

**From:** [Amr El Kasaby](#)  
**To:** [Basel Committee, Service](#)  
**Subject:** Comments on Consultative Document "The internal audit function in banks"  
**Date:** Wednesday 29, February, 2012 08:06:01

---

This comments' email represents my own professional views.

Basel Committee on Banking Supervision  
Bank for International Settlements

Dear Sirs,

I've reviewed the above referred to consultative document and would like to share with you my proposed amendments. Following are the details, my proposed amendments are shown in **red**:

| Reference                    | My Proposed Amendments                                                                                                                                                                                                                                                                             | Additional Comments                                                                                                                                                                                                                                                                                                                             |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Principle 4, item 19, page 5 | This provides the basis for reliance on the internal auditor's <b>professional</b> judgment.                                                                                                                                                                                                       | Fine tuning                                                                                                                                                                                                                                                                                                                                     |
| Principle 4, item 22, page 6 | , such as that of The Institute of Internal Auditors <b>and Information Systems Audit and Control Association</b> .                                                                                                                                                                                | There are two main sections within any Internal Audit Department, a General Audit section which caters for operational, financial, compliance audits and an IT Audit section which caters for the IT related audits. Accordingly, whenever we refer to the IIA related code of ethics, we should refer to ISACA related code of ethics as well. |
| Principle 5, item 24, page 6 | <ul style="list-style-type: none"><li>· <b>Vision and Mission of the IA department,</b></li><li>· <b>Operating principles of the IA dept.</b></li><li>· <b>Quality Assurance and improvement program,</b></li><li>· <b>Periodic Assessment of the Charter.</b></li></ul>                           | Some more items which I believe should be part of the minimum requirements to be in the IA Charter, as required by the IIA Standards.                                                                                                                                                                                                           |
| Principle 5, item 25, page 6 | , to examine any activity or entry, and <b>to have full and unconditional access to</b> any records, files, data.. etc.                                                                                                                                                                            | Important to add                                                                                                                                                                                                                                                                                                                                |
| Principle 6, item 27, page 7 | <ul style="list-style-type: none"><li>· <b>Achievement of the bank's strategic objectives and goals</b></li></ul>                                                                                                                                                                                  | Based on COSO framework.                                                                                                                                                                                                                                                                                                                        |
| Principle 6, item 29, page 7 | <ul style="list-style-type: none"><li>· 2<sup>nd</sup> line: The plan should be based on a risk assessment (including input from senior management, the board <b>and the external auditors especially when they place reliance on IA</b>), <b>fraud risk assessment and risk control</b></li></ul> | Based on our current practice; which is in-line with the best practices, in that respect.                                                                                                                                                                                                                                                       |

|                                   |                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                       |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                   | <p>self assessment (RCSA) results, and should be updated at least annually.</p> <p>7<sup>th</sup> line: The budget plan should be sufficiently flexible to adapt to variations (special requests and investigations) in the internal audit plan in respect of changes in the bank's risk profile.</p> |                                                                                                                                                                                       |
| Principle 7, (c), item 35, page 8 | , reliable and relevant reports internally for both internal senior management and the supervisor.                                                                                                                                                                                                    | Fine tuning.                                                                                                                                                                          |
| Principle 9, item 43, page 9      | Last line: <del>From time to time</del> Once every five years, the board of directors should consider commissioning an independent external quality assurance review of the internal audit function.                                                                                                  | As required by the IIA Standards.                                                                                                                                                     |
| Principle 9, item 44, page 9      | Insert after the 1 <sup>st</sup> sentence of the paragraph: Such a process may involve risk control self assessment (RCSA) workshops across the bank.                                                                                                                                                 | Based on our current practice; which is in-line with the best practices, in that respect.                                                                                             |
| Principle 9, item 45, page 9      | Insert the following by the end of the 2 <sup>nd</sup> line:<br>and ensure that internal audit gets involved early enough so that all associated risks, known (concerns) and anticipated (potential risks) are identified etc.                                                                        | Based on our current practice; which is in-line with the best practices, in that respect.                                                                                             |
| Principle 9, item 47, page 9      | Add "Board Audit Committee" at the beginning of the paragraph.                                                                                                                                                                                                                                        |                                                                                                                                                                                       |
| Principle 11, item 51, page 10    | should ensure compliance with sound internal auditing standards, such as The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing and Information Systems Audit and Control Association.                                                        | Whenever we refer to the IIA standards, we should refer to ISACA related standards as well.                                                                                           |
| Principle 13, item 55, page 11    | 2 <sup>nd</sup> line of defense – Risk management function, Compliance function, Internal Control function and other monitoring functions                                                                                                                                                             |                                                                                                                                                                                       |
| Principle 13, item 59, page 11    | and periodically provides an independent reassurance service to senior management and the board of directors.                                                                                                                                                                                         | 1 <sup>st</sup> and 2 <sup>nd</sup> lines of defenses are providing some kind of assurance service, hence IA as a 3 <sup>rd</sup> line of defense is providing a reassurance service. |

|                                |                                                                                                                                                                                                          |                                                           |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| Principle 14, item 61, page 11 | Add the following at the end of the paragraph: <b>The Internal Audit function at the Subsidiary must be independent and sufficiently resourced.</b>                                                      | To consider the minority interest of the subsidiary bank. |
| Principle 17, item 86, page 15 | <b>As a minimum, once every five years; the board audit committee should arrange for a quality assurance review of the IA function to be conducted by an external independent consultant/audit firm.</b> | As required by the IIA Standards.                         |

Thank you

Sincerely,,

**Amr Sami El Kasaby, CPA, CFE, CICA**  
**Group Chief Internal Auditor**  
**Burgan Bank Group**

Attention: Any non-official business related views, opinions and other information presented in this electronic mail are solely those of the sender/author. Burgan Bank does not endorse or accept responsibility for their opinions. If you are not the addressed indicated in this mail or responsible for delivering this message to the intended, you should delete this message and notify the sender immediately.

----- Burgan Bank S.A.K  
www.burgan.com et