EUROPEAN CENTRAL BANK

BANKING SUPERVISION

On-site inspections 2018: key findings

On-site inspections (OSIs) are the most intrusive of the supervisory tools used by Joint Supervisory Teams in supervising significant banks within the framework of the Single Supervisory Mechanism (SSM). They have proven to be particularly useful for scrutinising banks' internal control systems, business models and governance. Over the past four years, ECB Banking Supervision has carried out around 160 OSIs annually, which equates to 1-4 inspections per bank per year, depending on the size of the bank. The main focus has been on credit risk, followed by internal governance and IT risk.

ECB Banking Supervision recently conducted an in-depth analysis of the key findings from the 2018 OSIs. As in previous years, OSI findings were categorised using a four-point scale, from less severe to more severe, to reflect the strength of the potential impact if the issues remained unaddressed. In total, 1,200 findings of the two highest classes of severity were reported. Of these, 31% related to credit risk, 26% to governance

and 15% to IT risk. Other prominent risk areas included market risk, interest rate risk in the banking book, capital risk and liquidity risk.

In the area of credit risk, a significant proportion of the more severe findings concerned shortcomings in the identification of non-performing exposures and the calculation of loan loss provisions. Deficiencies were also observed at the credit-granting stage. For instance, some banks were found to carry out insufficient risk profiling of potential borrowers and/or to use inappropriate underwriting criteria. There were also weaknesses discovered in banks' credit monitoring processes, in particular with regard to high-risk borrowers. The banks concerned were asked to perform remedial actions such as strengthening their internal credit risk guidelines, improving their IT systems and holding additional capital.

Regarding internal governance, a high concentration of the more severe findings related to weaknesses in banks' internal control functions (risk control, compliance and internal audit). Inspectors also noted insufficient involvement of the management body in the design of the risk management framework and deficiencies in governance arrangements, among other issues. Such findings often reflect the risk culture of the institution, and are thus taken very seriously and followed up very closely by supervisors.

Many of the more severe findings in the area of IT risk concerned IT security management. In particular, inspectors found that measures for detecting and mitigating IT risks were not implemented as quickly and extensively as they should be. In some cases, vulnerability patches – software updates to address security vulnerabilities – were not applied frequently enough. In the light of the increasing importance of IT security management and the high concentration of findings, ECB Banking Supervision will continue to assess the IT and cyber risks facing banks and will launch a number of OSIs on IT risk-related topics in the coming months. Significant institutions will continue to report any significant cyber incidents to ECB Banking Supervision under the SSM cyber incident reporting process.

At the end of each OSI, findings undergo a strict quality assurance process to ensure consistency and a level playing field for the supervised banks. On the basis of the final OSI report, supervisors ask the banks to carry out various remedial actions, and follow up with them accordingly. In a number of cases, this has involved banks holding more capital in order to cover the risks identified. OSI findings and banks' responses are taken into account in the annual Supervisory Review and Evaluation Process. ECB Banking Supervision also uses the findings to detect emerging trends or common weaknesses, which will be addressed through thematic reviews, ECB guidelines or letters to banks setting out specific expectations.