UNIVERSITY OF TOLEDO INTERNAL AUDIT DEPARTMENT
ENSURE CONTINUITY OF SYSTEMS

Control practices

The following control objectives provide a basis for strengthening your control environment for the process of ensuring continuity of systems. 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. Management and users are involved in and approve IT systems development.
B. Testing and conversion standards are used.
C. Appropriate authorization and approval is required for any changes to IT systems.
D. Changes to IT systems are tested and properly implemented.
E. Access to IT systems documentation is restricted.
F. Information systems are available as needed.

UNIVERSITY OF TOLEDO INTERNAL AUDIT DEPARTMENT
ENSURE CONTINUITY OF SYSTEMS

Effectiveness and efficiency of operations

A. Management and users are involved in and approve IT systems development.

Business risks

- Systems will not be designed according to user needs.
- Systems will not be properly implemented.
- Data will not be processed accurately and properly, resulting in erroneous calculations, logical errors, or perpetuation of fraud through programming.
- Programmed controls such as validity tests will be omitted or deficient and, thus, will not prevent reasonably anticipated errors, such as erroneous or invalid input, internal inconsistencies, field overflows and truncations, or illogical changes in processing sequences.
- System reporting will not provide users with sufficient data to verify the accuracy, completeness, and appropriateness of processing, such as lack of key control totals, lack of edit reports, lack of reasonable transaction detail.
- Systems will be susceptible to unauthorized modification, resulting in irregularities and manipulation of the controls that might otherwise help detect these irregularities.
- Systems will not meet management expectations or will fail to operate in accordance with the original specifications.

ENSURE CONTINUITY OF SYSTEMS

Control practices

1. Require management and user involvement in the design, development, testing and conversion of new and enhanced IT systems.
2. Employ a systems development life cycle which includes the following key aspects or phases: request for systems design; feasibility study; general system design; detailed systems specifications; program development and testing; system testing; conversion; and system acceptance and approval.
3. Use project management procedures to ensure proper management of systems development activities.
4. Require management and user involvement in the selection and tailoring of newly purchased IT systems or modifications.
5. Require IT management review and approval of new systems prior to conversion.
6. Restrict programmers from transferring programs (source code and load modules) from test to production until IT management authorizes the transfer.
7. Review all design work for proper implementation of control practices (for example, they follow approved design and documentation standards, standards have been user-approved, conformity exists between established programming policies and procedures, and completed programs are reviewed for compliance to original functional and technical specs).
8. Secure user department approval for all report layouts, input forms, and control reports prior to conversion.
9. Secure appropriate user department participation in the software selection process.
10. Secure internal audit department participation in the software selection process.
11. Require compliance with system design, programming, and documentation standards.
12. Document systems as a continuing process throughout the design and implementation stages.
13. Use user manuals that contain system flowcharts, transaction definitions, input formats and procedures, output descriptions, and reports.
14. Use system manuals that contain general and program-specific flowcharts, computer set-up instructions, and record file layout, and file retention.
15. Develop program "run" books for use during testing, conversion, and subsequent operation.

B. Testing and conversion standards are used.

Business risks

- The probability will increase that logical programming errors will occur.
- Unauthorized changes will be made to programs, master files, and reference data.
- Users will not understand all aspects of the system or how to use the system correctly.

Control practices

1. Subject new or modified systems to comprehensive testing prior to implementation.
2. Prepare test plans and train employees on how to use the plan prior to testing.
3. Compare test output to planned or parallel system results.
4. Uncover all significant problems with the system during testing and correct prior to conversion.
5. Back up appropriate old system files prior to conversion.
6. Perform testing using test files that contain comprehensive test data and non-production copies of live files.
7. Use test data that simulates normal processing.
8. Incorporate all reasonable error conditions and unusual situations, such as exception transactions, maximum file size, transaction volumes and security, as part of standard testing.
9. Restrict programmers from using live files during testing.
10. Employ user manuals and procedures during systems testing to verify the accuracy of documentation as well as processing.
11. Ensure test results are reviewed and approved by user departments before the new system is implemented.
12. Involve users in preparing test data to ensure it appropriately simulates live data.
13. Perform testing on all interfacing systems to evaluate the integrity of the interface.
14. Test across all known combinations of conditions, including valid and invalid as well as realistic and unrealistic volumes of data.
15. Formalize a procedure for transfer of new or modified programs into production libraries.

C. Appropriate authorization and approval is required for any changes to IT systems.

Business risks

- Data will not be processed accurately or properly.
- Programmed controls, such as validity tests, that may prevent reasonably unanticipated errors will be rendered inoperative.
- Systems reporting will not provide users with sufficient data to verify the accuracy, completeness, and appropriateness of processing.
- Ongoing maintenance costs will be significantly higher.
- Operating efficiency (both technical and functional) will be reduced.

Control practices

1. Require IT group to authorize and approve all systems and program changes.
2. Control and report all emergency changes (such as quick fixes to systems).
3. Document emergency fixes properly and in a timely manner.
4. Require user department authorization and approval for all systems and program changes except those required to correct programming errors.
5. Require an approved change request for all changes.
6. Ensure that programming supervisors perform a thorough supervision and review of program changes. This involves a detailed code review, processing the change against test data, and parallel processing.
7. Require change requests to be in writing and include the reasons for the requested changes.
8. Require changes to be documented and approved by employees who do not have duties surrounding the execution of the change.
9. Retain original backup versions of pre-change files until several revisions have been processed and new programs are tested and updated.

D. Changes to IT systems are tested and properly implemented.

Business risks

- User departments will follow improper procedures and program errors will occur.
- Processing errors will occur.
- Preventative controls will be inoperable.
- Reporting will be insufficient for supporting error detection controls.

Control practices

1. Subject systems changes to comprehensive testing and approval prior to implementation.
2. Perform testing using comprehensive test files and non-production copies of live files.
3. Perform testing for month-end, quarter-end, and year-end activity as well as for daily activity.
4. Establish a generalized standard test plan for major systems and applications, including normal and special user situations.
5. Implement controls to ensure the production source code accurately represents the load modules used in processing.
6. Use program library software to prevent the movement of programs into production status before they have been tested and formally approved.
7. Authorize a separate group (often called quality assurance) to approve tested programs and move them into production status.

E. Access to IT systems documentation is restricted.

Business risks

- Developed systems will lack integrity.
- Unauthorized changes will be made to programs unintentionally.

Control practices

1. Ensure systems documentation, both physical and source library programs, are secure physically and logically, and access is restricted to authorized personnel.
2. Deny programmers access to operations and production programs.
3. Implement program library software that restricts access to production program code and reports all program changes to IT management for review and approval.
4. Deny system users access to systems technical documentation.

F. Information systems are available as needed.

Business risks

- Business continuation planning will be poor or lacking.
- IT safeguards will be inadequate.

Control practices

1. Establish and maintain senior management commitment for business contingencies.
2. Maintain a formal business continuity plan.
3. Assess the impact of new or modified systems on business continuation procedures.
4. Establish alternative processing arrangements.
5. Test business continuation procedures regularly.