BANCO DE PORTUGAL
EUROSYSTEM

International Operational Risk Working Group (IORWG)

12th Annual Conference (23 – 25 May 2017)

Lisbon

Opening Remarks by Governor Carlos da Silva Costa [1]

Welcome to Lisbon. Welcome to Banco de Portugal.

I am very glad to have with us representatives from about 60 different Central Banks, including all five continents, to reflect and exchange views on such an important topic.

The International Operational Risk Working Group (IORWG) is dedicated to advancing the management of operational risk in the central banking industry. IORWG is made up of 77 member institutions and has built a strong and effective network in central banking operational risk management.

A properly designed risk management framework in the central bank is a pillar of confidence and trust in the financial system. Therefore, the importance of IORWG's role cannot be overemphasised.

Central banks face risks both financial and non-financial in nature. In addition to the financial risks associated with monetary policy and asset management, central banks face a varied set of other risks, namely those related with cash issuance, payment systems and information and communication systems. The materialisation of any of these risks can have a severe impact on both the financial position and the reputation of the central bank. A risk management function that identifies, assesses, manages and monitors all kinds of risks is thus of vital importance in a central bank.

[1] As prepared for delivery.

The consolidation of a risk management culture in a central bank rests on a set of key conditions:

1. First, **governance** is needed where the roles and responsibilities of the various stakeholders within the organisation are clearly assigned and known to all;
2. Second, risk management requires strong **empowerment** from, and involvement of, senior management;
3. Third, risk management should be a **horizontal concern** within the organisation, involving all functions and a **top-down prioritisation** of risks;
4. Fourth, the **exchange and flow of information** are essential to ensure the involvement of the relevant stakeholders and facilitate the development of consistent standards among the business functions; and
5. Last but not least, **expertise and the right skills** are critical to the risk management function.

These conditions were at the heart of the changes implemented in the past few years. Banco de Portugal has strengthened its governance model, organisation and processes, reinforcing the management control mechanisms, notably in terms of risk and compliance.

Acknowledgment of the strategic importance of a global and integrated approach to risk led to the creation of a *Risk Management Department* and a *Risk Committee* in 2012. The *Risk Committee* is a forum for dialogue and reflection between the Board of Directors and senior managers on issues related to Banco de Portugal's business risk management and control. The *Committee*, which is chaired by the Governor, has an important say on the management of financial assets (e.g. guidelines and strategic benchmarking) as well as on operational risk, cyber-security and business continuity management.

A *Compliance Office* and an *Ethics Committee* were also set up. The former was created in 2015 as an autonomous functional unit within the General Secretariat of Banco de Portugal. The *Ethics Committee*, created in 2016, monitors the new ethics and conduct regime applicable to the Board of Directors.

This framework provides a shield in coping with the many and diversified threats currently faced by central banks. Chief among these are the risks related with cyber-crime and data fraud or theft,[2] so I will comment briefly on this specific category.

Cyber-threats are always present and every organisation is vulnerable to attack – no matter how good its security is – so it is important to test not only its controls but also how the organisation responds to a cyber-crisis.

Given the specific role of central banks, it is useful to consider both an internal and an external dimension of cyber risk management:

- On the internal dimension, central banks should develop an appropriate strategy and establish suitable governance for cyber risk, better coordinate the exchange of information and expertise among departments/units and increase levels of awareness and assessment;
- On the external dimension, central banks, as supervisors, should encourage the private sector to pursue a proper risk mitigation strategy, promote cooperation with and among the financial sector and support international cooperation.

At Banco de Portugal some action has been taken in the last few years:

- Development of a special programme for cyber-security, launched in 2011, which has helped reduce overall exposure, increase resilience and decrease operational and business risk;
- Setup of a SOC/CSIRT - Security Operations Centre / Computer Security Incident Response Team, focused on cyber-security matters and corporate and business defence;

[2] See The Global Risks Report 2017, issued by the World Economic Forum. The report features perspectives from nearly 750 experts on the perceived impact and likelihood of 30 prevalent global risks as well as 13 underlying trends that could amplify them or alter the interconnections between them over a 10-year timeframe.

- Creation of a data loss prevention programme supported in three layers (data governance, IT controls and support processes) in a consistent framework;
- Cyber-security incidents are thoroughly analysed, operational risk is assessed based on the attack's modus operandi and recovery time and, as mitigation, preventive and corrective measures are applied and processes updated.

The future will bring ever more data, more connections between devices and platforms, widespread recourse to outsourcing, including cloud services. This means that threats to cyber-security will keep on mounting. The financial sector is particularly sensitive due to its intense reliance on technology and the systemic nature of its risks. Central banks, given their special concerns about financial stability, must take these risks very seriously.

Let me conclude with the reminder that a 'risk-free' organisation does not exist. What is important is for senior management to define an appropriate level of risk appetite and tolerance, and to monitor it in an effective and suitable way.

Banco de Portugal is pleased to be part of an important network like IORWG. I wish you fruitful discussions and a very pleasant stay in Lisbon.