Information, Information Technology and Information Security Governance

Information management is an essential part of good IT governance, which in turn is a cornerstone in corporate governance. An integral part of the IT governance is information security, in particular pertaining to personal information.

An Information Technology (IT) Security Policy identifies the rules and procedures for all individuals accessing and using an organisation's IT assets and resources. Effective IT Security Policy is a model of the organisation's culture, in which rules and procedures are driven from its approach to information and work. Thus, an effective IT Security Policy is a unique document for each company, cultivated from its perspectives on risk tolerance, how the company sees and values their information, and the resulting availability that it maintains of that information.

The Security Policy document combines legal requirements and current best practice for an information security management policy for the Company. It provides a policy with information security objectives, strategy and defines roles and responsibilities.

Core principles for information security management, as defined in ISO/IEC 27002, are adapted to the local situation for the following areas:

- Risk assessment
- Organising information security
- Frequent monitoring of the capital & IT expenditures in line with budgets
- Asset management
- Human resources security
- Physical security and restrictions to access in some cases
- Communications and Operations management.
- Access control
- System development and maintenance
- Information security incident management
- Business continuity management
- Compliance

The Board's and the Management's involvement in Information and IT governance:

- Oversee the realised total capital expenditures in line with budget at each quarterly Board meetings
- Regular evaluation of the information security systems
- Assess the need for independent evaluation from external experts on IT governance