



**Regional Workshop on "Cyber Resilience for Central Banks"**

**Organized by Bank Al-Maghrib and the Bank of England**

**November 28-29, 2022**

**Opening remarks by the Director General**

*His Excellency the British Ambassador of His Majesty To Morocco, Dear Colleagues*

It is a real pleasure for me to welcome you to this joint workshop organized with the Bank of England on "cyber resilience for central banks"

First, I would like to convey my warmest thanks to His Excellency the Ambassador for honoring us with his presence, testifying to the historical friendship between our two countries and His kind and constant support for the fruitful cooperation between them.

I also extend my sincere thanks to the senior staff of the Bank of England who contributed to the organization and facilitation of this seminar, enriching its program with their expertise and feedback.

Besides, I would like to welcome our colleagues representing central banks from the African continent and the Middle East region, who have kindly made the trip to attend this seminar and share their experiences.

Likewise, I express my sincere gratitude to the "Direction Générale de la Sécurité des Systèmes d'Information", our national cyber security authority, for its willingness to take part in the proceedings of this workshop, in the tradition of our mutual cooperation which is continuously strengthening.

*Ladies and Gentlemen,*

The cooperation between the BoE and BAM, which we highly commend, has expanded steadily over the past few years.

It has covered a wide range of topics including fintech, small business financing, statistical data management and cyber risk. It has recently been extended to a particular theme of great relevance in the current context, which is the relationship between the Central Bank and the Parliament.

Today, the cooperation between our two institutions takes a new step with this event organized for the first time at the regional level on a topic of great importance for Central Banks.

Indeed, cyber attacks against financial institutions and financial market infrastructures are becoming more frequent and more sophisticated. They can generate significant macroeconomic costs and compromise the ability of central banks to carry out their missions.

The cyber threat is intensified by new ways of working and new methods of hosting data, in particular the Cloud.

As a result, Central Banks are adapting their strategies and are now aiming not only at ensuring cyber security but also cyber resilience to preserve their digital transformation processes, which must take into account these cyber resilience methods and tools in any development and innovation they undertake.

Thus, more than ever, they are required to ensure the effectiveness of their cyber resilience systems and their good coordination with those of the other stakeholders in the ecosystem.

And this is what we are working on at Bank Al-Maghrib, in order to develop and regularly test our Bank's cyber resilience system, through internal exercises and with the banking community.

We are also examining the possibility of extending these cyber crises exercises to a regional or even a more global level, through cooperation, such as what we are striving to build with the Bank of England.

Therefore, enhanced and expanded cooperation in this area is not just a good practice, but a necessity for central banks, as effective information sharing is essential to collectively reduce cyber risks, prevent major cyber incidents, and quickly contain them when they occur.

This workshop is also intended as a contribution to the momentum of cooperation within the central banking community. It is my hope that it will inspire similar endeavors aimed at pursuing the debate and sharing good practices and experiences within our Institutions.

I am convinced that the expertise of the speakers and the spirit of sharing that characterizes our exchanges will make this seminar an opportunity to identify relevant areas of improvement that will enable our institutions to build and strengthen their cyber resilience systems.

I am positive that the outcomes of this conference will meet your expectations.

Thank you for your attention and I wish you every success in your work.