UNIVERSITY OF TOLEDO INTERNAL AUDIT DEPARTMENT
MANAGE SECURITY

Control practices

The following control objectives provide a basis for strengthening your control environment for the process of managing security. 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.

UNIVERSITY OF TOLEDO INTERNAL AUDIT DEPARTMENT
MANAGE SECURITY

Control practices

1.

B. Physical security exists for computer resources.

Business risks

- Data will be added, modified, or deleted without proper authorization and will not be detected.
- Unauthorized changes will be made to application and systems software and will not be detected.
- Application programs will be used to process fraudulent data without detection.
- Sensitive information will be disclosed to unauthorized persons.
- Damage to data or to facilities will disrupt critical business activities and significant financial losses.

C. Security exists for all software and data.

Business risks

- Unauthorized changes will be made to application systems software and will not be detected.
- Application programs will be used to process fraudulent data without exception.
- Loss of, or unauthorized changes to, critical systems software or application programs will disrupt critical business activities and produce significant financial losses.
- Data will be added, modified, or deleted without proper authorization and will not be detected.
- Sensitive information will be disclosed to unauthorized persons.

Control practices

1. Install program library management software (PLS) to maintain systems software and production versions of application programs.
2. Identify critical and sensitive data specifically and categorize according to security requirements.
3. Restrict access to various applications and programs.
4. Maintain a record of program access for use as an audit or surveillance tool.
5. Install security software to control access to programs and program libraries.
6. Identify authorized users in the system by tools such as individual ID cards and confidential passwords, and make accountable all use of their ID and password.
7. Define access rules to restrict access to critical software on the basis of specific work requirements.
8. Ensure that procedures and responsibilities for the maintenance of user IDs and access rules following terminations or responsibility changes are defined and followed on a timely basis.
9. Require each new user, prior to receiving IDs and passwords, to complete a data sheet that enables the division manager to determine appropriate access and levels of security before forwarding access approval to the system administrator.
10. Require a forced change to IDs and passwords for initial log-on sessions.
11. Establish two levels of passwords. One for regular accounts (long-term employees with approved access to certain systems) and a second for privileged accounts (temporary users with access to a system for a defined time limit).
12. Require password changes every 90 days for regular accounts and every 30 days for privileged accounts.
13. Suspend user IDs and passwords upon a user transfer or termination.
14. Conduct periodic review of user activity to ensure those who no longer have or do not have access to the system are not using or attempting to use it.
15. Record unsuccessful log-on attempts via audit trails.
16. Record attempts to enter a supervisor mode or level via audit trails.
17. Review audit trails regularly for unusual occurrences.
18. Retain audit trails for at least one year.

UNIVERSITY OF TOLEDO INTERNAL AUDIT DEPARTMENT
MANAGE SECURITY

15. Create and distribute an intranet and Internet security policy to all employees with access to the intranet and Internet.
16. Prohibit inappropriate use of the Internet by personnel where it is inconsistent with business needs.
17. Restrict Internet access to those users whose job functions require the use of the Internet.
18. Provide access to Internet services through discrete, designated, and secured sources.
19. Prohibit workstations from connecting to the company network and to the Internet via modem at the same time.
20. Prohibit direct remote dial-in to the intranet for the purpose of connecting to the Internet or company facility.
21. Provide users with only necessary or standard Internet services, such as e-mail, navigation, file transfer protocol (FTP), or Telnet.
22. Restrict access to the intranet to users whose job functions require the use of the Internet.
23. Provide intranet/Internet services 24 hours a day, seven days a week.
24. Require employees to read the intranet and Internet security policy as part of their request for access. Require a statement to be signed stating they understand and will comply with the policy before granting access.
25. Provide intranet/Internet access through the user or user's manager submitting an access request form to the IT department along with an attached copy of a signed form acknowledging intranet and Internet security coverage.
26. Ensure that user IDs and passwords for Internet/intranet access are provided directly to the user by the IT department.
27. Keep documentation related to Internet/intranet access on file with the IT department that grants network access.
28.

UNIVERSITY OF TOLEDO INTERNAL AUDIT DEPARTMENT

E. Database and data file integrity is maintained.

Business risks

- Results of processing will be lost, altered, duplicated, or otherwise reflected incorrectly on the database or data files because of errors or software or hardware failure.
- Databases and master files will not be complete and current, resulting in inaccurate information.

Control practices

1. Establish a separate data administration function with broad responsibilities for data standards and data use in all areas related to IT.
2. Document and maintain data definitions on an automated data dictionary system for all systems significant to financial and operating information.
3. Implement data definitions to document the contents, attributes, and interrelationships of all data entities in significant systems.
4. Employ the data administrator to control the development and maintenance of all information stored in the data dictionary.
5. Define and enforce data naming standards, validation requirements, and other standards