EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company
ECIIA (European Confederation of Institutes of Internal Auditing)

Contact person

Mr/Ms
Vandenbussche

First name
Pascale

Surname

Email address
p.vandenbussche@eciia.eu

Telephone number
+32.491.10.44.98

☐ Please tick here if you do not wish your personal data to be published.

General comments

EUROPEAN CENTRAL BANK

BANKING SUPERVISION

We thank the ECB for the opportunity to comment - and welcome the guidance that will assist internal auditors in planning audits on cloud services usage and relevant providers. In general, the guidance assists organisations build the necessary control environment to mitigate risks associated with the usage of cloud.
ECIIA is the professional representative body of 34 national institutes of internal audit in the wider geographic area of Europe and represent 55.000 members.
ECIIA is the the consolidated voice of the profession of internal audit and aims representing and developing the internal audit profession as part of good corporate governance, by achieving thought leadership through publications on relevant topics and by interacting with the Regulators, as required, and any other appropriate institutions of influence at European level.

Role of Internal Audit
The role of internal audit is substantial in managing the risks associated with the usage of cloud services. Especially in regards to broad risk assessments which are integral to decisions being made to shift applications to the cloud and select software, platforms or infrastructure of cloud service providers. On that note, cloud providers should also perform risk assessments of their services and use the insights from internal auditors as part of this exercise. Internal audit as part of our 3rd Line responsibilities, provides assurance on cloud readiness assessments of existing vendor procurement and contract processes, and identify cloud control gaps. By reviewing the risk framework based on identified cloud risks, internal audit assists organisations in understanding and mitigating these risks. Internal audit will also assess data governance programs and ensure that regulatory requirements have been applied. Internal audit continues to be engaged in risk discussions, along with the organisation's security, risk, and compliance groups.

Technical Guidance and Best Practices
As this guidance covers certain technical topics, we advise to include more best practices (as in the section 2.3.1) to better illustrate the ECB's expectations.
Clear definitions of the governance framework (we recommend to use the 3 lines model*), including the roles, responsibilities, and oversight of the 1st and 2nd lines alongside the one of internal audit are crucial.

Interactions with Cloud Service Providers
Obtaining detailed, accurate and complete information from the CSPs is a challenge for all Financial Service Entities, including their internal audit functions. Although audit rights are included in contracts, necessary information from CSPs is not always forthcoming. Therefore, we recommend the ECB to specify the minimum audit requirements for services not impacting critical/important functions. Including best practices for situations where support from CSPs is lacking would also be beneficial.

General Recommendations
As a general comment, the ECB should consider enhancing its description of the mandatory work expected from the internal audit function for different types of cloud outsourcing services. We recommend clear definitions on key topics such as "critical functions", "undertaking", the different kinds of cloud categories, "major disruptions" and "assets". Although DORA includes definitions for many of these topics, the guidance references should be clearly stated.