IT Related Business Risks - Definitions

Integrity Risk

This risk encompasses all of the risks associated with the authorization, completeness, and accuracy of transactions as they are entered into, processed by, summarized by and reported on by the various application systems deployed by an organization. These risks pervasively apply to each and every aspect of an application system used to support a business process and are present in multiple places and at multiple times throughout the application systems; however, they principally manifest themselves in the following components of a system:

User Interface: Risks in this area generally relate to whether there are adequate restrictions over which individuals in an organization are authorized to perform business/system functions based on their job need and the need to enforce a reasonable segregation of duties. Other risks in this area relate to the adequacy of preventive and/or detective controls that ensure that only valid data can be entered into a system and that the data is complete.

Processing: Risks in this area generally relate to whether there are adequate preventive or detective balancing and reconciliation controls to ensure that data processing has been complete and timely. This risk area also encompasses risks associated with the accuracy and integrity of reports (whether or not they are printed) used to summarize results and/or make business decisions.

Error Processing: Risks in this area generally relate to whether there are adequate processes and other system methods to ensure that any data entry/processing exceptions that are captured are adequately corrected and reprocessed accurately, completely and on a timely basis.

Interface: Risks in this area generally relate to whether there are adequate preventive or detective controls to ensure that data that has been processed and/or summarized is adequately and completely transmitted to and processed by another application system that it feeds data/information to.

Change Management: Risks in this area may be generally considered part of Infrastructure risks but they significantly impact application systems. These risks are associated with inadequate change management processes and include user involvement and training as well as the process by which changes to any aspect of an application system are both communicated and implemented.

Data: Risks in this area may also may be generally considered part of Infrastructure risks but they significantly impact application systems. These risks are associated with inadequate data management controls including both the security/integrity of processed data and the effective management of databases and data structures. Integrity can be lost because of programming errors (e.g., good data is processed by incorrect programs), processing errors (e.g., transactions are incorrectly processed more than once against the same master file), or management/process errors (e.g., poor management of the systems maintenance process).

Relevance Risk

Relevance risk relates to the usability and timeliness of information that is either created or summarized by an application system. Relevance risk ties directly to Information For Decision-Making Risk as it is the risk associated with not getting "the *right* data/information to the *right* person/process/system at the *right* time to allow the *right* action to be taken." Information for Decision-Making Risk is the third category of risks.

Access Risk

Access risk focuses on the risk associated with inappropriate access to systems, data or information. It encompasses the risks of improper segregation of duties, risks associated with the integrity of data and databases, and risks associated with information confidentiality, etc. Access risk can occur at any, or all, of the following levels:

Business Process: The organizational decisions as to how to separate incompatible duties within an organization and to provide the correct level of empowerment to perform a function.

Application: The internal application security mechanisms that provide users with the specific functions necessary for them to perform their jobs.

Data & Data Management: The mechanism to provide users with access to specific data or databases within the environment

Processing Environment: The host computer system where application systems and related data are stored and processed from. The access risk in this area is driven by the risk of inappropriate access to the processing environment and the programs or data that are stored in that environment.

Network: The mechanism used to connect users with a processing environment. The access risk in this area is driven by the risk of inappropriate access to the network itself.

Physical: Protecting physical devices from damage, theft and inappropriate access.

Availability Risk

Availability risk focuses on three different levels of risk:

Risks that can be avoided by monitoring performance and proactively addressing systems issues before a problem occurs

Risks associated with short-term disruptions to systems where restore/recovery techniques can be used to minimize the extent of a disruption

Risks associated with disasters that cause longer term disruptions in information processing and which focus on controls such as backups and contingency planning

Infrastructure Risk

This is the risk that the organization does not have an effective information technology infrastructure (hardware, networks, software, people and processes) in place to support the current and future needs of the business in an efficient, cost-effective and well-controlled fashion. These risks are associated with the series of Information Technology processes used to define, develop, maintain and operate an information-processing environment (e.g., computer hardware, networks, etc.) and the associated application systems (e.g., customer service, accounts payable, etc.). These risks are generally considered within the context of the following core IT processes:

Organizational Planning: The processes in this area ensure that the definition of how IT will impact the business is clearly defined and articulated, that there is adequate executive level support and buy-in to this direction and that there is adequate organizational (people and process) planning to ensure that IT efforts will be successful.

Application system definition and deployment: The processes in this area ensure that application systems meet both business and user needs and that they function as users intend within the context of the business processes that the application systems support. These processes encompass the process of determining whether to buy an existing application system or to develop a custom solution. These processes also ensure that any changes to application systems (whether they are purchased or developed) follow a defined process that ensures that critical process/control points are consistently adhered to (e.g., all changes are tested and approved by users prior to implementation).

Logical security and security administration: The processes in this area ensure that the organization adequately addresses the Access risks defined above by establishing, maintaining and monitoring a comprehensive system of internal security that meets management's policies with respect to the integrity and confidentiality of the data and information within the organization and an organization's need to reduce its Empowerment and Fraud risks to acceptable levels.

Computer and network operations: The processes in this area ensure that information systems and related network environments are operated in a secured and protected environment as intended by management and that information processing responsibilities performed by operations personnel (as opposed to users) are defined, measured and monitored. They also involve the proactive efforts typically performed by IT personnel to measure and monitor computer and network performance to ensure that systems are consistently available to users at a satisfactory performance level.

Data and Database Management: The processes in this area are designed to ensure that data and databases used to support critical application systems and end-user reporting needs have both the internal integrity and consistency of definition to meet requirements and reduce the potential for redundancy.

Business/Data center recovery: The processes in this area are designed to address the Availability risks defined below by ensuring that adequate planning has been performed to ensure that information technologies will be available to users when they need them.

Lack of effective and well-controlled business processes in each of these areas is usually the root cause of access, relevance, and availability risks and application systems process integrity risks as noted above.