# UNIVERSITY OF TOLEDO INTERNAL AUDIT DEPARTMENT
# DEVELOP FRAMEWORKS TO ALIGN BUSINESS AND TECHNOLOGY

Control practices

The following control objectives provide a basis for strengthening your control environment for the process of defining and managing organization and strategy. 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. Responsibilities of IT personnel are defined and communicated.
B. Incompatible duties among IT personnel are segregated.

# UNIVERSITY OF TOLEDO INTERNAL AUDIT DEPARTMENT
# DEVELOP FRAMEWORKS TO ALIGN BUSINESS AND TECHNOLOGY

Effectiveness and efficiency of operations

**A. Responsibilities of IT personnel are defined and communicated.**

**Business risks**

- IT personnel will make operating mistakes as a result of misunderstood instructions, lack of proper supervision and review, poor work habits, shortcuts in performance of duties, or poor communication.
- IT personnel will make undetected errors because they will assume responsibilities that exceed their understanding or qualifications.
- IT effort and resources will be expended in ways unrelated to company objectives because of inadequate management control.

**Control practices**

1. Develop and continually update the information technology (IT) organizational chart.
2. Exercise adequate supervision, at appropriate levels, in each IT functional area. (Examples of functional IT areas may include applications development, IT user and technical support, networking services, and IT policy and administration.)
3. Stress adequate qualifications in the hiring policies for IT personnel.
4. Establish an integrated personnel training and development program in the IT department and recognize its importance.
5. Establish and regularly update formal job descriptions for IT roles. (Examples may include CIOs, project leaders, designers and developers, programmers, systems and technical specialists, end-user help desk staff, technical help desk staff, and administrators for local area networks (LANs), wide area networks (WANs), and telephony.)
6. Develop and continually update policy manuals. (Examples of areas requiring policy manuals include network administration, IT security, contingency planning, systems operations and maintenance, technical support, file backup and archiving, hardware selection and acquisition, and software selection and acquisition.)

**B. Incompatible duties among IT personnel are segregated.**

**Business risks**

- IT controls will be subject to override or circumvention as a matter of "convenience."
- Opportunities to perpetrate and conceal fraud will develop because IT personnel will have direct or indirect access to assets.
- IT employees and others inside or outside of the organization will conspire to commit fraud.

**Control practices**

1. Delegate adequate segregation of duties between operations, systems, programming, applications programming, and data control.
2. Ensure that programmers and developers do not approve or initiate changes to master file data or "live" data.
3. Ensure that IT personnel do not have other duties in other departments. (For example, an IT programmer who creates the purchasing system would not also act as a purchasing agent for the company.)
4. Instruct IT department to prepare reports covering the activities of its personnel. (Examples include time reports or Gantt charts highlighting the time element for specific projects.)
5. Require sensitive files and programs to be write-protected, password-protected, or encrypted, and limit access to authorized personnel only.