EBA launches consultation on ICT Risk

On 6 October 2016, the European Banking Authority (EBA) launched a Consultation Paper on the Guidelines on Information and Communication Technology (ICT) Risk Management under the Supervisory Review and Evaluation process (SREP). The draft Guidelines are addressed to competent authorities and aim at promoting common procedures and methodologies for the assessment of ICT risk.

The guidelines are structured around three **key areas**:

1. setting the **context and scope** of the ensuing assessment;
2. addressing what competent authorities should expect to see with regard to **management of ICT risks at senior management level and management body level**, as well as the assessment of an institution's ICT strategy and its alignment with the business strategy; and
3. covering the assessment of the institution's **ICT risk exposures and the effectiveness of controls**.

The guidelines supplement the existing (albeit, limited) information in the EBA SREP guidelines on how to assess ICT risk and harmonizing the methodology for doing so. The guidelines are complemented by an ICT risk taxonomy in the annex that includes a list of 5 ICT risk categories with a non-exhaustive list of examples of material ICT risks.

The EBA does not specify whether onsite or offsite inspections are most appropriate to conduct the assessments contained within these guidelines, nor do the guidelines introduce any additional reporting obligation for banks.

Application

These guidelines will be applied proportionally to the size, structure and operational environment of institutions as well as the nature, scale and complexity of their activities. They will be applied in line with the frequency and intensity as per the SREP categorization of institutions.

Findings and scoring will be used as following:

1. **Governance of ICT assessment** and score will feed into the assessment of Internal Governance and of the EBA SREP;
2. **Strategy of ICT assessment** and score will feed into the assessment of Business Model of the EBA SREP;
3. **ICT risk exposures and controls assessment** and score feed into the assessment of Operational risk of the EBA SREP.

If ICT risk is considered material, it could be assessed and scored individually as a sub-category of Operational Risk.

ICT Governance and Strategy

With regard to the ICT strategy development and implementation, the key elements addressed by these guidelines are:

- Involvement of Senior Business management in the ICT strategy definition: senior business management should be adequately involved in the definition of the institution's strategic ICT priorities.
- ICT managers' awareness of business strategy and objectives: senior ICT management should be aware of the development, design and initiation of major business strategies and initiatives to ensure the continued alignment between ICT systems, ICT services and the ICT function.
- Documentation and concrete implementation plans: the ICT strategy should be documented and supported by concrete

Angela Manolache
Partner, Governance, Risk & Reporting
amanolache@kpmg.com

Mihai Rada
Director, IT Advisory/ Management Consulting
mihairada@kpmg.com

Calina Iacob
Senior Manager, Governance, Risk & Reporting
ciacob@kpmg.com

Florin Mitrofan
Manager, Governance, Risk & Reporting
fmitrofan@kpmg.com

KPMG Romania SRL
Victoria Business Park,
DN1,Soseaua
Bucuresti - Ploiesti
nr. 69-71, Sector 1,
Bucuresti, Romania
P.O. Box. 19 - 191
Tel: +40 (372) 377 800
Fax: +40 (372) 377 700

Internet: www.kpmg.ro

implementation plans, in particular regarding the important milestones and resource planning.

- Periodic updates to ensure continued alignment with business: the institution should periodically update its ICT strategy, in particular when changing the business strategy, to ensure continued alignment between the ICT and business medium-term to long-term objectives, plans and activities.
- Approval and implementation monitoring by management body: the institution's management body should approve the ICT strategy, implementation plans and monitors its implementation.
- The existence of governance processes to effectively support the implementation: the control framework should include governance processes (e.g. progress and budget monitoring and reporting) and relevant bodies (e.g. a project management office (PMO), an ICT steering group or equivalent) to effectively support the implementation of the ICT strategic programs.
- Definition and allocation of roles and responsibilities for the implementation: the control framework should define and allocate the roles and responsibilities for the implementation of ICT strategic programs.
- Independent control and internal audit functions to provide assurance: the control framework should engage the independent control and internal audit functions to provide assurance that the risks associated with ICT strategy implementation have been identified, assessed and effectively mitigated and that the governance framework in place to implement the ICT strategy is effective.
- Planning and planning review process: the control framework should contain a planning and planning review process that provides flexibility to respond to important identified issues (e.g. encountered implementation problems or delays) or external developments (e.g. important changes in the business environment, technological issues or innovations) to ensure a timely adaptation of the strategic implementation plan.

With regard to the ICT Governance and its inclusion in the risk management framework, supervisors will check whether:

- a robust and transparent organizational structure with clear responsibilities on ICT exists;
- the management body knows and addresses the risks associated with the ICT;
- the impact of ICT outsourcing on the institution's business and business model is controlled;
- ICT risks are within the scope of institution-wide risk management and internal control frameworks;
- the risk appetite and the ICAAP cover the ICT risks.

Risk exposures and controls

The second important part of the Guidelines aims to identify the material ICT risks to which the institution is or might be exposed, which are mapped into the following ICT risk categories:

- ICT availability and continuity risk;
- ICT security risk;
- ICT change risk;
- ICT data integrity risk;
- ICT outsourcing risk.

For the identified material ICT risks, the Guidelines list the topics that should be reviewed:

- ICT risk management policy, processes and risk tolerance thresholds;
- Organizational management and oversight framework;
- Internal audit coverage and findings; and
- ICT risk controls that are specific for the identified material ICT risk.

Perspective from KPMG's ECB Office

IT risk is widely regarded as one of the biggest risks facing the banking sector. KPMG professionals from our ECB Office have been meeting with IT risk management experts, banks and supervisors to discuss the growing importance and increasing complexity of IT risk. Among the key issues, there are two key priorities emerging that need immediate attention in order to bring clarity across the industry and to level the playing field:

- IT risk taxonomy: The absence of a European common language to define a complete IT Risk referential; and
- Harmonization: There are currently no single, harmonized European requirements or best practices related to IT risk

management; or harmonized control and assessment guidelines.

Some IT risks can be covered by existing international frameworks and standards but also by national and/ or global requirements. Nevertheless, there are inconsistencies, overlaps, gaps and discrepancies between these standards and requirements. For example, cyber risk is a top IT risk for banks and is covered by different and very high level national binding requirements; while at the same time, banks refer to other international standards, such as COBIT, ISO 27001 and ITIL to address this risk.

Many of the existing requirements are very high level guidelines and do not provide concrete implementation or assessment guidance. Complicating the issue further, we have emerging technologies such as blockchain that present risks that are not covered at all by the existing requirements and standards.

The EBA's initiative was necessary. These guidelines are very important both for supervisors and banks as they provide supervisors with a common methodology to assess ICT risk by creating a 'same playing field' for all the European countries.

For the banks, these guidelines could be seen as ICT risk management requirements because:

- they offer a common language to define a common ICT Risk referential, and uniform principles and standards to manage ICT risk;
- avoid overlaps between mandatory national / international requirements;
- they fill many gaps to cover a large part of the ICT risk panorama;
- the guidelines further push the existing high-level guidelines towards more detailed requirements;
- they define how should ICT risk be self-assessed; and
- outline key questions that supervisors would ask with regard to IT risk management.

Generally for the assessment of ICT risk all banks have mechanisms and measures in certain forms. However, there are also variations in the current level of practices across banks. While some banks have practices in place that are fully or largely in line with the provisions of the draft guidelines, some banks have work to do to bring their practices in line with the guidance.

About us

Our team believes in knowledge and passion for what we do builds value. As such, we strive to proactively bring our clients top products to enable them to succeed in their business activities. At the forefront of advising banks on regulatory change, we are here to help you successfully navigate the complex maze of interlinked European regulations.

Let's meet and discuss on how we can add tangible value to your organization.