Information is a valuable asset in any organization, whether it's printed or written on paper, stored electronically, or sent by mail or electronic means, and consequently it must be suitably protected. The protection of information and the establishment of a security management system is relevant to all types of organizations, regardless of their size or the nature of their business. This is especially important in our increasingly interconnected business environment.

In today's fast-changing circumstances, it is more important than ever that organizations continue to mitigate risk and maintain data integrity. Data are an organization's lifeblood. The easiest way to lose trust, reputation, and business is to allow your data to be compromised. Data loss, whether through internal threats, accidental loss, or other forms of malicious intent can bring an organization quickly to its knees.

When most business information was paper-based, it was generally sufficient for a business to keep confidential information in a locked filing cabinet, employ trustworthy staff, and use security personnel to monitor its premises at night and on weekends.

In today's digital world, it is easy to fall into the trap of thinking that a similar approach is still good enough. But the media's almost-daily reports of IT-related security breaches show us that it is not. PCs, laptops, mobile phones, the internet, e-commerce, Wi-Fi, and devices like the Blackberry have brought major advances to how we do business. Each, however, has added potential risks to the security of the information that it stores and communicates.

Like any other valuable business asset, information must be seen as an asset that is valuable to the organization and, therefore, needs suitable protection against any type of threats. The threats come not just from the internet; in fact, over 50% of all security breaches result from insiders' activities.

One of the biggest trends we see is companies not focusing enough on the threat of data leakage from their own employees. Many threat analyses and risk models have been created that focus on preventing outside access to information. But we frequently see that internal employees who have a right to access sensitive information are making improper internal decisions that create serious compliance risks.

Another trend is accidental data leakage -- the concept of "one wrong click" being able to create a compliance risk. Data are increasingly linked in the World Wide Web. Most systems expose data as feeds that can be integrated into other systems. People increasingly multitask between mobile devices, tablets, and personal computers. Cutting and pasting content into the wrong location just once can constitute a risk. And what about people using internal networks to share credentials, server names, usernames, and passwords? Once a hacker has gained access to a small part of a system, it is now possible for that hacker to scan the network and find logins to a host or to other systems that may contain even more sensitive data.

Information security is concerned with three things:

1. **confidentiality**: making sure that information is available only to those who have a legitimate need or right to access it;
2. **integrity**: safeguarding the accuracy and completeness of information so that a recipient can be sure that information received has not been altered during transmission, and
3. **availability**: ensuring that legitimate users of information have access to it when required .

Information security is achieved by implementing a suitable set of controls in the form of policies, procedures, organizational structures, systems, and functions to ensure that the security objectives of the organization are met.

There is no shortage of technology to protect electronic information: we have virus checkers, encryption, firewalls, data back-up tools, password protection, and so forth. But how do we know whether it is being applied correctly and works effectively?

I think that this is a management issue rather than a technical issue. For example, access to an organization's computer systems normally is controlled by username and password. This precaution is pointless, however, if a staff member chooses a password that is easily guessed or keeps it on a notepad next to the PC.

Security, like quality, needs to be part of everyone's everyday thinking. The way to achieve this mindset is to include information security within the scope of the organization's overall management system, as described in the Provisions and Guidelines for Information Security Management issued by the Bank.

And today, my colleagues from the Central Bank and other experts on the different areas of Information Security Management will give you more insight into the importance of Information Security Management. And I am sure that all of today's presentations will broaden your knowledge and awareness on Information Security Management.