

Cross Current IT Audit Approach

Goal: The purpose of an IT audit is to identify risks to the current information technology system in its business environment and facilitate the alignment of IT with business processes in order to drive the company's business objectives. The objective is not only to identify shortcomings that jeopardize privacy, security, and business concerns, but also to make recommendations that lead to regulatory compliance and the enhancement of overall efficiency.

Overview: We undertake a top-down approach to put the audit elements in context and determine where the review emphasis should be focused. The procedure involves meetings with appropriate management personnel, including IT management and the firm's Audit Committee, and the review of available documentation. This allows us to do the following:

- Develop an overview of the IT system and its interaction with the business units, particularly with respect to IT involvement in the financial reporting process. This includes evaluating existing systems and controls.
- Analyze risk in terms of impact to the business or IT environment and their probability of occurrence with respect to business, security, disaster recovery, and customer privacy concerns.
- Develop the scope of the IT audit plan, with emphasis on those areas identified as being of greatest risk. The plan accounts for undocumented procedures, adequacy of physical and logical security, disaster recovery procedures, testing plans to be included in the audit, and other elements. Well-documented procedures with sufficient review on a periodic basis are de-emphasized so that the audit is efficient. Measurement is assessed against a standard framework.
- In the case of regulatory audits, such as Sarbanes-Oxley, Cross Current anticipates working closely with an accounting firm partner so that the audit of IT controls is integrated with the business review conducted by its auditors.

Procedure: Cross Current will employ an applicable subset of the COBIT IT governance model (mapped to the COSO and PCAOB Auditing Standard No. 2 models where appropriate), based on the evaluation of the organization undertaken in the initial overview phase. While the specific control objectives applied may vary, the general model consists of the following domains:

- Planning and Organization, including strategic planning, policies and communication of policies, compliance with appropriate laws and regulations, policies on staff cross-training and backup, quality management and quality assurance, and risk management.
- Acquisition and implementation, including hardware and software inventory, licensing, preventive maintenance, change management, purchasing and vendor management and procedures documentation.
- Delivery and support, including performance and capacity management, disaster recovery, configuration management, security of both the physical plant and networks, Intrusion Detection, Help Desk and training.
- Monitoring, including detection controls, data collection and alerts of system problems.

Final Report: A report will be issued on the audit findings and discussed with our accounting partner for the audit and then the client. Emphasis will be on internal control deficiencies, significant internal control deficiencies, and material weaknesses, as defined by the IT Governance Institute. Cross Current will give its opinion as to the adequacy of existing documentation and where further or missing documentation should be supplied. Finally, recommendations for improvement will be presented for the firm's consideration.

