with the heads of the risk management, compliance and internal audit functions to identify and address significant risks and issues, as well as determine areas that need improvement. **Rationale** Same as for point 41
10	43. The board should select the CEO and may select other key members of senior management, as well as the heads of the control functions.	43. The board should select the CEO and may select other key members of senior management, as well as the heads of the control functions and internal audit. **Rationale:** Addition needed as internal audit is no control-function.

14	68. The audit committee is responsible, among other things, for : • … • providing oversight of and interacting with the bank's internal and external auditors; • …	68. The audit committee is responsible, among other things, for : • … • providing oversight of the bank's internal audit function, ensuring that it is independent of senior management and has the appropriate standing, access and authority to challenge the executive; • providing oversight of and interacting with the bank's external auditors; • … **Rationale :** Internal and external audit need to be treated separately as the relationship are very different and need to be spelled out.
18	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.	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. Senior management should implement a ~~•~~ ~~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. **Rationale:** a) No bullet points, as the two following sentences are NO subpoint of the first sentence: The audit function is NO function of managing or controlling risks. These are tasks of the second line of defence only. b) Risk Management and Compliance might act independently to some respect, but OF COURSE the ultimative responsibility for managing risks is with board/senior

		management, who MUST interfere if functions of the second line of defense show lacks in exercising their duties.
19	95. In order to fulfil its responsibilities, the board of the parent company should: • establish a group structure …; • define an appropriate subsidiary board …; • assess whether the group's corporate governance framework includes …; • ensure the group's corporate governance framework …; • approve policies …; • assess whether there are …; • have sufficient resources to monitor compliance of subsidiaries with all applicable legal, regulatory and governance requirements; and • maintain an effective relationship with ...	95. In order to fulfil its responsibilities, the board of the parent company should: • establish a group structure …; • define an appropriate subsidiary board …; • assess whether the group's corporate governance framework includes …; • ensure whether the group's corporate governance framework …; • approve policies …; • assess whether there are …; • have sufficient resources to monitor compliance of subsidiaries with all applicable legal, regulatory and governance requirements; • maintain an effective internal audit function which ensures audits being performed within or for all subsidiaries and parts of the group and the group itself; and • maintain an effective relationship with … **Rationale:** It is important mentioning the audit function here - especially as risk management and compliance function are mentioned as well. Especially in group structures it is of vital importance having implemented an effective audit function covering the whole group. In addition the addendum is neccessary to be consistent with # 100, last bullet point.
22	**Principle 6: Risk management** **Banks should have an effective independent risk management function, under the direction of a Chief Risk Officer (CRO), with sufficient stature, independence, resources and access to the board.**	**Principle 6: Risk management** **Banks should have an effective independent risk management function, under the direction of a Chief Risk Officer (CRO), with sufficient stature, independence, resources and access to the board. Independence in this respect primarily refers to market / business units, but does not mean independence from the board nor does it equate to the independence of the internal audit function, which as third and last line of defence has to audit and give assurance about risk management.**

		Rationale: Clarification to make it coherent with, amongst others, # 11 and # 104. Risk Management is independent from business units, but, as rightfully stated in # 120, ´may reduce or hedge risks. This ´operational´ management may reduce to some extent the component of the audit function, for instance, the absence of any means of decision making. It must be crystal clear that there is a difference of the independence of the internal audit function from the independence of second line of defense functions. The ultimate responsibility of banking risks mangement is not with risk management but with the managing board. In this respect ´independence´ should not be used in a way which might lead to a misinterpretation about ultimate responsibilities.
28	131. An independent compliance function[26] is a key component of the bank's second line ofdefence. This function is responsible, among other things, for promoting and monitoring that the bank operates with integrity and in compliance with applicable, laws, regulations and internal policies.	131. An independent compliance function[26] is a key component of the bank's second line of defence. This function is responsible, among other things, for promoting and monitoring that the bank operates with integrity and in compliance with applicable laws, regulations and internal policies. Independence in this respect does not refer to and does not mean the independence of the board nor such from the internal audit function, which as third and last line of defence has to audit the compliance function. **Rationale:** Clarification to make it coherent with, amongst others, # 11, 134, 136 and Principle 6 (new). As rightfully statet in # 134, the board and management are accountable for the bank´s compliance. So ´independence´ should not be used in a way which might lead to a misinterpretation about ultimate responsibilities. # 136 clarifies that compliance is independent from management - but it does not say independent from senior

		management or board. It must be clear that there is a difference between the independence of the internal audit function and the independence of the second line of defence functions.
29	**Principle 10:** Internal audit **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.**	**Principle 10:** Internal audit **The internal audit function provides independent assurance to the board of directors and senior management on the quality and effectiveness of a bank's internal control, risk management and governance systems and processes, thereby helping the board and senior management protect their organisation and its reputation. ~~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.** **Rationale:** Changes mainly adapt the respective wording of the 2012 BIS Paper: The internal audit function in banks. It is meaningful not using different definitions amongst BIS papers covering the same subjects. In addition, the added version covers the tasks of audit more correctly.
	140. An effective internal audit function provides an independent assurance to the board of directors and senior management on the quality and effectiveness of a bank's internal control, risk management and governance systems and processes, thereby helping the board and senior management protect their organisation and its reputation.	140. An effective internal audit function provides - amongst other things - an independent assurance to the board of directors and senior management on the quality and effectiveness of a bank's internal control, risk management and governance systems and processes, thereby helping the board and senior management protect their organisation and its reputation. **Rationale:** The definition is good; however the tasks of the audit function are not limited to what is stated.

29	142. The board and senior management can enhance the effectiveness of the internal audit function by: • requiring the function to independently assess the effectiveness and efficiency of the internal control, risk management and governance systems and processes; • requiring internal auditors to adhere to national and international professional standards, such as those established by the Institute of Internal Auditors; and • ensuring that audit staff have skills and resources commensurate with the business activities and risks of the bank.	142. The board and senior management can enhance the effectiveness of the internal audit function by: • requiring the function to independently assess the effectiveness and efficiency of the internalcontrol, risk management and governance systems and processes; • ensuring that the scope of internal audit is unrestricted; • requiring internal auditors to adhere to national and international professional standards, such as those established by the Institute of Internal Auditors; and • ensuring that audit staff have skills and resources commensurate with the business activities and risks of the bank. • recognizing the importance of the audit processes and communicating their importance throughout the bank; • requiring timely and effective correction of audit issues by senior management. • ensuring that the internal audit function has an internal quality assurance capability,its performance is regularly evaluated against appropriate criteria, and it is subject to an independent, external assessment at least every five years; • requiring a periodic assessment of the bank's overall risk governance framework including, but not limited to, an assessment of: o the effectiveness of the risk management and compliance functions; o the quality of risk reporting to the board and senior management; and o the effectiveness of the bank's system of internal controls. • ensuring that the Chief Audit Executive and other senior internal audit managers have an open, constructive and co operative relationship with the regulators. **Rationale:** The first bullet point added was part of the 2010 BIS Paper ´Principles for enhancing corporate governance´ and should be left in. Some others are added as meaningful or transferred from # 143, as they are no indicators or garant for independence as stated there.

29	143. The board and senior management should respect and promote the independence of the internal audit function by, for example: • ensuring that internal audit reports are provided to the board without management filtering and that the internal auditors have direct access to the board or the board's audit committee. • requiring timely and effective correction of audit issues by senior management. • requiring a periodic assessment of the bank's overall risk governance framework including, but not limited to, an assessment of: o the effectiveness of the risk management and compliance functions; o the quality of risk reporting to the board and senior management; and o the effectiveness of the bank's system of internal controls.	143. The board and senior management should respect and promote the independence of the internal audit function by, for example: • ensuring that internal audit reports are provided to the board without management filtering and that the internal auditors have direct access to the board or the board's audit committee. ~~• requiring timely and effective correction of audit issues by senior management.~~ ~~• requiring a periodic assessment of the bank's overall risk governance framework including, but not limited to, an assessment of:~~ ~~o the effectiveness of the risk management and compliance functions;~~ ~~o the quality of risk reporting to the board and senior management; and~~ ~~o the effectiveness of the bank's system of internal controls.~~ • ensuring that the primary reporting line of the Chief Audit Executive is to the board or audit committee, including his/her appointment, dismissal, remuneration and appraisal. • where internal audit has a secondary reporting line, requiring that this is to the Chief Executive Officer. • giving internal audit the right to attend or observe executive committee meetings and to have timely access to key management information. **Rationale:** As the deleted issues have nothing to do with independence, they are better transferred to # 142. The added examples are strong indicators for the independence of the internal audit function.
29		*To be added after # 143:* 144. Appointment, dismissal and other changes to the Chief Audit Executive position should be approved by the board or its audit committee. If the CAE is removed from his or her position, this should be disclosed publicly. The bank should also discuss the reasons for such removal with its supervisor. **Rationale:**

		Addendum necessary to make it coherent with # 109. It would not be meaningful protecting second line of defence functions more than the third line function.
30	148. For employees in risk, compliance and other control functions, compensation should be determined independently of any business line overseen, and performance measures should be based principally on the achievement of their own objectives so as not to compromise their independence.	148. For employees in risk, compliance and other control functions of the second line of defence as well in the audit function, compensation should be determined independently of any business line overseen, and performance measures should be based principally on the achievement of their own objectives so as not to compromise their independence. **Rationale:** Addendum just for completeness. We deem the same should apply for the audit function as well.
33		***Between # 156 and 157 as new # 157:*** 157. The bank should also disclose key statements regarding an effective audit function being implemented as third line of defence. **Rationale:** As the audit function is regarded as a key parameter of the governance of a bank, it would be meaningful having implemented a disclosure of an effective audit function being in place.