IT Governance

Corporate Governance
Corporate governance is a set of responsibilities and practices used by an organization's management to provide strategic direction to the business. Governance ensures that goals are achievable, risks are properly addressed, and organizational resources are properly utilized.

IT Governance
IT governance is an integral part of corporate governance and consists of the leadership, structures, and processes that ensure IT extends the organization's strategy and objectives. IT governance is the responsibility of the board of directors and executive management.

IT governance helps ensure the alignment of IT with business objectives. Fundamentally, IT governance is concerned with:
- *Value* - IT delivers value to the business by strategic alignment of IT with the business
- *Risks* - IT risks are mitigated by embedding accountability into the business

IT Balanced Scorecard
The IT Balanced Scorecard is a management technique that assists in assessing IT functions and processes. It aids the IT Steering Committee and management in achieving IT and business alignment and typically consists of:
- *Mission statement* – IT's charter and function
- *Strategies* – methods of supporting the mission statement
- *Measures* – a balanced set of metrics and key performance indicators (KPI's) to guide business oriented IT decisions

Information Security
Information security helps to strategically align IT with business strategy. In addition, it manages and executes appropriate measures that mitigate risks. Effective information security can add significant value to the organization by:
- Improving trust in customer relationships
- Protecting the organization's reputation
- Providing greater reliance on interactions with business contacts
- Enabling new and better ways to collect, store, and retrieve information

Information Systems Strategy
Information systems strategy provides direction and guidance that assists the board of directors and executive management in IT governance responsibilities. In addition, information systems strategy focuses on IT value, risks, and performance.
- *Strategic planning* – provides long-term direction leveraging IT to improve

business processes.
- *Steering committee* – senior management should appoint a steering committee to oversee the information systems functions and activities. This committee reviews major IT projects, assigns priorities, allocates resources such as funding and staffing, and helps ensure harmony with the corporate mission and objectives.

Policies and Procedures
Policies and procedures reflect management's guidance and direction in development controls over information systems and related resources. An information security policy provides management the direction and support for information security in accordance with business requirements and relevant laws and regulations.

Security Policy
An information security policy communicates a security standard to users, management, and technical staff. A security policy for information and related technology is a first step toward building the security infrastructure.

An information security policy should be approved by management and distributed to all employees and relevant external business contacts. A security policy may contain:
- Definition – a definition of information security and its overall objective and scope
- Intent – supporting the goals of information security in line with business strategy
- Framework – control objectives including risk assessment and risk management
- Requirements – principles, standards, and compliance relevant to the organization
- Responsibilities – general and specific responsibilities for information security management
- References – refers to documentation that may support the policy

Risk Management
Effective risk management begins with a clear understanding of the organization's risk appetite and compliance requirements. This drives all risk management efforts and impacts future investments in technology, the extent to which IT assets are protected, and the level of assurance required.

Risk management involves identifying, analyzing, evaluating, treating, monitoring, and communicating the impact of risk on IT processes. Dependent upon the type of risk and its impact on the business, management may:
- *Avoid* – choose not to implement certain activities or processes that increase risk

- *Mitigate* – implement controls to reduce inherent risk down to residual risk
- *Transfer* – share risk with partners or transfer using insurance coverage
- *Accept* – formally acknowledge and monitor certain types of risk
- *Eliminate* – where possible, remote the source of the risk

The following risk management process is used to form an overall view of risk:
- *Assets* - identify and classify information resources or assets that need protection
- *Threats* – identify threats such as errors, malicious damage, theft, software failure, etc. and their likelihood of occurrence
- *Vulnerabilities* – threats occur due to vulnerabilities such as lack of user knowledge, security functionality, poor passwords, etc.
- *Impact* – evaluate the impact or loss including breach of legislation, impact on reputation, loss of opportunity, etc.

Audits
Network security audits play a significant role in the successful implementation and delivery of IT services. IT governance initiatives require an independent and balanced view of IT that help facilitate and improve IT processes and initiatives. Altius IT assessments provide independent best practice review and recommendations that improve the quality, effectiveness, and delivery of IT services.

Publication Information
Altius IT is a security audit, security consulting, and risk management firm. We are certified by the Information Systems Audit and Control Association (ISACA) as a Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Controls (CRISC), and Certified in the Governance of Enterprise Wide IT (CGEIT). For more information, please visit www.AltiusIT.com.