# 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 strategic plans.
B. Formal operating procedures are used for IT processing.
C. IT operations are supervised and reviewed.
D. Access to IT operations is restricted.
E. All approved input is accepted by the IT system, and only approved input is accepted.
F. Data is accurately converted.
G. Access to online systems is controlled.

Effectiveness and efficiency of operations

**A. IT is used to carry out the company's strategic plans.**

**Business risks**

- Information technology (IT), financial, and operating management will not interact sufficiently when developing strategic plans.

**Control practices**

1. Develop an information technology (IT) strategic plan that optimizes companywide investment in and use of IT.
2. Develop IT initiatives that support the company's long-range plans.
3. Involve users in the development and maintenance of the strategic IT plan.
4. Guide strategic IT planning by using an IT steering committee.

## 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, file disposition, error response, restart, and recovery. These instructions are control-oriented, are kept current, and are followed for each application and system.
2. Require written approval, including user involvement where appropriate, for departures from authorized set-up 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 review reports processed by the IT group for functional users to ensure that appropriate scheduling standards are being met, appropriate run labels are used, and appropriate databases are calculating and aggregating data accurately.
2. Use access control software and appropriate security controls to restrict access to reporting features to authorized individuals only.
3. Use audit trail logging to identify users who access and run reports to ensure only authorized individuals view the reports.
4. Use an error log to track incidents of reporting errors or unusual occurrences (such as abnormal job end, system failures, or incorrect data or calculations) and document the resolution of the event.
5. Use an exception report to log temporary or "quick fix" solutions to errors or unusual occurrences, and document the rationale for the "quick fix" and the resolution of a long-term solution.

## D. Access to IT operations is restricted.

**Business risks**

- Theft, errors, and irregularities will increase because of the lack of sound physical and logical controls.
- Unauthorized personnel will gain access to computer hardware, systems, and application programs.

**Control practices**

1. Implement clearly defined and approved policies to restrict access to specific electronic files and electronic information to authorized individuals. Policies cover files distributed on CDs and floppy disks, through networks, over the Internet or intranets, and by e-mail.
2. Use physical barriers (such as locked doors and cable locks on laptops) to restrict access and movement of computers and peripheral equipment.
3. Use guards, badges, and other identification measures to restrict access to computers and peripheral equipment to authorized personnel.
4. Implement identification and password measures to restrict report commands and the execution of report runs to authorized individuals.

## E. All approved input is accepted by the IT system and 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 links.
- Incomplete, outdated, or erroneous files will be used in running reports.

### Control practices

1. Use passwords and access authorization tables to restrict input and access of systems databases to authorized individuals.
2. Review data input for elements such as completeness, accuracy, viruses, and formatting before it is entered or downloaded into systems and databases.
3. Build logical safeguards into databases to ensure that data being entered is reasonable, or appropriate to the format. (For example, a spreadsheet requiring numbers would alert the user attempting to enter text that the data was not acceptable.)
4. Review data frequently for reasonableness after input, and use exception reports and validation routines to flag any unreasonable data inputs.
5. Reconcile input control totals with source data after processing to ensure completeness and accuracy.
6. Use user departments to maintain logs of data entry for all data entered by batch and account for all batches in a timely manner.
7. Use monitoring controls to track the entry details for data entered by batch, such as date, time, user, and department making the entry.
8. Limit attempts to gain access to unauthorized databases, programs, and reports to a defined number of users who are logged and reviewed.
9. Limit access to databases, programs, and reports to authorized individuals or groups, determined through a formal procedure.
10. Program the system to protect against unauthorized access by controlling user actions by menus, linking authorized users and resources, and using tables to define specific user and resource authorizations.
11. Use terminal polling and callback procedures to ensure requests for data access are authorized.

## F. Data is accurately converted.

### Business risks

- Loss or alteration of data during transmission will go undetected.
- Errors in data entry or conversion will not be detected.

### Control practices

1. Use key verification on all critical input fields.
2. Implement a data control function to reconcile processing totals to input totals of source data.
3. Confirm that the technology used to transmit data during uploads and downloads over network, Internet, extranet, or intranet has built-in controls for checking data transmission accuracy and completeness.

## G. Access to online systems is controlled.

### Business risks

- Unauthorized individuals will make undetected additions or modifications to data or program files.
- Sensitive data will be disclosed to unauthorized individuals.
- Significant losses will result from disruptions of business activities caused by damage to data files, program files, or other resources.

# UNIVERSITY OF TOLEDO INTERNAL AUDIT DEPARTMENT
# MANAGE INFORMATION TECHNOLOGY

**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 any pre-authorized locations requesting service on systems with dial-up capability.
13. Log and report all attempted security violations to an appropriate level of management.
14. Implement controls such as access control software and file password protection to prevent unauthorized access to production or data files, program libraries, and system libraries.
15. Ensure that adequate recovery controls are in place to record history or transaction logs for all transactions entered, and to alternate procedures for short- and long-term shutdowns.
16. Ensure that backup or recovery procedures are in place and are functioning as designed. (For example, if policy requires network backup daily, network backup is performed daily.)
17. Verify that dial-up telephone numbers are changed periodically.
18. Verify that dial-up lines are restricted from issuing critical commands.
19. Implement a 24-hour, toll-free communications link that allows callers to report anonymously on a variety of situations such as computer crime and employee theft.