Final Guidelines on internal governance

European Banking Authority (EBA)

www.managementsolutions.com

Research and Development

November 2017

Index

Introduction

In September 2017 the EBA published Final Guidelines (GL) on internal governance, that update the existing GL 44 and puts more emphasis on the duties and responsibilities of the management body in its supervisory function in risk oversight

Introduction

In recent years, internal governance framework issues have received increasing attention of various international bodies. In fact, their main effort has been to correct the institution's 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.

According to the CRD IV, the EBA is mandated to further harmonise institutions' internal governance arrangements, processes and mechanisms within the EU. 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.

- In this context, following the consultation launched in October 2016, the EBA published **Final Guidelines on internal governance** that update GL 44 and 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 and composition of the **management body and committees** (risk, nomination and remuneration committees)
  - The **governance framework**.
  - The **risk culture** and **business conduct**.
  - The **internal control framework** and mechanisms.
  - The **business continuity management**.
  - The principles of **proportionality** and **transparency.**

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

Index

Executive summary

These GL provide guidance on : i) role of the management body and committees; ii) governance framework; iii) risk culture and business conduct; iv) internal control; v) business continuity management; and vi) principles applied to the internal governance framework

Executive summary

Scope of application	Regulatory context	Next steps
• These GL are addressed to **credit institutions** and **investment firms**, as defined in the CRR.	• **Guidelines on internal governance** (GL 44), published by the EBA in September 2011.	• These GL will apply as of **30 June 2018** to CAs, and to institutions. • The GL 44 will be repealed on the same date.

Main content

Management body and committees

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

Governance framework

- Organisational framework and a suitable and transparent structure, organisational framework in a group context and outsourcing policy considering the impact of outsourcing on an institution's business and the risks it faces.

Risk culture and business conduct

- Integrated and institution-wide risk based on, among other, the risk they face, conflicts of interest, internal alert procedures, reporting of breaches to CAs.

Internal control framework and mechanisms

- Internal control framework and risk management framework, new products, internal control functions (heads and resources), as well as RMF[1], compliance and internal audit.

Business continuity management

- Implementation of a Business Continuity Management to reduce the consequences from a disaster or extended interruption.

Principles applied to the internal governance framework.

- Principles of proportionality (according to their size, internal organization and the nature, scale and complexity of their activities) and transparency when defining their internal governance framework.

(1) Risk Management Function.

Index

Detail

Role and composition of the management body and committees

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

Management body and committees (1/4)

Role 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. These duties should be clearly defined distinguishing between **executive members**[1] and **non-executive members**[2].
- The responsibilities and duties of the management body should be described in a **written document** and duly approved by the management body and should include setting, approving and overseeing the implementation of, among others:
  - The **overall business strategy** and also the **overall risk strategies** (e.g. risk appetite, risk management framework)
  - 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 these GL.
  - Arrangements for ensuring the management body's **individual** and **collective suitability assessment**.
  - Arrangements aimed at ensuring the internal functioning of each **committee**.
  - Adequate **risk and corporate cultures**.
- 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 weakness identified on the implementation of processes, strategies, etc.

Management function

- The management body should **engage actively in the business** of an institution and should **take decisions** on a sound and well- informed basis.
- The management function of the management body involves, among others:
  - **Implementation of the strategies** set by the management body and discuss regularly their implementation and appropriateness of those strategies.
  - Constructively **challenge and critically review** propositions, explanations and information received, when exercising its judgement and taking decisions.
  - **Report and inform** regularly the management body in its supervisory function of the relevant elements for the assessment of a situation, the risks and developments affecting or that may affect the institution.

(1) Members of the management body in its management function.
(2) Members of the management body in its supervisory function.

Role and composition of the management body and committees

… and the supervisory 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 and committees (2/4)

Supervisory function

- The management body should, among others:
  - Monitor and constructively **challenge the strategy** of the institution, oversee the management body in its management function, including monitoring and scrutinising its individual or collective performance.
  - Periodically assess the effectiveness of its **internal governance framework**.
  - Oversee the implementation of the **risk culture**, **audit plan** and institution's strategic objectives, as well as the the integrity of financial information and **reporting**.
  - Ensure that heads of internal control functions are able to act **independently** to other internal bodies.
  - Oversee the implementation and maintenance of a code of conduct or similar and effective policies to identify, manage and mitigate actual and potential **conflicts of interest**.

Chair of the management body

- The chair of the management body should lead the management body, should contribute to an **efficient flow of information** within the management body and between the management body and the committees thereof, should 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 a **non-executive member**. Therefore, the chair in the supervisory function and the **CEO of an institution must not be the same person**, unless justified by the institution and authorised 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 duties** between members of the management body and the existence of an efficient flow of information between them.

Role and composition of the management body and committees

Moreover, they also provide guidance on the committees in particular regarding their setting up, composition and processes

Management body and committees (3/4)

Committees

- All institutions which are themselves **significant**[1] (at individual, sub-consolidated and consolidated level) **must establish risk, nomination and remuneration committees** to advise the management body in its supervisory function[2].
- **Non-significant institutions**, including when they are within the scope of prudential consolidation of an institution that is significant in a sub-consolidated or consolidated situation, **are not obliged to establish those committees**. Where no risk or nomination committee is established, those committees should be construed as applying to the management body in its supervisory function
- Institutions may establish **other specialised committees** (e.g. ethics, conduct and compliance committees).
- Regarding the **composition of the committees**:
    - All committees should be chaired by a **non-executive member** of the management body, should be composed of at least **three members**, and should not be composed of the same group of members that forms another committee.
    - Institutions should consider the **occasional rotation of chairs** and members of committees, taking into account the specific experience, knowledge and skills.
    - The risk and nomination committees should be composed of **non-executive members**.
    - Further, in **G-SIIs and O-SIIs**, the risk and nomination committees should include a majority of members who are independent and be chaired by an independent member.
    - In **other significant institutions**, determined by CAs or national law, the risk and nomination committees should include a sufficient number of members who are independent and the risk committee should be chaired, where possible, by an independent member.
    - In **all institutions**, the chair of the risk committee should be neither the chair of the management body nor the chair of any other committee.
- Likewise, the committees should regularly report to the management body in its supervisory function, have access to all relevant information and data necessary, etc.

(1) Global systemically important institutions or 'G-SIIs', and other systemically important institutions or 'O-SIIs', and, as appropriate, other institutions determined by the CA.
(2) Non-significant institutions could establish only one committee which should exercise duties of both.

Detail

Role and composition of the management body and committees

The GL also specify the duties of the risk, the audit and the combined committees

Management body and committees (4/4)

Risk committee

- Among other tasks, this committee should:
  - Advise and support 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 other relevant risks of an institution (i.e. market, credit, operational and reputational risks).
  - Provide **recommendations** on necessary adjustments to 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 function**.
  - Oversee the establishment of **accounting policies** by the institution.
  - Monitor the **financial reporting process** and submit recommendations to ensure its integrity.

Combined committees

- CAs may allow institutions that are not considered significant to **combine the risk committee** with, where established, **the audit committee**.
- Where risk and nomination committees are established in **non-significant institutions**, they may combine the committees. If they do so, those institutions should document the reasons why they have chosen to combine the committees and how the approach achieves the objectives of the committees.
- Institutions should at all times ensure that the members of a combined committee possess, individually and collectively, the necessary **knowledge, skills and expertise**.

Detail

Governance framework

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

Governance framework (1/2)

Organisational framework and structure[1]

- Regarding the **organisational framework**, the management body should:
  - Ensure a **suitable and transparent organisational and operational structure** for that institution and should have a written, clear and detailed description of it.
  - Ensure that the internal control functions are **independent of the business lines** they control, considering the appropriate financial and human resources and powers to effectively perform their role. The reporting lines and the allocation of responsibilities, in particular among key function holders, should be clear, well-defined, coherent, enforceable and documented.
  - Oversee and manage effectively the **risks the institution or the group faces** or the ability of the CA to effectively supervise the institution.
  - Assess whether and how **material changes** to the group's structure (e.g. setting up of new subsidiaries, mergers and acquisitions, etc.).
- Regarding the **structure**, the management body should among others:
  - Fully know and understand the organisational and operational structure (**know-your-structure**) and ensure that it is in line with the business and 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.

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

Governance framework

Further, the GL establishes that the institution's governance policy should be implemented at group level, and that institutions are fully responsible for all outsourced services

Governance framework (2/2)

Organisational framework in a group context

- The consolidating institution (at consolidated or sub-consolidated level) 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).
- A consolidating institution should consider the **interests of all its subsidiaries**, and how strategies and policies contribute to the interest of subsidiaries and the interest of the group as a whole over the long term.

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.
- An institution **remains fully responsible** for all outsourced services and activities and management decisions arising from them.
- 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.

Detail

Risk culture and business conduct

The GL established that institutions should have an integrated and institution-wide risk culture developed based on the risk that the institution faces, and that the management body should develop high ethical and professional standards

Risk culture and business conduct (1/2)

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**, thus 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.

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:
  - Remind that activities should be conducted in compliance with **applicable laws** and **corporate values**.
  - Promote **risk awareness** through a strong risk culture.
  - Provide **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**.

Risk culture and business conduct

Moreover, institutions should have in place a policy to identify, manage and mitigate actual and potential conflicts of interest at institutional level and for staff. The GL also provide guidance on the internal alert procedures and on the reporting of breaches

Risk culture and business conduct (2/2)

Conflicts of interest

- **Conflicts of interest policy at institutional level**[1]. The management body should be responsible for establishing, approving and overseeing the implementation and maintenance of effective policies to identify, manage and mitigate actual and potential conflicts of interest at institutional level. Institutions' measures to manage or where appropriate mitigate conflicts of interest should be documented and include, inter alia, appropriate segregation of duties, information barriers, etc.
- **Conflicts of interest policy for staff**. The management body should be responsible for mitigating actual and potential conflicts between the interests of the institution and the private interests of staff, including members of the management body which could adversely influence the performance of their duties and responsibilities.
  - A duly **approved policy** should be established and it should cover, among other, certain situations or relationship where conflicts of interests may arise (e.g. economic interests, personal or professional relationships, other employment, etc.).
  - This policy should set out **procedures** (e.g. entrusting conflicting activities or transactions to different persons, preventing staff from having inappropriate influence, etc.) for preventing conflicts of interests.

Internal alert procedures

- Institutions should put in place appropriate procedures for the **staff to report potential or actual breaches of regulatory requirements** (available to all staff within an institution)[2]. To avoid conflicts of interest, reporting of breaches by staff should take place **outside regular reporting** lines (e.g. through the compliance function, the audit function or an independent internal whistleblowing procedure).
- 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, among others, be documented, protect staff who raise concerns, etc.

Reporting of breaches

- CAs should **establish effective and reliable mechanisms** (e.g. for the receipt of report on breaches) **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**.

(1) A consolidating institution should consider the interests of all its subsidiaries
(2) It should not be necessary that reporting staff has evidence of it, but a level of initial certainty that provides sufficient reason to launch an investigation.

Internal control framework and mechanisms

These GL provide guidance on how internal control framework should be organised and how internal control is implemented

Internal control framework and mechanisms (1/5)

Internal control framework

- Institutions should develop and maintain a **positive culture** towards risk control and compliance within the institution and a **robust and comprehensive internal control framework**.
- Under this framework, **institutions' business lines** should be responsible for managing the risks they incur in conducting their activities and should have controls in place that aim to ensure compliance with internal and external requirements.
- The internal control framework should be adapted on an individual basis to the specificity of its **business**, its **complexity and the associated risks**, taking into account the group context.
- The internal control framework should cover the **whole organisation**, including the management body's responsibilities and tasks, and the activities of all business lines and internal units, including internal control functions, outsourced activities and distribution channels.
- Among other aspects, the **internal control framework** of an institution should ensure effective and efficient operations, prudent conduct of business, etc.

Implementing an internal control

- The **management body** should be responsible for establishing and monitoring the adequacy and effectiveness of the internal control framework processes and mechanisms, and for overseeing all business lines and internal units, including internal control functions (such as risk management, compliance and internal audit functions).
- 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. Internal control functions should verify the implementation.

Internal control framework and mechanisms

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 and mechanisms (2/5)

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** that the institution may be exposed to (i.e. financial and non-financial risks[1]).
  - **Evaluate risks** from the **bottom up and** from the **top down**, within and across business lines, using consistent terminology and compatible methodologies at consolidated or sub-consolidated level.
  - 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 consolidated or sub-consolidated levels.
  - 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 determination of the level of risk taken should not only be based on **quantitative information** or model outputs, but should use a **qualitative approach** (including expert judgment and critical analysis).
- 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).
- Effective **risk reporting** (i.e. well defined, documented and duly approved by the management body) involves sound internal consideration and communication of risk strategy and relevant risk data (e.g. exposures and key risk indicators).

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

Internal control framework and mechanisms

The GL provide that institutions should adopt a new product approval policy (NPAP) and that the internal control framework should include a risk management function, a compliance function and an internal audit function

Internal control framework and mechanisms (3/5)

Internal control: new products

- Institutions should have in place a well-documented **new product approval policy (NPAP)**, approved by the management body, that addresses the development of new markets, products and services and significant changes to existing ones, as well as exceptional transactions.
- The policy should in addition encompass **material changes** to related processes (e.g. new outsourcing arrangements) and systems (e.g. IT change processes).
- In this regard, a NPAP should: i) **cover every consideration** before deciding to enter new markets, deal in new products, launch a new service or make significant changes to existing products or services; ii) 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; iii) set out the **main issues** to be addressed before a decision is made (e.g. regulatory compliance, accounting, pricing models, etc.).
- 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**.

Internal control: functions

- The internal control functions should include a **risk management function**, a **compliance function** and an **internal audit** function. The risk management function and compliance function may be combined. The internal audit function should not be combined with another internal control function.

Heads and independence of the functions

- Heads of internal control functions should be set out at an adequate hierarchical level with appropriate authority and stature to fulfil his or her responsibilities. They should be **independent** of the business lines or units they control, and should report and be directly accountable to the management body.
- In order to ensure their independence, several conditions should be followed (e.g. their staff should not perform operational tasks that they are intended to monitor, they should be separately organised, etc.).

Resources of internal control functions

- Internal control functions should **have sufficient resources**. They should have an **adequate number of qualified staff** (both at parent level and subsidiary level) and should be qualified on an on- going basis, and should receive training as necessary.

Internal control framework and mechanisms

Regarding these internal control functions, the GL specify that the risk management function should consider the risk policies and the risk management framework of the institution,…

Internal control framework and mechanisms (4/5)

Internal control functions: RMF

- Institutions should establish a RMF with **sufficient authority**, **stature**, **resources** to implement risk policies and the risk management framework.
- Accordingly, it should be a **central organisation feature of the institution**[1] and should have **direct access to the management body** in its supervisory function and committees, to all business lines and other internal units that have the potential to generate risk, and 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. Interaction between the operational functions and the RMF should facilitate the objective that all the institution's staff bears responsibility for managing risk.
- 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 and decisions (e.g. the RMF should provide the management body with all relevant risk-related information to enable it to set the institution's risk appetite level, should assess the robustness and sustainability of the risk strategy and appetite, etc.); in material changes; in identifying, measuring, assessing, managing, monitoring and reporting risks; and in unapproved exposures.
- 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** or can be performed by another senior person (with no conflict of interest).

(1) Significant 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.

Detail

Internal control framework and mechanisms

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

Internal control framework and mechanisms (5/5)

Internal control functions: compliance

- Institutions should establish a **permanent** and **effective** compliance function to manage **compliance risk** and should appoint a person responsible for this function across the entire institution (the compliance officer or head of compliance).
- 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.
- The management body in its supervisory function should **oversee the implementation** of a well-documented compliance policy, which should be **communicated to all staff.**
- Moreover, it should **advise the management body** on laws, rules, regulations and standards the institutions need to comply with and assess the impacts of changes in the regulatory environment.

Internal control functions: internal audit

- Institutions 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 (e.g. monitoring tools and risk analysis methods).
  - 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 internal control objectives.

ManagementSolutions
Making things happen

Detail

Business continuity management

Institutions should have a Business Continuity Management to reduce risk´s impacts arising from a disaster or extended interruption

Business continuity management

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.
- In this regard, 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 establish **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].

(1) Advanced Measurement Approaches (AMA)

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

These Final GL on internal governance will apply as of 30 of June 2018.
The existing GL 44 will be repealed on the same date

Next steps

- These GL will apply as of **30 June 2018** to CAs across the EU, as well as to institutions on an individual and consolidated basis.
- The existing Guidelines on internal governance (GL 44) will be repealed on the same date.

Index

Annex
Internal governance 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

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) Specialised committees
  i. composition
  ii. functioning

b) Executive 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

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

ManagementSolutions
Making things happen