UNIVERSITY OF TOLEDO INTERNAL AUDIT DEPARTMENT
IMPLEMENT AND MANAGE TECHNOLOGY SOLUTIONS

Control practices

The following control objectives provide a basis for strengthening your control environment for the process of acquiring, developing, deploying, and supporting technology solutions. 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. Modifications to systems software are authorized and approved.
B. Systems software modifications are appropriately tested.
C. Access to systems software is restricted.
D. Systems software and related documentation are evaluated adequately.

Effectiveness and efficiency of operations

A. Modifications to systems software are authorized and approved.

Business risks

- Improper or uncoordinated modifications to systems software will cause errors in application processing or provide the means of committing fraud.
- Changes to systems software will not conform to management priorities and objectives and will have undesirable effects on application processing.

Control practices

1. Require IT management to authorize and approve all modifications to systems software.
2. Ensure that change requests for modifications to systems software provide reasons for the change as well as a description of the change.
3. Analyze the possible impact the change could have on systems operations and performance when responding to a change request form for modifications to systems software.
4. Permit only authorized individuals to request systems changes.
5. Permit only authorized individuals to approve requests for systems changes.
6. Ensure an appropriate audit trail exists to support all changes to systems software (for example, program library software or manual procedures).
7. Implement quality assurance procedures to ensure systems software changes are performed in accordance with formal policies, procedures, and standards.
8. Implement procedures to ensure that changes to systems programs do not adversely impact the application programs.
9. Control, report, and document emergency fixes (quick fixes to systems that happen during processing, frequently performed at night).
10. Use incident reports to document emergency fixes.
11. Review emergency fixes at least annually to determine their appropriateness in terms of nature and frequency.

B. Systems software modifications are appropriately tested.

Business risks

- Inadvertent errors in systems software modifications will not be detected and, subsequently, will affect the accuracy of application processing.

Control practices

1. Establish formal standards for determining the testing scope, test plan documentation, approvals, and test environment requirements for systems software modifications.
2. Subject systems software modifications to comprehensive testing prior to implementation, in accordance with testing standards.
3. Analyze periodically the nature and frequency of post-implementation failures in systems software.
4. Test systems software modifications via an independent group of employees who are not involved in implementing the modifications.
5. Review test results of system software modifications and require management to sign off on them.
6. Retain test results of system software modifications as evidence of successful testing and for future reference.

C. Access to systems software is restricted.

Business risks

- Unauthorized routines will be attached to systems software to perpetrate and conceal fraud.
- Individuals will circumvent access controls and fraudulently alter application programs or data files by modifying authorization tables or bypassing program library software.

Control practices

1. Prohibit systems programmers from operating the computer while production systems are running.
2. Allow systems software support personnel only supervised access to application program documentation in either hard copy or through logical access to production source code or documentation libraries.
3. Report systems software modifications with either library software or manual procedures.
4. Ensure that systems utility programs that allow bypassing of normal systems or application controls and functions are prohibited or password-protected. Such programs are used only in circumstances of legitimate operational need and when IT management supervises their use.

D. Systems software and related documentation are evaluated adequately.

Business risks

- Systems software will be unproven and contain latent errors.
- Systems software will contain inadequate error-checking features.
- Erroneous changes to systems software will lead to extensive modifications or inadequate documentation.

Control practices

1. Obtain generally reliable systems software from reputable vendors exclusively.
2. Use current versions of systems software that are fully supported by vendors.
3. Log systems software and hardware problems and resolve exceptions in a timely manner.
4. Recognize exceptions (where the software has not had extensive prior use and field-testing) and exercise due care in maintaining backup and in performing manual balancing and reasonableness checks.
5. Ensure that documentation of all systems software is complete and current.