

RISK ADVISORY SERVICES

# IT CONTROL DESIGN AND EVALUATION

## THE INTERNAL CONTROLS ENVIRONMENT HAS CHANGED RADICALLY IN LIGHT OF REGULATORS IMPOSING STRICT GOVERNANCE, FINANCIAL DISCLOSURE AND INFORMATION SECURITY REQUIREMENTS ON ORGANIZATIONS.

Companies battle to meet various compliance holidays and Basel II obligations, which require establishing, evaluating and monitoring the effectiveness of internal controls over financial reporting.

Controls can be manual or automated; as simple as regularly generating reports and reviewing them or, as in-depth as preventing particular classes of users from accessing data on specific screens.

A basic example of an internal control is the segregation of duties for an Enterprise Resource Planning (ERP) system. Where different persons are responsible for handling separate, specific details of a transaction. In the case of Information Technology (IT) personnel, the segregation of duties through access control is critical to preventing unauthorized changes to confidential information such as payroll databases.

### IT General Controls (ITGC)

With the BDO methodology, ITGCs are defined as a system of controls responsible for ensuring the confidentiality, integrity, and availability of IT systems, applications, data files and system workflows. The five key areas of ITGCs are:

- **IT control environment:** Sets the tone of the IT layout within the organization, influencing the control consciousness of IT staff and users.

- **Change management:** Controls ensuring that only approved modifications are made to the infrastructure and the computer applications which govern calculations, creation of reports and functional changes.
- **Computer operations:** Controls which help ensure automated processing is accurate, complete and running on a daily basis.
- **Access to program data:** Controls which ensure access to systems, resources and data is limited to authorized personnel.
- **Program development:** Controls which ensure the suitability and effective implementation of the proposed programs in the work environment.

### Application Controls

Automated controls are preferred whenever possible because they reduce the possibility of human error. BDO defines application controls as either:

- Automated control procedures embedded computer applications (e.g., calculations, posting to accounts, generation of reports, edits, control routines) or;
- Manual control procedures that are dependent on computer application (e.g., the review of an exception report). This control is dependant on the accuracy and completeness of a system generated report.



## CONTACT BDO

### National

Sam Khoury  
416 369 6030  
skhoury@bdo.ca

### Central Canada

Carlo Mariglia  
416 369 3078  
cmariglia@bdo.ca

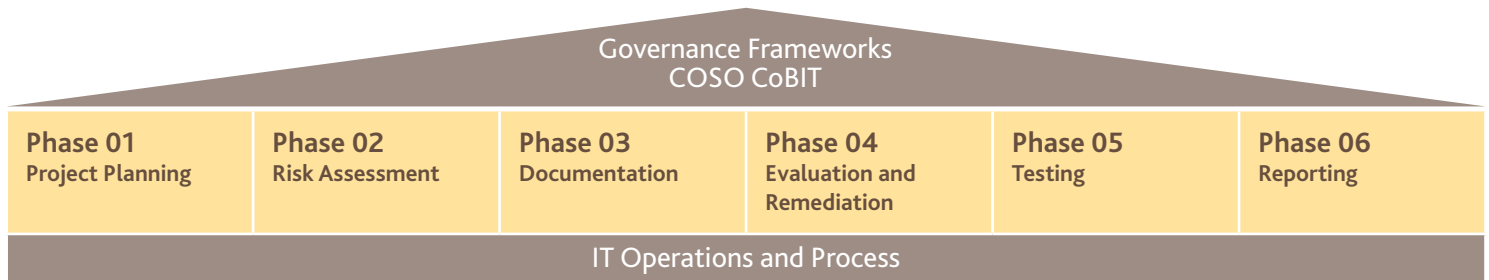
### David Knott

416 815 3016  
dknott@bdo.ca

### Eastern Canada

Pierre Taillefer  
514 934 7806  
ptaillefer@bdo.ca

## SERVICE SOLUTION METHODOLOGY



Application controls can be categorized into the following areas:

- **Calculations:** Mathematical / logical system based calculations/ system routines;
- **Postings:** Automated postings to specific accounts or summarization to specific accounts;
- **Edits/Validations:** System checks as well as edit/validation safeguards embedded within an application to ensure the accuracy and validity of data;
- **Interfaces:** Incoming and outgoing interfaces and data exchanges; and
- **Access restrictions:** Access privileges to specific functions of the application (e.g. functionality, databases, utilities).
- **Reports:** Various types of system generated reports used for reliance (e.g. custom built and vendor developed reports with complex calculations);

### End-User Computing

End-User Computing (EUC) tools are generally used to:

- generate financial data within significant processes
- generate financial or other data in keymanual controls

Examples of EUC tools include ad-hoc reporting tools, queries run from data warehouses, spreadsheets and databases.

Key concerns to management when evaluating the use of EUC tools include:

- Actual use of the element (e.g. financial, operational or analytical)
- Complexity of the performed function
- Possibility of logic errors
- Number of EUC users

- Change management procedures and
- Access control over the logic and sensitive data

### The Solution

BDO's approach to IT control design and evaluation is risk-based, covering financial operational and analytical risks to the organization. It includes key components of recognized frameworks and standards (COSO, CoBIT, ISO 17799/27001) as well as IT guidelines prescribed by the AICPA and CICA.

Our roadmap to successful requirements for ICFR includes the following six phases:

**Phase 01 – Project Planning:** Establish a team comprised of both BDO and client personnel. We will then develop the appropriate course of action to complete the scoping and planning of the overall assignment.

**Phase 02 – Risk Assessment:** Conduct a risk assessment evaluation of the organization's financial reporting processes, the technology used to support them and finalize significant locations.

**Phase 03 – Documentation:** Identify and document IT and application controls using our tools and templates. The BDO process ensures that application controls, IT systems and business processes are integrated to support the accuracy, completeness and validity of all transactions.

**Phase 04 – Evaluation and Remediation:** Evaluate controls to ensure they are designed effectively and provide management with recommendations for improvement.

**Phase 05 – Testing:** Develop and implement test plans to confirm the operating effectiveness of the controls in place. Summarize findings upon completion and establish remediation requirements.

**Phase 06 – Reporting:** Present conclusions on the design and operating effectiveness of the implemented controls. Assess the significance of each deficiency and provide management with suggestions for improvement and assist in planning for sustainability.