UNIVERSITY OF TOLEDO INTERNAL AUDIT DEPARTMENT
MANAGE INFORMATION TECHNOLOGY

Control practices

The following control objectives provide a basis for strengthening your control environment for the process of managing information technology. When you select an objective, you will access a list of the associated business risks and control practices. That information can serve as a checklist when you begin reviewing the strength of your current process controls.

This business risk and control information can help you assess your internal control environment and assist with the design and implementation of internal controls. Please note that this information is at the generic business process level, and many companies will need to go beyond generic models to address the specific business processes that support the financial and nonfinancial disclosures being made. You can combine the insight of this business risk and control information with your industry-specific knowledge and understanding of your company's environment when conducting internal control assessments and designing and implementing recommendations.

Effectiveness and efficiency of operations

A. IT is used to carry out the company's strategies.
B. Formal operating procedures are used for IT processing.
C.

B. Formal operating procedures are used for IT processing.

Business risks

Users will make mistakes because of inadequate application instructions and file handling procedures.
Incorrect programs, files, and procedures will be used.
Processing errors will occur because of such actions as executing wrong versions of programs, mounting incorrect data files, improper handling of error messages, faulty restart and recovery procedures, and loss of duplicate processing of input.
System users will make mistakes when trying to accomplish tasks more suited to IT professionals.
IT professionals will make mistakes when trying to accomplish tasks more suited to functional users.

Control practices

1. Ensure that detailed, written operating instructions are in place for setup, disposition, error response, restart, and recovery. These instructions are controlled, are kept current, and are followed for each application and system.
2. Require written approval, including user involvement where appropriate, for departures from authorized setup and execution procedures.
3. Ensure that reports run by IT for functional users are subject to formal scheduling procedures.
4. Minimize required user actions to process reports through system and program structures. (For example, dates, critical processing parameters, and similar user data entry are automated to the greatest extent possible.)
5. Ensure reports have adequate run labels. The labels are standardized and include information such as the data set name and number, creation date, expiration date, report owner, and department owner.
6. Ensure programs that run standard or custom reports are the most current programs available and are distinguished from out-of-date and test versions.
7. Use access control software and appropriate security controls to restrict access to reporting features to authorized individuals only.

C. IT operations are supervised and reviewed.

Business risks

Operators will make mistakes, resulting in processing errors, because they will ignore or be inconsistent in following instructions and prescribed procedures.
Systems will be used for unauthorized purposes including the perpetration and concealment of irregularities.

Control practices

1. Supervise and re>BDC /C2_0 (d r)-10.7 .9.2.125 Td [1.3 (ns)7 (p5 Td [1.3ti)-34.5 (s)45.2 (pr)-1
   oitets391.2 (e)310.7 (s391.2 ac)0.5 rt e

E. All approved input is accepted by the ITsystemand only approved input is accepted.

Business risks

Data submitted for processing will not be authorized, complete, or accurate.
Spurious data entry will lead to unreliable processing results.
Unauthorized or fraudulent input will be accepted.
Data will be lost or misrouted during transmission.
Data will not be submitted on a timely basis.
Outsiders will gain access to the system through unauthorized communication link.

Control practices

1. Implement a method to identify authorized system users (for example, a system of passwords).
2. Implement a security system that effectively separates duties, authorizing users or user groups to access only those systems and files necessary to perform their job functions.
3. Ensure that policies for passwords and identification numbers require changing passwords periodically, voiding identification numbers and passwords when employees transfer or leave the company, and changing identification numbers and passwords when employees feel theirs have been compromised.
4. Train users in appropriate security procedures (for example, not taping ID numbers and passwords to their monitors).
5. Implement passwords and identification numbers that do not print and are masked on the PC monitor.
6. Enable the system or program to disable the user ID or shut down after a predetermined number of unsuccessful attempts to access the system or program.
7. Authorize a system or program that is idle for a specified length of time to automatically log off.
8. Store password files, authorization tables, communications software, and key application programs in logically protected areas or otherwise protect from read and write access.
9. Program the system to restrict the number of individuals who can use critical commands (such as overrides).
10. Restrict sensitive or critical commands to one or more workstations.
11. Limit restricted workstations to physically secure locations.
12. Authorize the operator or system to disconnect and call back authorized locations only.