for PUBLICATION

28 February 2012

UniCredit's reply to the Basel Committee Consultation on Internal Audit

UniCredit is a major international financial institution with strong roots in 22 European countries, active in approximately 50 markets, with about 9.500 branches and more than 160.000 employees. UniCredit is among the top market players in Italy, Austria, Poland and Germany. In the CEE region, UniCredit operates the largest international banking network with around 4.000 branches and outlets. UniCredit Group is a market leader in the CEE region. Furthermore UniCredit was recently recognized as Global Systemically Important Bank.

Executive Summary

UniCredit fully supports the Basel Committee on Banking Supervision (BCBS)'s exercise and appreciate the opportunity to provide comments. In general most of the proposed Principles are agreeable and UniCredit is already aligned with them. Particularly welcome are the principles supporting the independent role of Audit, the continuous improvement of the effectiveness of internal control, risk management and governance processes. and the attention paid to the communication between internal audit and Supervisory Authorities / External Auditors, in order to allow a more effective and efficient information sharing.

At the same time, there are some areas that could be further clarified or expanded as follows::

1) the different responsibilities of bank's Governing Bodies, according to the possible different governance models (one-tier or two-tier);

2) the application and consequences of a risk-based audit approach;

3) relationships with other internal control functions (e.g. compliance) and the performance of audit activities on them;

4) roles and responsibilities of the internal audit function of the parent company in case of banking groups;

5) supervisory assessment of the internal audit function.

A. Supervisory expectations relevant to the internal audit function

Principle 1: An effective internal audit function independently and objectively evaluates the quality and effectiveness of a bank's internal control, risk management and governance processes, which assists senior management and the Board of Directors in protecting their organisation and its reputation.

1. The internal audit function

- It is suggested to complete the definition of the purpose of Internal Audit (IA) functions including also the goal to improve the effectiveness of internal control, risk management and governance processes.
- It is suggested to give appropriate emphasis to the consultancy role which IA may perform, accordingly with the definition of "internal auditing" included in the international professional standards issued by IIA.
- Should the term "quality" (concerning bank's internal control, risk management and governance processes) be intended as "adequacy" or as "efficiency" or both? It is suggested to make it consistent with provision of paragraph 59 "*The internal audit function employs a risk-based approach to assess the efficiency and effectiveness of the design and operation of internal control* […]"?
- Paragraph 8: it is appreciated more emphasis on the concept concerning "risk based approach" to determine the work plans and actions of the relevant involved parties. For example this could be highlighted in a dedicated principle or specific guidelines could be provided about how to pursue this kind of approach.
- Paragraph 8: with reference to the phrase "*The internal audit function plays a crucial role in the ongoing maintenance and assessment of a bank's internal control*", it is suggested to clearly state that the "ongoing maintenance" is responsibility of bank's Management.

2 Key features of the internal audit function

(a) Independence and objectivity[3]

Principle 2: The bank's internal audit function must be independent of the audited activities. This requires that the internal audit function has an appropriate standing within the bank, enabling internal auditors to carry out their assignments with objectivity.

Paragraph 12: "*On the basis of the audit plan established by the head of the internal audit function and approved by the board of directors […]*", it suggested to define more clearly and unambiguously the responsibilities for audit plan approval keeping in due consideration the different governance models

(One-Tier or Two-Tier).

(b) Professional competence and due professional care

Principle 3: Professional competence, including the knowledge and experience of each internal auditor and of internal auditors collectively, is essential to the effectiveness of the bank's internal audit function.

UniCredit agrees with this principle.

(c) Professional ethics

Principle 4: Internal auditors should act with integrity.

UniCredit agrees with this principle.

3. The internal audit charter

Principle 5: Each bank should have an internal audit charter that articulates the purpose, standing and authority of the internal audit function within the bank.

- It is suggested to add also "responsibilities" of IA as a key aspect to be defined in the charter, in order to be consistent with the respective paragraphs of the principle.
- Paragraph 23: Shall the phrase "*The charter […] It should be available to all internal and external stakeholders of the organisation*", be intended that the bank gives due publicity to its audit charter e.g. by publishing it on its website?
- Paragraph 24: it is suggested to use "must" instead of "should" in "*At a minimum, an internal audit charter should establish: […]*", according with provision coming from IIA International Standards (PA 1000-1).

4 Scope of activity

Principle 6: Every activity (including outsourced activities) and every entity of the bank should fall within the overall scope of the internal audit function.

- Paragraph 26: it is suggested to add a specific reference to the scope of the internal audit activities of Parent Company in case of banking groups. This should allow an appropriate role of steering and coordination along with a proper monitoring and control over group risks (see Bank of Italy Supervisory Instructions – Title IV – Chapter 11 – Section III).
- Paragraph 29: it is suggested to rephrase the sentence "[…] *The head of internal audit should ensure that all material entities and all material activities of the bank are audited at least once within an appropriate period of time (audit cycle)*". The rephrasing would be more consistent with a risk-oriented approach stated at page 4, Paragraph 8 "*both internal auditors and supervisors use risk based approaches to determine their respective work plans and actions*").
- Furthermore, in order to pursue more effectively a risk-based approach, it is believed that the

annual internal audit plan should be based on a risk assessment which includes an appropriate input also from other control functions (e.g. Compliance and Risk Management), in addition to inputs coming from "senior management and the board". Therefore it is suggested to rephrase the sentence "[…] *The plan should be based on a risk assessment (including input from senior management, the board and other control functions) […]*".

Principle 7: The internal audit function should ensure adequate coverage of regulatory matters within the audit plan.

- With reference to the "adequate coverage of regulatory matters", consistently with principles defined in other parts of the document (e.g. paragraph 8), our interpretation is that such coverage should be ensured in a risk-based approach perspective; clarification/confirmation might be helpful in this regard.

- Paragraph 30: with reference to the term "relevant authorities", the same interpretation as at the bullet point above (risk-based perspective) is understood.

(d) Compliance

- Consistently with paragraph 30, considering that further functions other than Compliance (e.g. "Human Resources", "Legal", "Tax"), may be in charge to manage specific compliance risks, due to the particularity and technicalities of those risks, it is suggested to duly consider this aspect in the definition of the scope of activities on Compliance function subject to audit review and on other functions which may assist the Bank in the management of specific compliance risks, outside Compliance function's scope.

5. Corporate governance considerations

(a) Permanency of the internal audit function

Principle 8: Each bank should have a permanent internal audit function.

UniCredit agrees with this principle.

(b) Responsibilities of the board of directors and senior management

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

UniCredit agrees with this principle and believes that the Board of Directors is responsible for establishing and maintaining an adequate, effective and efficient internal control framework and

internal audit function. The Board of Directors has sole responsibility for laying down the guidelines for the internal control system and periodically reviewing the adequacy, efficiency and effectiveness of the system, to ensure that all principal corporate risks are being correctly identified and adequately measured, managed and monitored.

With regard to paragraph 43, UniCredit agrees with the recommendation that there should be an independent review of the internal audit function from time to time.

In case of large and complex organizations, UniCredit considers that a two-tier Quality Assessment Review system (both internally and externally) should be adopted to assess and improve the quality of the service provided by the internal audit function. An Internal Quality Assessment Review is regularly performed every three years, with ad-hoc reviews when needed for specific cases. It may vary in scope from the assessment of the entire spectrum of audit activities (full scope) to the assessment of only selected activities or specific areas of activity of local internal auditors. An External Quality Assessment Review is performed at least every five years, in line with IIA standards, by a qualified and independent external team.

With regard to paragraph 45, UniCredit considers that it is vital to provide internal auditors with full knowledge and an overview of the whole business in order to perform their duties. Each bank to which the Guidance applies, shall judge what is the best way to implement this according to the way it is organized, without prejudicing the independence of Internal Audit.

(c) Responsibilities of the audit committee in relation to the internal audit function

Principle 10: The audit committee, or its equivalent, should oversee the bank's internal audit function

UniCredit agrees with this principle.

UniCredit believes that large and complex financial companies should create a specialised Audit Committee within the Board of Directors with proposing and consultative functions, to cover all control matters within the competence of the Board of Directors.

With regard to paragraph 49, UniCredit considers, in line with the mentioned role of the Audit Committee, that the approval of the Audit Plan is a specific task of the Board of Directors, with the support of the Audit Committee, which gives an opinion and recommends its approval to the Board of Directors (this is also a requirement of the newly issued Italian Corporate Governance Code, which UniCredit helped to revise). In addition, the opinion of the Audit Committee should cover the adequacy of the Audit Plan prepared by the Head of Internal Audit and, when necessary, request that specific audits be performed.

Please note that the responsibility of the Board of Directors to approve the Audit Plan is already mentioned in paragraph 29.

(d) Management of the internal audit department

Principle 11: The head of the internal audit department should be responsible for ensuring that the department complies with sound internal auditing standards and with a relevant code of ethics.

UniCredit agrees with this principle.

(e) Reporting lines of the internal audit function

Principle 12: The internal audit function should report to the audit committee or the board of directors and should inform senior management about its findings.

Paragraph 54: consistently with the risk-based approach, it is suggested to amend the last sentence of the paragraph as follows: "*The head of the internal audit function should report to the board, or its audit committee, the status of significant findings that have not (yet) been rectified by senior management*".

(f) The relationship between the internal audit, compliance and risk management functions

Principle 13: Internal audit should both complement and assess operational management, risk management, compliance and other control functions.

- UniCredit would recommend to amend the verb "complement" as it may be intended that the IA function is expected to assume (and not only assess, as it is in its mission) operational roles in operational management, risk management and compliance activities, in contrast with principles included in Paragraph 13 to support IA's independence and objectivity.

- Paragraph 59: it is suggested to reconsider the following sentence "*…the assessment of "efficiency" of the design and operation of internal control"* as it does not seem consistent with the definition of Internal Audit given in Paragraph 9, where the evaluation is referred to "effectiveness" of risk management, control and governance processes.

- Paragraph 59: in the perspective of supporting a risk-based approach, it is suggested to specify that, in performing its assessment, the internal audit function, when applicable, should take in due consideration the results of controls carried out by other control functions (e.g. Compliance and Risk Management).

6. Internal audit within a group or holding company structure

Principle 14: The internal audit function in a group structure or holding company structure should be established centrally by the parent bank.

- It is suggested to better define the meaning of "established centrally by the parent bank". Does the "establishment" refer to aspects such as the organization of the internal audit functions in a banking

group perspective, the definition of group common audit methodologies and of the overall budget?

- Paragraph 60: in order to support a risk-based approach also in the organization of internal audit functions in a group perspective, it is suggested to amend the sentence as follows: "*In a group structure […] for ensuring that internal audit policies and mechanism are appropriate to the structure, business activities and risks of all material components of the group*"

- Paragraph 61: it is suggested to better define what is to be intended for "group's internal audit strategy": e.g. budgets, methodologies, organizational structures, IT tools and staff, risk assessment, audit plans?

7. Outsourcing of internal audit activities

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

UniCredit agrees with this principle.

B. The relationship of the supervisory authority with the internal audit function

- Paragraph 67: UniCredit believes that, in order to ensure that "respective perceived and actual independence and status" are not undermined, the supervisory authorities' challenge of the work of the internal auditors does not regard Internal Auditors' professional judgment and opinion, which are the sole responsibility of Internal Audit, but the assessment and challenge of the adequacy and effectiveness of audit approaches, methodologies and procedures.

I. Benefits of enhanced communication between the supervisory authority and the internal audit function

Principle 16: Supervisors should have regular communication with the bank's internal auditors to (i) discuss the risk areas identified by both parties, (ii) understand the risk mitigation measures taken by the bank, and (iii) monitor the bank's response to weaknesses identified.

- Paragraph 73: a risk-based audit approach should lead to flexible audit plans. Accordingly, it is suggested the following rephrasing: "*In case of major divergence from the internal audit plan, supervisors should obtain an understanding of the circumstances which led to the changes* […]".

2 Potential topics for discussion between supervisors and internal audit

Paragraph 79: UniCredit believes that, in order to foster the completeness of the overall picture, supervisory authorities should evaluate audit results also keeping in due considerations relevant information which may be acquired by the compliance function (e.g. results of second level controls, mitigation actions closed and ongoing etc).

C. Supervisory assessment of the internal audit function

1 Assessment of the internal audit function

Principle 17: Bank supervisors should regularly assess whether the internal audit function has an appropriate standing within the bank and operates according to sound principles.

- UniCredit supports the principle and considers the assessment of the internal audit function by Bank Supervisors as a fundamental step to contributing to an internal control framework that is fit for the purpose, including timely and effective reporting and a holistic approach to risk management.

- Paragraph 83: concerning the introduction of "key internal auditors" related to compensation matter, UniCredit believes that each bank should identify its key internal auditors on the basis of a self-assessment as provided in Directive 2010/76/UE dated 24 November 2010 ("CRD III").

- Paragraph 87: UniCredit considers that the formal communication *stricto sensu* of the appointment of a new Head of the Internal Audit function (or his cessation) to the Supervisory Authority should be made by the same Body of the bank which approved the appointment/cessation of the previous Head of Internal Audit.

- UniCredit is of the opinion that (as required by its current regulations) the Board of Directors should approve the appointment and removal of the Head of the Internal Audit function. The Audit Committee should advise on a proposal made by the Chairman of the Board of Directors on the appointment or replacement of the Head of the Internal Audit function.

- UniCredit is of the opinion that the term "regularly assess" seems to be too broad: i) we suggest to define more precisely the timing, e.g. by determining a minimum requirement for the frequency (e.g. at least every three years) ii) we suggest to define how this assessment is expected to be performed (e.g. on going assessment based on the regular relationships with IA function, based on direct inspections or, considering current practices existing in some jurisdictions, by external audit firms).

2 Actions to be undertaken by the supervisory authority

Principle 18: Supervisors should formally report all weaknesses identified in the internal audit function to the board of directors and require remedial actions.

UniCredit agrees with this principle. We consider that Supervisory Authorities already have the appropriate powers to address the mentioned issues.

Principle 19: The supervisory authority should consider the impact of its assessment of the internal audit function on its assessment of the bank's risk profile and on its own supervisory work.

UniCredit agrees with this principle.

Paragraph 91: UniCredit notes that the assessment of the internal audit function by Supervisory Authority shall contribute primarily to the overall evaluation of the bank's internal control system, and then, to the bank's overall risk profile.

Principle 20: The supervisory authority should be prepared to take informal or formal supervisory actions requiring senior management and the board to remedy any identified deficiencies related to the internal audit function within a specified timeframe and to provide the supervisor with periodic written progress reports.

- Paragraph 94: Are the following sentences to be intended as synonyms "to take informal or formal supervisory action" and "public or non-public nature" (see principle 20)? If not, it could be appropriate to explain or provide examples to clarify them.

Comment on Annex 2

UniCredit agrees that the duties and functions of the Audit Committee should be determined by each bank especially in light of the many local regulations and practices. For example, under Italian Legislation, careful consideration shall be put on the paragraph related to "Statutory or External Auditors", in light of decree 39/2010 on annual certification of company and consolidated accounts.

CONTACT PEOPLE (name.surname@unicredit.eu)
Please find below the list of the key people involved in this work, whose contribution made possible to coordinate and provide UniCredit answers to this Consultation. Some other experts have been involved alongside the UniCredit Group, but are not listed below.

Regulatory Affairs (Public Affairs) – Coordination Team
Lugaresi Sergio – Head of Regulatory Affairs - Public Affairs
Laganà Marco – Regulatory Affairs
Mantovani Andrea – Regulatory Affairs

KEY CONTRIBUTOR
Internal Audit
Avanzi Giovanni Battista – Head of Audit Methodologies & Processes
Cregut Massimo – Head of Global Methodologies Development
De Angelis Lorenzo – Head of Group Audit Policies
Balit Patrizia – Head of Advisory & ICRC Secretariat
Di Stefano Giovanna – Advisory & ICRC Secretariat

OTHER CONTRIBUTORS

Banking Supervisory Relations
Moscon Guido – Head of Banking Supervisory Relations
Cremonino Andrea – Head of Banking Supervision College and EU

Compliance
Bertulessi Enrico – Head of Global Regulatory Counsel
La Rocca Antonio – Head of Global Regulatory Counsel
Lattuada Paola – Head of Global Banking Services Counsel
Cevini Alessandro – Global Banking Services Counsel

Corporate Law
Bonessi Ermanno – Head of Corporate Law Advice
Nuzzo Manlio – Corporate Law Advice

Group Corporate Bodies
Natale Secondino – Head of Group Corporate Bodies
Romisondo Maria Daria – Group Corporate Bodies

Group Organization Development
Francescucci Paola – Head of Group Organization Development
Veneziani Ettore – Head of Organization Development - Structures & Rules

Group Risk Management
Arnaboldi Fadio – Head of Group Risks Control (GRM dept Coordinator)
De Mori Valeria – Head of Risk Integration & Capital Adequacy (GRM dept Coordinator)

HR Compensation
Lanati Giovanni – Head of Group Compensation
Carson Sian – Compensation
De Matteo Mariangela – Compensation