UniCredit Group

FOR PUBLICATION

13 January 2011

UniCredit Group's reply to the CEBS 44 on internal governance

GENERAL REMARKS

Concerning Structure, Organisation and Management Body (sections A, B and C)

- UniCredit appreciates the principles-based approach that tries to take into consideration the very different dimensions, complexities and national legal frameworks of the banks (principles 2, 7, 8 10).
- Principle 6 on management and supervisory functions requires in our view some adaptations to take into account different governance models

Concerning risk management (section C)

- UCG has a robust risk management governance process and framework in place to cover its major risks, and is already in compliance with most of the stated principles in CEBS44.
- Despite the fact that UCG is a complex organization, a great deal of thought and effort has gone into creating a homogenous approach to risk management throughout the group, which helps ensure consistency of action.
- The bank regularly seeks opportunities to improve and refine its risk management process, which is important given the dynamic nature of the financial markets and operating environment.

Concerning internal controls (section D)

In an innovative financial environment, the internal control Functions and Bodies should be able to play a much more active role in corporate management, contributing to reach an integrated view of the Internal Control System, including timely and effective information flow and reporting and an holistic approach to the risk management (with the involvement of business lines).

The overall assessment of the Internal Control System, which falls under the responsibility of the CEO who reports to the Board of Directors, results both from the Internal Audit's independent evaluation of the adequacy, effectiveness and efficiency of the internal control system, and the management's self-assessment of the status and implementation of controls and criticalities found in the managed processes.

The Internal Audit should develop the Audit Plans taking into account also the results of the risk assessment process, which should influence the planning phase by defining priorities, nature, frequency and coverage of audits. The Board of Directors should approve the annual audit plan and any relevant changes to it

Experts suggest considering to amend the principle allowing other risk and control functions to assist the institution in managing "compliance risk" for certain laws/regulations which are very specialized or technical (e.g. Tax, Labour and Workplace Health and Security, Accounting law, Basel II etc) where specific, expert or technical knowledge is required. This will avoid duplication of structures and competences on such matters. We suggest introducing another paragraph which allows an institution to have several policies to manage Compliance risk in each single matter of competence, instead of one single policy covering all Compliance topics.

Concerning Systems, continuity and Transparency (sections E and F)
Unicredit agrees with the proposed principle and is already complying with them

SPECIFIC CONSIDERATIONS

A. Corporate Structure and Organisation
Principle 1 - Organisational framework
UniCredit agrees with the principle of effective and prudent management including at group level. Furthermore, reporting lines and the allocation of responsibilities and authority within an institution should be clear, well-defined, coherent and enforced.

Principle 2 - Checks and balances in a group structure
In general, UniCredit agrees with this principle. In a group structure, the parent company's management body has overall responsibility for adequate internal governance across the group.
However, with specific reference to paragraph 33, "… *in a subsidiary, an element of strong governance is to have independent members on the management body (e.g. non-executives who are independent of the subsidiary and of its group, and of the controlling shareholder)*…",

Suggestion to the regulator: UniCredit considers that such rule should be calibrated to the organisational and operational characteristics of the various types of subsidiaries which belong to a banking group. In particular, it may not be useful to apply this principle to smaller subsidiaries which only provide services to the holding company.

Principle 3 - Know-your-structure
UniCredit agrees with this principle.

Principle 4 - Non-standard or non-transparent activities
UniCredit agrees with this principle.

B. Management body

Principle 5 - Responsibilities of the management body

UniCredit agrees with this principle.

Principle 6 - Management and supervisory functions

Some of the paragraphs enclosed under this principle probably refer to companies which have a separate management board and supervisory board model (the so-called "two-tier model" e.g. in German companies) or only one corporate body which carries out directly the management functions and through internal committee the supervisory functions (the so-called "one-tier model") (e.g. see para. 46, 48, 50, 51 and 59).

Current situation

In Italy, most banks adopt a different model where the management body (*consiglio di amministrazione*) performs the management and strategic supervisory functions and the board of statutory auditors (*collegio sindacale*) performs only control functions. Usually, the management body assigns its management functions to one or more executive directors (amministratore delegato).

Suggestion to the regulator:

With this governance model in mind, it is not clear how Italian banks can apply provisions such as "*the supervisory function oversees the management function and provides advice to it*", "*effective interaction should mean the management body in its management function coordinating the institution's business and risk strategies with the management body in its supervisory function and discussing regularly the implementation of these strategies with the management body in its supervisory function*", or "*the management function proposes the direction for the institution; ensures the effective implementation of the strategy and is responsible for the day-to-day running of the institution*".

UniCredit would suggest CEBS to adapt relevant paragraphs in order to take into consideration other exiting governance models

Principle 7 - Composition, appointment and succession

Current situation

According to Italian Law, shareholders have exclusive competence to propose appointments to the Board of Directors. UniCredit is of the opinion that, in terms of qualifications, members of the governing bodies must have experience adequate to the size and operational complexity of the relevant company and come from sufficiently diverse backgrounds.

Suggestion to the regulator:

UniCredit is in favour of submitting policies to the shareholders in order to raise awareness of the company's opinion about the qualifications a director of the company should have in addition to the professional requirements prescribed in domestic laws.

Considering large differences in the dimension and complexity of the banks subject to this prescription, UniCredit suggests that the CEBS does not prescribe specific contents to be included in recruitment policies. Instead, the Commission could set general principles which would facilitate banks to implement the policies.

Principle 8 - Commitment, independence and managing conflicts of interest

Current situation

UniCredit fully agrees with the principle that board members should devote sufficient time and resources to the fulfilment of their duties. In this regard it should also be pointed out

verifying and evaluating the number of similar positions held by board members is a general principle contained in the codes of best practice on corporate governance which are applied by the large majority of listed, European companies.

Suggestion to the regulator: In line with the provisions contained in such codes, and considering the large differences in the dimension and complexity of both the financial companies which will implement the rule and the other companies in which the directors may cover a similar positions, UniCredit considers it appropriate not to refer to a minimum expected time commitment for the members of the management body (see paragraph 58) but to set up a general principle on this matter. According to the Bank of Italy, "*on the occasion of the appointment of board members and continuing over time, the number of similar positions held must be verified and evaluated, with special attention to those requiring greater involvement in the current business of the company. The limits to the holding of multiple positions must be the subject of specific provisions of company bylaws or rules*".

Principle 9 - Qualifications

UniCredit fully agrees that members of the management body should be and remain qualified for their positions. Training can assist qualification. Furthermore, they should have a clear understanding of their institution's governance arrangements and their role in them.

Principle 10 - Organisational functioning

With regard to paragraph 68, UniCredit does not disagree with the recommendation of making recourse to an external advisor to evaluate the individual and collective efficiency and effectiveness of its activities, governance practices and procedures, as well as the functioning of committees. However, considering the very different dimensions, complexities and national legal frameworks of the banks which should implement such a proposal, it seems appropriate not to set up specific rules on the contents and procedure to evaluate the board (namely not provide for a mandatory procedure). Rather, general principles should be defined which are aimed at facilitating Europe-wide implementation.

Suggestion to the regulator: Paragraph 72 states that "*specialised committees may include an audit committee, a risk committee, a remuneration committee, a nomination or human resources committee and/or a governance or ethics or compliance committee*". UniCredit believes that in the case of large, highly complex banks a recommendation should be considered to create a specialized committee within the board of directors to benefit the board's activities through proposing and consultative functions. Aside from bigger and very complex banks, the organisation and set-up of committees should be done according to the complexity and dimension of the banks. Nomination or human resources committees and/or a governance or ethics or compliance committee may not be very useful and could be unduly burdensome in smaller banks or in banks totally owned by one shareholder.

UniCredit strongly believes in the Audit Committee and in the Risk (Board) Committee functions (the last specialized with proposing and consultative functions to the benefit of the board for its activities regarding risk management, evaluation of risk appetite), and in the cooperation and information flows between the two Committee. The interaction can be assured through the cross-participation of the Members and by the same Chairman who can chair both.

Principle 11 - Corporate values and code of conduct

The management body should develop and promote high ethical and professional standards.

- ***Current situation:*** currently UniCredit has several Codes of Conduct within the Group. They have been issued autonomously in recent years and each one is specific to a single legal entity or specific business area. Even though they have a common purpose - that is to set rules for appropriate behaviour in doing business – there is only a partial coverage of UniCredit Group employees, both in terms of business and of geography.

- *Planned action to fill the gap:* a Group Code of Conduct – in the form of a Global HR and Compliance Policy – is under preparation and it is expected to be issued by 1Q11.
The Code's main purpose is to set out the basic principles and minimum standards to guide all UniCredit Group employees in their day-to-day activity.
It will act as an "umbrella" and will have to be read in conjunction with other relevant policies and procedures which are issued by specific legal entities, businesses or countries.

- *Suggestion to the regulator:* add to paragraph 79 as follows:

> *79. When the reputation of an institution is called into question, due to employee misbehaviour, the loss of trust can be difficult to rebuild and can have repercussions throughout the market.*

- *Suggestion to the regulator:* modify paragraph 80 as follows:

> *80. Implementing appropriate standards (e.g. a code of conduct and/or a set of structured policies) for professional and responsible behaviour throughout an institution should help reduce the risks to which it is exposed. In particular, operational risk will be reduced if these standards are given high priority and implemented soundly. The management body should therefore have clear policies for how these standards should be met and should perform a continuing review of their implementation.*

Principle 12 - Conflicts of interest at institution level

- *Current situation:* UniCredit Group complies with the provisions of Principle 12 through the principles and processes set out by "Groupwide Compliance Guidelines Conflicts of Interest" (hereinafter the "Guidelines"), it is supplemented by "Groupwide Compliance Policy Conflicts of Interest" (hereinafter the "Policy").
The Guidelines:

- have been created to assist all Group employees to detect and manage conflicts of interests;
- apply to all UniCredit Group's business activities and provide a high level framework to enable all UniCredit Group directors (e.g. members of strategic, control and executive bodies), employees and tied agents (e.g. financial advisors) to identify and manage actual, apparent and potential conflicts of interest that may arise.

The Policy:

- supplements the Conflicts of Interest Guidelines and supplies a more detailed representation of the activities and responsibilities that govern conflicts of interest management. A particular focus is on conflicts of interest involving Group customers - in the provision of investment services, activities and ancillary services (as defined by MIFID) and in the provision of specific financial services (i.e. distribution of financial products issued by banks or by insurance companies, distribution of investment services supplied by third parties);
- also applies to business conflicts where two clients' interest conflict, which could raise reputational risk for the Group or breach of contractual agreements;
- covers particular conflict of interest situations which could arise from multiple roles performed by an employee;

- defines organisational measures to be adopted to manage conflict of interest situations.

A supplement to the Guidelines, the Global Compliance Policy "Conflicts of Interest – Focus on Personal Interests" which aims to support all the management in the definition of restrictions, exclusions, behaviour rules, procedures for the notification and monitoring of cases related to Employee's Outside Business Activities is under preparation. It is expected to be issued by 1Q11.

Suggestion to the regulator: none

Principle 13 - Internal alert procedures
UniCredit agrees with this principle.

Principle 14 - Outsourcing

UniCredit Group supports the principle and considers the Outsourcing Policy (OP) as a valid tool for the management body to achieve a proper internal governance. It is equally important that the supervised entities can apply with such a principle with the necessary flexibility, taking into account the specific business model and relevant economic/cost factors which may differ from firm to firm.

At this moment, UniCredit Group is considering the development of an OP.

In our intentions such an OP needs i.a. to reflect the business model adopted by the management body, the features of a cross-border group and the regulatory and legislative frameworks.

In this respect, the OP could:

1) reflect strategic and competitive issues;
2) establish a comprehensive assessment framework, coherent with the management body's long term objectives, that: allows potential cases for outsourcing to be identified and measures risks, costs and benefits, when possible;
3) take care of key issues including: accountability/reputation, risk management, confidentiality, relationships with the stakeholders, etc;
4) reflect both the internal business model and strategy as well as the external factors such as the legislative and regulatory environment;
5) identify the scope of application for the activities to be potentially outsourced and the relevant owners;
6) include eligibility criteria that may be grouped in business criteria, risk management criteria, and legal/regulatory criteria, as well as the relevant owners.
7) define high level criteria to evaluate the outsourcer and in particular the professional competence and ability to perform tasks as provided in the contract;
8) draft standard Service Level Agreements and related Key Performance Indicators to evaluate the outsourcer's activities
9) provide for the periodical checks of the outsourcer activities and provide for monitoring this activity.

Suggestion to the regulator:

Besides "CEBS Guidelines on Outsourcing", according to our experience, it could be useful to have Member States uniform law and regulation, in order to make "outsourceable" - within large banking Group - activities (for example Internal controls activities). In fact we noticed that laws and regulation about this issue is quite different from one European country to another. We wish simply to convey the benefits of centralising these kinds of activities, in terms of quality improvement, without intending to contravene any supervisory restrictions.

Principle 15 - Governance of remuneration policy
We generally agree with the principles regarding the governance of remuneration policy as set out in the FSB Principles and Implementation Standards and the Capital Requirement Directive. In order to avoid possible confusion or overlap due to multiple sources and possible differences in wording, interpretation or application, we suggest that Principle 15 should only contain a reference to these key regulatory documents without reporting a subset of specific clauses.

Principle 16 - Assessment of the internal governance framework
UniCredit agrees that the management body should monitor and periodically assess the effectiveness of the institution's internal governance framework.

C. Risk management

Principle 17- Risk culture
Current Situation:

UniCredit Group has recognized the importance of reinforcing risk practices by creating a proper risk culture. It has been developing mechanisms and behaviours that are intended to strengthen this aspect of the control process.

Risk Culture can be defined in many ways. UniCredit Group Risk Management has adopted the following definition as a guiding principle:

"*An internal sensibility, reflected in the daily thoughts and actions of all of the bank's employees, that reflects knowledge of, and respect for, risk.*"

Establishing a risk culture is a long-term process that occurs by embedding into the organization various elements such as a clearly defined risk philosophy, a comprehensive risk appetite framework, a proper organizational structure and dedicated educational programs that focus attention on Risk Culture. More detailed information is available in the annex.

Suggestion to the regulator: none

Principle 18 - Alignment of remuneration with risk profile

Current Situation:

Guidelines on remuneration policy should not be prescriptive and should leave the institution flexibility to decide on the parameters to be used to design incentive systems. Distortion, rigidity and complexity should be avoided due to unintended side effects. It is important to have the flexibility to address the topic at group wide level, especially for cross-

border groups. Any prescriptive hint from any regulator could jeopardise the group's overall approach.

Based on the identified internal perimeter of application and relevant measures to be considered, institutions should be given the time and the opportunity to develop a roadmap to develop the resources required to properly obtain and analyse the data required. In general, UniCredit Group favours simplified approaches which consider the overall group results when defining such items as deferral payments.

Suggestion to Regulators:

We generally agree with the principles regarding the governance of remuneration policy as set out in the FSB Principles and Implementation Standards and the Capital Requirement Directive. In order to avoid possible confusion or overlap due to multiple sources and possible differences in wording, interpretation or application, we suggest that Principle 15 should only contain a reference to these key regulatory documents without reporting a subset of specific clauses. For example, the wording regarding "staff whose responsibilities have a material impact on the risk profile of an institution" is different from the CRD and CEBS text and superfluous in a context where further reference for details is in any case made to the full Guidelines.

Principle 19 - Risk management framework

Current Situation

UniCredit Group agrees with the stated principle and is already in compliance with it. There are no material gaps to be covered.

Planned Actions: None anticipated**.**

Principle 20 - New products

UniCredit SpA believes that a reliable control process for product development and distribution is key element to avoiding potential risks related both to traditional credit/market risks and reputational/operating risks. In order to guarantee preventive management of those risks, UniCredit has already put in place specific processes that tackle not only new initiatives but also the ongoing business.

Two perspectives of second level control functions are provided: a) compliance, b) risk management

a) Compliance perspective

Current situation:

Among the Management Committees of UniCredit S.p.A, the **Product Committee** - which includes the CEO, the Credit Risk Office and the Head of Compliance - is **in charge of** approving the introduction of specific innovative products and services issued or commercialised by UniCredit S.p.A. Applications are analysed according to a customer-centric approach to meet specific customer needs. The Product Committee **evaluates** new

products' impacts on risks, reconciling both business and customer needs, in a time-to-market perspective.

Furthermore, the Product Committee's **mission** is to define, at a group level, the overall commercial strategies and policies (involving offer, pricing, distribution channels, impacts on risk) maximizing the effectiveness of the business model specialized by customer segments within the framework of a strong, unitary and shared strategic vision.

In addition, the Product Committee is responsible to approve or define the proposal for approval by the Bodies of guidelines/policies related to principles, rules and processes regarding the development, issuance and commercialization of products/services by UniCredit Spa and Strategic Business Areas (including suggestions concerning composition/functioning of the Strategic Business Area/Business Unit and Legal Entity Product Committees).

Second level Product Committees are in place in UniCredit S.p.A. and in other main Italy legal entities: applying the same methodology and process structure (i.e. Committee composition, deliberation rules, issues/risks to be analyzed, legal and compliance control), those Committees cover all kind of products (new and traditional) to be issued or distributed through the Italy Network of the Group.

Other legal entities of the Group have identified alternative operating models which provide the establishment of (i) special multifunctional Product Committees or (ii) processes in place for the authorisation or development of new products.

Planned Actions:

Technical Instructions are under preparation by the Compliance Function (expected release by the 1st quarter 2011) to ensure at global level a uniform Compliance approach in the product evaluation process. They could be implemented by establishing appropriate organisational solutions for each individual legal entity.

The above mentioned Technical Instructions will be focused on Compliance matters and in particular on "client" risks.

b) Risk management

Current situation:

Group Risk Management representatives are members of all Group Product Committees, including at divisional level. In addition, the Holding Company Risk Management Function, defines guidelines for issuing and monitoring credit products (e.g. minimum requirements in terms of granting, monitoring, workout procedures, pilot phase definition, regular performance measurement, sustainable and sound introduction and growth criteria etc.),

Some cornerstones and minimum principles and characteristics of the credit products are also established by the Holding Company Risk Management Function, in order to define boundaries and an overall credit profile coherent with the risk appetite and reputational risk of the Group.

Business divisions of the legal entities and of the Holding Company are allowed to design, develop and launch – in coordination with the relevant Global Banking Services (GBS) - new credit products, provided they have been shared with legal entities' risk officers and are aligned with the above mentioned guidelines and principles. If the features of the products

diverge from the guidelines, a timely validation by the Holding Company Risk Management Function is required.

Planned Actions:

When considering any potential gap between the stated principle and the current situation, the magnitude of the gap depends on the actual meaning of Principle 20. If the Principle refers to the entire set of policies, rules, committees related to new products, although not included in one single document, the gap is relatively small. Policies, rules, committees are largely in place. A possible action to better comply with the Principle could be the introduction of a more comprehensive approach to this topic across Strategic Business Areas/Competence Lines/Legal Entities.

If, instead, Principle 20 refers to a sole comprehensive document covering all aspects (risk, commercial, reputational, tax, accounting, operational, etc) the gap is relatively large. At present such a document is not available and, given the complexity of the topic, an internal working group across all the relevant competence lines (CRO, CFO, Organisation, Compliance etc) to tackle the issue may be needed. It is assumed that this is not the spirit or intent of the Principle.

Suggestions to the regulator:

We consider that Principle 20 provides the necessary flexibility, especially in consideration of the scope of the topic. One important aspect that could be clarified is the exact scope of New Product Approval Policy (one single document vs. a set of rules, principles, committees that do not necessarily result in one single policy document). For the sake of completeness, it could be clarified what kind of products it refers to (products for clients - corporate, retail, private, corresponding banking, etc.).

D. Internal control

Principle 21 - Internal control framework

UniCredit agrees with the detailed contents of principle 21.

UniCredit is of the opinion that, in an innovative financial environment, like the current one, the internal control functions and bodies should be able to play a much more active role in corporate management, thus contributing to drive banking operations toward business areas that would allow the achievement of both goals of internal growth and cautious governance,

UniCredit considers very important to reach an integrated view of the internal control governance, meaning that not only the internal control function has to be considered in the process, but also the various Supervisory Control Bodies, including the specialized Board Committees (audit and risk).

UniCredit believes that an effective information flow should be established between the internal control system, the Board of Statutory Auditors, External Auditors and Directors. Controls are essential as their aim is to implement effective management. This implies that

the system should be organized in a way that the involved subjects should talk directly with all corporate bodies involved in this area.

Special attention should be paid to ensuring timely and comprehensive information reporting from company functions and the management to the above mentioned corporate bodies, thus avoiding duplications and redundant information.

In UniCredit's opinion, the issue of self-regulating guidelines concerning the division of responsibilities between the Board of Statutory Auditors (or Supervisory Board – Consiglio di Sorveglianza) and Board Committees (especially the Audit Committee) could rationalize the internal control system and may be desirable to achieve an integrated governance system.

In compliance with the IIAA[1] 's Paper "Integrated approach for the internal control system for effective and efficient corporate governance -February 2008", UniCredit believes that the possibility to establish a real corporate governance system is subject to the capacity to coordinate in an efficient and cost-effective manner all subjects contributing to the various sectors of the internal control system, failing which governance information would turn out to be fragmented and not effective. Furthermore, corporate risks would be inconsistently addressed, both in terms of numbers, as highlighted by the number and size of corporate risks managed against the Group's total significant risks, and of the quality of the risk management system.

Additionally, UniCredit considers that an effective and efficient internal control system is closely linked to the actual role of operational and business functions in charge of first-level, hierarchical, procedural controls.

Referring to an integrated internal control system framework, UniCredit believes that the main pillars of the proposed approach are:

- Holistic approach to the risk management (with the involvement of business lines)
- Introduction of a structured internal control system validation process to assess and maintain the overall process
- Development of programs to "spread" the risk culture across the Entity
- Enhancement of the reporting structure to facilitate the circulation and understanding of risks

Finally, UniCredit believes that the overall assessment of the internal control system, which falls under the responsibility of the Chief Executive Officer, who reports to the Board of Directors, results both from the Internal Audit's independent evaluation and the management's self assessment of the progress and implementation of controls and criticalities found in the managed processes.

Suggestion to the regulator: none

Principle 22 - Risk Control function

<u>Current Situation</u>:

[1] Italian Internal Audit Association

UniCredit Group agrees with the stated principle and is already in compliance with it, with no material gaps to be covered. In particular,

- UniCredit Group possesses an independent Risk Control function - Group Risk Management department, hereafter GRM – which has been established to ensure coverage of all material risks with a holistic view
- GRM regularly provides senior management and the Board of Directors with independent analysis on risk exposures and recommendations on relevant risk decisions and managerial actions to be taken
- GRM recommends improvements to the risk management framework through a dedicated, independent Internal Validation function, and proposes remedial actions in case of limit breaches
- The GRM structure ensures a proper balance between the need for independence and the risk of excessive isolation from business

Planned Actions: None anticipated.

Principle 23 – The Risk Control function's role

Current Situation:

UniCredit Group agrees with the stated principle and is already in compliance with it, with no material gaps to be covered. In particular:

- *Strategy and decisions*. GRM regularly provides the management body with risk information and analysis. Risk strategies are set in accordance with risk appetite, which also includes target levels for the relevant risk metrics (in addition to limits). Budget is defined consistently with this framework.
- *Transactions with related parties*. GRM is involved in the assessment of transactions with related parties.
- *Complexity of the legal structure*. GRM is involved in assessing the risk impact of creating legal entities and vehicles, and in the defining appropriate capital and liquidity plans in ordinary and stressed circumstances, including the so called living wills for going and gone concern phases.
- *Material changes.* GRM is involved in any relevant corporate structure or business reengineering initiative, and through the DRO structures assesses transactions that may materially affect risk profile
- *Measurement and assessment.* Assumptions on scenarios and correlations are managerially assessed in the stress testing and ICAAP processes, and also subject to independent review in internal validation and audit processes.
- *Monitoring.* Enterprise Risk Management and ICAAP reporting ensure that the current risk profile is monitored and compared with risk appetite and limits. Back-testing procedures are in place for the main risk models. Consistency of subsidiaries activities vis-à-vis defined strategies is assessed through periodic portfolio reporting.
- *Unapproved exposures.* GRM plays a key role in setting risk appetite and risk limits/strategies, as well in assessing reasons underlying limits breaches and recommending corrective measures. Fraud prevention, detection and consequence management involve risk management as appropriate, together with other relevant parties (internal audit and HR).

Planned Actions: None anticipated.

Principle 24 - Chief Risk Officer

Current Situation:

Within UniCredit Group, the Group CRO is assigned responsibility for the Risk Control Function ("RCF") at Group level and maintains managerial responsibility for local RCFs in each relevant legal entity. The Group CRO is directly accountable to the Chief Executive Officer and is a member of the senior-most management body of the bank (the "Executive Management Committee"). He is deputy-chairman of the Group Risk Committee and proposes the Risk Appetite Framework to the Board. The Group CRO also chairs internal CRO committees, including (but not limited to) the Risk Executive Committee and the Portfolio Management Committee.

The CRO has the necessary expertise, independence and operating authority to challenge risk exposures that might otherwise violate risk appetite or operating strategies. Risk related policies describe clearly the approval/veto/escalation process for all major categories of risk, including the role and authority of the CRO.

Planned Actions:

None anticipated.

Suggestion to Regulators:

With reference to the highlighted concept of the CRO's exclusive responsibility for the RCF, we deem it appropriate to stress that in any institution the capability to effectively discharge the role actually depends on several conditions, including:

- the resources allocated,
- the freedom to use resources as needed,
- the soundness of the system's level of performance, including other components of the internal control system.

It is important that responsibility for these prerequisites be clearly assigned to proper persons or bodies at an adequate hierarchical level.

Additionally, in order to permit high quality human resources, it is important that mechanisms exist (within the given fixed and variable compensation framework) to:

- attract and retain skilled people
- permit sufficient exchange of resources so as to improve connections with the business and spread risk culture across the organisation over time.

Principle 25 - Compliance function
Current Situation:
UniCredit has appointed a Group General Counsel, Group Compliance Officer and Head of UniCredit Legal & Compliance Department. It has set up a Global Compliance Department

whose head is responsible for the Group Compliance Function. This latter department assists UniCredit's Board and Committees and UniCredit Group to manage compliance risk, the definition of which is consistent with paragraph 148. Management of these risks is accomplished through the following:

Advice on a pro-active and reactive basis

- Providing advice on existing, proposed and implementing laws, regulations, rules, codes, standards, businesses, products and offices as well as on the structure and set-up of new businesses, products and offices.

Communications

- Issuance of policies and procedures; notes, memos, opinions and notices, the provision of training - in person and electronically - to ensure that documentation reflects UniCredit Group's policies and procedures. In this regard we underline that the several compliance policies are issued to manage compliance risk in each single matter of competence (e.g. AML, Antitrust etc.)

Monitoring and Surveillance

- Performing compliance risk assessment; ranking compliance risk; performing routine surveillance; monitoring the identified issues; escalation of identified issues.

Regulatory Interaction

- Assisting in or managing regulatory audits in its perimeter of competence; self-assessments; regulatory investigations and inquiries; responses to regulatory consultations; responses to *ad hoc* queries; and the development and maintenance relationships with regulators in its perimeter of competence.

In particular, Compliance's responsibility is not extended to fiscal, labour (including D. Lgs n. 81/2008), financial statements (including Law 262/05), BIS II and business continuity, as these areas are overseen by other competence lines including Planning, Finance and Administration, Risk Management and HR, amongst others.

Planned Actions:
Compliance policy issuance follows the defined planning approved by the Board of Directors.

Suggestion to Regulators:
see general remarks

Principle 26 - Internal Audit function

UniCredit definitely agrees with the detailed contents of principle 26.

UniCredit is of the opinion that an Internal Audit Function should be established in each Group's Legal Entity (or bank) and have a formal status within the company (or the bank) ensuring the appropriate standing, authority and independence. In this respect, the Internal Audit Function should be organizationally separated from the activities it should monitor and control. Moreover, it should report directly to the Board of Directors.

The Internal Audit Function should have the right to communicate on its own initiative with any bank staff member and obtain access to any records or files necessary to enable it to fulfill its responsibilities.

UniCredit is of the opinion that the Internal Audit Function should carry out third-level controls,

also by performing on-site audits. In particular, the Internal Audit Function should perform audits in order to check the effectiveness and efficiency of IT systems, organizational processes and company procedures, as well as risk governance and management models and mechanisms, including compliance risk.

Following its audit activities and based on the related findings, Internal Audit should express recommendations to the competent company or function and monitor the implementation of corrective measures, in order to help improve organizational, risk management and control processes.

UniCredit suggests that the Internal Audit Function should provide the Board of Directors with an independent evaluation of the adequacy, effectiveness and efficiency of the whole internal control system. This should be done either directly or through the Audit Committee, and take place periodically (for example, once a year) or, in cases of greater urgency, at the first possible meeting.

UniCredit is of the opinion that Internal Audit should develop methodologies for each phase of the internal audit process in accordance with the International Professional Practices Framework issued by the Institute of Internal Auditors. Additionally, the Function maintains, enhances, updates and distributes them to the Group's internal audit functions.

UniCredit suggests that the Audit Plans should be prepared also based on the results of the Risk Assessment process, which is conducted at least annually on the main elements of the audit universe. The Risk Assessment should influence the planning phase, by defining priorities, nature, frequency and coverage of audits. The Board of Directors (also through the Audit Committee), should approve the Annual Audit Plan and any relevant changes to it.

E. Systems and continuity
Principle 27 - Information system and communication

Current Situation
UniCredit already applies Principle 27.

The information system and communication framework, particularly focused on Information Security, is in place since 2007. This framework, by pyramid design, foresees a General Security Policy and some vertical specific Security policies all issued by HC Security Dpt. The below part of this pyramid framework foreseeees that all LEs have to design and implement all the security procedures compliant with the above mentioned policies. Particularly important, concerning Information system, is the Information Security Management System and related security procedures and processes released by the Information Provider of the UniCredit Group.

158. Management decision making could be adversely affected by unreliable or misleading information provided by systems that are poorly designed and controlled. Thus a critical component of an institution's activities is the establishment and maintenance of information and communication systems that cover the full range of its activities. This information is typically provided through both electronic and non-electronic means.

Current situation:
UniCredit already applies sub-principle n.158,

In order to apply UniCredit Group security policy and protecting adequately the information system, the Group Information Provider has implemented a new Information Security Management Sysytem (ISMS) Framework concerning also Information and communication systems and its activities. The ISMS is fully compliant with ISO 27002 International Security norm. This framework concerns:

- the Organizational chart with related responsibilities and activities in charge to HC and its Information Provider.
- Mission of both Security Departments
- Mission and responsibilities of the Security and Information Risk Committees
- Risk Assessment methodology
- Security processes
- Security procedures vertical for each control objectives declared in ISO27001 norm
- Security portfolio
- Security Key Indicators in terms of Size, Performance and Risk

159. An institution should be particularly aware of the organisational and internal control requirements related to processing information in electronic form and the need to have an adequate audit trail. This also applies if IT systems are outsourced to an IT service provider.

Current situation:
UniCredit already applies sub-principle n.159.

UniCredit defines and publish organizational requirements and internal control requirements inside its own Group policies. According to the UniCredit guidelines the Group Information Provider designed its own processes, in line with ITIL framework and Cobit controls objectives, where for each step formalized in all processes, a specific control is defined and measured in terms of criticality and probability. The target of Risk committee, Organizational Governance and Security Department is to demonstrate that each control defined in processes and procedure is effectively in place. This is done downloading the evidences concerning the control interested.
All these evidences are formally used for 262 (Italian law for corporate responsibilities) assessment and self -certification and also for SAS70 certification that the Group Information Provider is obtaining. This certification will be formally obtained after the audit analysis, performed by external third part (Ernst &Young), that is at the moment in on going phase.
These activities will be finish till the first quarter 2011.

160. Information systems, including those that hold and use data in electronic form, should be secure, independently monitored and supported by adequate contingency arrangements. An institution should consider generally accepted IT Standards when implementing IT systems.

Current situation:
UniCredit already applies sub-principle n.160

The Group Information Provider designed and implemented the above mentioned ISMS in compliance with ISO27001 Control Objectives and ISO 27002 Security requirements.
This framework is implemented by "Shewhart cycle" or "Deming cycle" that could be summarized in the "PLAN – DO- Check- Act" activities.
In particular, the monitoring and improving phase is implemented by Security Key Indicators activities. these indicators help the UniCredit group to understand all the Information

arguments that need of IT and Security improvement to reach and constantly maintain a good level of security in terms of Confidentiality, Integrity and Availability.
Each security indicators is linked to security process or security procedures. This specific link assure that all the topics are measured because the Security procedures itself is fully linked to all the ISO 2700x norm.

Principle 28 - Business continuity management
Current situation:
UniCredit already fully applies Principle 28.

In Italy, the business continuity management has been regulated since 2004 with one of the most advanced and comprehensive regulations in Europe. The main regulations issued are:

- Supervisory regulations on business continuity for banks authorised to do business in Italy [published in the Bank of Italy's Bulletin, no. 7, July 2004].
- Bank of Italy regulations on business continuity – Special Requirements [File No. 311014 dated 23.03.2007]

The last regulation is applied only to the Banking Group personally identified by Bank of Italy as critical player for the Italian financial market. UniCredit has been appointed to follow such regulation.

161. *An institution's business relies on several critical resources (e.g. IT systems, communication systems, buildings). The purpose of Business Continuity Management is to reduce the operational, financial, legal, reputational and other material consequences arising from a disaster or extended interruption to these resources and consequent disruption to the institution's ordinary business procedures. Other risk management measures might be to reduce the probability of such incidents or to transfer their financial impact (e.g. through insurance) to third parties.*

Current situation:
UniCredit already fully applies sub-principle n.161,

The principles and objectives of Business Continuity Management are regulated internally by UniCredit Group policies: Business Continuity Management (including Disaster Recovery), and Crisis Management, both inspired by the main international standards (British Standard BS17799, BS25999).
The above policies have been submitted and approved by the Group's Board of Directors in and outside Italy.
In particular, the Business Continuity Management policy provides that:

- an impact assessment (Business Impact Analysis - BIA) is carried out for each business process in the case of failure to identify the level of "criticality" (analyzing the impact from economic, legal/regulatory and reputational points of view) and "vulnerability".
- the most common crisis scenarios are faced by business continuity plans regarding: the unavailability/destruction of premises, personnel, information system, infrastructure services (such as energy and telecommunications), documentation and special equipment.
- the main strategies of continuity include: the treatment of operational risk (business continuity plan), risk transfer (insurance), the acceptance of risk (risk tolerance/appetite), the elimination of risk (stop activity)

162. *By taking into account external data and performing scenario analysis, an institution should*

carefully analyse its exposure to severe business disruptions and assess (quantitatively and qualitatively) their impact. This analysis should cover all business and support units and the RCF and take into account their interdependency. In addition, a specific independent Business Continuity function, the RCF or the Operational Risk Management function[18] should be actively involved. The results of the analysis should ~~enable~~ contribute an institution to define its recovery priorities and objectives.

Current situation:
UniCredit already fully applies paragraph 162

UniCredit since 2005 has appointed an independent function of Business Continuity Management who has in charge to perform impact analysis and to test the chosen continuity solution.
Furthermore the UniCredit Group has been authorized by the Bank of Italy (since 2008) to use the AMA approach for Capital Measurement and Capital Standards related to operational risk.
In accordance with the requirements of the Basel II AMA approach, periodically (at least once a year) are made specific scenario analysis under the supervision of RCF function.

Suggestion to the regulator:
It would be better to replace "enable" with "contribute" because the scenario analysis is not the only type of risk analysis carried out to determine the criticality of a process (which in turn affects the priorities for recovery).

163. *Contingency and business continuity plans should be in place to ensure an institution reacts appropriately to emergencies and is able to maintain its most important business activities if there is disruption to its ordinary business procedures.*

Current situation:
UniCredit fully complies with sub-principle n. 163.

Business continuity plans are in place to ensure the resumption of company "critical" business processes. A Disaster Recovery Plan has been prepared to restart the information system.

164. *An institution should have recovery plans for critical resources in place to enable it to return to ordinary business procedures in an appropriate timeframe. Any residual risk from potential business disruptions should be consistent with the institution's risk tolerance/appetite.*

Current situation:
UniCredit already fully applies sub-principle n. 164.

One of the main parameters (defined for each process) in the Business Impact Analysis assessment - and that affects the definition of strategies for business continuity - is the RTO (Recovery Time Objective). As a result, each business continuity plan provides and ensures that in the case of a crisis the recovery time is less than or equal to the RTO established for that process.
Furthermore, in accordance with the provisions of the Bank of Italy Regulation and with the Group policies, all risks not managed by the business continuity plans are documented and explicitly accepted by the company. The BC and DR Plans take into account the return to normal operations.

Planned action:
In 2011 the Business Impact Analysis will be performed for all processes considered to be "less critical" in order to formally evaluate all business processes.

165. *Contingency, business continuity and recovery plans should be documented and carefully implemented. The documentation should be available within the business, support units and the RCF, and stored on systems that are physically separated and readily accessible in case of contingency. Appropriate training should be provided. Plans should be regularly tested and updated. Any challenges or failures occurring in the tests should be documented and analysed, with the plans reviewed accordingly.*

Current situation:
UniCredit already fully applies sub-principle n. 165.

In compliance with the Bank of Italy Regulation and the Group policy, all business continuity plans are documented and submitted to the board. The documentation is available in both paper and electronic format.
A copy of the plans was delivered to the Operational Risk Management function as required by the AMA approach and by Operational Risk Management Group-wide Policy.
All organisational units, "owners" of critical processes for which the continuity requirement was requested, have detailed business continuity plans available.
All plans are regularly tested and updated. The tests and the related reports are supervised by the internal audit function. Any matter affecting the operation of the plans which emerge during the test is recorded and, if necessary, the resolution is planned.

F. Transparency
Principle 29 - Empowerment
UniCredit agrees with this principle

Principle 30 - Internal governance transparency
UniCredit agrees with this principle

Contact people:

Heads of Departments/Areas,
Lorenzo Lampiano, Corporate Affairs (CA)
Bailham Mark, Global Compliance (GC)
Massimo Ferrari, Audit Advisory & Quality Assurance
Gabriele Stinco, Risk Management Control
Maurizio Francescatti, Group Risk Management Operating Office
Guido Moscon, Banking Supervisory Relations (BSR)
Giovanni Lanati, Compensation (HR-C)
Sergio Lugaresi, Regulatory Affairs (RA)
Paola Francescucci, Group Organization Development (GOD)
Buson Susanna, Business Continuity & Crisis Management (BC&CM)
Pietro Blengino, Policy Development, Security

CEBS contact:
Marco Laganà, (RA), *Coordinator*, Marco.Lagana@unicreditgroup.eu

Main contributors
Ermanno Bonessi, Head Corporate Law Advice, CA, section A, B and F
Manlio Stefano Nuzzo, Corporate Law Advice, CA. section A, B and F

Enrico Bertulessi, Co-Head of Regulatory Counsel, GC, Principles 11, 14, 25
Antonio La Rocca, Co-Head of Regulatory Counsel, GC, Pr. 12, 25
Marco Ferrari, Head of Global Policies Coordination Unit, GC, Pr. 14
Giuseppe Silvestro, Head of CAMP Monitoring and Reporting Department, GC, Pr. 15, 20, 25
Paola Lattuada, Global Banking Services Counsel Unit, GC, Pr. 14

Ettore Veneziani, Head of Organization Development - Structures And Rules, GOD
Andrea Cremonino, BSR

Erik Banks, Group risk management staff, section C and D
Prezhdarova Ivanka, Group risk management staff, section C and D
Inge Susanne Luppold-Raff, Head of Group Risk Policies Principle 20
Davide Bazzarello, Head of Operational & Reputational Risks Portfolio Management, Pr. 28
Valeria De Mori, Head of Risk Integration & Capital Adequacy, Pr. 18, section C and D
Abhishek Darbari, Group Risk Reporting & Projects, Pr. 18
Massimo Prestipino, Group Risk Policies Principle 20

Patrizia Balit, Head of Audit Advisory & Governance, AA&QA., Principles 21 and 26

Sian Carson, HR-C, Principle 15 and 18
Mariangela De Matteo, HR-C, Principle 15 and 18

Massimo Giambelli, Head of Global Outsourcing Strategy And Governance, Pr. 14
Anna Vicelli, Head General Services, HQ Operational Organization & General Services Pr. 14
Gianni Penzo, ICT Data Protection, Security Pr. 27
Carlo De Marco, BC&CM Pr. 27 and 28
Roberto Saracino, ICT Security, Pr. 27

Regulation & Documentation Management
Andrea Mantovani, Group Organization & Logistics