Consultation paper on draft Guidelines on internal governance

European Banking Authority (EBA)

Index

Introduction

In October 2016 the EBA published draft Guidelines (GL) on internal governance to update the existing GL 44 and introduce additional aspects that aim to foster a sound risk culture

Introduction

In recent years, internal governance issues have received increasing attention from various international bodies. Their main effort has been to correct the institutions' weak or superficial internal governance practices as these faulty practices, while not a trigger for the financial crisis, were closely associated with it and were questionable.

In this regard, in September 2011 the EBA published its Guidelines on internal governance (GL 44) with the objective of enhancing and consolidating supervisory expectations and improving the internal governance framework. Nonetheless, in order to address the potentially detrimental effects of poorly designed corporate governance arrangements on the sound management of risk, and to take into account the new requirements introduced in the CRD in this area, the EBA is updating its GL 44.

- In this context, the EBA published in October 2016 a **Consultation Paper on draft Guidelines on internal governance** that intends to update the GL 44. These draft GL put more emphasis on the duties and responsibilities of the management body in its supervisory function in risk oversight. In particular, this document covers the following aspects:
  - The **role of the management body** regarding internal governance.
  - The **internal governance policy**, **risk culture** and **business conduct**.
  - The **internal control framework**.
  - The principles of **proportionality** and **transparency** that will be applied to the internal governance framework.

This document includes an **analysis of the requirements** arising from the CP GL on internal governance.

Index

Executive summary

These GL on internal governance provide guidance on the following aspects: i) role of the management body; ii) internal governance policy, risk culture and business conduct; iii) internal control framework; and iv) principles applied to the internal governance framework

Executive summary

Scope of application

- These GL are addressed to **credit institutions** and **investment firms**, as defined in the CRR.

Regulatory context

- **Guidelines on internal governance** (GL 44), published by the EBA in September 2011.

Next steps

- Comments to this consultative document shall be submitted by **28 January 2017**.
- CAs across the EU will be expected to implement these GL by **mid-2017**.

Main content

Management body

- Duties and responsibilities of the management body, supervisory and management function, chair of the management body, organisational framework and structure, and committees.

Internal governance policy, risk culture and business conduct

- Internal governance policy (including in a group context), risk culture, corporate values and code of conduct, conflicts of interest, internal alert procedures, reporting of breaches to CAs, and outsourcing policy.

Internal control framework

- Internal control framework, internal control functions (risk management function, compliance function and internal audit function), risk management framework, new products and significant changes, and business continuity management.

Principles applied to the internal governance framework

- Principles of proportionality and transparency applied by institutions when defining their internal governance framework.

Index

Draft GL on internal governance

Role of the management body regarding internal governance

These GL provide guidance on the duties and responsibilities of the management body, which should be defined distinguishing between the supervisory function…

Management body (1/4)

Duties and responsibilities

- The management body must have the **ultimate and overall responsibility** for the institution, and defines, oversees and is accountable for the implementation of the governance arrangements. Its duties should be defined distinguishing between its **management function**, composed of executive members; and its **supervisory function**, composed of non-executive members.
- The responsibilities and duties of the management body should be described in a **written document** and duly **approved by the management body in its supervisory function**. They should include setting, approving and overseeing the implementation of, among others:
  - The **overall strategy** and the **overall risk strategy** (e.g. risk appetite).
  - An adequate, effective and independent **internal control framework**.
  - The amounts, types and distribution of both **internal capital and regulatory capital**.
  - A **remuneration policy** in line with the CRD IV and the EBA GL on sound remuneration policies.
  - Arrangements for ensuring that the **suitability assessment** of its members is carried out effectively.
  - An adequate **risk culture**, and also adequate **corporate culture and values**.
- The management body must oversee the process of **disclosure and communications** and its members should be informed about the overall activity, financial and risk situation of the institution. Moreover, it should monitor and **periodically review** any weaknesses identified regarding the implementation of processes, strategies, etc. related to the above-mentioned responsibilities.

Supervisory function

- The management body in its supervisory function should, among other aspects:
  - Monitor and constructively **challenge the strategy** of the institution, **oversee** the management body in its **management function**, and ensure the **integrity** of the financial information and reporting, and internal control framework, including effective and sound risk management.
  - Have suitable members who do not perform any **executive function**.
  - Oversee the implementation of the **risk culture** and the **strategic objectives**.
  - Ensure that heads of internal control functions are able to act **independently**.
  - Periodically assess the effectiveness of the institution's **internal governance framework**.
  - Implement policies to identify, manage and mitigate actual and potential **conflicts of interest**.

Draft GL on internal governance

Role of the management body regarding internal governance

… and the management function. Moreover, the GL also provide guidance on the role of the chair of the management body as the main responsible for its effective overall functioning

Management body (2/4)

Management function

- The management body in its management function should:
  - **Engage actively in the business** of an institution and **take decisions** on a sound and well-informed basis.
  - Be responsible for the **implementation of the strategies** set by the management body and discuss regularly the implementation and appropriateness of those strategies.
  - Constructively **challenge and review** critically propositions, explanations and information received when exercising its judgement and taking decisions.
  - Comprehensively **report and inform** regularly and without delay the **management body in its supervisory function** of the relevant elements for the assessment of the risks developments affecting or that may affect the institution (e.g. material decisions on business activities and risks taken, the evaluation of the institution's economic and business environment, etc.).

Chair of the management body

- The chair of the management body should lead the management body and be **responsible for its effective overall functioning**, and should also encourage and **promote open and critical discussion** to ensure that dissenting views can be expressed.
- As a general principle, the chair should be an **independent or non-executive member**. The chair in the supervisory function and the CEO of an institution must not be the same person, unless justified by the institution and authorized by the CA.
- The chair should, among other duties:
  - Set the **meeting agenda** and ensure that strategic issues are discussed with priority.
  - Contribute to ensure **clear allocation of responsibilities** between executive and non-executive members of the management body and the existence of an efficient flow of information between them.

Draft GL on internal governance

Role of the management body regarding internal governance

Moreover, the GL also include provisions regarding the management body's committees, in particular in relation to their setting up, composition, processes and types. The GL also specify the duties of the risk and the audit committees

Management body (3/4)

Committees

- All institutions which are themselves **systemic**[1] must establish a **risk and a nomination committee** to advise the management body in its supervisory function[2]. In any case, systemic and non-systemic institutions may establish **other specialised committees** (e.g. ethics, conduct, compliance, etc.).
- Regarding the **composition of the committees**:
  - The members of the risk and nomination committees should not perform **executive functions**.
  - The risk committee should include a **majority of members who are independent** and all of its members should have individually and collectively **appropriate knowledge**, **skills** and **experience**.
  - The specialised committees should be composed of a **sufficient number of independent members**.
  - Each committee should have a chair that is an **independent member** of the management body in its supervisory function.
- Regarding the **processes**, the committees should, among others, have access to all **relevant information** and periodically **review** the content, format and frequency of the information on risk to be reported to them.

Risk committee

- Among other tasks, this committee should:
  - Advise and support the management body in its supervisory function on the monitoring of the institution's overall actual and future **risk appetite** and **strategy** taking into account all types of risks.
  - Assist the management body in its supervisory function to oversee the implementation of the **institution's risk strategy** and corresponding **limits** set.
  - Oversee the implementation of the strategies for **capital and liquidity management** as well as for all the remaining relevant risks of an institution (e.g. market, credit, operational, reputational and IT risks).
  - Provide **recommendations** on necessary adjustments of the risk strategy.

Audit committee

- Among other tasks, this committee should:
  - Monitor the effectiveness of the institution's **internal quality control**, **risk management systems**, and, where applicable, its **internal audit**.
  - Oversee the establishment of **accounting policies** by the institution.
  - Monitor the **financial reporting process** and submit recommendations to ensure its integrity.

(1) Global systemically important institutions or 'G-SIIs', other systemically important institutions or 'O-SIIs', and, as appropriate, other institutions determined by CAs.
(2) Non-systemic nstitutions may establish one committee which exercises the duties of both.

Draft GL on internal governance

Role of the management body regarding internal governance

According to these GL, the management should ensure an organisational framework and structure suitable and transparent. In this regard, they should avoid setting up complex structures and should consider the application of mitigation actions

Management body (4/4)

Organisational framework and structure

- Regarding the **organisational framework**, the management body should:
  - Ensure a **suitable and transparent organisational and operational structure** for the institution and should have a written, clear and detailed description of it.
  - Ensure the **highest level of independence of the internal control functions**, considering the appropriate financial and human resources and powers to effectively perform their role. The allocation of responsibilities within an institution should be clear, well-defined, coherent, enforceable and documented.
  - Be fully aware of the **structure of the management body**, the division of tasks and responsibilities within the management body, its committees, and within the institution.
  - Assess the **elements** of the organisational and operational structure and the **impact of changes** to the groups structure on the soundness of the organisational framework.
- Regarding the **structure**, the management body should:
  - Fully know and understand the organisational and operational structure (**know-your-structure**) and ensure that it is in line with the business, risk strategy and risk appetite.
  - Be responsible for the **approval of sound strategies and policies**.
- Institutions should **avoid setting up complex and potentially non-transparent structures**, taking into account several aspects (e.g. the extent to which the jurisdiction in which the structure will be set up complies effectively with international standards on tax transparency, anti-money laundering, etc.; the extent to which the structure serves an obvious economic and lawful purpose; etc.). The management body should ensure that **appropriate mitigation actions are taken** to avoid the risks of the activities within such structures, including that:
  - The institution has in place **adequate policies and procedures** and documented processes for the consideration, compliance, approval and risk management of such activities.
  - Information concerning these activities and risks is **accessible** to the consolidating institution, internal and external auditors and is reported to the management body in its supervisory function and to the CA.
  - The institution **periodically assesses** the need to maintain such structures.

Draft GL on internal governance

Internal governance policy, risk culture and business conduct

The GL establishes that institutions should have in place an internal governance policy with well-defined, transparent and consistent lines of responsibility, and also a integrated and institution-wide risk culture developed based on the risks that institutions face

Internal governance policy, risk culture and business conduct (1/3)

Internal governance policy[1]

- The management body should **define, adopt and maintain a governance policy** to implement a clear organizational and operational structure with well-defined, transparent and consistent lines of responsibility.
- The **management body in its management function** is responsible for the implementation of that policy whereas in its **supervisory function** is responsible for overseeing its implementation, monitoring the policy's effects and reviewing its design and effectiveness.
  - This policy should be **clear**, **well documented** and **transparent**. Internal control functions should **provide effective input** in accordance with their roles considering how the policy affects the institution's compliance with legislation, regulations and internal policies.
  - Any **amendments** to this policy should also be duly **approved by the management body** and should be communicated to the CA.

Governance policy in a group context

- At the consolidated or sub-consolidated level, the consolidating institution and CAs should ensure that a **group-wide written internal governance policy** describing arrangements, processes and mechanisms is implemented and complied with by all institutions and other entities within the scope of prudential consolidation (including their subsidiaries not subject to the CRD IV).

Risk culture

- A sound and consistent risk culture should be a **key element of institutions' effective risk management** and should enable institutions to make sound and informed decisions. Therefore, institutions should develop an **integrated and institution-wide risk culture** (based on, among others, the risks they face).
- **Staff** of the institution should be **fully aware of their responsibilities** relating to risk management. Thus, business units under the oversight of the management body, should be primarily **responsible for managing risks on a day-to-day basis**, taking into account the institution's risk capacity/appetite.
- A strong risk culture should include at least the followings aspects: i) **tone from the top** (the management body should be responsible for setting and communicating the institution's core values and expectations), ii) **accountability**, which means that relevant staff at all levels should know the core values of the institution, its risk appetite and risk capacity, iii) **effective communication and challenge**, and iv) **incentives** to align risk-taking behavior to the institution's risk profile and its long term interest.

(1) The annex includes a list of the aspects that should be considered when developing and documenting the written internal governance policy.

Draft GL on internal governance

Internal governance policy, risk culture and business conduct

The management body should develop high ethical and professional standards. Moreover, institutions should have in place a policy to identify, manage and mitigate actual and potential conflicts of interest of staff

Internal governance policy, risk culture and business conduct (2/3)

Corporate values and Code of conduct

- The **management body** should develop, adopt, adhere to and promote **high ethical and professional standards** taking into account the specific needs and characteristics of the institution, aimed at reducing the risks to which the institution is exposed. The management body should have **clear and documented policies** for how these standards should be met. In particular, these policies should:
  - Recall that activities should be conducted in compliance with the **applicable laws** and **corporate values**.
  - Promote **risk awareness** through a strong risk culture.
  - Define **acceptable and unacceptable behaviors** (e.g. misconduct, fraud, money laundering, etc.).
  - Clarify that staff are expected to conduct themselves with **honesty** and **integrity**.
  - Ensure that staff are aware of the **potential internal and external disciplinary actions**.

Conflicts of interest

- The **management body** should be responsible for establishing and overseeing the implementation and maintenance of **effective policies** to identify, manage and mitigate actual and potential conflicts of interest of staff. **Material conflict of interest** at management body level, individually and collectively, should be adequately documented, communicated to, discussed and duly managed by the management body.
- A duly approved **written policy** should identify the relationships, services, activities or transactions of an institution[1] in which conflicts of interest may arise (e.g. relationships between an institutions and its qualifying holders, member of the management body, etc.) and should state how these conflicts should be managed.
- The conflict of interest policy should **set out procedures and measures** (e.g. adequate segregation of duties, information barriers, etc.) to be adopted to prevent, identify actual or potential conflicts of interest, assess their materiality, decide on mitigating measures and communicate any material actual or potential conflicts of interest of staff to the management body[2].
- If any conflict of interest is identified, the institution should issue a **statement** as to how this conflict has been satisfactorily mitigated or remedied.

(1) This policy should equally cover the conflict of interest risk specific to the management body in its supervisory function.
(2) A consolidating institution should consider the interests of all its subsidiaries.

Draft GL on internal governance

Internal governance policy, risk culture and business conduct

The GL also provide guidance on the internal alert procedures, the mechanisms for reporting breaches to CAs, and the outsourcing policy of institutions

Internal governance policy, risk culture and business conduct (3/3)

Internal alert procedures

- Institutions should put in place appropriate procedures for the **staff to report potential or actual breaches of regulatory requirements**[1]. To avoid conflicts of interest, reporting of breaches should take place **outside regular reporting lines** (e.g. through the compliance/audit function, or though a 'whistleblowing' procedure[2]).
- The alert procedures should be made **available to all staff** within an institution.
- Information provided by the staff via the alert procedures should, if appropriate, be made available to the management body and other responsible functions (anonymously).
- Institutions should also ensure the **protection of personal data** concerning both the person who reports the breaches and the natural person who is allegedly responsible for a breach.
- The **internal alert procedures** should be documented, and among other aspects they should:
  - Provide clear rules that ensure that confidentiality is guaranteed in all cases.
  - Ensure that the potential or actual breaches raised are assessed and escalated.
  - Ensure that the confirmation of receipt to staff who raised potential or actual breaches is provided.
  - Ensure the tracking of the outcome of reported breaches and appropriate record keeping.

Reporting of breaches to CAs

- CAs should **establish effective and reliable mechanisms to encourage** institutions' **staff to report CAs** on potential or actual breaches of regulatory requirements. They may also encourage employees to first try and seek to use their **institutions' internal alert procedures**.

Outsourcing policy

- The management body should **approve** and regularly **review** and **update the outsourcing policy**, considering the **impact of outsourcing on an institution's business** and the risks it faces (e.g. operational, reputational, concentration risk, etc.). The policy should include the reporting and monitoring arrangements to be implemented.
- The policy should state that outsourcing arrangements should **not hinder effective on-site or off-site supervision** and should not contravene any supervisory restrictions on services and activities.
- An institution **remains fully responsible** for all outsourced services.

(1) It is not be necessary that reporting staff has evidence of it, but a level of initial certainty that provides sufficient reason to launch an investigation.
(2) Procedure to report breaches in an anonymised way.

Draft GL on internal governance
Internal control framework

The GL provide guidance on how internal control functions should be organized, on the resources of the internal control functions, on outsourcing, and on how the internal control framework is implemented

Internal control framework (1/5)

Internal control

- Institutions should develop and maintain a strong and comprehensive **internal control framework** that should cover the whole organization, including the **management body's responsibilities and tasks**, and **activities of all business lines and internal units** including internal control functions, the outsourced activities and distribution channels.
- It should also include **risk management**, **compliance** and **internal audit functions**. In this regard, the risk management function and compliance function may be combined whereas the internal audit function should not be combined with another internal control function.

Heads of internal control functions

- A **member of the management body in its management function** may be responsible for an internal control function provided that the member does not have other mandates which would compromise the members' internal control activities and the independence of the internal control function.
- When a head is **not part of the management body in its management function**, the position should be established at an adequate hierarchical level and be independent of the business areas it controls.

Resources

- Internal control functions should **have sufficient resources** and **access to necessary training** to fulfil their mission. They should have an **adequate number of qualified staff** (both at parent level and subsidiary level).

Outsourcing

- The **operational tasks of the internal control functions may be outsourced** considering the proportionality principle, to the consolidating institution or another entity within or outside of the group with the **consent of the management bodies** of the institutions concerned.

Implementation

- Institutions should establish, maintain and regularly update **adequate written internal control policies**, mechanisms and procedures that should be approved by the management body.
- They should also **communicate those policies, mechanisms and procedures to all staff** and every time material changes have been made.
- The internal control functions should verify that these policies, mechanisms and procedures are **correctly implemented**.

Draft GL on internal governance

Internal control framework

The internal control framework should include a risk management function, which should be established to implement risk policies and the risk management framework of the institution…

Internal control framework (2/5)

Internal control: functions

- The internal control functions include a **risk management function**, a **compliance function** and an **internal audit** function.

Risk management function (RMF)

- Institutions should establish a RMF with **sufficient authority**, **stature**, **resources** to implement risk policies and the risk management framework.
- Accordingly, it should be an **institution's central organisation feature**[1] and should have **direct access** to the management body in its supervisory function and committees, and to all business lines and other internal units that have the potential to generate risk as well as to relevant subsidiaries and affiliates.
- Staff within RMF should possess **sufficient knowledge**, **skills** and **experience** on risk management techniques and procedures and on markets and products and have access to regular training.
- The RMF should be **independent of the business lines and units whose risks it controls** but should not be prevented from interact with them.
- The RMF should provide **relevant independent information**, analyses and expert judgment on risk exposures, and advice on proposals and risk decisions made by business lines or internal units and the management body as to whether they are consistent with the institution's risk appetite and strategy.
- The RMF may recommend **improvements** to the risk management framework and **corrective measures** to remedy breaches of risk policies, procedures and limits.
- Regarding the **RMF's role**, it should be actively involved in risk strategy; in identifying, measuring, assessing, managing, monitoring and reporting risks; etc.
- The **head of the RMF** should be responsible for providing comprehensive and understandable information on risks. When is not justified to appoint a person only dedicated to this function, it **can be combined with the compliance function**.

(1) Systemic institutions may consider establishing dedicated RMFs for each material business line. However, there should be a central RMF, including a group RMF in the consolidating institution of a group.

Draft GL on internal governance
Internal control framework

…as well as a compliance function to manage the institution's compliance risk, and an internal audit function which should assess, among others, the quality of the internal control framework

Internal control framework (3/5)

Compliance function

- An institution should establish a permanent and effective compliance function to manage its **compliance risk** and appoint a person responsible for this function across the entire institution (the Compliance Officer or Head of Compliance).
- The **head of the compliance function** should be able to **report directly** where appropriate and on his or her own initiative the **management body in its supervisory function**.
- The compliance function should be **independent** of the business lines and internal units it controls and have **sufficiently authority, stature and resources**.
- Staff within the compliance function should possess **sufficient knowledge**, **skills** and **experience** on compliance and procedures and have access to regular training.
- Moreover, it should **advise the management body** on laws, rules, regulations and standards the institutions need to comply with and assess the possible impact of changes in the regulatory environment.

Internal audit function (IAF)

- An institution should set up an **independent and effective internal audit function** taking into account the proportionality criteria and appoint a person responsible for this function across the entire institution. In this regard, the IAF should:
  - Be **independent** and have sufficiently authority, stature and resources.
  - Perform an **independent review** of the compliance of all activities and units of an institution.
  - Assess the **quality of the internal control framework** by taking into account, among others, the appropriateness of the institution's governance framework, whether existing policies and procedures remain adequate and comply with legal requirements and with its risk appetite and strategy, etc.
- The **head of the IAF** should be able to **report directly** and on his own initiative the **management body in its supervisory function** of the non-implementation of the corrective measures decided on.
- Internal audit work should be performed in accordance with an **audit plan** that should be drawn up **at least once a year** on the basis of the annual control objectives in line with the guidance of the management body in its supervisory functions.

Draft GL on internal governance
Internal control framework

Institutions should have a risk management framework across all the institution's business lines and internal control functions. The GL include provisions on how this framework should be set

Internal control framework (4/5)

Internal control: risk management

- As part of the overall internal control framework, institutions should have a holistic wide **risk management framework** extending across all its business lines and internal control functions. This framework should:
  - Encompass **on and off balance sheet risks** and **actual and future risks** may be exposed to (i.e. financial and non-financial risks[1]).
  - Include **policies**, **procedures**, **risk limits** and **controls** ensuring adequate, timely and continuous identification, measurement or assessment, monitoring, management, mitigation and reporting of the risks at the business line, institution and group level.
  - **Evaluate risks through bottom up and bottom down** assessments.
  - Provide specific **guidance** on the **implementation of its strategies** which should establish and maintain internal limits consistent with the institution's risk appetite, capital base and strategic goals.
  - Ensure that whenever **breaches of risk limits** occur, there is a defined **process to escalate and address them** with an appropriate follow up.
  - Be subject to **independent internal review** and reassessed regularly against the institution's risk appetite, taking into account information from the RMF and, where established, the risk committee.
  - Develop appropriate methodologies when identifying and measuring risks, including both **forward-looking** (e.g. scenario analysis and stress tests) and **backward-looking tools** (that should assess the actual risk profile and compare it against the institution's risk appetite).
- The **ultimate responsibility** for risk assessment lies solely **with the institution** which accordingly should evaluate its risks and should not exclusively rely on external assessments (e.g. external credit ratings).
- Decisions which determine the level of risks taken should not only be based on **quantitative information** or model outputs, but should use a **qualitative approach** (including expert judgment and critical analysis).
- Regular and transparent **reporting mechanisms** should be established so that the **management body**, its **risk committee**, and **all relevant units** in an institution are provided with reports in a timely, accurate, concise, understandable and meaningful manner. The reporting framework should be well defined, documented and duly approved by the management body.

(1) Including credit, market, liquidity, concentration, operational, information technology, reputational, legal, conduct, compliance and strategic risks.

Draft GL on internal governance
Internal control framework

Furthermore, institutions should have a new product approval policy (NPAP) to address the development of new markets, products and services, and a sound Business Continuity Management

Internal control framework (5/5)

Internal control: new products

- Institutions should have in place a well-documented **new product approval policy (NPAP)**, approved by the management body, which addresses the development of new markets, products and services and significant changes to existing ones. They should also have appropriate **change policies for material changes** to processes (e.g. new outsourcing arrangements) and systems (e.g. IT change processes)[1].
- In this regard, a **NPAP** should:
  - **Cover every consideration** to be taken into account before deciding to enter new markets, deal in new products, launch a new service or make significant changes to existing products or services.
  - Include the **definition of 'new product/market/business/significant changes'** to be used in the organisation and the internal functions to be involved in the decision-making process.
  - Set out the **main issues** to be addressed before a decision is made (e.g. regulatory compliance, accounting, pricing models, impacts on risk profile, etc.). The decision to launch a new activity should clearly state the business unit and individuals responsible for it.
- The **RMF** should also be involved in **approving new products** or **significant changes** to existing products, processes and systems and should have a clear overview of the **roll-out of new products**.

Business Continuity Management

- Institutions should establish a sound Business Continuity Management to **reduce the operational, financial, legal, reputational and other material consequences** from a disaster or extended interruption on several critical resources (e.g. IT systems).
- They should analyse their **exposure to severe business disruptions** and assess (quantitatively and qualitatively) their potential impact, using internal and/or external data and scenario analysis.
- On the basis of the above analysis, an institution should put in place **contingency and business continuity plans** and **recovery plans** which should be documented and carefully implemented.
- In addition, a specific independent Business Continuity function part of the RMF, the **operational risk management function**, should be actively involved for those institutions permitted to use AMA.

(1) The compliance function, in collaboration with the RMF, should be responsible for ensuring internal compliance with these policies.

Draft GL on internal governance

Principles applied to the internal governance framework

The EBA specifies that institutions should apply the proportionality and transparent principles in order to establish internal governance arrangements in line with the individual risk profile and business model of the institution and to inform and update the relevant staff, respectively

Principles applied to the internal governance framework

Proportionality

- Institutions should take into account their **size**, **internal organization** and the **nature**, **scale** and **complexity** of their activities when developing and implementing internal governance arrangements.
- Among others, **institutions** and **CAs should consider** the geographical presence of the institution and the size of the operations in each jurisdiction, the legal form and whether the institution is part of a group, etc.
- According to the proportionality principle:
  - Systemic institutions and more complex institutions and groups should have **more sophisticated governance arrangements**.
  - Small and less complex institutions and groups may implement **simpler governance arrangements**.

Transparency

- The management body should **inform and update the relevant staff** about the institution's strategies and policies in a clear and consistent way, at least to the level needed to carry out their particular duties (e.g. through written policies, manuals, etc.).
- Where parent undertakings are required by CAs to publish annually a description of their legal structure and governance and organisational structure of the group of institutions, the information should include **all entities within its group structure**, **by country**.
- The **publication should include**, among others:
  - An overview of the **internal organization** of the institution and its group structure, including the main reporting lines and responsibilities.
  - Any **material changes** compared to the previous publication and respective date thereof.
  - New **legal**, **governance** or **organizational structures**.
  - An overview of **material outsourcing** of activities, processes and systems.
  - The nature, extent, purpose of close links between **other credit institutions** and other natural or legal persons, including the names and seat.
  - Information on the structure, organization, responsibilities and members of the **management body**.
  - A list of the **committees of the management body** in its supervisory function and their composition.

Index

Next steps

Comments to this consultation paper shall be submitted by 28 January 2017.
CAs will be expected to implement these GL by mid-2017

Next steps

- Comments to this consultative document shall be submitted by **28 January 2017**.
- CAs across the EU will be expected to implement these GL by **mid-2017**. The existing Guidelines on internal governance (GL 44) will be repealed when the revised Guidelines enter into force.

Index

Annex

Internal governance policy (written and documented policy)

Institutions should consider several aspects (e.g. shareholder structures, group structure if applicable, etc.) when developing and documenting the written internal governance policy

Internal governance policy (written document)

1. Shareholder structure

2. Group structure if applicable (legal and functional structure)

3. Composition and functioning of the management body (with impact on the group, if applicable)

a) selection criteria
b) number, length of mandate, rotation, age
c) independent members of the management body
d) executive members of the management body
e) non-executive members of the management body
f) internal division of tasks, if applicable

4. Governance structure and organization chart (with impact on the group, if applicable)

a) Specialized committees
  i. composition
  ii. functioning

b) management committee, if any
  i. composition
  ii. functioning (internal regulation)

5. Key functions holders

a) Head of risk management function
b) Head of compliance function
c) Head of internal audit function
d) Chief Financial Officer (CFO)
e) other key function holders

6. Internal control framework

a) description of each function (its organisation resources, stature, authority
b) description of the risk management framework including risk strategy
c) weaknesses identified by each internal control functions and measures taken
d) recommendations made by the internal audit function and measures taken

7. Organisational structure (with group impact, if applicable)

a) operational structure, business lines, and allocation of competences and responsibilities
b) outsourcing
c) range of products and services
d) geographical scope of business
e) free provision of services
f) branches
g) subsidiaries, joint ventures, ...
h) use of off-shore centres

8. Code of conduct and behaviour (with group impact, if applicable)

a) strategic objectives and company values
b) internal codes and regulations, prevention policy
c) conflicts of interest policy
d) whistleblowing

9. Status of the internal governance policy with date

a) development
b) last amendment
c) last assessment
d) approval by the management body