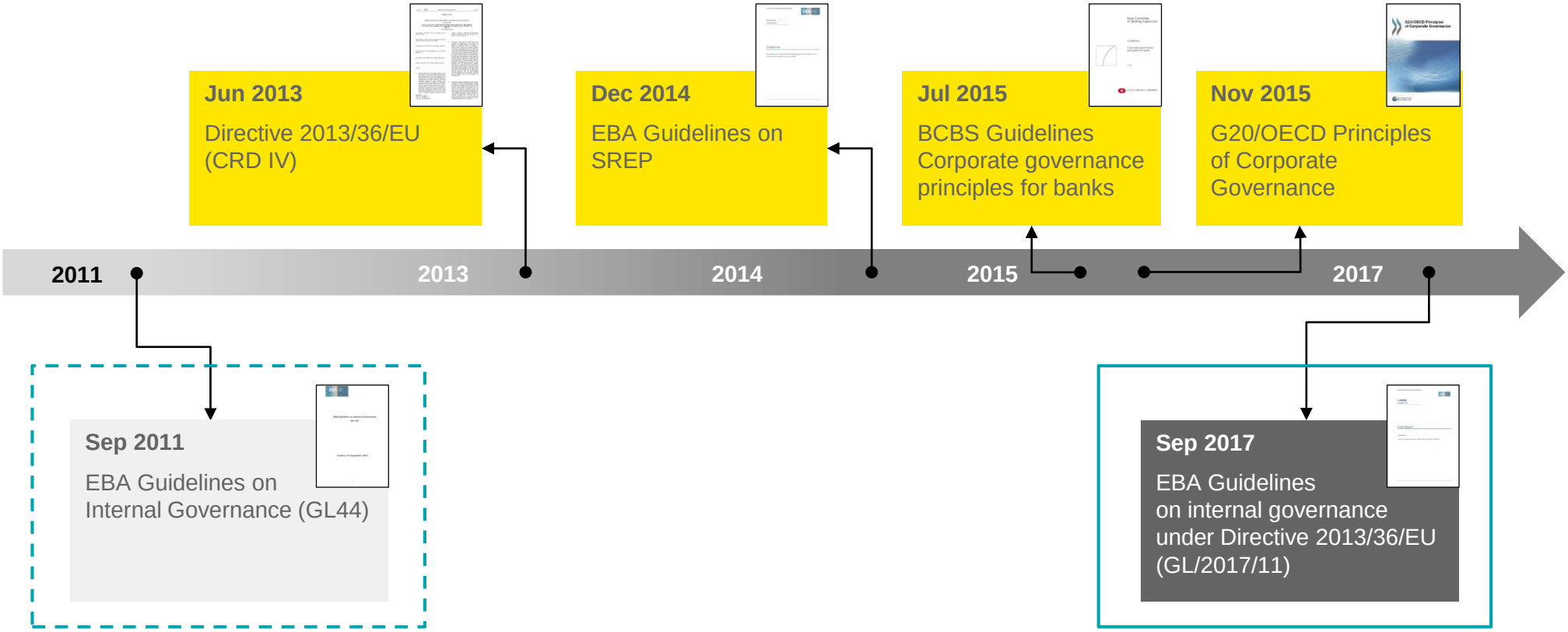
New EBA Guidelines (GL/2017/11) on internal governance

What's new?

7. november 2018

Building a better working world

Overview of the new EBA Guidelines (GL/2017/11) on internal governance



Summary of GL/2017/11

- **Regulatory references**: Based on GL44 and taking into consideration a number of global principles and EU guidelines on corporate governance
- **Objectives:** To further harmonize institutions' internal governance arrangements, processes and mechanisms within the EU in line with the requirements introduced by Directive 2013/36/EU (CRD IV)
- **Scope of application:** Applicable for governance arrangements of CRR credit institutions and investment firms, incl. their organizational structure, corresponding lines of responsibility, processes to identify, manage, monitor and report risks, and internal control framework
- **Timeline:** To enter into force on 30 June 2018 and effectively repeal GL44 of 27 September 2011

A general comparison between GL44 and GL/2017/11

MAIN CONTENT IN GL44

A. Corporate Structure and Organization
B. Management body
C. Risk management
D. Internal control
E. Information systems and business continuity
F. Transparency

MAIN CONTENT IN GL/2017/11

I. Proportionality
II. Role and composition of the management body and committees
III. Governance framework
IV. Risk culture and business conduct
V. Internal control framework and mechanisms
VI. Business continuity management
VII. Transparency

General Comparison

- **New content** introduced in GL/2017/11
  - New terminology, new expectation and new topic
- **Significant changes** to requirements in GL/2017/11 as compared to GL44
  - Risk culture, Management oversight, Risk management, Offshore activities and Change processes

New terminologies, expectations and topics have been introduced in GL/2017/11

TERMINOLOGY

Risk appetite / risk capacity & Risk Management Function

- Terms **"risk appetite" and "risk capacity"** are introduced as aligned with BCBS principles and EBA SREP guidelines, to **replace "risk tolerance / appetite"** in GL 44
  - "Risk capacity" means the maximum level of risk an institution is able to assume, and "risk appetite" the aggregate level and types of risk it is willing to assume within risk capacity
- In line with CRD IV, the term **"risk management function (RMF)"** is referenced regarding 2nd line of defense instead of **"risk control function (RCF)"** as in GL 44

EXPECTATION

Proportionality (Title I, 17 – 19)

- As required under CRD IV Art. 74(2), internal governance arrangements should be consistent with the individual risk profile and business model of the institution
  - When developing and implementing internal governance arrangements, institutions should take into account **size** and **internal organization**, as well as **nature**, **scale** and **complexity** of their **activities**
  - **Significant institutions** should have more sophisticated governance arrangements, while **small and less complex institutions** may implement simpler governance arrangements
  - A **list of criteria** for institutions and CAs in applying the principle of proportionality

TOPIC

Conflict of interest policy for staff (Title IV, 106 - 116)

- The **management body** should be responsible for **establishing**, **approving** and **overseeing** the **implementation** and **maintenance of effective policies** to identify, assess, manage and mitigate or prevent **actual** and **potential conflicts** between **the interests of the institution** and **the private interests of staff**, including members of the management body
- The policy should set out set out the **processes** for **reporting** and **communication** to the responsible function under the policy; should lay out **procedures**, **measures**, **documentation requirements** and **responsibilities** for the identification and prevention of conflicts of interest, for the assessment of their materiality and for taking mitigating measures; and should specifically cover **the risk of conflicts of interest** at the level of the **management body**

Reporting of breaches to CAs (Title IV, 124 - 125)

- CAs should establish **effective** and **reliable mechanisms** to enable institutions' staff to **report** to competent authorities **relevant potential** or **actual breaches of regulatory requirements**, including protection measures and a dedicated whistleblowing department, unit or function

Significant changes have also been made to strengthen various aspects of internal governance

- **Additional requirements in GL/2017/11 aim in particular to address the following aspects of internal governance**

1 Risk culture	2 Management oversight	3 Risk management & Compliance	4 Offshore activities	5 Change processes
► To foster a sound risk culture implemented by management body	► To strengthen management body's oversight (in particular in its supervisory function) of the institution's activities	► To strengthen the risk management frameworks ► To strengthen the compliance framework	► To increase the transparency of institutions' offshore activities	► To ensure the consideration of risks within institutions' change processes

6 Internal Audit

A sound risk culture implemented by the management body

GL 44

- An institution shall develop an integrated and institution-wide risk culture, based on a full understanding of the risks it faces and how they are managed, taking into account its risk tolerance/appetite
- An institution should develop its risk culture through policies, examples, communication and training of staff regarding their responsibilities for risk

GL/2017/11

- **Management body's responsibilities** include the setting, approving and overseeing the implementation of a **risk culture** (1.23.j)
- **Management body in its supervisory function** should monitor that the **risk culture** of the institution is implemented consistently (3.33.f)
- **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 (9.94)
- **A strong risk culture should include** but not limited to (9.98):
  - Tone from the top
  - Accountability
  - Effective communication and challenge
  - Incentives
- **Management body** should have **clear and documented policies** for how to promote risk awareness through **a strong risk culture** (10.101.b)

IMPLICATION

- Institutions required to place a much stronger focus on risk culture and integrate into its overall risk management
- Scope and components of risk culture to be aligned with global principles
- Management body to take an active role in defining, implementing and monitoring an institute-relevant risk culture
- Management body to set up documented policies to enhance risk culture and risk awareness across the institution

The management body's oversight of the institution's activities

GL 44

- The management body in its supervisory function should
  - challenge and critically review the propositions, explanations and information provided by the management body in its management function
  - monitor that the strategy, the risk tolerance/appetite and the policies of the institution are implemented consistently
  - monitor the performance of the members of the management body
  - consider setting up specialized committees, each with a documented mandate and established working procedures

GL/2017/11

- The management body in its supervisory function should **monitor** and **constructively challenge** the **strategy** of the institution (3.31)
- The management body in its supervisory function should (3.33)
  - oversee and monitor **management decision-making** and **actions** and provide **effective oversight** of the management body in its management function
  - oversee and monitor the consistent implementation of the institution's **strategic objectives**, **organizational structure** and **risk strategy**
  - oversee the implementation and maintenance of a **code of conduct**
  - oversee the integrity of **financial information and reporting**, and the **internal control** framework
  - monitor the implementation of the **internal audit plan**
- Significant institutions **must** establish **risk**, **nomination** and **remuneration committees** to advise the management body in its supervisory function (5.1.39)
- Detailed requirements on the **composition**, **processes** and **roles** of the committees (5.2 - 5.6). The expectations are deatailed.

IMPLICATION

- Management body's supervisory functions to take on broader and more specific oversight responsibilities especially with regard to code of conduct, reporting and internal control framework
- Mandatory requirements for significant institutions to set up risk, nomination and remuneration committees within supervisory boards
- Review the composition, processes and responsibilities of special committees of the supervisory boards for compliance with detailed requirements

The risk management and compliance frameworks of institutions

GL 44

- An institution should have a holistic risk management framework extending across all its business, support and control units, subject to independent internal or external review and regular reassessment
- An institution's risk management framework
  - shall include policies, procedures, limits and controls
  - should provide specific guidance on the implementation of its strategies

GL/2017/11

- Institutions should have a **holistic institution-wide** risk management framework as part of the **overall internal control framework** (17.136)
- An institution's risk management framework should (17.138, 17.139)
  - provide **specific guidance** on the implementation of its **strategies**
  - establish and maintain **internal limits** consistent with the institution's **risk appetite** and commensurate with its **sound operation**, **financial strength**, **capital base** and **strategic goals**
  - be **overseen** and **monitored** by the management body in its supervisory function
  - be subject to **independent internal review** performed by the **internal audit function**, and **reassessed regularly against** the institution's **risk appetite**, with information from the risk management function and the risk committee
- The institution takes the **ultimate responsibility** for risk assessment and should evaluate its risks critically, not rely exclusively on external assessments, and use both quantitative and qualitative tools (17.142)
- Regular and transparent **reporting framework** should be defined and documented to inform the management body about the identification, measurement/assessment, monitoring and management of risks (17.145)
- Effective **communication** and **awareness** regarding **risks** and **the risk strategy** is crucial for the risk management process (17.146)

IMPLICATION

- Risk management framework needs to be institution-wide and integrated into internal control framework
- Management body to be responsible for overseeing and monitoring the risk management framework
- Internal audit to regularly conduct independent review on the risk management framework
- Need to establish and document a regular risk reporting framework for the management body

Transparency of institutions' offshore activities (1/2)

GL 44

- Where an institution operates through special-purpose or related structures or in jurisdictions that impede transparency or do not meet international banking standards, the management body shall understand their purpose and structure and the particular risks associated
- The management body should set, maintain and review appropriate strategies, policies and procedures governing the approval and maintenance of such structures and activities
- The management body should ensure appropriate actions are taken to avoid or mitigate the risks of such activities
- Same measures should be taken when an institution performs non-standard or non-transparent activities for clients
- All these structures and activities should be subject to periodic internal and external audit reviews

GL/2017/11

- Institutions should **avoid** setting up **complex** and **non-transparent structures**, and as part of the decision-making, perform a **risk assessment** to identify whether such structures could be used for a purpose connected with money laundering or other financial crimes and the respective controls and legal framework in place (6.3.75)
- When setting up such structures, the **management body** should **understand** them and their purpose and the particular risks associated, and **ensure** that the **internal control functions** are appropriately involved (6.3.77)
- Institutions should **document their decisions** and be able to **justify** their decisions to **competent authorities** (6.3.78)
- The **management body** should ensure that **appropriate actions** are taken to avoid or mitigate the risks of activities within such structures (6.3.79)
- Institutions should take the **same risk management measures** as for the institution's own business activities when they perform **non-standard or non-transparent activities** for clients (e.g. helping clients to **set up vehicles in offshore jurisdictions**, developing complex structures, financing transactions for them or providing trustee services) that pose similar internal governance challenges and create significant operational and reputational risks (6.3.81)
- In particular, institutions should **analyze the reason** why a client wants to set up a particular structure (6.3.81)

Transparency of institutions' offshore activities (2/2)

GL 44

- Under transparency requirement, an institution should publicly disclose at least
  - its governance structures and policies, structure and organization of the management body, and the incentive and remuneration structure of the institution
  - the nature, extent, purpose and economic substance of transactions with affiliates and related parties
  - its business and risk strategy, and foreseeable risk factors
  - its established committees and their mandates and composition
  - its internal control framework
  - its financial and operating results

GL/2017/11

- Where parent undertakings are required under CRD IV to publish annually a description of legal structure and governance and the organizational structure of the group of institutions, the information should cover all entities within the group structure and include at least (216 - 217)
  - an overview of the **internal organization** of the institutions and group structure
  - **material changes** and their **dates** since the previous publication
  - **new legal, governance or organizational structures**
  - The structure, organization and members of the **management body**
  - **key responsibilities** of the management body
  - a list of the **committees** of the management body in its supervisory function and their **composition**
  - an overview of the **conflict of interest policy**
  - an overview of the **internal control framework**
  - an overview of the **business continuity management framework**

IMPLICATION

- Management body to be fully aware and approved of setting up non-standard/non-transparent structures, and prepared to explain to competent authorities why such structures are necessary
- Management body to be responsible for adequate risk management measures for activities under complex structures
- Institutions to conduct analysis on special structure requested by clients and to apply appropriate risk management standards accordingly
- Institutions required to disclose more details on governance and structure, incl. conflict of interest policy, framework of business continuity management, and more information on the management body

Consideration of risks within institutions' change processes

GL 44

- Risk Control Function (RFC) should evaluate how any material risks identified could affect the institution or group's ability to manage its risk profile and deploy funding and capital under normal and adverse circumstances
- RCF should be involved in the evaluation of the impact of material changes and exceptional transactions on the overall risk before decisions are taken

GL/2017/11

- The **management body** should **assess** whether and how material changes to the group's structure impact on the soundness of the institution's organizational framework, and **make** necessary **adjustments** swiftly where weaknesses are identified (6.1.69)
- The new product approval policy (NPAP) should encompasses **material changes** to **related processes** (e.g. new outsourcing arrangements) and **systems** (e.g. IT change processes), and ensure that **approved products** and **changes** are **consistent** with the risk strategy and risk appetite, or that necessary revisions are made (18.147)
- An institution should have **specific procedures** for assessing compliance, including a **systematic prior assessment** and **documented opinion** by the compliance function for **new products** or **significant changes** to existing products (18.149)
- RMF should evaluate the **impact of material changes** and exceptional transactions on the institution's and group's **overall risk**, and should **report** its findings **directly** to the management body before a decision is taken (20.2.172)

IMPLICATION

- Management body to take direct responsibilities in identifying the risks associated with and assessing the impact of material organizational changes of the institutions
- Review institution's NPAP to ensure its compliance with specific content requirement and its alignment with risk strategy/risk appetite
- Compliance function to develop procedures for assessing and documenting the compliance of changes in products

Internal Audit

GL 44

- Internal Audit function (IAF) shall assess whether the quality of the internal control framework is both effective and efficient
- The IAF should evaluate the compliance of all activities and units with its policies and procedures
- Specially focus on the internal models and quality of the qualitative risk identifications process
- Be independent.
- Report to the management body

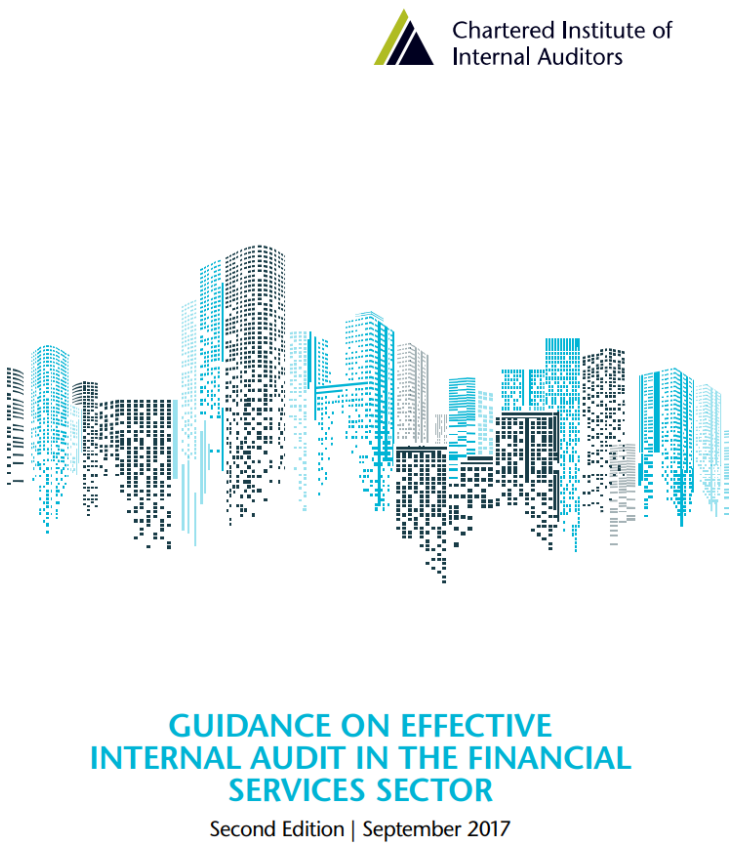
GL/2017/11

- Set up an **independent** and **effective** internal audit function (IAF) taking into account the **proportionality** criteria. IAF should have sufficient authority, stature and resources. The **qualification** of the IAFs staff should be adequate hereunder the tools and risk analyses methods.
- Follow a **risk based** approach and provide **objective** assurance of the compliance of all activities including outsourced activities.
- IAF should **assess** whether the **internal control framework** is both effective and efficient. Specially assess the methods and assumption used in internal models.
- At least have an **annual audit plan** with detailed working programs following a risk based-approach.
- Formal follow up procedures related to **audit recommendations**.
- Should adhere to national and international professional standards (**IIA**)

IMPLICATION

- In reality not much change. The text is somewhat broader, but cover the same topics and refer to IIA standards
- **Proportionality** – what does that really imply?

CIIA – Guidance is much broader then the EBA guidelines. The industry struggles to adapt the standard



«The primary role of internal auditor should be to help BoD and Executive management to protect the assets, reputation and sustainability of the institution»

Internal Audit mandate to cover:

- Internal governance
- The information presented to the BoD and Executive Management for strategic and operational decision making
- The setting of, and adherence to, risk appetite
- The risk and control culture of the organization
- Risk of poor customer treatment, giving rise to conduct or reputational risk
- Capital and liquidity risk
- Key corporate events
- Outcome of processes – should not adopt a tick-the-box approach
- Assessment of the adequacy and effectiveness of the Risk Management, Compliance and Finance Function