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.

Effectiveness and efficiency of operations

A. Physical and logical security measures are implemented.
B. Physical security exists for computer resources.
C. Security exists for all software and data.
D. Security exists for communications (networks, intranets, Internets)
E. Database and data file integrity is maintained.

Effectiveness and efficiency of operations

A. Physical and logical security measures are implemented.

Business risks

- Data files will be subjected to unauthorized access.
- Data will be added, modified or deleted without proper authorization and will not be detected.
- Data will be lost due to improper control over batch and online systems.
- Unauthorized changes will be made to application and systems software and will not be detected.
- Application programs will be used to process fraudulent data and will not be detected.
- The auditor will misunderstand representations by IT personnel regarding the security measures in place, if IT lacks a business perspective.
- Sensitive information will be disclosed to unauthorized persons.
- Damage to files or facilities will disrupt critical business activities and significant financial losses.
- Personnel whose jobs are productivity oriented will not recognize the importance of security management and may inadvertently expose systems and data to undue risk.
- Expenditures for security devices, software, and related projects will prove inadequate and uneconomic.
- Management will not have adequate information about security measures to recognize their inherent limitations.

UNIVERSITY OF TOLEDO INTERNAL AUDIT DEPARTMENT
MANAGE SECURITY

Control practices

1. Establish formal policies that define information security objectives and responsibilities.
2. Establish standards, procedures, and guidelines that translate the security policy into rules and compliance criteria.
3. Establish security guidelines that detail the responsibilities of management, security administration, resource (data, programs or assets) owners, computer operations, system users, and internal auditors.
4. Establish guidelines that address issues such as: ownership of resources; procedures for granting access; procedures for establishing users' access privileges; required authorizations; security monitoring; the consequences of non-compliance with policy, standards, and procedures; and the security implementation plan, if applicable.
5. Obtain active and visible senior management support for IT security policies.
6. Appoint an information security officer (ISO) to be responsible for creating and maintaining IT security policy and procedures, reporting security issues to management, and ensuring policies and procedures are current and operating as designed.
7. Develop formal position descriptions that incorporate levels of sensitivity to restricted data and programs.
8. Perform and periodically update a security risk analysis and controls evaluation, and inform management of current exposures.
9. Establish the independence of the information security officer from IT management.
10. Establish a formally documented process for the information security officer to report and manage IT security incidents.
11. Require users of computer resources to click on a button indicating their agreement to comply with all information security policies at the time they log into information systems or networks.
12. Provide all users of computer resources with an information security manual, and require that they sign a form to verify their receipt and understanding of the security policies and procedures.
13. Post signs near computer resources to remind personnel of IT security issues and policies.
14. Provide training on appropriate IT security practices to all users of computer resources.
15. Establish a hot line for employees to report IT security violations.

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.

UNIVERSITY OF TOLEDO INTERNAL AUDIT DEPARTMENT
MANAGE SECURITY

Control practices

1. Employ policies and procedures to restrict access to computer rooms and other sensitive areas to only those individuals with job-related needs.
2. Establish electronic systems, such as use of electronic cards or keys that control physical access to computer rooms or other restricted areas.
3. Establish electronic systems that monitor physical access to computer rooms or other restricted areas by sensing information, which is coded in devices such as magnetic cards or keys, that uniquely identifies the individual requesting access and creates an audit trail of granted or denied access requests.
4. Ensure that an authorized individual always escorts visitors to areas where IT equipment is housed.
5. Locate computer centers where there is no access to ground floor exterior windows.
6. Ensure that computer centers and data closets have approved access lists that are maintained by the information security officer.
7. Secure and restrict data input and data storage locations.
8. Restrict tapes, disks, and other devices containing data to a storage area when not in use, and control materials in use via a sign-out or comparable procedure.
9. Locate computer workstations (desktops and laptops) in physically secured areas or lock up during non-working hours.
10. Design personal directories as a tool for information backup. Place only information considered to be germane to general business operations on shared directories.
11. Ensure each division has structured levels of passwords that engage separate business functions.
12. Employ a key card to open office suites after-hours and during weekends and holidays, and require manual sign-in in off-peak hours to track individuals that are onsite in case of an emergency.
13. Ensure laptops and other ancillary PC devices taken offsite are cabled to a secure station while located offsite and secured in the trunk of a vehicle while in transportation to and from sites.
14. Conduct a physical inventory of all computer equipment. Perform a reconciliation of IT equipment from the physical inventory to the books to true-up the books and investigate causes of differences.
15. Label all computer equipment with a tracking number, such as a bar code serial number, to identify to whom it is issued and the date of issuance.

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.

19. Define responsibilities for the investigation and resolution of all attempts at unauthorized access.
20. Restrict access to data files and databases according to the identity of the user, the specific data to be accessed, and the operation to be performed.
21. Define database definitions and program views of the database according to the specific needs of processing, and use only authorized predefined views in processing.
22. Keep particularly sensitive or critical data online only when it is needed or being used.
23. Require the information security officer, along with functional or department owners, to maintain a list of restricted databases and software applications for each area.
24. Require the IT security function to provide the functional and business managers with a list of personnel in their areas who have access to restricted applications and databases every 6 months. Entrust each manager with the responsibility to communicate to the IT security personnel any necessary modifications to the approved access list.
25. Employ antivirus programs on all systems where such programs are available. Install them on employee workstations as a part of workstation setup.
26. Classify data according to whether it is highly restricted with high disclosure risks and, thus, confidential; moderately restricted with moderate to high risks and available only to internal audiences; or unrestricted with no risk and freely disclosed to any interested party. These classifications drive security parameters to protect the data.
27. Strictly enforce the terms of all third-party licensed software on company systems.

D. Security exists for communications (networks, intranets, Internets)

Business risks

- Data will be added, modified, or deleted by persons at remote, and perhaps unknown, locations without proper authorization and will not be detected.
- Unauthorized changes will be made to application and systems software from remote locations and will not be detected.
- Sensitive information will be disclosed to unauthorized persons at remote, and perhaps unknown, locations.
- Damage to software or to data, caused maliciously or accidentally by persons making unauthorized use of communications facilities, disrupt critical business activities and produce significant financial losses.

Control practices

1. Provide dial-up access only to authorized users for valid business purposes.
2. Use an automated call-back procedure for dial-up purposes to safeguard against unauthorized access.
3. Use communications software that limits the number of log-on attempts from remote terminals before session termination occurs (usually three failed attempts lock the user out of the system).
4. Protect extremely critical or sensitive data for transmission through the use of message authentication codes or data encryption.
5. Adequately train and supervise personnel responsible for the maintenance and support of communications network.
6. Ensure login to systems from remote workstations do not contain operating system version or company identification information.
7. Require login messages from remote workstations to display no trespassing messages.
8. Reside servers (such as database servers, file and print servers, mid-range servers) in computer centers.
9. Reside all network infrastructure components such as bridges, gateways, routers, and switches in computer centers or data closets.
10. Employ LANs (local area networks) to limit the aggregation of data that is subject to unauthorized interception.
11. Create, publish, and keep current all network documentation, including: documentation of schematics of networks and connections; user documentation; system documentation and configuration; problem reporting procedures and contingency plans; and operations documentation.
12. Employ special controls such as firewalls to safeguard systems connected to public or shared networks.
13. Install virus protection on each local area network, PC, and gateway that is process critical or stores sensitive information.
14. Prohibit discussion and transmission of sensitive information on wireless modems or cellular telephones unless encryption software is used.

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. Require contractors (those who are not directly employed by the company) to have contracts that state they will adhere to the restrictions on intranet/Internet use and information dissemination.
29. Ensure that contractors' access rights to the Internet/intranet do not exceed a period of 180 days before requiring reauthorization.
30. Discontinue Internet/intranet access immediately when an employee terminates or a contractor's term has expired.
31. Revoke user IDs and passwords for Internet/intranet services if they are inactive for a period of 30 days or more.
32. Require all Internet/intranet users who attempt to enter internal networks to authenticate themselves through the authentication mechanism established by the company network.
33. Prohibit direct remote dial-in to the intranet.
34. Require digital signatures whenever message integrity is considered important.
35. Prohibit specific information from being sent over the intranet/Internet including data classified as confidential, such as: personnel information; payroll information; systems access passwords; information file encryption keys; and sensitive customer or supplier information.
36. Encrypt data classified as internal company information (accounting, budgets, memos, local operations manuals, and policies and procedures) when sending over the Internet.

37. Ensure that all software or any other information or files downloaded from non-company sources through the intranet/Internet are screened with virus detection software before being invoked.
38. Prohibit specific types of Internet/intranet usage. Such usage includes: acquiring, storing, and disseminating data that is illegal or pornographic, or that negatively depicts race, sex, or creed; knowingly disseminating false or libelous materials; accessing information not within the scope of one's work; misusing or disclosing customer or personnel information; deliberately damaging or disrupting networks; negligently introducing computer viruses; decrypting without authorization; installing sniffing or spoofing packets; downloading files without authorization; deliberately linking to web sites containing prohibited content; transmitting confidential information; playing games; doing personal shopping online; gambling; forwarding chain letters; accepting gifts as promotions; and engaging in any conduct that would constitute a criminal offense, lead to civil liability, or otherwise violate regulations or laws.
39. Review and clear each evening all publicly writeable directories on Internet-connected computers.
40. Monitor Internet activities periodically to ensure adherence to policies and procedures.
41. Empower management with the right to examine without prior notice e-mail, personal file directories, web access, and other information stored on company computers, at any time.
42. Prepare a business implementation and maintenance plan when developing a web site, and require the marketing or corporate communications group to approve all content for the site before it is published.

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 and guidelines that promote data quality.
6. Implement procedures and responsibilities to ensure that after all database reorganizations; control totals are reconciled to the control totals prior to reorganization.