IT AND OPERATIONAL RISK REVIEW

9-11 May

Description

This seminar presents the key aspects to consider when planning and conducting operational and IT risk inspections.

Aim and content

It aims to introduce the basic concepts of operational and IT risk management processes to those not familiar with them and to identify the main operational and IT risks that financial institutions face.

It also introduces the key aspects of operational and IT risk inspections by way of practical examples and common findings based on experience.

Contents:

Operational risk

- Introduction: definition and concepts.
- Governance and lines of defence.
- Operational losses. Identification, recording and action plans.
- Capital: minimum own funds requirements (Pillar 1) and new regulatory developments.
- Operational risk appetite and indicators.
- Supervisory evaluation.
- Supervision manual.
- Aspects to be reviewed: risk map, procedures, governance and reporting, recording of losses, approval of new products, fraud management and legal risk, capital calculation.

IT risk

- Introduction: IT risk in the financial system.
- IT risk management. Three lines of defence model.
- IT strategy vs. business strategy. IT systems architecture.
- IT governance and organisation. Outsourcing risks.
- Information security: protection measures, access management, physical security, monitoring.
- Operations management: change management, systems availability and capacity management, incident and problem management, back-up copies and IT asset inventory.
- Project management and software development.
- IT systems continuity management.
- Data quality.

Professional profile of attendees

Banking supervision inspectors and junior analysts.

Organisation, duration and format

The seminar is organised jointly by the Banco de España and ASBA. It will be held in Spanish, online, and will be run by Banco de España expert trainers. Participation is by invitation only from ASBA.