ISACA®
Serving IT Governance Professionals

COBIT® AND APPLICATION CONTROLS

A MANAGEMENT GUIDE

Application Controls Defined

Design and Implementation of Application Controls

Operation and Maintenance of Application Controls

Application Controls and IT General Controls

Application Controls Assurance

ISACA®

With more than 86,000 constituents in more than 160 countries, ISACA® (*www.isaca.org*) is a recognised worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *ISACA® Journal*, and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 60,000 professionals since 1978; the Certified Information Security Manager® (CISM®) designation, earned by more than 10,000 professionals since 2002; and the new Certified in the Governance of Enterprise IT® (CGEIT®) designation.[1]

Disclaimer

ISACA has designed this publication, *COBIT® and Application Controls: A Management Guide* (the 'Work'), primarily as an educational resource for control professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, control professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or information technology environment.

Reservation of Rights

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *info@isaca.org*
Web site: *www.isaca.org*

ISBN: 978-1-933284-85-9
COBIT® and Application Controls: A Management Guide
Printed in the United States of America

[1] CGEIT is a trademark/servicemark of ISACA. The mark has been applied for or registered in countries throughout the world.

ACKNOWLEDGEMENTS

ISACA wishes to recognise:

Authors

Eugene Atangan, CISA, PMP, Deloitte & Touche LLP, Canada
Gary S. Baker, CGEIT, CA, Deloitte & Touche LLP, Canada
Steven Cauwenberghs, CISA, CISM, CIA, Deloitte, Belgium
Candy (Yi-Ting) Chen, Deloitte & Touche LLP, Canada
Dan Cimpean, CISA, CISM, CIA, Deloitte, Belgium
Cosmin Croitor, CISA, CGEIT, ACCA, CIA, Deloitte, Belgium
Jessica Galland, Deloitte, Belgium
Gary Hardy, CGEIT, IT Winners, South Africa
Tony Jiang, CISA, CPA, Deloitte & Touche LLP, Canada
Gord Kilarski, I.S.P., Deloitte & Touche LLP, Canada
Monica Tang, Deloitte & Touche LLP, Canada
Geert Thoelen, Deloitte, Belgium
Johan Van Grieken, CISA, CGEIT, Deloitte, Belgium

Expert Reviewers

Mark Adler, CISA, CISM, CIA, CISSP, Allstate Insurance Company, USA
Kenneth C. Brancik, Ph.D., CISA, CISM, CISSP, ITIL, Northrop Grumman Information Systems, USA
Dirk Bruyndonckx, CISA, CISM, MCA, KPMG Advisory, Belgium
Luis A. Capua, CISM, Sigen, Argentina
Muhammad Fadli Davies, CISA, Old Mutual, South Africa
Seda Demircioglu, PricewaterhouseCoopers, The Netherlands
Heidi L. Erchinger, CISA, CISSP, System Security Solutions, Inc., USA
Robert F. Frelinger, CISA, CGEIT, Sun Microsystems, Inc., USA
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
J. Winston Hayden, CISA, IT Governance Service Consultants, South Africa
Monica Jain, CGEIT, CSQA, CSSBB, Covansys–A CSC Company, USA
Kamal Khan, CISA, Saudi Aramco, Saudi Arabia
Suzana S. Keller, CISM, CISSP, Coca Cola Enterprises, USA
John W. Lainhart IV, CISA, CISM, CGEIT, IBM Global Business Services, USA
Charles Mansour, CISA, Charles Mansour Audit & Risk Services, UK
Malcolm R. Pattinson, CISA, CISM, University of South Australia, Australia
Cheryl Faye Santor, CISA, CISM, CISSP, CNE, Metropolitan Water District of SoCal, USA
Maxwell J. Shanahan, CISA, FCPA, MACS, MII, Max Shanahan & Associates, Australia
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA
Peter Van Mol, CISA, Atos Worldline nv, Belgium
Greet Volders, CGEIT, Voquals, Belgium

ACKNOWLEDGEMENTS (*cont.*)

ISACA Board of Directors
Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, KPMG LLP, UK, International President
George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control SA, Belgium, Vice President
Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Vice President
Jose Angel Pena Ibarra, CGEIT, Consultoria en Comunicaciones e Info. SA & CV, Mexico, Vice President
Robert E. Stroud, CGEIT, CA Inc., USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President
Frank Yam, CISA, CCP, CFE, CFSA, CIA, FFA, FHKCS, FHKIoD, Focus Strategic Group Inc., Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young, USA, Past International President
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA, Director
Tony Hayes, CGEIT, FCPA, Queensland Government, Australia, Director
Jo Stewart-Rattray, CISA, CISM, CGEIT, CSEPS, RSM Bird Cameron, Australia, Director

IT Governance Committee
Tony Hayes, CGEIT, FCPA, Queensland Government, Australia, Chair
Sushil Chatterji, Edutech Enterprises, Singapore
Kyung-Tae Hwang, CISA, Dongguk University, Korea
John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA
Hugh Penri-Williams, CISA, CISM, CCSA, CIA, Glaniad 1865 EURL, France
Gustavo Adolfo Solis Montes, CISA, CISM, Grupo Cynthus, Mexico
Robert E. Stroud, CGEIT, CA Inc., USA
John Thorp, CMC, I.S.P., The Thorp Network Inc., Canada
Wim Van Grembergen, Ph.D., University of Antwerp Management School and IT Alignment and Governance Research Institute, Belgium

COBIT Steering Committee
Robert E. Stroud, CGEIT, CA Inc., USA, Chair
Gary S. Baker, CGEIT, CA, Deloitte & Touche LLP, Canada
Rafael Eduardo Fabius, CISA, Republica AFAP SA, Uruguay
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Jimmy Heschl, CISA, CISM, CGEIT, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
Greet Volders, CGEIT, Voquals, Belgium

TABLE OF CONTENTS

TABLE OF CONTENTS (*cont.*)

1. INTRODUCTION

The dependence of enterprises on automated processing of information is indisputable. Virtually every aspect of day-to-day business activity is dependent on timely, accurate and reliable information—information that is generated, processed, accumulated, stored and reported by automated information systems. Customers, suppliers, employees, line management, middle management, the C-suite, board of directors, shareholders and all other stakeholders make decisions based on the information they receive—information whose integrity and reliability depend almost exclusively on the application systems and surrounding control processes that are used to process the information. These decisions can be only as good as the quality of the information upon which they are based. Bad information will almost invariably result in bad decisions—garbage in, garbage out. The examples of bad information leading to fateful decisions are numerous and no enterprise is immune. There are many examples within anyone's personal experiences.

THE IMPORTANCE OF CONTROL

Because enterprises depend so heavily on the reliability of information, it is essential that risks in the underlying application systems processing the information be managed and controlled. The mechanisms built into these applications and surrounding business processes to ensure and protect the accuracy, integrity, reliability and confidentiality of this information are the key ones, and are the subject of this publication.

That is not to say that the information used must be 'perfect'. Perfection is not always needed—information should be *as reliable as it needs to be for the purpose for which it is used*. Consider a simple example: the information provided by an automobile's speedometer. In normal, day-to-day use this information does not need to be absolutely accurate. This information is typically used as a guide to determine, for example, how long it will take to get to a destination or when to ease off the accelerator because of an upcoming speed trap. Typically, the speedometer does not need to be calibrated to within a fraction of a kilometer (or mile) per hour. Some degree of imprecision can usually be tolerated, depending perhaps on the precision of the local traffic authorities. Medical practitioners, on the other hand, may require a very high degree of precision for patient monitoring systems since the decisions made based on that information can be life-or-death choices.

The significance of this analogy is to understand that the importance of and need for control are dependent on the intended use of the information and the impact associated with loss of the accuracy or integrity of that information. A 'reasonably accurate' speedometer may be required to avoid unfortunate encounters with the authorities and to predict destination arrival times. Medical practitioners need highly accurate, reliable patient monitoring systems to enable reliable patient health decisions. Enterprises need reliable information to manage the enterprise and its commercial, legal, contractual and regulatory responsibilities. As such, business management needs to ensure that the controls within the application systems are sufficient to provide an appropriate degree of reliability of the resulting information. Decisions on the nature, extent and precision of controls must be based on an assessment of the importance of the information and the risks or outcomes associated with a loss of accuracy or integrity of that information.

GUIDANCE ON APPLICATION CONTROLS

This publication provides guidance on application controls and is targeted to business and IT management, business process owners, developers, users, auditors and compliance practitioners. Historically, management and users have focused primarily on the business functionality of the application systems, and the concept of application controls has been the domain of the auditors and compliance practitioners. However, because of the importance of reliable information, this publication is designed to reinforce the concept that application controls do represent business functionality—and are not the sole domain of the audit community.

This publication is written primarily for the business and IT community and, as such, uses business language and tries to minimise 'audit-speak'. The publication is structured based on the life cycle of application systems—from defining requirements through implementation, operation and maintenance, and, finally, providing assurance on application controls. While the concepts have been structured along this life cycle, it is not intended to imply that the concepts apply only to new applications as they enter the requirements definition stage of the cycle; far from it. Rather, the concepts apply equally to both new and existing legacy application systems. For legacy applications, there may need to be some 'catch-up' activities (that would otherwise be done as part of requirements definition and implementation) to complete. These activities could include, for example, performing a risk analysis and identifying the relevant control objectives and associated control activities. These activities are crucial to understanding the key risks within legacy applications and ensuring that appropriate risk management activities are in place, or in developing additional activities necessary to close any gaps or exposures.

Application controls are identified and addressed as part of the COBIT 4.1 framework,[2] as well as within its companion publications, including the *IT Assurance Guide: Using COBIT®*, *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition* and the *IT Governance Implementation Guide: Using COBIT® and Val IT, 2nd Edition*. These are important sources providing specific technical details related to application controls (e.g., relevant objectives, value and risk drivers, and control practices). It is not the intent of this publication to replace that material. Rather, this publication is designed to provide additional guidance to support existing material. The publication makes heavy use of cross references to relevant sections within the COBIT family of publications, and the reader is encouraged to leverage these resources as appropriate.

Throughout the publication, the key messages are highlighted in separate boxes. These are intended to provide the reader with key points from the application controls guidance. These key messages are also summarised in appendix H—Summary of Key Messages.

[2] For an overview of COBIT 4.1, please refer to appendix G—Overview of COBIT.

2. EXECUTIVE SUMMARY

Enterprises demand accurate, complete and reliable information. This information is used by management to make critical, informed business decisions and, increasingly, to demonstrate regulatory compliance. Information is accumulated and reported to stakeholders to enable them to make informed business decisions. Healthcare professionals use patient care information to make informed diagnostic and treatment decisions. Air traffic controllers use inbound and outbound flight information to make critical, informed landing priority decisions. Mail and courier companies use priority and destination information to make routing and delivery decisions.

The concepts of application systems and application controls have significantly evolved since the terms were originally coined. Nevertheless, they are still often primarily associated with the financial aspects of an enterprise's activities. In their work on balanced scorecards in the mid-1990s, Kaplan and Norton[3] pointed out the need for management to look beyond the financial dimension, viewing in a balanced manner the customer, process and learning dimensions of the enterprise. Performance measurement and change management information, for example, enables management to drive business improvement. Business intelligence and a human resource skills database can help to position the enterprise to meet future requirements. Customer information (e.g., from a customer relationship management [CRM] or helpdesk application) can be used to increase customer satisfaction and have a positive influence on the financial performance of the enterprise. Because of the speed and complexity of business, all applications (not just financial applications) need to include controls to ensure that they provide reliable information.

APPLICATION CONTROLS OVERVIEW

Application controls are a subset of internal controls that relate to an application system and the information managed by that application. Timely, accurate and reliable information is critical to enable informed decision making. The timeliness, accuracy and reliability of the information are dependent on the underlying application systems that are used to generate, process, store and report the information. Application controls are those controls that achieve the business objectives of timely, accurate and reliable information. They consist of the manual and automated activities that ensure that information conforms to certain criteria—what COBIT refers to as business requirements for information. Those criteria are effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability.

Management is accountable for the business decisions it makes and for the reliability of the information upon which those decisions are based. Management is also accountable for the reliability of the information it generates and provides to stakeholders and to gather its regulatory compliance requirements. Ensuring that sufficient application controls are in place to mitigate key risks (including fraud risks) and are operating with sufficient effectiveness to provide reliable information is a management responsibility. Activities, roles and responsibilities for various aspects associated with application controls are shared amongst a number of parties throughout the life cycle of the respective application.

DESIGN AND IMPLEMENTATION OF APPLICATION CONTROLS

Business and functional requirements of application systems are commonly identified, clarified and defined during the initial phases of application system development or acquisition. It is during this phase that business requirements for control—or control objectives—also need to be identified and defined. The business requirements for ensuring that the application collects, processes and reports accurate, reliable information need to be explicitly defined—to ensure that these business requirements are ultimately provided by the solution when it is implemented. The business requirements for control will be based on the corresponding risks associated with inaccurate or unreliable information and, therefore, must be determined by the business management responsible for that information.

[3] Kaplan, Robert S.; David P. Norton; *Balanced Scorecard: Translating Strategy Into Action*, Harvard Business School Press, USA, 1996

Explicitly defined control objectives enable business users and system analysts to develop an efficient and effective balance of control activities that ensures that those objectives are achieved. They can leverage a combination of manual or automated activities—activities that would prevent errors or detect them. They can determine such things as how frequently the control procedure should be applied and who should be performing the activities. These decisions are essential to ensure a balanced, cost-effective and efficient combination of control activities. Business management needs to be satisfied that control activities are appropriately designed and that key business risks and related control objectives will be addressed.

Functional specifications for an application system define the business requirements for that application. As such, the control activities become the functional specifications that are necessary to meet the business requirements for control. These specifications form the foundation for either the developers to develop the code or the vendor solution evaluation team to evaluate alternative solutions. The specifications will also include manual control activities, which can be used by the team designing the future-state business process or acquiring the vendor solution to create processes and work flows. Defining application controls should be a discrete step in each system development life cycle (SDLC) process, along with steps associated with defining other business functionality requirements.

Once developed or acquired, the business solution is configured and tested to ensure that it operates according to the specifications and will achieve the desired business objectives. In the same way, and at the same time, application controls are configured and tested to ensure that they meet their specifications and objectives. An essential component of management's 'go/no-go' systems implementation decision should be the results of designing, building, configuring and testing the key application controls that ensure the accuracy, integrity, reliability and confidentiality of information and information processing by the application.

Many systems implementations have failed because of inadequate controls and the application consequently generating unreliable information. Many of these failures could have been prevented by a more diligent focus on the design and testing of controls prior to implementation.

Proactive focus on designing a cost-effective, efficient balance of controls as part of the solution design activities also enables maximising efficiencies associated with automating control activities. The need to add expensive, manual control procedures post-implementation to compensate for control deficiencies can be minimised through a diligent process of considering control requirements and proactively developing cost-effective control solutions.

Assessing risks, identifying relevant control objectives and determining the sufficiency of design of application controls are important parts of the design and implementation processes for new systems. It is equally important that these activities also be performed for existing applications being used as part of the enterprise's business and management processes.

Responsibility for design and implementation of application controls is shared. Business management is accountable for ensuring that application control requirements have been appropriately designed and implemented to meet the business objectives for control. IT management is accountable for developing application controls in accordance with defined business requirements.

OPERATION AND MAINTENANCE OF APPLICATION CONTROLS

Responsibilities for application controls do not cease when systems are implemented. The IT processing environment in which the application operates needs to be controlled and maintained to ensure the continued reliability of information processing. Application controls need to be operated and/or executed on an ongoing basis, as part of regular information processing activities to ensure their effectiveness. Changes in business requirements and business processes will drive the need to update and improve application controls.

IT is typically responsible for ensuring the reliability of the IT processing environment. In addition to providing key elements to protect the confidentiality of data, this processing environment provides for the ongoing reliability and availability of information processing and the integrity of the application and its data.

Business management needs to monitor the ongoing effectiveness of its application controls. It needs to ensure that the manual activities necessary to supplement and support the automated activities are being completed appropriately. Depending on the business risk and the importance of the information, monitoring mechanisms need to be adopted and followed to enable identification of situations that may suggest possible control failures.

As business needs evolve, changes will be required to the application controls. Application control changes need to be managed and controlled to ensure the continuing reliability of the information upon which management is basing its decisions.

Responsibilities for operating and maintaining application controls are shared between business and IT management and need to be clearly understood by all parties. Business management is accountable for monitoring the ongoing effectiveness of the application controls and for identifying and defining requirements for changes. IT management is accountable for providing a reliable processing environment and for developing and delivering changes based on defined business requirements.

APPLICATION CONTROLS AND IT GENERAL CONTROLS

Applications and application controls depend on a reliable IT processing environment for their continued effectiveness. IT general controls are those controls within the IT processing environment that provide for this ongoing reliability (e.g., information security and change management controls, IT operations and job scheduling controls). As such, failures or breakdowns in IT general controls can have a significant impact on the effectiveness of the application controls.

Therefore, it is important that the effectiveness of IT general controls be understood throughout the application control design, implementation, operation and maintenance activities. A strong system of IT general controls can enable more reliance on automated application controls, whereas a less reliable system of IT general controls may suggest that greater emphasis should be placed on manual controls.

Also, when designing application controls, there may be choices as to whether some activities could be performed in a way that is common to all applications and incorporated as part of the IT general controls. This may be a more efficient and effective alternative than separately designing, building and implementing such controls within each application system. For example, it may be more efficient and effective to design user access controls using common tools and approaches for all applications, rather than to develop a unique security management capability into each application. In addition to efficiency and effectiveness considerations, other factors may also impact these decisions, including, for example, technical feasibility.

Where some or all IT activities are outsourced to third-party service providers, responsibility for a given control activity may be delegated to the service provider; however management retains ultimate accountability for the effectiveness of that outsourced environment and for developing and implementing appropriate controls and processes internally, taking the service provider controls into account.

APPLICATION CONTROL ASSURANCE

Assurance practitioners are frequently called upon to provide assurance on the effectiveness of application controls. Assurance can be provided ‘pre-implementation’ by assessing the planned design of the application controls as part of the overall future-state solution and business process. Assurance can also be provided ‘post-implementation’ and can take the form of assurance on the design of controls as well as on the operating effectiveness of those controls.

The approach for an assurance practitioner to provide such assurance should follow normal processes for providing assurance, including defining the scope and objectives, obtaining an understanding of the solution and the relevant control objectives, assessing whether the designed activities would achieve the control objectives if they operated satisfactorily, assessing whether the control activities did operate with sufficient effectiveness to achieve the objectives, and documenting and reporting on control weaknesses found and recommendations for improvement.

When providing assurance relative to application controls, the assurance provider should carefully consider the impact of known or potential IT general control weaknesses in the IT environments within which the application operates since this may have a significant impact on the determination of the effectiveness of the application controls.

The concept of providing assurance is commonly thought of in the context of an auditor (either internal or external) providing assurance to management, the board of directors and shareholders. However, the concept is increasingly relevant to financial and operational management in terms of providing assurance to relevant stakeholders. Examples where management is providing assurance to stakeholders include chief executive officer (CEO)/chief financial officer (CFO) certification of the design and operating effectiveness of internal controls as required by legislation, such as the US Sarbanes-Oxley Act, and line management (such as the chief information officer [CIO]) providing 'sub-certification' to the CEO/CFO on the effectiveness of controls within its operating units.

3. Application Controls Defined

For the purposes of this publication, applications consist of the programmed logic and automated business rules that are used to process information. The term 'application', or 'automated solution', is used in its generic sense—programmed logic and business rules can exist within specific 'modules', collections of modules can comprise an 'application' and a collection of applications and related procedures can comprise a 'system'. For the purposes of this publication, such differences or distinctions are not meaningful.

The effectiveness of application controls is an important business objective—ensuring the integrity and reliability of information used by management to make key decisions about the business and, increasingly, to meet regulatory requirements. While these concepts may be relatively well understood by auditors and control specialists, they may not be so well understood by business and IT management. An objective of this guide is to help management grasp these concepts since management needs to define the requirements, approve their design and ensure their reliable operation.

As with any discussion of controls, it is important to incorporate risk concepts and the need for management to be involved in the decisions related to the control activities necessary to reduce risk to an acceptable level.

BUSINESS PROCESSES AND AUTOMATED SOLUTIONS

Business management (i.e., the business process owner) is responsible for defining the appropriate business rules to ensure that the enterprise's objectives are achieved and the requirements for business processes. Automated tasks and activities are a significant, integral component of most business processes.

Business and IT should work together to design the business processes, covering both manual procedures and automated solutions in a properly integrated manner.

IT management is typically responsible for designing and implementing the automated solutions that enable achievement of management's business rules and objectives and for providing an environment for the reliable operation of those automated solutions.

Business management has overall responsibility for operating the entire business process including the manual and automated controls.

Automated solutions implemented will typically take one of the following two forms:

- **Management information systems**—These solutions are designed to automate the collection and processing of information related to the execution and financial aspects of the enterprise core activities, but are also related to the collection and processing of information about enterprise processes, resources and customers. Common examples include integrated enterprise resource planning (ERP) systems that automate the collection and processing of financial information, and the data warehouse or similar executive information systems/decision support systems (EIS/DSS) used to support business decision making.
- **Process automation systems**—These solutions are designed to automate the specific activities within the process. An example of process automation is a robotic system used in automobile manufacturing.

This guide focuses on application controls related to all types of systems. The objective is to provide guidance relative to the design, implementation and execution of control activities related to information systems—no matter what type—since each type provides critical information with which key decisions are made.

WHAT ARE APPLICATION CONTROLS?

In simple terms, application controls are a subset of internal control that relate to an application or application system. To better understand application controls it may be helpful to start from a basic understanding of internal control and control activities.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines internal control as:

> *Internal control is a process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:*
> • *Effectiveness and efficiency of operations*
> • *Reliability of financial reporting*
> • *Compliance with applicable laws and regulations*
>
> *COSO defines control activities as the policies and procedures that help ensure management directives are carried out.*[4]

In this context:

> Application controls can be viewed as those policies, procedures and activities designed to provide reasonable assurance that objectives relevant to a given automated solution are achieved.

Some common examples of application controls include:
• Logical access controls (i.e., those that limit access to application functionality)
• Data entry/field validations (e.g., validation of entered credit card numbers)
• Business rules
• Work flow rules (e.g., routing and sign-off of purchase requests)
• Field entries being enforced based on predefined values (e.g., pricing information)
• Work steps being enforced based on predefined status transitions (e.g., open > reviewed > closed)
• Reconciliations
• Review and follow-up of application-generated exception reports
• Automated activity logs
• Automated calculations
• Management and audit trails

Application controls refer to controls over the processing of transactions and data within an application system and, therefore, are specific to each application. The objectives of application controls, which may be manual or programmed, are to ensure the accuracy, integrity, reliability and confidentiality of the records and the validity of the entries made therein, resulting from both manual and programmed processing.

APPLICATION CONTROL OBJECTIVES

As noted previously, application controls are intended to provide reasonable assurance that management's objectives relative to a given application have been achieved. Management's objectives are typically articulated through the definition of specific functional requirements for the solution, the definition of business rules for information processing and the definition of supporting manual procedures. Examples include:
• **Completeness**—The application processes all transactions and the resulting information is complete.
• **Accuracy**—All transactions are processed accurately and as intended and the resulting information is accurate.

[4] *www.coso.org/resources.htm*

- **Validity**—Only valid transactions are processed and the resulting information is valid.
- **Authorisation**—Only appropriately authorised transactions have been processed.
- **Segregation of duties**[5]—The application provides for and supports appropriate segregation of duties and responsibilities as defined by management.

To satisfy business objectives, information needs to conform to certain control criteria, which CobiT refers to as business requirements for information. Seven distinct but overlapping information criteria are defined in CobiT:

- **Effectiveness**—Deals with information being relevant and pertinent to the process as well as being delivered in a timely, correct, consistent and usable manner
- **Efficiency**—Concerns the provision of information through the optimal (most productive and economical) use of resources
- **Confidentiality**—Concerns the protection of sensitive information from unauthorised disclosure
- **Integrity**—Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations
- **Availability**—Relates to information being available when required by the process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
- **Compliance**—Deals with complying with the laws, regulations and contractual arrangements to which the process is subject, i.e., externally imposed business criteria as well as internal policies
- **Reliability**—Relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities

These requirements can vary depending on the nature of the specific business process. Satisfying these information criteria is accomplished through a system of internal control activities. Some of these control activities (application controls) are employed within the business processes and application systems themselves while others (IT general controls) may be employed within the IT processes and services that manage the environment within which the applications operate. The relationship between application controls and IT general controls is further discussed in chapter 6: Relation and Dependencies of Application Controls With IT General Controls.

CobiT 4.1 identifies six control objectives and a number of illustrative control practices that are relevant for application controls.[6]

- AC1 *Source data preparation and authorisation*—Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Errors and omissions can be minimised through good input form design. Detect errors and irregularities so they can be reported and corrected.
  1. Design source documents in a way that they increase accuracy with which data can be recorded, control the workflow and facilitate subsequent reference checking. Where appropriate, include completeness controls in the design of the source documents.
  2. Create and document procedures for preparing source data entry, and ensure that they are effectively and properly communicated to appropriate and qualified personnel. These procedures should establish and communicate required authorisation levels (input, editing, authorising, accepting and rejecting source documents). The procedures should also identify the acceptable source media for each type of transaction.
  3. Ensure that the function responsible for data entry maintains a list of authorised personnel, including their signatures.
  4. Ensure that all source documents include standard components, contain proper documentation (e.g., timeliness, predetermined input codes, default values) and are authorised by management.
  5. Automatically assign a unique and sequential identifier (e.g., index, date and time) to every transaction.

[5] IT Governance Institute, CobiT® 4.1, USA, 2007
[6] *Ibid*., p. 16

6. Return documents that are not properly authorised or are incomplete to the submitting originators for correction, and log the fact that they have been returned. Review logs periodically to verify that corrected documents are returned by originators in a timely fashion, and to enable pattern analysis and root cause review.

- AC2 *Source data collection and entry*—Ensure that data input is performed in a timely manner by authorised and qualified staff. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.
  1. Define and communicate criteria for timeliness, completeness and accuracy of source documents. Establish mechanisms to ensure that data input is performed in accordance with the timeliness, accuracy and completeness criteria.
  2. Use only pre-numbered source documents for critical transactions. If proper sequence is a transaction requirement, identify and correct out-of-sequence source documents. If completeness is an application requirement, identify and account for missing source documents.
  3. Define and communicate who can input, edit, authorise, accept and reject transactions, and override errors. Implement access controls and record supporting evidence to establish accountability in line with role and responsibility definitions.
  4. Define procedures to correct errors, override errors and handle out-of-balance conditions, as well as to follow up, correct, approve and resubmit source documents and transactions in a timely manner. These procedures should consider things such as error message descriptions, override mechanisms and escalation levels.
  5. Generate error messages in a timely manner as close to the point of origin as possible. The transactions should not be processed unless errors are corrected or appropriately overridden or bypassed. Errors that cannot be corrected immediately should be logged in an automated suspense log, and valid transaction processing should continue. Error logs should be reviewed and acted upon within a specified and reasonable period of time.
  6. Ensure that errors and out-of-balance reports are reviewed by appropriate personnel, followed up and corrected within a reasonable period of time, and, where necessary, incidents are raised for more senior-level attention. Automated monitoring tools should be used to identify, monitor and manage errors.
  7. Ensure that source documents are safe-stored (either by the business or by IT) for a sufficient period of time in line with legal, regulatory or business requirements.
- AC3 *Accuracy, completeness and authenticity checks*—Ensure that transactions are accurate, complete and valid. Validate data that were input, and edit or send back for correction as close to the point of origination as possible.
  1. Ensure that transaction data are verified as close to the data entry point as possible and interactively during online sessions. Ensure that transaction data, whether people-generated, system-generated or interfaced inputs, are subject to a variety of controls to check for accuracy, completeness and validity. Wherever possible, do not stop transaction validation after the first error is found. Provide understandable error messages immediately to enable efficient remediation.
  2. Implement controls to ensure accuracy, completeness, validity and compliance to regulatory requirements of data input. Controls may include sequence, limit, range, validity, reasonableness, table look-ups, existence, key verification, check digit, completeness (e.g., total monetary amount, total items, total documents, hash totals), duplicate and logical relationship checks, and time edits. Validation criteria and parameters should be subject to periodic reviews and confirmation.
  3. Establish access control and role and responsibility mechanisms so that only authorised persons input, modify and authorise data.
  4. Define requirements for segregation of duties for entry, modification and authorisation of transaction data as well as for validation rules. Implement automated controls and role and responsibility requirements.
  5. Report transactions failing validation and post them to a suspense file. Report all errors in a timely fashion and do not delay processing of valid transactions.
  6. Ensure that transactions failing edit and validation routines are subject to appropriate follow-up until errors are remediated. Ensure that information on processing failures is maintained to allow for root cause analysis and help adjust procedures and automated controls.

- AC4 *Processing integrity and validity*—Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions does not disrupt the processing of valid transactions.
  1. Establish and implement mechanisms to authorise the initiation of transaction processing and to enforce that only appropriate and authorised applications and tools are used.
  2. Routinely verify that processing is completely and accurately performed with automated controls, where appropriate. Controls may include checking for sequence and duplication errors, transaction/record counts, referential integrity checks, control and hash totals, range checks and buffer overflow.
  3. Ensure that transactions failing validation routines are reported and posted to a suspense file. Where a file contains valid and invalid transactions, ensure that the processing of valid transactions is not delayed and all errors are reported in a timely fashion. Ensure that information on processing failures is kept to allow for root cause analysis and help adjust procedures and automated controls, to ensure early detection or prevent errors.
  4. Ensure that transactions failing validation routines are subject to appropriate follow-up until errors are remediated or the transaction is cancelled.
  5. Ensure that the correct sequence of jobs has been documented and communicated to IT operations. Job output should include sufficient information regarding subsequent jobs to ensure that data are not inappropriately added, changed or lost during processing.
  6. Verify the unique and sequential identifier to every transaction (e.g., index, date and time).
  7. Maintain the audit trail of transactions processed. Include date and time of input and user identification for each online or batch transaction. For sensitive data, the listing should contain before and after images and should be checked by the business owner for accuracy and authorisation of changes made.
  8. Maintain the integrity of data during unexpected interruptions in data processing with system and database utilities. Ensure that controls are in place to confirm data integrity after processing failures or after use of system or database utilities to resolve operational problems. Any changes made should be reported and approved by the business owner before they are processed.
  9. Ensure that adjustments, overrides and high-value transactions are reviewed promptly in detail for appropriateness by a supervisor who does not perform data entry.
  10. Reconcile file totals. For example, a parallel control file that records transaction counts or monetary value as data should be processed and then compared to master file data once transactions are posted. Identify, report and act upon out-of-balance conditions.
- AC5 *Output review, reconciliation and error handling*—Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient and protected during transmission; verification, detection and correction of the accuracy of output occur; and information provided in the output is used.
  1. When handling and retaining output from IT applications, follow defined procedures and consider privacy and security requirements. Define, communicate and follow procedures for the distribution of output.
  2. At appropriate intervals, take a physical inventory of all sensitive output, such as negotiable instruments, and compare it with inventory records. Create procedures with audit trails to account for all exceptions and rejections of sensitive output documents.
  3. Match control totals in the header and/or trailer records of the output to balance with the control totals produced by the system at data entry to ensure completeness and accuracy of processing. If out-of-balance control totals exist, report them to the appropriate level of management.
  4. Validate completeness and accuracy of processing before other operations are performed. If electronic output is reused, ensure that validation has occurred prior to subsequent uses.
  5. Define and implement procedures to ensure that the business owners review the final output for reasonableness, accuracy and completeness, and output is handled in line with the applicable confidentiality classification. Report potential errors; log them in an automated, centralised logging facility; and address errors in a timely manner.
  6. If the application produces sensitive output, define who can receive it, label the output so it is recognisable by people and machines, and implement distribution accordingly. Where necessary, send it to special access-controlled output devices.

- AC6 *Transaction authentication and integrity*—Before passing transaction data between internal applications and business/operational functions (within or outside the enterprise), check the data for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.
  1. Where transactions are exchanged electronically, establish an agreed-upon standard of communication and mechanisms necessary for mutual authentication, including how transactions will be represented, the responsibilities of both parties and how exception conditions will be handled.
  2. Tag output from transaction processing applications in accordance with industry standards to facilitate counterparty authentication, provide evidence of non-repudiation and allow for content integrity verification upon receipt by the downstream application.
  3. Analyse input received from other transaction processing applications to determine authenticity of origin and the maintenance of the integrity of content during transmission.

Figure 1 shows the relationship between the information criteria and how achievement of those criteria can be enabled by the various application control objectives defined previously.

Figure 1—Application Control Objectives and Information Criteria

Application Control Objectives	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
AC1 Source Data Preparation and Authorisation	S	P	S	P		S	
AC2 Source Data Collection and Entry	S	S	S	P		S	
AC3 Accuracy, Completeness and Authenticity Checks	S	P	S	P	S	P	P
AC4 Processing Integrity and Validity			P	P	P	P	P
AC5 Output Review, Reconciliation and Error Handling	P	S	P	P	P	P	P
AC6 Transaction Authentication and Integrity		S	P	P		P	

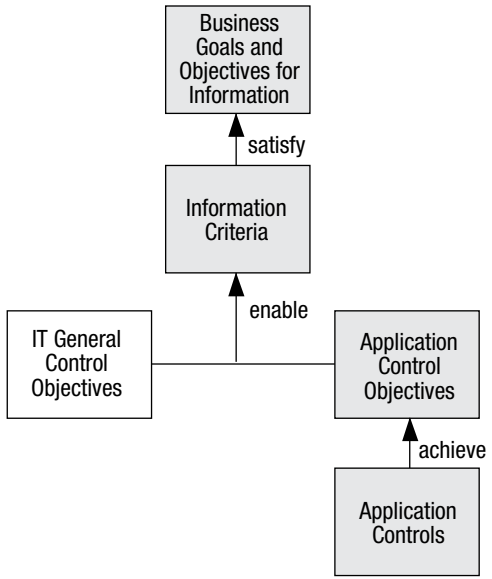
Information Criteria

P = Primary; S = Secondary

This provides a framework for positioning application controls as illustrated in **figure 2**. Please note this diagram is not intended to show a complete view for the IT general control objectives, but merely that some IT general controls may be necessary to achieve all of the information criteria (e.g., security controls). See chapter 6: Relation and Dependencies of Application Controls With IT General Controls for additional information relative to IT general controls.

Figure 2 depicts that application controls, together with IT general controls, enable achievement of the information criteria to satisfy management's business goals and objectives for information relative to that application.

Figure 2—Application Controls



BUSINESS PROCESS CONTROLS AND APPLICATION CONTROLS

Business process controls are activities designed to achieve the broad range of management objectives for the process as a whole.[7] Application controls, on the other hand, are the sub-set of business process controls that relate specifically to the applications and related information used to enable those business processes. **Figure 3** illustrates the relationship between application controls and business process controls.

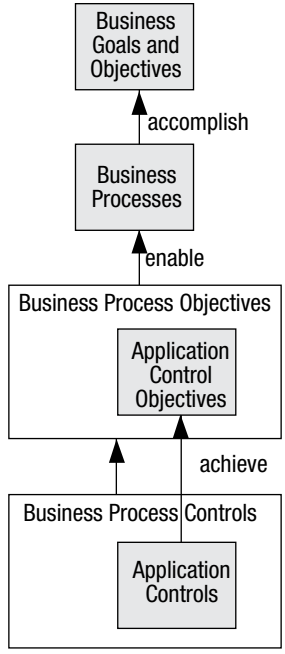
BUSINESS RISKS AND INFORMATION PROCESSING

There are a number of risks associated with any business process and complex processing of business information will introduce further risks. While automated solutions can be much more reliable than manual procedures, this will be the case only if the key risks within the automated solutions have been identified and appropriate controls have been implemented. While not intended to be comprehensive, examples of some key information-related risks and information processing-related risks include:

- **Incomplete and/or inaccurate information processing**—This risk relates to errors that may be made during the collection, input or processing of information.
- **Invalid or unauthorised transactions being processed**—While the previous risk relates to errors that may be made relative to processing legitimate business transactions, this risk relates to the risk of erroneous or illegitimate transactions being processed.
- **Unauthorised changes to standing data**—This is the risk of unauthorised changes to information subsequent to processing by the system.

[7] CobiT 4.1 identifies the following process control objectives: PC1 *Process goals and objectives*, PC2 *Process ownership*, PC3 *Process repeatability*, PC4 *Roles and responsibilities*, PC5 *Policy, plans and procedures* and PC6 *Process performance improvement*.

Figure 3—Business Process and Application Controls



- **Bypasses, overrides, manual entries that circumvent controls**—This is the risk of misuse of bypasses, overrides or manual entries to avoid automated application controls (these functions are inherent in most, if not all, application systems).
- **Inefficiencies**—This risk relates to incurring unnecessary cost or delays during the collection, input, processing, output or transfer of information.
- **Loss of confidentiality**—This risk relates to the inadvertent or intentional disclosure of information that has been identified by management to be sensitive or confidential (such as for business or regulatory compliance reasons).
- **Unavailability of information**—Information is not available when required, causing unnecessary processing delays and inability to make appropriate decisions.
- **Lack of integrity**—This risk relates to lack of reliability of data processed.

APPLICATION CONTROL OBJECTIVES AND INTERNAL CONTROL OVER FINANCIAL REPORTING

The requirement for effective internal controls has been well established for some time.[8] However, as a result of the Sarbanes-Oxley Act in the USA and similar legislation in other jurisdictions around the world, significant attention has been focused recently on a specific subset of management's objectives as they relate to financial information: ensuring that internal controls over financial reporting have been designed appropriately and are operating effectively to reduce the risk of a material misstatement in financial statements and related disclosures.

[8] Including such publications as the: National Commission on Fraudulent Financial Reporting (Treadway Commission), *Report of the National Commission on Fraudulent Financial Reporting*, USA, 1987; The Institute of Chartered Accountants in England and Wales, *Internal Control Guidance for Directors on the Combined Code* (Turnbull report), UK, 1999, *www.icaew.com/index.cfm/route/120907/icaew_ga/pd*; King Committee on Corporate Governance, King Report on Corporate Governance for South Africa (King I Report), Institute of Directors in Southern Africa, South Africa, 1992; King Committee on Corporate Governance, King Report on Corporate Governance for South Africa (King II Report), Institute of Directors in Southern Africa, South Africa, 2002, *www.iodsa.co.za/king.asp#King%20I%20Report%20-%201994.*

3. Application Controls Defined

If an enterprise is subject to Sarbanes-Oxley or similar financial reporting regulations, management is required to attest to the effectiveness of its controls relative to its financial information. When management is identifying the relevant control objectives for each of its finance-related business processes, it needs to consider whether each of the relevant assertions[9] related to financial information has been addressed. Application control objectives and application controls are an important component of management's overall control assessment activities since most finance-related business processes are supported by automated application systems. Guidance on application control objectives and application controls specifically related to satisfying the Sarbanes-Oxley requirements are provided in the ITGI publication *IT Control Objectives for Sarbanes-Oxley, 2nd Edition*.

[9] The American Institute of Certified Public Accountants (AICPA), AU326.03,USA, 2008, *www.aicpa.org/download/members/div/auditstd/AU-00326.PDF* defines assertions with respect to financial information as: *Assertions are representations by management that are embodied in financial statement components. They can be either explicit or implicit and can be classified according to the following broad categories: existence or occurrence, completeness, rights and obligations, valuation or allocation, presentation and disclosure.*

4. DESIGN AND IMPLEMENTATION OF APPLICATION CONTROLS

As noted in chapter 3, application control requirements should be based on the business requirements for control (using COBIT's information criteria) and management's assessment of risk. Priority should be given to managing the risks most likely to impact the business. Implementing control activities comes at a cost. Management must make cost-benefit trade-off decisions when determining which activities to implement to manage the identified risks and achieve the desired control objectives. Management should understand the residual risks and either accept them, or further strengthen control activities to mitigate the risks to an acceptable level.

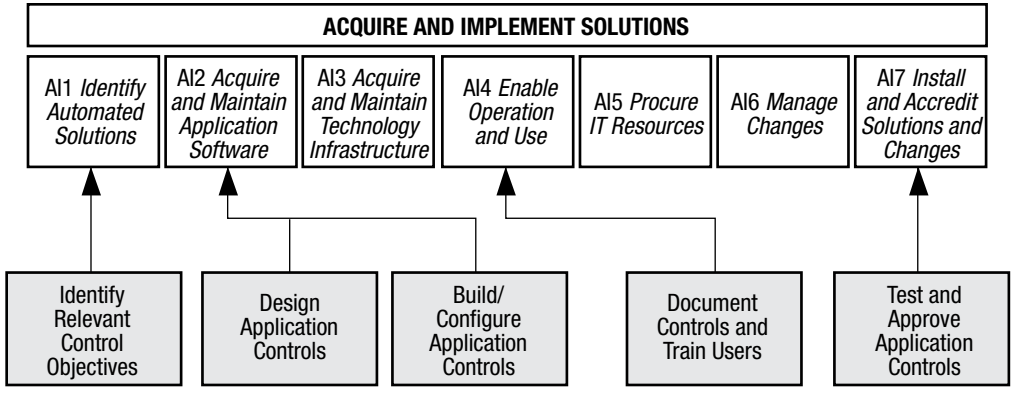
APPLICATION CONTROLS AND THE SYSTEM DEVELOPMENT LIFE CYCLE

A number of SDLC models exist to develop or acquire the application systems to meet the needs of enterprises. The 'waterfall' SDLC approach is perhaps the best known of these models and is based on systematic, sequential phases of application development (or third-party purchase) in which the output of each stage becomes the input for the next. Iterative development approaches such as Agile are also becoming popular. Agile includes multiple repetitions (or iterations) in small, workable pieces of functionality. Each iteration passes through the development cycle, including planning, requirements analysis, design, coding and testing, with a focus on delivering measurable business value early, continually improving it and adding functionality throughout the life cycle of the project. Regardless of the SDLC approach that enterprises follow, integrating the design, development and implementation of application controls is an important step to ensure that the information criteria and management's control objectives are met from the outset of system implementation. Defining application controls should be a discrete step in each SDLC process, along with steps associated with defining other business functionality requirements.

Some enterprises use enterprise data modeling to generate an integrated view of the data produced and consumed across the enterprise. An enterprise data model represents a single integrated definition of data, independent of 'how' the data are collected, stored, processed or accessed. As part of defining its data, an enterprise can include a complete range of business requirements for those data and associated information systems, including the seven COBIT information criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability).

COBIT 4.1 identifies the principal activities undertaken in this area within the Acquire and Implement (AI) domain. **Figure 4** shows the relationship between the AI processes and where application controls are designed, built and tested.

Figure 4—Integrating Application Controls Into Software Development/Acquisition



Appendix A—Mapping Activities Related to Application Controls to CobiT 4.1 Processes and Control Objectives provides a more detailed mapping of the application control design and implementation activities and integration with the CobiT 4.1 Acquire and Implement activities.

Identify Relevant Control Objectives Based on Business Requirements and Risk—AI1

The first step in the development/acquisition life cycle is to understand and define the business requirements, as part of AI1 *Identify automated solutions*, based on the relevant business goals/objectives. Next, an assessment of the business and related information risks associated with the automated solution is performed to define the control requirements that need to be addressed by the proposed solution. A feasibility study is usually undertaken that considers the high-level business risks from both the perspective of what the proposed application is designed to address as well as the business and information risks associated with the development and implementation of the solution. The goal of the feasibility study is to provide a basis for management to evaluate the feasibility of proceeding with the proposed solution.

Key activities at this stage of the SDLC include:

- Identify key stakeholders and assign application control-related roles and responsibilities, including defining application control requirements and designing and approving application control design.
- Perform an assessment of information-related risks and information processing-related risks based on the objectives and functional requirements of the application.
- Identify and document relevant control objectives that would reduce the identified risks to an acceptable level. At this stage of the process, control objectives represent the functional requirements for the application controls, i.e., the application solution needs to include sufficient control activities to achieve the identified control objectives, including any specific regulatory controls objectives.
- For situations involving the selection and acquisition of third-party software, identified control objectives should be included as part of the functional requirements in the request for proposal (RFP).

Designing Application Controls—An Example

Consider an example where an enterprise wishes to develop or purchase an application system to support its accounts payable and vendor payment processes. One of the significant risks inherent in this process is the risk of processing duplicate payments—multiple payments for the same set of goods or services. As part of its risk assessment, management concludes that the significance and likelihood of this risk is sufficient to warrant implementing controls to reduce the risk to an acceptable level. Using application control AC3 as a reference point, management could identify a control requirement of the application to include control activities to ensure that amounts posted to accounts payable represent valid goods or services received and that such amounts are not posted more than once. This example demonstrates how control requirements can be identified and incorporated as part of defining the functional requirements of an application system.

Relevant business management and users should be actively involved in identifying and defining control requirements, based on the assessment of risk, as part of the requirements definition phase. The business process owner has responsibility and accountability for assessing risks inherent to the process and ensuring that sufficient and appropriate control requirements have been defined. In fulfilling this responsibility, the process owner will seek advice from risk and control specialists and knowledgeable users. Appropriate and timely involvement of control specialists will ensure that the application control requirements are identified as required and the business objectives are met.

Additional Considerations for Performing Risk Assessments and Identifying Relevant Control Objectives

Key Message #1

Enterprises regularly consider business and functional requirements as part of application design, but mostly do not explicitly consider 'control' requirements. This can create implementation and operational challenges if necessary controls are not built into the solution from the start and a 'retrofit' of control activities post-implementation is required. In addition to the costs associated with fixing integrity problems, retrofitting controls post-implementation can be very costly. Management should ensure that control requirements are appropriately identified, based on the business risks, and included in functional requirements.

The primary focus of the AI1 *Identify automated solutions* stage is to ensure accurate definition of business requirements. Performing a thorough risk assessment and identifying the relevant control objectives are critical steps that will determine the completeness, effectiveness and efficiency of the resulting application control activities that are designed and built during the next phases. Some additional considerations that are useful at this stage of the process include:

- **Have all key risks been considered in the risk assessment?**—Challenge the completeness of the risks that have been identified, giving consideration to the overall objectives of the business process, the objectives of the application system within that business process, the information criteria and the application control objectives identified in COBIT 4.1 (AC1 through AC6).
- **Has the importance of the identified risk been appropriately prioritised?**—Risks are typically assessed and prioritised based on their likelihood of occurrence and the significance of the impact should the risk occur. Consult with risk and control specialists, including internal and external audit, in completing this assessment. For finance-related risks, consider the materiality of the potential impact. Involve management and the business process owners to ensure that their perspectives on the significance of the risks have been considered.
- **Will the identified control objectives adequately address or mitigate the identified risks?**—It may not be necessary to eliminate the various risks—but to reduce them to an acceptable level. Management needs to be involved in determining whether risks have been reduced to an acceptable level. The process of mapping the application control objectives to information criteria will serve as a checkpoint to validate completeness of identified control objectives. Compensating controls (possibly manual) may complement or replace automated controls. The entire control framework needs to be taken into account in this activity.

Design Application Controls—AI2

The design of application controls should be completed as part of developing and/or acquiring the automated solution. Based on control requirements and control objectives defined in the previous phase, the specific application control activities necessary to achieve those control objectives are developed along with the activities and procedures necessary to accomplish the other business requirements of the system. Often, activities and procedures designed to meet the business requirements will also be activities that satisfy the control requirements. Application controls should not be developed or assessed in a vacuum. To maximise the efficiencies and effectiveness of application controls, it is important to consider and understand the interrelationships among business processes, among the various application systems and the IT processing environments and amongst the various control activities themselves. For example, interrelationships between applications or among processes can create or otherwise impact risk, while existing control activities or activities in other processes may be leveraged to help mitigate risk. Controls should be considered within the context of other interrelated applications and systems and other components of the entire information management infrastructure.

4. Design and Implementation of Application Controls

As with business requirements, the key stage in this activity is performing a thorough design of the necessary activities and procedures to meet both the business requirements as well as the control requirements. Key activities in this stage of the SDLC include:

- **Develop a detailed application specification design (custom developed applications)**—In this activity the business analyst translates the business requirements into a set of detailed design specifications to enable the development team to build the application. For custom-developed applications, the programming/analyst team may define the overall software architecture and decompose that architecture into its constituent parts, such as modules and components. Those modules and components should include the automated application controls necessary to accomplish the identified control requirements.
- **Evaluate vendor solution (purchased software applications)**—In this activity, the vendor responses to the business and control requirements identified in the RFP are evaluated to assess the degree to which the proposed solution meets the enterprise's business and control requirements and the detailed specifications. Gaps between the control requirements and the proposed solution's capabilities need to be evaluated in terms of the degree to which the desired risk mitigation may not be achieved and its impact on the entity. Alternative manual control activities may need to be incorporated into the future-state business process design (see next bullet) to compensate for any significant gaps.
- **Develop re-design future-state business process**—In this activity, the business process team designs the activities and work flows that need to be performed in conjunction with the new application system to meet the business objectives. The design of the future-state business process should include the design of the manual control activities necessary to achieve the identified control requirements.
- **Assess and determine sufficiency of the design of application controls to achieve the identified control objectives**—In this activity, the quality of control activity design is assured as part of the overall application quality assurance (QA) plan, and reviewed and validated by management in terms of whether those activities, if operating effectively, will achieve the identified control objectives and reduce the corresponding risks to an acceptable level.

Attributes of Application Controls

In designing application controls (and determining the sufficiency of their design) a number of attributes should be considered. These attributes are not unique to application controls and are consistent with the considerations in assessing the sufficiency of other business process controls as well. The intent of this publication is not to repeat internal control theory that is widely available in other sources, but rather to focus on how that theory applies to application controls.

Key Message #2

Management can optimise the efficiency and effectiveness of its control design through a balance of various attributes, types and nature of control activities. For example:

- Should a given control activity be a manual activity, automated or some combination of both—a hybrid control? If automated, should the control be designed to be 'configurable' to facilitate changes to business rules over time?
- Is it more cost-effective/efficient to design the control activity to prevent errors from occurring or to design a procedure that would detect any error situations should they arise?
- Are the frequency of the control, the proximity of the control activity to the risk event and the role of the individual performing the activity going to be sufficient to reduce the risk of error conditions to an acceptable level?
- Will the benefits to be realised from reducing a risk outweigh the cost of building, testing and performing the added control activity?

Manual/automated/hybrid/configurable application controls can consist of manual activities, automated activities, or activities that consist of both manual and automated elements:

- **Manual application controls**—Control activities performed without the assistance of applications or automated systems. Examples include supervisory controls; written authorisations, such as a signature on a check; or manual tasks, such as reconciling purchase orders to goods receipt statements. Manual controls are subject to the inherent risk of human error and, as a result, are often considered less reliable than automated controls.
- **Automated application controls**—Controls that have been programmed and embedded within an application. Examples include input edit checks that validate order quantities and check digits that validate the correctness of bank account numbers.
- **Hybrid or computer-dependent application controls**—Controls that consist of a combination of manual and automated activities, all of which must operate for the control to be effective. For example, the order fulfillment process might include a control whereby the shipping manager reviews a report of unshipped orders. For this control to be effective, both the automated activity (generation of a complete and accurate unshipped orders report) and the manual activity (review and follow-up by management) are necessary for the control activity to be effective. Care must be taken to ensure that hybrid or computer-dependent controls are not inappropriately identified as being manual controls. Because of the need for all parts of a hybrid control to be effective, there is a significant risk of key elements of the true control not being considered as part of the overall design effectiveness if such controls are incorrectly identified. For example, if the review of the unshipped orders report in the previous example was incorrectly identified as a manual control, there is a risk that the design of controls to ensure the completeness and accuracy of the unshipped orders report may be overlooked.
- **Configurable controls**—Typically, automated controls that are based on and, therefore, dependent on the configuration of parameters within the application system. For example, a control in automated purchasing systems that allow orders only up to preconfigured authorisation limits is dependent on controls over changes to those configurable authorisation limits. Most of the current commercial and in-house developed application systems are heavily dependent on the configuration of various parameter tables. In these cases, it may be appropriate to consider the design of controls over the configuration tables as a separate element of the control design.

Preventive/detective application controls are defined as:

- **Preventive application controls**—These controls, as the name implies, prevent an error from occurring (based on predefined business logic or business rules) and are typically executed at the transaction level, before an action is performed or confirmed. An example is an input validation control in a human resources (HR) application, which blocks the user when entering a new employee without specifying a valid bank account number for salary payment.
- **Detective application controls**—These controls are designed to detect errors based on predefined logic or business rules. They are usually executed after an action has taken place and often cover a group of transactions. An example is an exception report that is periodically generated by the purchasing application and lists critical changes that have been performed to the supplier master file (e.g., changes to supplier bank account numbers).

Preventive controls are often considered more efficient and effective, especially where detecting and correcting an error can result in significant incremental costs. Preventive controls may also be easier to automate than detective controls. Detective controls are often manual activities. Effective control design should consider a reasonable balance of preventive and detective controls.

Control characteristics include:

- **Frequency of the control**—This control characteristic is related to a measurement of how frequently the control is applied and needs to be considered in the context of the underlying risk. Reviewing payroll expenditures annually may not be an effective control to detect potential errors in payroll calculations or invalid payments to terminated employees. In this case, the control may be applied too infrequently to be effective since an annual review may not be able to detect a material misstatement in the payroll amounts. The same activity performed more frequently, such as during each payroll cycle, may

provide a higher degree of effectiveness. Similarly, a daily reconciliation of bank balances may be so labor-intensive that it increases the risk of human error in the activity and, therefore, may be less effective, whereas a monthly review may be more effective and reliable (automation of the control activity may also be a possible solution to controls that should be applied frequently and have a high risk of human error).

- **Proximity of the control activity to the risk event**—This characteristic or attribute considers where in the process the control activity is applied relative to where the underlying risk event is most likely to occur. For example, if the risk of incomplete or inaccurate data input is a concern, a control activity that is applied as close as possible to the data input event may be more effective and efficient than a control activity applied later in the processing cycle. Management needs to balance the cost that may be associated with applying the control with the benefit that may be achieved through reductions in re-work and cycle times. Additional guidance on this area can be found in appendix B—Additional Guidance on Types of Application Controls.
- **Who performs the control activity**—This characteristic is primarily relevant to manual controls and considers roles, responsibilities and who is accountable for control-related decisions and approvals. This attribute is also used to consider whether responsibilities for controls have been appropriately segregated from other potentially incompatible responsibilities. While equally applicable to all types of applications, additional guidance for financial applications is provided in appendix C—Segregation of Duties in Significant Accounting Applications, which has been extracted from the ITGI publication IT Control Objectives for Sarbanes-Oxley, 2nd Edition section related to segregation of duties.

For automated application controls, it can be useful to use the 'who performs' attribute to document the specific application/module within which the automated control resides. This will facilitate linking to the effectiveness of the underlying IT processing environment in which the application operates. The relationship between automated application controls and IT general controls and the need to establish a definitive linkage between the automated application control and the IT processing environment is discussed further in chapters 6: Relation and Dependencies of Application Controls With IT General Controls and 7: Application Controls Assurance.

In appendix D—Control Practices, Value and Risk Drivers for Achieving Application Control Objectives, guidance is provided on control practices that may be relevant to application controls from the ITGI publication *CobiT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*.[10] This information can be used by management, business analysts, and risk and control specialists as guidance for designing application control activities.

Build/Configure Application Controls—AI2

For custom-developed applications, after the detailed design has been completed and approved, the system developers and programmers are responsible for building the application code to accomplish the design requirements, including designed automated application controls. For purchased applications, this stage typically involves the application vendor and application specialists installing and configuring the application consistent with the detailed design requirements, including requirements for parameters for application controls in general and configurable controls in particular. In many situations involving purchased applications, it is necessary to custom-develop certain functional capability (such as data interfaces with legacy application systems).

Key activities performed in the build/configure application controls phase include:

- Develop program code and debug the automated application controls within custom-developed applications (along with coding and debugging of other software functionality).
- Install and configure applications, including configurable controls.

[10] IT Governance Institute, *CobiT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*, USA, 2007

Document Controls and Train Users—AI4

To enable the operation and use of the application and related application controls, manual or automated, effective user and operational manuals and training materials need to be developed or updated to reflect the current application environment, including application controls. Key activities include:

- Develop/update application control documentation to reflect control activities that have been designed to achieve the relevant control objectives.
- Develop/update user training materials and provide training as required to affected staff.
- For new employees, provide full training on the application and relevant application controls.

Documenting the activities that have been designed to achieve management's control objectives and incorporating that information into user training is an important step to ensure that there is clarity of roles and responsibilities associated with the ongoing operational effectiveness of the application and control activities.

Application controls are part of the overall business process controls and are an integral part of, and need to be integrated with, the business process documentation.

Test and Approve Application Controls—AI7

Testing is an essential part of the software development and implementation process that verifies and validates that the system, including application controls, performs according to the approved requirements and acceptance criteria. Testing also determines whether the units being tested operate without adverse effects on other components of the system. Testing strategies, methods and approaches are varied and often depend on the nature of the application system being implemented and the underlying business process. Irrespective of the testing strategies selected, testing of application controls as part of the overall test plan is an essential component to ensure that the automated and manual application controls function as intended.

Key Message #3

Because testing validates whether or not the designed control activities operate as they were intended, it is essential that the systems accreditation activities include testing of these application control activities.

Having a clearly documented trail of testing automated application controls and the automated components of hybrid and configurable controls may also provide the necessary evidence to demonstrate the effective operation of these controls.

Having a clearly documented trail of testing/validation of manual controls and the manual activities associated with hybrid controls can reinforce their viability and user understanding of the activities.

Key activities regarding application controls in this phase include:

- Develop, document and approve the test plan, including plans for testing manual and automated components of the application controls. Test plans should cover the functional and technical requirements and test acceptance criteria for automated and manual application controls and identify the testing phases appropriate for the respective controls. Examples of such testing phases include, but are not limited to, unit test, system test (recovery, security, stress/volume and performance), integration test, regression test and acceptance testing. User acceptance testing (UAT) is particularly important and enables the user to validate the operation of automated controls and enables testing of manual control activities.
- Conduct application control testing in accordance with the test plan. Involve business process owners and end users in the test team.
- Identify, log, prioritise and resolve errors and issues identified during testing.

- Document and interpret the final test results, including unresolved issues, in a form that is understandable to business process owners. The testing process and the review and evaluation of results should be appropriately documented. An audit trail of test results should be maintained.
- Approve test results. The final acceptance evaluation should be measured against the success criteria set out in the testing plan and should also consider the risks associated with unresolved issues and, if necessary, the need to implement alternative process activities or compensating controls.
- Approve the design and implementation of application controls. Before approving the implementation of automated solutions, business management needs to be satisfied that appropriate application controls have been designed and built, are working as intended, and are planned for implementation relative to the assessment of risk and identified application control objectives.

Key Message #4

In approving the design and implementation of application controls, management needs to consider the relative efficiency and effectiveness associated with various control design choices and be satisfied that the controls designed are cost-effective and achieve the control objectives, and the relevant information criteria are satisfied.

Appendix E—Tools for Designing and Implementing Application Controls provides some example templates that may be useful in the design and implementation of application controls. COBIT Online can be leveraged to define application control requirements and to assist in identifying relevant application control objectives. In appendix E, the section on Defining Application Control Requirements/Identifying Relevant Application Control Objectives provides a screen capture of the COBIT Online tool for identifying application control objectives. Also in appendix E, the section on Template for Design of Application Controls provides a template that can be used to identify the application control activities and to map those activities against the relevant application control objectives. The template provides for documenting the various attributes associated with the control activities and confirming management's conclusion on the effectiveness of the control design to achieve the corresponding objective.

Application Controls and Existing Applications

While the concepts discussed previously have been presented in the context of a new application being acquired/developed, the concepts are equally relevant for existing applications. For existing applications it is important for management to:

- Identifies relevant application control objectives based on the business objectives and related risks (covered in the previous section Identify Relevant Control Objectives Based on Business Requirements and Risk—AI1).
- Assess and conclude on the sufficiency of the design of the application controls to achieve the identified control objectives (covered in the previous section Design Application Controls—AI2).
- Ensure that the application controls are appropriately documented and users have the appropriate training and skills to perform the control activities effectively (covered in the previous section Document Controls and Train Users—AI4).

Key Message #5

Assessing risks, identifying relevant control objectives and determining the sufficiency of design of application controls are as relevant to existing applications as they are to new applications being acquired/developed and implemented.

Completing these activities for existing applications provides the necessary foundation to enable management to fulfil its role and responsibility with respect to the ongoing operation and maintenance of the application controls, which is discussed in chapter 5: Operation and Maintenance of Application Controls.

THE CASE FOR AUTOMATING APPLICATION CONTROLS

In most cases, the automation of certain controls reduces the risks associated with manual controls and brings efficiency gains. For example, an enterprise can implement an automated three-way matching control among purchase orders, goods receipt notes and supplier invoices. Previously, manual controls would include a check that the quantity received was in line with the quantity ordered and the subsequent invoice reflected the quantity received at the agreed price. Automating the three-way matching activity brings considerable time savings to the warehouse and accounting personnel. It also strengthens the controls over ordering and receiving functions. In an ERP environment, the control automation goes one step further. Once documents such as goods receipt notes and invoices are checked and validated by the application, the corresponding accounting entries are also systematically generated and posted to the general ledger. These automated application controls (three-way matching, systematic generation of accounting entries, etc.) contribute to the integrity of logistic and financial information within this process.

Key Message #6

Automated application controls should be used where possible to provide a more cost-effective and sustainable system of internal controls, but they require effective IT general controls.

Automated application controls are in general more reliable than manual controls since they significantly reduce the risk of human error or manipulation of information. While automated, these controls still require monitoring to identify and resolve exceptions on a timely basis. When automated controls are well configured and followed up, management should be comfortable that exceptions from normal information processing will rarely occur. In addition, in today's fast-moving 24/7 environment when entire business flows are automated, inserting manual control activities can introduce a significant bottleneck to processing throughput. Examples of such highly automated environments include retail and high-volume consumer goods, credit card processing, telecommunications and airline companies. In these cases, manual intervention occurs mainly on standing data (for example pricing tables), and automated controls are relied upon heavily for timely, accurate processing.

In addition to throughput and its impact on process performance, manual activities can be very expensive. Automating activities (including control activities) can achieve significant savings in labor costs. The cost associated with manual control activities grows exponentially with the number of activities and the size and complexity of the business process.

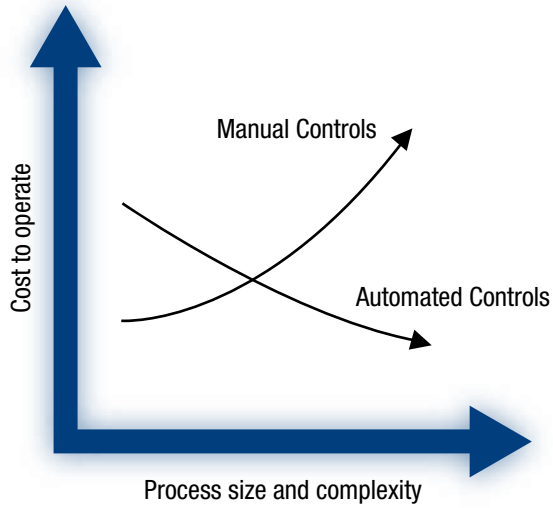
Figure 5 depicts the costs of automated vs. manual controls and makes a compelling case for automating application controls whenever possible.

The ongoing reliability and effectiveness of automated application controls can depend on other, related application control activities as well as on the effectiveness of IT general controls. For example, a prerequisite for the effectiveness of the automated three-way matching control is that:

- Only authorised users can change the application system parameter that enables that functionality (typically an IT general control managed by DS5 *Ensure system security*).
- Only authorised users, such as business controllers have access to change tolerances among purchase orders, goods receipts notes and supplier invoices, in accordance with business needs.
- These changes are appropriately documented and approved.
- There are effective controls over changing the application functionality associated with three-way matching (typically an IT general control managed by AI6 *Manage changes*).

The relationship between automated application controls and IT general controls is discussed more fully in chapter 6: Relation and Dependencies of Application Controls With IT General Controls.

Figure 5—The Case for Automating Control Activities



ROLES AND RESPONSIBILITIES FOR DESIGNING AND IMPLEMENTING APPLICATION CONTROLS

The design, development, testing and implementation of application controls are integral parts of the SDLC process and should be implemented as components of these processes.

The following section includes a Responsible, Accountable, Consulted and Informed (RACI) chart in **figure 6** based on the detailed activities outlined in the previous section; however, in summary, business management is responsible for:

- Performing risk assessment
- Correctly defining and confirming application control requirements
- Participating throughout the SDLC to ensure that control requirements are being met and to ensure that appropriate testing of application controls is performed
- Being satisfied that the application systems, including the application controls function, is in accordance with the requirements
- Ensuring that users are adequately trained in the use of the application system, including automated and manual application control activities
- Monitoring the use of the automated systems and the operating effectiveness of the control activities (additional guidance is provided in chapter 5: Operation and Maintenance of Application Controls)
- Maintaining business process documentation, including application controls

IT management is responsible for:

- Collaborating with business users to optimise application controls, including providing insight and recommendations regarding opportunities to automate application controls and whether some control activities may be more effective if performed as part of IT general controls (e.g., it may be more efficient and effective to design and build user security provisioning and management into IT general controls rather than within each specific application solution)

- Designing, building, and implementing business functionality and automated application controls as defined by the business users
- Implementing IT management processes and controls to maintain the integrity of information systems and information processing
- Establishing IT management processes and controls to maintain the availability and timeliness of information processing in accordance with business requirements
- Establishing IT management processes and controls to maintain and protect the confidentiality of information systems and data in accordance with business requirements
- Establishing IT management processes and controls to operate the infrastructure supporting the application systems effectively and reliably

Key Message #7

Responsibility for design and implementation of application controls is shared. Business management is accountable for ensuring that application control requirements have been appropriately designed and implemented to meet the business objectives. IT management is accountable for developing application controls in accordance with business requirements.

In **figure 6** the roles and responsibility matrix is set out for the key activities associated with the risk assessment, identification of relevant control objectives, and the design and implementation of application controls, as discussed previously.

MANAGE RISKS RELATED TO THE DESIGN AND IMPLEMENTATION OF APPLICATION CONTROLS

There are many potential risks that can occur when designing and developing application controls. Some of these risks include:

- **Incomplete or inappropriately designed application controls**—Since application controls may appear to be IT-related, management may mistakenly believe that it is solely IT management's responsibility to design and implement the application controls. Without the involvement and support from the business side, IT management may not fully understand the business processes or may misunderstand the business expectations. As a result, the business requirements that should be addressed by the application controls may not be fully captured and addressed. In such a case, even if they were implemented, they may not fully meet the business needs and relevant control objectives.
- **Designed controls may not be as efficient as possible**—Opportunities to automate control activities may not be leveraged, potentially leading to either costly manual procedures to compensate and/or system enhancement requests to retrofit control automation subsequent to implementation.

To mitigate the risks and ensure effective and efficient design, implementation and operation of application controls, a common risk and control framework should be adopted. This framework should include formalised processes and procedures as well as clear definition of roles and responsibilities for involvement of business management, users and other stakeholders, as outlined in the RACI chart in **figure 6**. Adopting COBIT as a framework and formalising processes and accountabilities help to ensure use of a 'common language' and reduce the risk of misunderstandings and misinterpretations.

Proactive involvement and assistance from internal control subject matter experts (SMEs), such as internal/external audit and the compliance team, are other important elements to manage and mitigate application controls-related risks. These stakeholders should be involved throughout the design and implementation processes to provide timely advice. For example, during the requirements definition phase, the SME could provide insights into the completeness of control objectives/requirements that were identified by management. During the design phase, the SME could review the application controls and provide feedback on the appropriateness of the design. During the testing phase, the SME could review the test plan for evidence of user participation and examine the security testing and user acceptance testing (UAT) for user sign-off of test results.

4. Design and Implementation of Application Controls

Appendix F—Common Issues and Challenges With Application Controls provides additional guidance on some of the common risks and challenges associated with application control design and implementation for various types of applications, and related potential control practices to reduce these risks and challenges.

Figure 6—Responsibility for Application Control Design and Implementation: RACI Chart

Activities		Stakeholders							
		Business Executives	Business Process Owners/Application Owners	Business Analysts	End Users	Project Managers	Programmers/IT Specialists/IT Application Owners	Risk and Control (and/or Security) Specialists	Internal and External Auditors
Identify Relevant Control Objectives	Identify key stakeholders and assig application control-related roles and responsibilities	A	R	C	C	C		C	I
	Perform an assessment of information-related risk and information processing-related risks.	C	A	R	C	I		R	C
	Identify and document relevant control objectives.	C	A	R	C	I		R	C
	For third-party software, include control requirements in the RFP.	C	A	R	C	I		R	I
Design/Build/Configure Application Controls	Develop a detailed application specification design (including automated application controls).	C	A	R	C	R	C	C	C
	Evaluate vendor solution (including fit with control requirements.		A	R	C	R	C	R	C
	Develop future state business process design (including design of manual application controls to meet control objectives).		A	R	C	R	C	R	C
	Assess and determine sufficiency of the design of application controls.	A	R	C	C	R	C	C	C
	Develop program code and debug automated application controls as part of software development.		C	C	C	A/R	R	C	
	Install and configure commercial applications, including configurable controls.		C	R	C	A/R	R	C	I
Document Controls and Train Users	Develop/update application control documentation.		A	R	C	R	C	C	C
	Develop/update user training materials and provide training as required to affected staff.		A	R	R	R	C	C	I
	For new employees, provide full training on the application and relevant application controls.		A		R				
Test and Approve Application Controls	Develop, document and approve the test plan.		A	R	C	R	R	I	I
	Conduct application control testing in accordane with the test plan.		R	C	C	A/R	R	R	C
	Identify, log priorities and resolve errors and issues identified during testing.		R	C	C	A	R	R	I
	Document and interpret the final test results, including unresolved issues.		A	R	C	R	R	C	
	Approve test results.	A	R	C	C	R	C	C	I
	Approve design and implementation of application controls.	A	R	C	C	R	C	C	I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

APPLICATION CONTROL DESIGN AND IMPLEMENTATION GOALS AND METRICS

In **figure 7**, a number of key performance indicators/metrics are identified that may be useful to measure the process activities and outcomes associated with designing and implementing application controls. This table also identifies a linkage to corresponding IT process goals identified in COBIT.

Figure 7—Application Control Design and Implementation Performance Metrics

	Application Control Metrics	Relevant COBIT 4.1 IT/Process Goal	
Application Control Design and Implementation	Percent of projects where roles and responsibilities for application control design and implementation are defined and documented	PO10	Make timely project managmenet decisions at critical milestones.
	Percent of projects where application control requirements/ objectives are documented and signed off by the business process owner(s)	PO10	Make timely project management decisions at critical milestones.
	Perent of software acquisition projects where requests for proposals (RFPs) for applications specifically include application control requirements	AI1, DS5	Consider security and control requirements early.
	Percent of applications with application control design specifiations documented and business process owner determination of design effectiveness documented and signed off	AI1	Define how business functional and control requirements are translated into effective and efficient automated solutions.
	Ratio of application controls by type (manual, automated, hybrid, configurable) and by nature (preventive, detective)	AI7	Define how business functional and control requirements are translated into effective and efficient automated solutions.
	Number of application control design deficiencies identified by internal/external auditors	AI7	Reduce solution defects and rework.
	Percent of applications with test plans and test results documented for application controls testing	AI7	Ensure that new business applications and changes to existing applications are free from errors.
	Tracking number of application control testing defects and issues identified, resolved and outstanding	AI7	Ensure that new business applications and changes to existing applications are free from errors.
	Percent of application controls that have satisfied design specifications and acceptance critieria	AI7	Reduce solution defects and rework.
	Percent of projects with application control topics included in user training curriculum	AI4	Provide effective user manuals and training materials for applications.
	Number of work-arounds developed to facilitiate go-forward approvals	AI7	Reduce solution defects and rework.
	Percent of applications implemented with sign-off by business executive/business process owner	AI7	Verify and confirm that applications are fit for the intended purpose.

5. Operation and Maintenance of Application Controls

In this chapter, application controls are addressed within the next logical stage of the life cycle of automated solutions—operation, use and maintenance of the automated solutions as part of business operations.

APPLICATION CONTROL OPERATION AND MAINTENANCE

Management's responsibility and accountability for ensuring internal controls are in place and operating effectively need to be widely accepted. Even when certain functions or processes are outsourced, management retains the accountability for the effectiveness of internal controls of those functions/processes. For example, COSO identifies internal control as an integral part of enterprise risk management (ERM) and places ultimate responsibility with the chief executive officer (CEO), while others within the enterprise may have responsibilities for executing, providing support, promoting compliance, and managing risks within their sphere of influence.[11] Ongoing operation of application controls consists of the following three major types of activities:

- **Operate the automated solution**—This is typically a responsibility of IT and addressed by several CobiT 4.1 processes in the Deliver and Support (DS) domain, but principally DS13 *Manage operations*.
- **Monitor application control effectiveness**—The business process owner is typically accountable for the effective operation of the business process, including performing relevant manual control activities and monitoring automated application controls and responding as required to ensure overall effectiveness. As such, business management needs to monitor the effective operation of the application controls. In addition, this is addressed in the CobiT 4.1 Monitor and Evaluate (ME) domain, principally ME2 *Monitor and evaluate internal control*. Management may wish to consider use of continuous controls monitoring (discussed later in this chapter) as a tool to assist in monitoring the effectiveness of application controls.
- **Manage changes to application controls**—Changes to business processes and manual application controls are typically the responsibility of the business process owner. Changes to automated application controls are shared responsibilities between the business (identification of change requirements, testing and approval of changes to be implemented) and IT (development and implementation of requested changes) and is addressed in CobiT 4.1 by AI6 *Manage changes* and AI7 *Install and accredit solutions and changes*.

Appendix A—Mapping Activities Related to Application Controls to CobiT 4.1 Processes and Control Objectives provides a more detailed mapping of the application control operation and maintenance activities and integration with the CobiT 4.1 Acquire and Implement (AI) activities.

Operate the Automated Solution

Effective and reliable operation of the automated solution is an essential element to ensure the ongoing effectiveness of the automated application controls as well as the manual activities that depend on information generated by the solution. Otherwise the integrity and reliability of the automated controls and the underlying data can be questioned.

Responsibility and accountability for ensuring effective and reliable operation of automated solutions typically resides with the chief information officer (CIO) and the IT group. Guidance, objectives, metrics and measures related to the effective operation of automated solutions can be found in CobiT 4.1 (principally DS13 *Manage operations*). The DS13 control objectives provide guidance relative to the complete and accurate processing of automated solutions based on effective management of data processing procedures and diligent maintenance of hardware.

[11] The Committee of Sponsoring Organisations of the Treadway Commission, *Enterprise Risk Management—Integrated Framework, Executive Summary*, USA, 2004, p. 6

Monitor Application Control Effectiveness

Application control activities are a subset of the overall activities for a given business process and should be included in management's overall business process monitoring activities. Management's monitoring should include both manual and automated controls and the integrated operation of these to ensure completeness and accuracy of business processing.

Key Message #8

Ongoing monitoring of application controls is important and necessary to ensure their continuing effectiveness.
Key elements for management to consider include:
- Periodically re-assessing application control effectiveness
- Monitoring effective operation of manual control activities including the manual component of hybrid controls
- Monitoring automated control activities (including the automated component of hybrid controls) to ensure that they continue to operate as intended
- Monitoring effective operation of application controls delegated and performed by other parties
- Monitoring business process and application control key performance indicators (KPIs) that may indicate a control failure

Management needs to ensure careful and diligent performance of manual procedures, monitoring of the output from the automated controls, and review of actions taken on system-generated exception reports. In today's complex systems there is the danger that business users may develop a tendency to assume the 'system works' and overlook key risk indicators (KRIs) that would otherwise point to possible system and control issues. It is important for management to operate control activities as well as develop the processes to react and respond appropriately to the control issues as they arise. In some situations, to maximise their efficiency and effectiveness, some application controls may be executed by individuals outside of the business process area, including, for example:
- Controls over batch processing and data transfers between application systems that may be performed as part of the IT general controls
- Application control activities that may be performed by third-party service enterprises

In these situations, while responsibility for execution of the control may be delegated, business management retains accountability for its effective operation. Business management needs to ensure that it has appropriate visibility to control activities of this nature and develop the processes to enable monitoring of its ongoing effectiveness. This may include the following activities, for example:
- Supervise and oversee performance of key manual control activities.
- Supervise and oversee the identification, prioritisation, escalation and resolution of control exceptions, failures and processing errors, based on business needs, risk profile, and regulatory and compliance requirements.
- Monitor ongoing effectiveness of application controls at third-party service providers through periodic vendor management meetings and review of service auditor reports on internal control effectiveness.
- Monitor incident and problem management reporting related to application controls that may operate at the IT general control level.
- Monitor process metrics and key performance indicators defined as part of the process and control design activities noted in chapter 4: Design and Implementation of Application Controls.
- Perform periodic assessments of control effectiveness considering approaches such as internal self-assessments, internal audit reviews, and external or third-party reviews.
- Identify, initiate, track and implement remedial actions arising from control assessments and reporting.

Continuous Controls Monitoring (CCM)

While inherently more reliable than manual processing, management should not assume that automated business processes and the corresponding automated application controls are fault-free. Internal controls, including automated controls, do not **eliminate** the risk of undetected errors. Many internal controls have some dependency on other activities (including the IT general controls upon which the automated controls depend). As such, there is always a risk that transactions are incorrectly processed and not detected by the automated application controls. These systemic errors can produce significant misstatements and affect the integrity of data.

The Institute of Internal Auditors (IIA) Research Foundation summarises the challenge as:

> *The … challenge will be to develop an effective information, communication, and monitoring system that will identify when the controls that are built into the system are not working within their prescribed tolerances, and then signal evaluation activities and monitor correction.*[12]

Key Message #9

Continuous controls monitoring (CCM) can be an effective mechanism for management to monitor the ongoing effectiveness of its internal control activities.

Continuous controls monitoring is emerging as a concept for management to enable effective monitoring of key control activities. Continuous controls monitoring can be summarised as:

> *The use of a combination of monitoring software and defined business rules to detect, prevent and monitor the operating effectiveness of internal controls.*[13]

There have been many recent advances in tools and techniques to support continuous controls monitoring. These tools can be used to detect changes in configurable controls, and analyse data and identify transaction exceptions that do not meet business rules, policies or other criteria and may be indicative of a control failure. Emerging tools are designed both to operate with specific ERP application systems and to be application-agnostic, focusing primarily on analysis of the underlying data. Many of the latter category of tools have evolved from their prior history as auditor tools for data analysis to become tools for use by business management.

[12] IIA Research Foundation, *Sarbanes-Oxley Section 404 Work*, *Looking at the Benefits*, USA, 2005
[13] ISACA Houston Chapter, Continuous Control Monitoring Presentation, USA, 2006, *http://isacahouston.org/documents/ISACACCMPresentation_000.pdf*

Continuous Controls Monitoring—An Example

Major application vendors are increasingly incorporating CCM capabilities as a fundamental component of their ERP systems. For example, governance, risk and compliance (GRC) solutions are designed to automate end-to-end GRC processes, including corporate governance and oversight, risk management, and compliance management and reporting. GRC solutions for monitoring automated application controls include:

- **GRC access control**—Identifies and prevents access and authorisation risks in cross-enterprise IT systems to prevent fraud and reduce the cost of continuous compliance and control
- **GRC process control**—Optimises business operations and ensures compliance by centrally monitoring key controls for business processes and cross-enterprise IT systems

A GRC process control module can monitor whether automated controls, such as three-way matching, are enabled and the associated tolerances. GRC access control functionalities can monitor user access to change application configuration parameters, such as three-way matching tolerances.

Maintaining Evidence of Operating Effectiveness

In some circumstances[14] management may be required to maintain evidence supporting the effective operation of key controls and the timely disclosure of events, including control failures, which may have a material impact on financial reporting. Even if an enterprise is not required to maintain such evidence of the effective operation of key controls, monitoring the ongoing effectiveness of its control activities is a prudent business practice that helps to ensure that the enterprise achieves its overall business objectives.

In chapter 7: Application Controls Assurance, there is additional information relative to management's responsibilities for maintaining evidence to support the effective operation of key controls.

Manage Changes to Application Controls

Business changes are inevitable as enterprises adapt to changing business and market conditions. These business and marketplace changes will drive the need for change in business processes and in the underlying applications that enable the processes. The need for change can also be driven by continuous improvement initiatives such as improvements to reduce process throughput time, improve process efficiencies, reduce costs and strengthen/improve internal controls. As part of defining business process changes and application changes to respond to changing business requirements, management should carefully assess the impact of those business changes on existing application controls. These controls should be adjusted accordingly, considering opportunities to strengthen and optimise controls to improve the overall effectiveness and efficiency of the process. Changes to business processes can be a common source of control weaknesses as controls are not updated or adjusted to reflect the new situations.

Changes to application controls should be managed following the same standard process for managing other changes to the business process and the underlying business applications. Responsibility and accountability for managing these changes, including application controls are shared responsibilities. Management is responsible for identifying and defining change requirements. Management also retains responsibility for designing and implementing business process changes, while IT is typically responsible for designing, building and implementing the changes requested in automated solutions.

[14] Such as enterprises required to comply with Sarbanes-Oxley or similar legislation

Key activities include:
- Identify the need for change in business processes and underlying automated solutions and define business requirements.
- Assess the impact of changes on application controls and define necessary control requirements and changes.
- Design, build, test and implement changes to automated solutions, including automated application controls, based on defined and agreed business requirements.
- Design, build and implement business process changes, including manual application control procedures based on defined business requirements and changes to automated solutions.
- Manage changes to business information tables, standing data and other 'user-managed' configuration tables.
- Manage changes to business rules and other 'IT-managed' configuration tables (see also CobiT control objective AI2.5).

Responsibility for designing and implementing changes to automated solutions, based on business requirements, follows the same requirements as outlined in chapter 4: Design and Implementation of Application Controls. Guidance, objectives, metrics and measures related specifically to the effective management and implementation of changes can be found in CobiT 4.1 control processes AI6 and AI7:
- AI6 *Manage changes* satisfies the business requirement for IT to respond to business requirements in alignment with the business strategy, while reducing solution and service delivery defects and rework.
- AI7 *Install and accredit solutions and changes* satisfies the business requirement for IT to implement new or changed systems that work without major problems after installation.

The objectives of these CobiT 4.1 processes need to be achieved to ensure that the application controls continue to meet the business requirements and the relevant application control objectives.

Manage Configurable Parameters of Automated Application Controls

In chapter 4, configurable controls were identified as automated application controls that are dependent on the configuration of parameters within the application system. Common examples include business information tables, standing data such as authorisation limits and rate tables, and parameters that provide adoption of alternative business rules such as requiring three-way vs. two-way matching in purchasing inventory applications.

The effective and reliable operation of configurable controls depends on the integrity and accuracy of the underlying parameters. Errors in the parameter tables will have a direct impact on the accuracy and reliability of the associated information and information processing. For example, errors in the discount types will have a direct impact on the accuracy of sales invoice amount. The initial integrity and accuracy of these configuration tables is typically addressed as part of the system testing and implementation processes as outlined in chapter 4. However, it is equally important for sufficient and appropriate controls to be in place to manage changes to these configuration tables over time.

Common techniques for controlling changes to configuration tables include:
- Restricting to authorised individuals access to system functionality related to change configuration tables
- Segregating responsibility for changing configuration tables from responsibilities for processing related transactions. Some examples of this include:
  - IT (such as an application support group) responsibility for managing changes to tables that impact business processing rules (such as configuring the purchasing/inventory system to require three-way matching prior to payment) rather than the business process staff handling this responsibility. These changes should be subject to change management processes and approvals.
  - HR responsibility for managing changes to employee benefits, pay rate and income tax tables rather than the payroll department handling this responsibility

- Subjecting certain classes of parameter changes, based on management's assessment of the risks, to formal change management processes—this can be particularly useful for tables that reflect defined business rules and/or otherwise change the behavior of the application system and are not expected to change frequently. The change management process can enable management to formalise the change in business requirements, the correction needed to meet the new business requirements, and to permit these changes to be tested and authorised prior to implementation. COBIT 4.1 control objective AI2.5 provides additional guidance for managing these types of application configuration changes.
- Management approving parameter table changes
- Management reviewing system-generated change activity reports
- Maintaining system-generated logs of changes to parameter tables

ROLES AND RESPONSIBILITIES FOR OPERATION AND MAINTENANCE OF APPLICATION CONTROLS

Roles and responsibilities for key activities associated with managing the operation and maintenance of application controls are set out in **figure 8**.

Key Message #10

Responsibility and accountability for operating and maintaining application controls are shared between business management and IT. Business management is accountable for monitoring the ongoing effectiveness of the application controls and for identifying and defining requirements for changes to application controls. IT is accountable for providing a reliable environment for operating the application and related automated application controls and for developing/delivering changes based on user requirements.

MANAGE RISKS RELATED TO THE OPERATION AND MAINTENANCE OF APPLICATION CONTROLS

Some of the key risks relative to the operation and maintenance of application controls include:

- Failure to perform consistently and on a timely basis manual activities associated with automated application controls, including hybrid and configurable controls (e.g., the manual review and follow-up of system-generated activity logs). There is a risk that individuals may not fully understand the importance of the manual activities and may jeopardise the overall effectiveness of the control activity.
- Complacency with automated application controls and over-developed 'trust' that the automated application controls continue to operate effectively. Like any other internal control, automated application controls are not fool-proof and are subject to inherent risk.
- Unintended impact on application controls resulting from changes. Changes to systems or business processes can have unintended or unanticipated consequences that may impair the ongoing effectiveness of application control activities.

To mitigate the risks and ensure effective and efficient operation and maintenance of application controls, management needs to provide appropriate oversight and supervision of day-to-day operating activities, and implement a reasonable degree of higher-level monitoring of ongoing control effectiveness, depending on the risks and impact associated with potential control failures.

Involvement and assistance from internal control subject matter experts, such as internal/external audit and the compliance team, are important elements for managing and mitigating application controls operation and maintenance risks. These stakeholders should be involved to periodically provide an objective assessment of the operating effectiveness of the control activities.

Appendix F—Common Issues and Challenges With Application Controls provides additional guidance on control operation and maintenance for various types of applications, and related potential control practices to reduce these risks and challenges.

Figure 8—Responsibility for Application Control Operation and Maintenance: RACI Chart

Activities		Stakeholders								
		Business Executives	Business Process Owners	Business Analysts	End Users	Project Managers	Systems Operators	Programmers/Application Support	Risk and Control (and/or Security) Specialists	Internal and External Auditors
Operate the Automated Solution	Enable effective and reliable operation of automated solutions (see also CobiT 4.1 control objective DS13).	I	C/I		I		R/A			C/I
Monitor Application Control Effectiveness	Supervise performance of key manual control activities.		A/R		R					C
	Supervise the identification, prioritisation, escalation and resolution of control exceptions, failures and processing errors.	I	A/R		R					C
	Monitor ongoing effectiveness of application controls at third-party service providers.									
	Monitor process metrics and key performance indicators.	I	A/R		R					C
	Perform periodic assessments of control effectiveness.	I	A/R		R					C
Manage Changes to Application Controls	Identify need for change in business processes and underlying automated solutions and define business requirements.	C	A/R	R	C	I				I
	Assess impact of changes on application controls and define necessary control requirements and changes.		A/R	R	R	I		C	C	C
	Design, build, test and implement changes to automated solutions, including automated application controls, based on defined business requirements.	See CobiT 4.1 processes AI6 and AI7								
	Design, build and implement business process changes, including manual application control procedures based on defined business requirements.	C	A/R	R	R	R			C	C
	Manage changes to business information tables, standing data and 'user managed' configuration tables.		A/R		R					C
	Manage changes to business rules and other 'IT managed' configuration tables (see also CobiT control objective AI2.5).	C	A				R			C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

APPLICATION CONTROL OPERATION AND MAINTENANCE GOALS AND METRICS

In **figure 9** a number of key performance indicators/metrics are identified that may be useful to measure the process activities and outcomes associated with the key activities involved with operating and maintaining application controls. This table also identifies a linkage to corresponding IT process goals identified in COBIT. Reference should also be made to **figure 7** for metrics to measure key activities associated with managing changes to application controls.

Figure 9—Application Control Operation and Maintenance Performance Metrics

	Application Control Metrics	Relevant COBIT 4.1 IT/Process Goal	
Application Control Operation and Maintenance	Number of application control incidents/failures or instances where application controls did not achieve performance thresholds	AI7	Ensure proper use and performance of the applications.
	Average time to resolve identified application control incidents	DS8	Ensure proper use and performance of the applications.
	Number of change requests and change implementations due to rework after implementation, impacting application controls	AI7	Ensure proper use and performance of the applications.
	Average time to implement application control change requests	AI6	Ensure minimum business impact in the event of a change.
	Number of days/months since last independent application control review	ME2	Monitor the achievement of the internal control objectives.
	Number of application control deficiencies identified at service providers	AI7	Ensure proper use and performance of the applications.
	Number of automated application control operating effectiveness deficiencies identified by internal/external auditors	AI7	Ensure proper use and performance of the applications.
	Average time to resolve identified application control deficiencies	DS10	Ensure the satisfaction of end users with service offerings and service levels.

USING MATURITY MODELS FOR CONTINUOUS IMPROVEMENT OF APPLICATION CONTROLS

A maturity model is an increasingly common tool that management can use as a mechanism for continuously improving its capabilities relative to application controls. The maturity model approach measures the relative quality or maturity of the subject matter against an accepted continuum or scale of attributes associated with the subject matter. This approach is based on the original concept of the Capability Maturity Model (CMM), which was intended as a tool for objectively assessing the ability of government contractors' processes to perform a contracted software project. Though it comes from the area of software development, it can be useful as a generally applicable model to assist in understanding the process capability maturity of enterprises in diverse areas.[15]

Key Message #11

Periodic assessment of the maturity of application control design, implementation, operation and maintenance processes can be an effective tool to monitor ongoing reliability and identify improvement opportunities.

[15] Software Engineering Institute of Carnegie Mellon University, *The Capability Maturity Model: Guidelines for Improving the Software Process* (also known as the CMM and SW-CMM, this title was retired and replaced by the *CMMI®: Guidelines for Process Integration and Product Improvement* in 2003), Addison-Wesley Professional, USA, 1995

5. Operation and Maintenance of Application Controls

Capability maturity models are typically used to provide an assessment of the relative maturity of a process and can be an effective benchmarking tool to help ensure that process capability and controls are aligned with business requirements. Capability maturity model assessments are completed by comparing the attributes of the subject business process with an accepted model of 'best practices' for similar processes. The maturity of application control activities is typically considered as part of the overall process maturity and considers such attributes as set out in **figure 10**.

Figure 10—Internal Control Maturity

Maturity Level	Maturity Attributes
0 Non-existent	Internal controls, including application controls, are not explicitly considered as part of the design of the processes and underlying applications, are not documented, and ownership and responsibilities have not been assigned.
1 Initial/*ad hoc*	Business process owners and users are generally involved in the design, development and implementation of processes and enabling applications. Responsibility for control design and operation may be unclear, inconsistent and not well understood. Emphasis may be primarily focused on fixing issues when they arise. Individuals determine sufficiency and appropriateness of their activities.
2 Repeatable but Intuitive	Internal controls, including application controls, are considered and documented; however, they are performed differently by the people undertaking the same task. Responsibilities for performing control procedures are generally known. Control emphasis is primarily focused on detecting and correcting processing issues.
3 Defined	Internal controls, including application controls, are documented and appropriate to business needs across different people and applications; however, control exceptions may exist and procedures may not always be followed consistently. Responsibilities and accountabilities for performing controls are documented and communicated across the business process.
4 Managed and Measurable	Internal controls, including application controls, are documented and appropriate to business needs and are based on consistently applied control frameworks across the enterprise. Roles, responsibilities and accountabilities are defined and communicated. Controls are performed consistently and reliably, and performance is measured and monitored by management.
5 Optimised	Regular control monitoring and management reporting processes are in place. Internal controls, including application controls, are regularly reviewed and updated to stay in line with best practices. Process activities, performance metrics, key control indicators and key risk indicators (KRIs) are captured and monitored using automated tools and solutions.

CobiT 4.1 provides additional guidance for IT process maturity models for each of the CobiT processes, including processes related to application system acquisition, implementation and delivery. (See also appendix A—Mapping Activities Related to Application Controls to CobiT 4.1 Processes and Control Objectives for mapping to CobiT processes.) These process maturity models can be helpful in assessing application control design/development and operating capability.

6. RELATION AND DEPENDENCIES OF APPLICATION CONTROLS WITH IT GENERAL CONTROLS

Application controls are controls relative to the accuracy, integrity, reliability and confidentiality of processing by the application and are specific to that application. IT general controls are controls to ensure the reliability and integrity of the environment in which those applications operate and typically apply to all applications operating in that processing environment.

In chapter 3, application controls were defined as the policies, procedures and activities designed to achieve the objectives relevant to a given automated solution. Application controls support business objectives of providing accurate and reliable information for decision making by management and for stakeholders to rely on the information produced by the application system. IT general controls, on the other hand, are the controls that relate to the environment within which computer-based applications are developed, maintained and operated, and whose objectives are to ensure the proper development and implementation of applications, the integrity of program and data files, and the integrity of computer operations. IT general controls can protect the integrity of the application (including control activities such as testing and change control), the integrity of IT operations (e.g., data management controls, job scheduling controls) and control over data access (e.g., physical and logical security controls). For additional details and guidance, refer to the COBIT 4.1 management guidelines.

In this chapter, the distinction, the relationship and the interdependencies between application controls and IT general controls are further detailed.

RELATIONSHIP BETWEEN APPLICATION CONTROLS AND IT GENERAL CONTROLS

Application systems operate within a computer processing environment and depend on the reliability of that environment. This reliability is, itself, dependent on the effectiveness of the controls within the environment which, because of their relatively pervasive impact on all applications operating within that environment, are often referred to as IT general controls. Ineffective IT general controls impact the reliability of the computer processing environment, which in turn impacts the reliability and effectiveness of the application controls that operate within that environment.

Key Message #12

Application controls, especially automated application controls and the automated components of hybrid and configurable controls, are dependent on the reliable operation of the IT environment in which the application operates. IT general control deficiencies in this environment can impair the operating effectiveness of application controls, while effective IT general controls can provide opportunities to increase reliance on automated application controls.

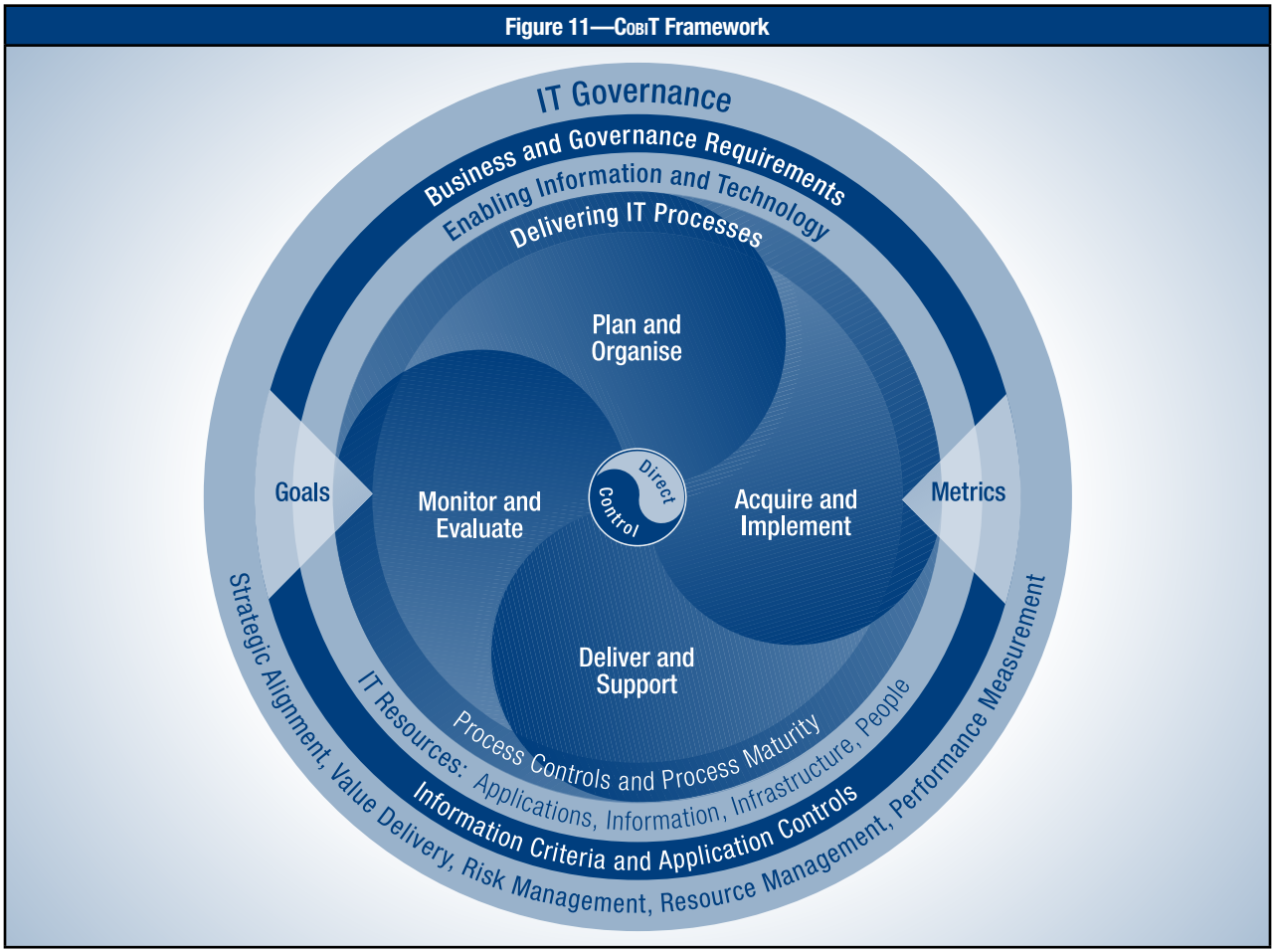
When designing the system of internal controls, there may be choices as to whether some activities should be performed in a way that is common to all applications and incorporated into the IT general control environment or whether the activity needs to be unique to an application and perhaps is better retained as part of the business process management of the application. In general, it can be argued that it is typically better to have controls such as security at the 'environment' level rather than in specific applications since it may increase efficiencies associated with testing and relying on a common security solution. Piecemeal solutions can also create integration problems and gaps in the end-to-end control solution. As such, these types of controls are typically designed into IT management processes as part of the IT general control environment. Specific business requirements will ultimately guide decisions such as this one. The important issue is that care be taken to ensure that there is a complete, end-to-end system of internal controls between activities performed within the business processes and activities performed within the IT processing environment.

6. Relation and Dependencies of Application Controls With IT General Controls

Understanding Computer Processing Environments

Computer processing environments consist of the computer equipment (and related software and infrastructure components) and the IT management and governance processes necessary to operate the business application systems. CobiT 4.1 provides guidance, including process descriptions, control objectives, management guidelines and maturity model guidelines for the effective governance and management of IT as summarised in **figure 11**.

Figure 11—CobiT Framework

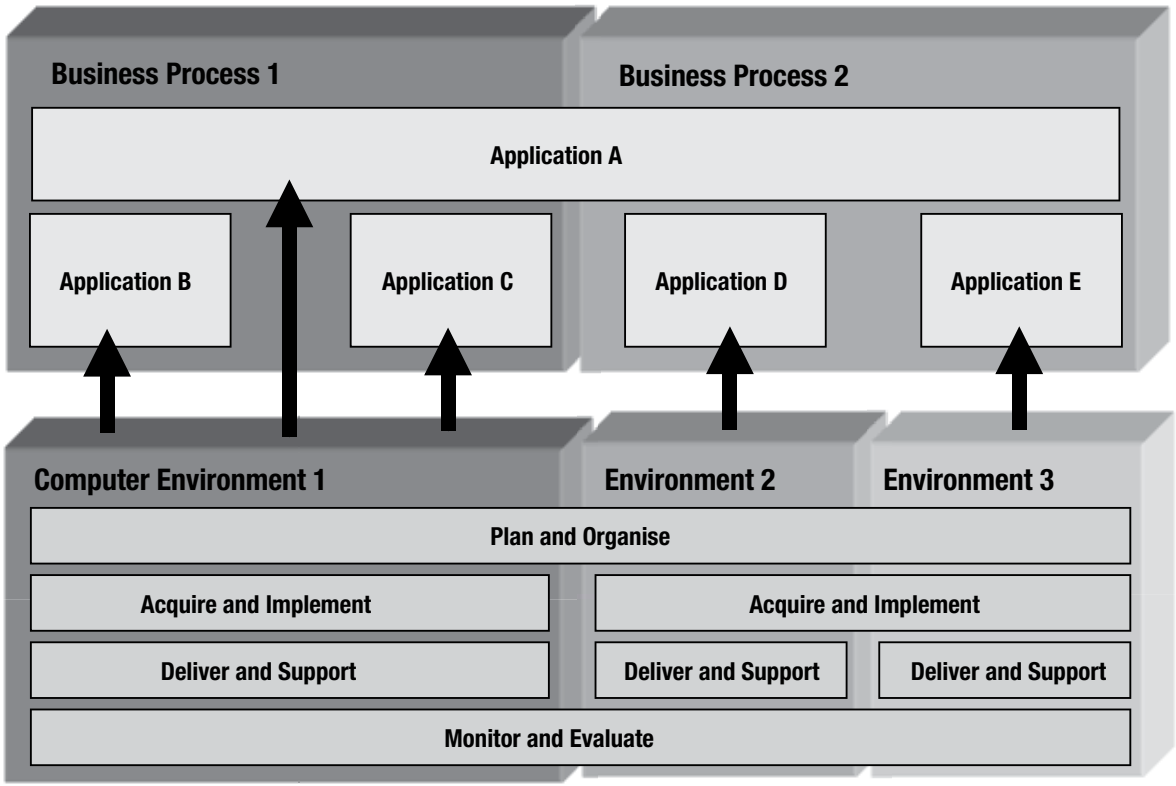


Within these processes, there is significant overlap with application control activities identified in this publication. In chapters 4 and 5, a number of specific areas within these IT process domains were identified that specifically relate to the reliability and effectiveness of the corresponding application controls, and appendix A—Mapping Activities Related to Application Controls to CobiT 4.1 Processes and Control Objectives provides a table summarising some of these key areas.

The Impact of IT General Controls

Ineffective IT general controls impact the reliability of the computer processing environment, which in turn impacts the reliability and effectiveness of the application controls that operate within that environment. In today's business environment, the complexity of information processing can result in complex architecture with key applications operating in a variety of processing environments. Consider the relatively simple example illustrated by **figure 12**.

Figure 12—Understanding Computer Processing Environments



In this example, application A is used across multiple business processes and, while applications B and C operate within computer environment 1, applications D and E support business process 2 and operate in different computer environments (environments 2 and 3, respectively). The effectiveness of the various computer processing environments will have a different impact on the reliability of the various application controls. For example:

- Control gaps in processes that are common across all environments (such as Plan and Organise and Monitor and Evaluate, in this example) may impact all applications.
- Control gaps in processes that are unique to a given sub-set of applications (such as Deliver and Support processes for environment 2) will impact only the applications that operate in that environment (in this case, application D).

6. Relation and Dependencies of Application Controls With IT General Controls

Enterprises may wish to consider similar approaches to map their information processing environment to help management understand the impact of a control weakness within a particular environment or application and to determine how that weakness can impact other environments and applications.

In general, IT general control processes with the most impact relative to application controls are within the Acquire and Implement (AI2 *Acquire and maintain application software*, AI6 *Manage changes*) and Deliver and Support (DS5 *Ensure systems security*, DS11 *Manage data*, DS13 *Manage operations*) domains.

ROLES AND RESPONSIBILITIES FOR IT GENERAL CONTROLS

CobiT defines the responsibility for application controls to be an end-to-end joint responsibility between business and IT. The business is responsible for properly:

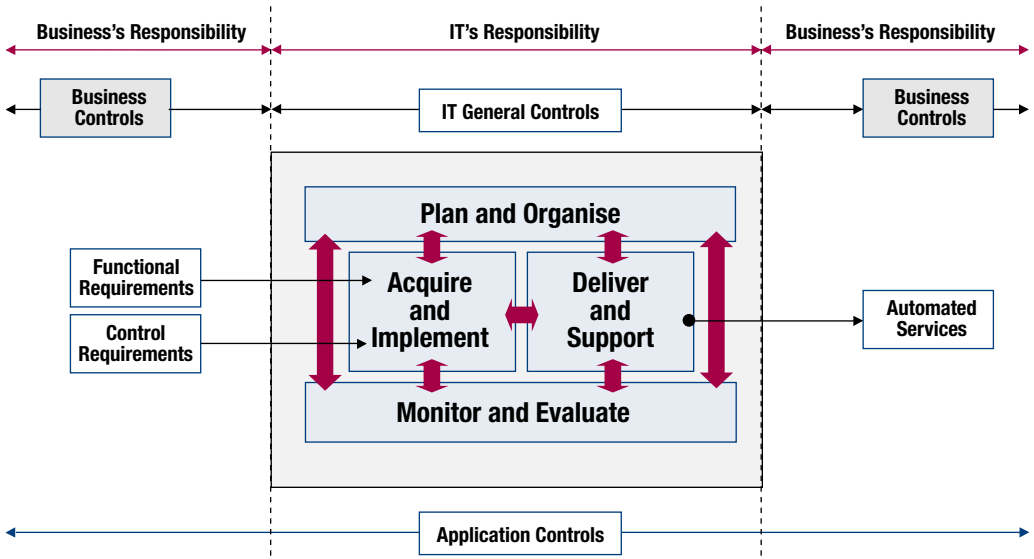
- Defining functional and control requirements
- Using automated systems and services

IT is responsible for:

- Automating and implementing business functional and control requirements
- Establishing controls to maintain the integrity of applications systems

Figure 13 is a graphic representation of the control boundaries and responsibilities of business, IT and applications.

Figure 13—Boundaries Amongst Business, IT General Controls and Application Controls



In satisfying this joint, end-to-end responsibility, it is important for there to be clear and open communication between IT and business management in the following areas:

- **IT general control strengths and limitations**—A reliable, well-controlled IT processing environment can enable business management to adopt greater reliance on automated application controls and thereby reduce the need for costly, manual activities. Conversely, an environment less well-controlled may require business management to adopt more manual application controls to provide the same degree of comfort over the reliability of information processing. When making decisions relative to the design of application controls, it is important for business management to work with IT to have an understanding of the IT environments in which the applications that support its business processes operate, including relative strengths and limitations in the respective IT general controls.
- **Communication of processing issues and IT general control failures**—Issues or failures in IT general controls may create a ripple effect, impairing the reliability of automated application controls and potentially impacting the integrity of the business processes and data. In such circumstances, it is important for business management to be involved in assessing the impact of processing issues or control failures on the business processes and any additional investigative or corrective measures that may be warranted.
- **Awareness of planned changes in IT general control activities**—Because of the importance of IT general controls on the reliability of application controls, it is important for affected business users to be involved in assessing the potential impact on application controls of planned significant changes to the IT general control activities. Improvement in IT general controls may be leveraged by the business to increase reliance on application controls, potentially reducing costly manual control activities.

IMPACT OF OUTSOURCING IT PROCESSING AND OPERATIONS

In today's business environment, enterprises often outsource some or all of their IT processing environment, ranging from outsourcing responsibility for hosting the data center to full outsourcing of IT operations and management. In an outsourced environment, responsibility for executing many of the management and control activities rests with the service provider. However, management retains the accountability for the effectiveness of its internal controls and needs to incorporate the impact of both the strengths and limitations of the service provider's internal controls into its own internal control activities. The user enterprise must define its requirements for internal control and take appropriate measures to monitor the effectiveness of those activities performed by its service enterprises. Some of the tools and techniques available to management to monitor the effectiveness of controls at service enterprises include monitoring performance against service level agreements (SLAs) and obtaining third-party assurance on the effectiveness of the service provider's system of internal controls. Such techniques are a part of an overall governance and management framework for third-party service providers. For additional information, refer to CobiT 4.1 IT process DS2 *Manage third-party services*.

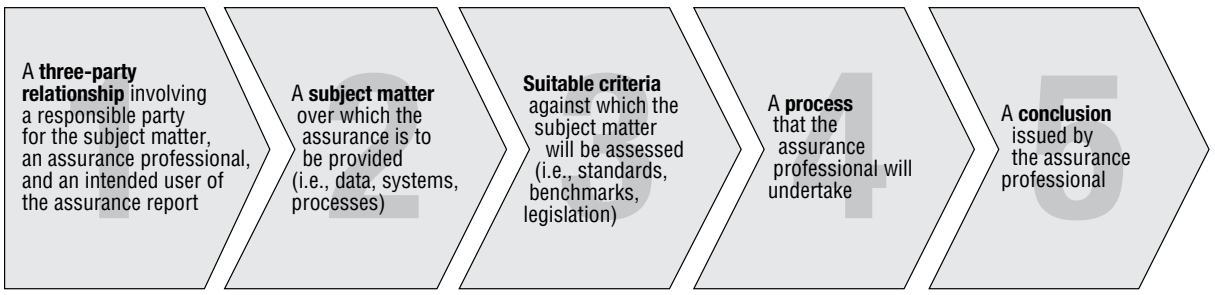
7. Application Controls Assurance

WHAT IS ASSURANCE?

Formal standards such as the International Auditing and Assurance Standards Board's (IAASB's) International Framework for Assurance Engagements (IAASB Assurance Framework) may be referenced for concepts and guidance for assurance. However, these standards are developed and presented from the perspective of an independent auditor providing assurance to third parties. In this publication, 'assurance' is used in a broader context than 'audit' and covers evaluation activities not governed by internal and/or external auditing standards.

The concept of 'assurance' requires five components to be present (**figure 14**[16]).

Figure 14—Five Components of an Assurance Activity



In summary, 'assurance' is the added information or conclusions reached by the assurance provider and provided to the interested parties as to whether the subject matter achieves or satisfies the relevant criteria.

COMMON EXAMPLES OF ASSURANCE

Common examples of situations involving the provision of assurance include:

- **Financial statement audit opinion**—The opinion of the independent auditors (assurance provider) to the board of directors and shareholders (interested parties) that the enterprise's financial statements (subject matter) are fairly stated (conclusion) in accordance with generally accepted accounting principles (criteria)
- **Internal audit report on review of a given business process**—Report by the internal auditor (assurance provider) to management and the board of directors (interested parties) that the risks within the given business process (subject matter) are being appropriately mitigated (conclusion) based on the COSO ERM framework (criteria)
- **ISO 27001 accreditation**—An accreditation, often for public display (interested parties), as a result of an examination conducted by an authorised accreditation enterprise (assurance provider) that the enterprise's information security management system (subject matter) complies with the criteria established by ISO 27001 (criteria)
- **Service auditor reports**—The audit and corresponding opinion provided by an independent service auditor (assurance provider) that the internal control activities of the service enterprise (subject matter) have been appropriately designed and operate effectively (conclusion) to achieve control objectives of interest to the user enterprises and their auditors (interested parties)
- **Management assertion on internal controls as required by Sarbanes-Oxley section 404**—The assertion by management (assurance provider) to the shareholders and capital markets (interested parties) that internal controls over financial reporting have been appropriately designed and are operating effectively (conclusion), in accordance with an internal control framework such as COSO (criteria)

[16] See also the ITGI publication *IT Assurance Guide: Using COBIT*, USA, 2007.

- **CIO 'sub-certification'[17] to the chief financial officer (CFO)/CEO as to the reliability of IT general controls**—The 'certification' by the CIO (assurance provider) that the IT general controls within his/her span of control and relevant to financial reporting (subject matter) have been appropriately designed (conclusion) in accordance with COBIT (criteria) and are operating effectively (conclusion)

Key Message #13

The concept of providing assurance is commonly thought of in the context of an auditor (either internal or external) providing assurance to management, the board of directors and the shareholders. However, the concept is increasingly relevant to financial and operational management in terms of providing assurance to relevant stakeholders. Examples where management is providing assurance to stakeholders include CEO/CFO certification of the design and operating effectiveness of internal controls as required by legislation such as Sarbanes-Oxley, and line management (such as the CIO) providing 'sub-certification' to the CEO/CFO on the effectiveness of controls within its operating units.

ASSURANCE OVER APPLICATION CONTROLS

Application controls relate to the transactions and master file, or standing data pertaining to each automated application system, and are specific to each application. They ensure the accuracy, integrity, reliability and confidentiality of the information and the validity of the entries made in the transactions and standing data resulting from both manual and automated processing.

The objectives relevant for application controls have been discussed in greater detail in chapters 4 and 5 and generally involve ensuring that:
- Data prepared for entry are authorised, complete, valid and reliable.
- Data are converted to an automated form and entered into the application accurately, completely and on time.
- Data are processed by the application accurately, completely and on time, and in accordance with established requirements.
- Data are protected throughout processing to maintain integrity and validity.
- Output is protected from unauthorised modification or damage and distributed in accordance with prescribed policies.

Providing assurance over application controls typically involves an assurance provider (the process/application owner, internal auditor, external auditor, etc.) following a process for gathering sufficient evidence that the application controls (subject matter) are appropriately designed and are operating effectively (conclusion) relative to established criteria (such as COBIT's application control objectives).

COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition and appendix VI of the *IT Assurance Guide: Using COBIT* provide detailed guidance for relevant application control practices, assurance steps and possible tests of controls for each of COBIT's six application control objectives.

Materiality

Materiality needs to be considered in determining whether a given set of application controls is sufficient to satisfy the control objectives and criteria. The assessment of what is material is a matter of professional judgement and includes consideration of the potential effect on the enterprise's ability to meet its business objectives in the event of errors, omissions, irregularities and illegal acts that may arise as a result of control weaknesses.[18]

Materiality can be used as a:
- Factor in determining the amount of evidence necessary to support the assurance provider's conclusion
- Measure of the significance of a finding relative to the subject matter

[17] 'Sub-certification' is a method to enable the CFO and CEO to obtain assurance for internal controls over financial reporting within enterprises where responsibility for control has been delegated to operational management.
[18] ISACA IS Auditing Guideline G6 Materiality Concepts for Auditing Information Systems, section 3.1.1

When conducting or supporting financial statement audits, assurance providers ordinarily measure materiality in monetary terms since what they are auditing is also measured and reported in monetary terms. Application control assurance providers may be required to provide assurance on non-financial systems (e.g., air traffic control system) or records (e.g., healthcare diagnostic codes) and, therefore, alternative measures are required. With respect to a specific control objective, a material control is a control or group of controls without which control procedures do not provide reasonable assurance that the control objective will be met. ISACA IS Auditing Guideline G6 Materiality Concepts for Auditing Information Systems specifies that where the assurance objective relates to systems or operations processing financial transactions, the value of the assets controlled by the system(s) and the value of transactions processed per day/week/month/year should be considered in assessing materiality.

For systems and controls not affecting financial transactions, the following are examples of measures that could be considered to assess materiality:
- Criticality of the business processes supported by the system or operation
- Cost of the system or operation (e.g., hardware, software, staff, third-party services, overhead costs, a combination of these)
- Potential cost of errors (possibly in terms of reputational risk, loss of client/consumer trust, lost sales, warranty claims, irrecoverable development costs, cost of publicity required for warnings, rectification costs, health and safety costs, unnecessarily high costs of production, high wastage)
- Number of accesses/transactions/inquiries processed per period
- Nature, timing and extent of reports prepared and files maintained
- Nature and quantities of materials handled (e.g., where inventory movements are recorded without values)
- SLA requirements and cost of potential penalties
- Penalties for failure to comply with legal and contractual requirements
- Loss of end-user productivity
- Degradation of end-user efficiencies

Assurance Risk

Assurance risk is the risk that an incorrect conclusion is reached by the assurance provider regarding the presence (or absence) of material misstatement of the subject matter. In the context of application controls, the risk of an incorrect conclusion could, for example, be the risk of concluding that the application controls operated effectively when, in reality, they did not. Assurance risk is a function of the risk of material error or control failure and the risk that the assurance provider will not detect associated errors or control failures (sometimes refered to as detection risk).

The risk of material error has two components:[19]
- **Inherent risk**—The susceptibility of the subject matter (such as an assertion by the responsible party) to a misstatement that could be material
- **Control risk**—The risk that a material misstatement could occur in an assertion and not be prevented, detected or corrected on a timely basis by the entity's internal controls

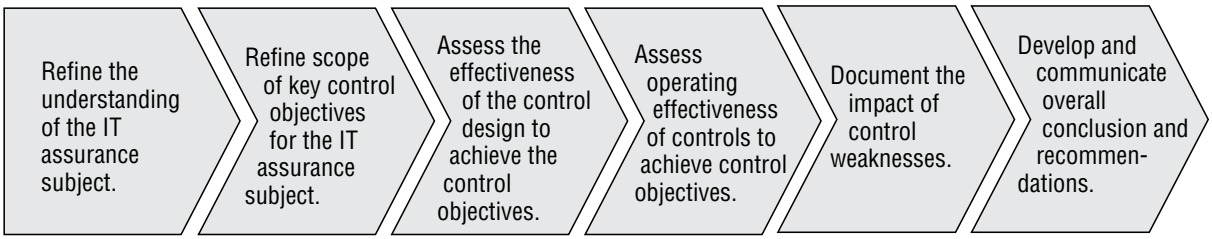
When planning an assurance activity, it is important to consider the inherent risk associated with the subject matter to determine the nature and extent of procedures and to design those procedures to reduce detection risk to an acceptable level.

[19] These definitions are drawn from the International Accounting and Assurance Standards Board. Refer to International Federation of Accountants (IFAC), 'International Standard on Auditing (ISA) 330 (redrafted)', USA, 2006, for examples.

A PROCESS FOR OBTAINING APPLICATION CONTROL ASSURANCE

Figure 15 describes a process road map that assurance providers can follow as they execute a particular assurance activity.

Figure 15—Road Map for Application Control Assurance



Step 1—Refine Understanding

The first step of the execution stage is obtaining or refining an understanding of the subject matter for which assurance is necessary. With respect to application controls, this implies understanding the business process, including its goals and objectives, as well as the application supporting the business process. In obtaining this understanding, it is necessary to understand such elements as:

- Identifying the in-scope applications (including dependent applications and interface applications)
- Identifying the in-scope inputs, outputs and data stores
- The types and sources of information processed by the application—significant inputs
- The nature of processing the application performs (e.g., calculations, summarisations, translation/transformation)
- The types and destinations of information output by the application
- The importance of the information to the business process in decision making by the enterprise and its stakeholders

The output from this step consists of documented evidence regarding:

- Key suppliers of information to the application
- Significant types or classes of information necessary for the application in its processing
- Form, content and methods for how information is input into the application
- Details of significant processing activities performed by the application
- Dependencies on other applications, processes or sub-processes
- Details concerning key data stores or tables where significant information is stored for subsequent use (either by this application or others)
- Form, content and methods for how information is output from the application
- Key stakeholders or recipients of the information generated by the application

Depending on his/her existing level of knowledge of the business process and applications, the assurance provider can structure this step along the following lines:

- Interview business process owners, application subject matter experts and application users.
- Collect and read application user and system support documentation, policies, systems input/output, issues logs, meeting minutes, past assurance reports and recommendations, management reports, etc.
- Prepare or utilise existing information flow diagrams and narratives summarising key elements of information processing.

- Summarise relevant business objectives and stakeholder expectations for the information in terms of the information criteria of effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability.
- Summarise relevant assertions upon which assurance is to be provided, including completeness, accuracy, validity, authorisation and segregation of duties.

Step 2—Refine Scope

Based on the detailed understanding of the application and related business processes, the assurance provider can determine the scope necessary to provide the desired assurance. This process consists of:

- Assessing the potential threats that may impact the relevant information criteria and the associated risk or impact on the relevant assertions (e.g., threats may impact the integrity of the information and the risk or impact they would have relative to the assertion of completeness or accuracy)
- Identifying the application control objectives relevant for the identified threats/risks and for providing assurance that meets the requirements of the interested parties

Step 3—Assess the Design of Controls

In this step of the assurance process, the assurance provider identifies the control activities that have been implemented to achieve the relevant, in-scope control objectives and reaches a conclusion as to whether the application control activities, as designed, would reasonably achieve the identified control objective if those activities were to operate effectively. In reaching a conclusion on the design effectiveness of controls, the assurance provider typically considers the same application control attributes outlined in chapter 4 that management considers in designing application controls, including:

- The type of the activity—Automated vs. manual vs. hybrid vs. configurable
- The nature of the control—Preventive vs. detective
- The frequency of the control—Considering the risk of material misstatement in the event of control activity failure
- The proximity of the control activity to the risk event that could result in a material control failure
- Who performs the control activity and whether that responsibility is sufficiently segregated from other, incompatible activities associated with the processing of the information

As part of this step, the assurance provider performs sufficient procedures to confirm that the control activities have been placed into operation. Commonly referred to as a 'walkthrough', this activity provides confirmation that the assurance provider has an accurate understanding of the application control activities and those activities operate as described. The nature of the activities performed by the assurance provider in this regard can be similar to those outlined in step 4, but are typically performed to a limited extent.

Step 4—Assess the Operating Effectiveness of Controls

In this step of the process, the assurance provider gathers evidence that the control activities are operating as described. In the case of an independent assurance provider (such as internal or external auditors or a corporate compliance group), this activity typically involves 'testing' the control activities. In situations where assurance is provided by management, the evidence to support the assurance assertions may be accumulated within the business process and subjected to review by management.

While the testing procedures that are appropriate for a given control activity will vary depending on the specifics of the activity, four common, generic testing techniques are used:

- Inquire and confirm
  - Search for exceptions/deviations and examine them.
  - Investigate unusual or non-routine transactions/events.
  - Check/determine whether transaction/event has (not) occurred.
  - Interview staff members and assess their knowledge and awareness.
  - Ask management questions and obtain answers to confirm findings.

- Inspect
  - Review plans, policies and procedures.
  - Compare input data to source documents.
  - Search audit trails, problem logs, etc.
  - Trace transactions through the process/system.
  - Physically inspect presence (documentation, assets, etc.).
  - Compare actual with expected findings.
- Observe
  - Observe and describe process activities and procedures.
  - Compare actual with expected behavior.
- Re-perform and/or recalculate
  - Reconcile transactions (e.g., reconcile transactions to bank statements).
  - Independently develop and estimate the expected outcome.
  - Attempt what is prevented.
  - Re-perform what is detected by detective controls.
  - Re-perform transactions, control procedures, etc.
  - Recalculate independently.
  - Compare expected value with actual value.
  - Compare actual with expected behaviour.
  - Trace transactions through the process/system.

Computer Assisted Audit Techniques (CAATs)

Since applications involve collecting, processing, summarising and storing data in electronic form, the availability of these data in electronic form creates the opportunity for the assurance provider to design automated analysis techniques (commonly referred to as CAATs) that can be used to test the effectiveness of control activities or perform tests of outcomes of the control activities. Examples of commonly used CAATs include:

- Identifying and analysing all bypasses, overrides or manual entries that are not subject to the internal controls contained in the system
- Analysing exception files to determine the number of exceptions, age of exceptions, types of exceptions and root causes of exceptions
- Analysing data for existence or absence of relevant attributes or elements (i.e., status flags, validity of field contents, blank fields, digital authorisations)
- Checking the sequential numbering of items or transactions
- Identifying unusual or non-routine items and checking whether appropriate controls (e.g., approvals) were applied to those items
- Independently estimating or recalculating expected output from a given automated calculation(s)
- Analysing trends and potential anomalies in the data that may indicate breach of control activities
- Comparing/reconciling data between different systems
- Re-performing calculations or report generation routines

Other Considerations

In addition to meeting the specific assurance objectives associated with the information and the application's information processing objectives, assurance providers may consider other attributes such as the cost-effectiveness of the control design and operation as part of their assessment. Steps that could be considered include:

- If the design of the control practice set is effective, assess whether it can be made more efficient by optimising steps, looking for synergies with other control mechanisms, and reconsidering the balance of prevention vs. detection and correction. Also, consider the effort spent in maintaining the control practices.
- If the control practice set is operating effectively, investigate whether it can be made more cost-effective. Consider analysing performance metrics of the activities associated with this control practice set and additional automation opportunities.

Step 5—Document and Communicate the Impact of Control Weaknesses

When control weaknesses (i.e., deficiencies in design or failure in operating effectiveness) are found, they need to be properly documented, taking into account their often sensitive and confidential nature, and brought to the attention of the process owner. Particular care is required to correctly analyse and assess the severity of the observed weaknesses and the potential business impact.

The objective of this step is to conduct the necessary analysis to provide a thorough understanding of the control weaknesses and the resulting threats, vulnerabilities and impact.

The following activities can be performed to document and communicate the impact of not achieving the control objectives:
- Conduct further investigative analysis to determine and document the impact of actual control weaknesses in terms of bottom-line impact, integrity of financial reporting, hours lost in staff time, loss of sales, ability to manage and react to the market, customer and shareholder requirements, etc.
- Document the cost (e.g., customer and financial impact) of errors that could have been caught by effective controls.
- Identify consequences of non-compliance with regulatory requirements and contractual agreements.
- Measure the actual impact of disruptions and outages on business processes and objectives, and on customers (e.g., number, remediation and/or alternative processing effort, downtime, customer satisfaction, cost).
- Measure and document the cost of rework (e.g., ratio of rework to normal work) as an efficiency measure affected by control weaknesses.
- Link known performance indicators to known outcomes and, in their absence, link the cause to its effect (cause-effect analysis).
- Clarify vulnerabilities and threats that are more likely with controls not operating effectively.
- Illustrate what the impact would affect (e.g., business goals and objectives, enterprise architecture elements, capabilities, resources).
- Relate the impact of not achieving the control objective to actual cases in the same industry and leverage industry benchmarks.
- Illustrate the impact of control weaknesses with numbers and scenarios of errors, inefficiencies and misuse.
- Use benchmarking and survey results to compare the enterprise performance with others.

The assurance provider should document any identified control weaknesses and resulting threats and vulnerabilities, and identify and document the actual and potential impact (e.g., through root cause analysis).

The objective is to identify items of significance to be able to articulate to management the recommended actions and reasons for taking action. This phase includes aggregating the results of the previous phases, developing a conclusion concerning the identified control weaknesses and communicating:
- The impact of identified control weaknesses and how prepared the enterprise is to address them
- Recommended actions to mitigate the impact of the control weaknesses
- Performance comparison to standards and best practices
- The risk position regarding the process

Step 6—Reaching a Conclusion on Application Controls

In this step of the process the assurance provider forms a conclusion as to whether there is sufficient appropriate evidence to provide reasonable assurance that the subject matter has satisfied the criteria. In the case of application controls, this is determining whether the control activities have been appropriately designed and are operating with sufficient effectiveness to provide reasonable assurance over the accuracy, integrity, reliability and confidentiality of information processing. In reaching a conclusion, the assurance provider considers all of the information gathered thus far in the assurance process, including:
- The understanding of the business process objectives and the objectives of the application
- The evidence supporting the design effectiveness of the application controls to meet the identified objectives
- The sufficiency and appropriateness of evidence supporting the operating effectiveness of the control activities

In forming a conclusion, the assurance provider needs to be mindful of formal assurance communication and compliance with assurance standards, including reporting standards and guidelines.

GUIDANCE FOR DETERMINING APPROPRIATE SAMPLE SIZES FOR TESTING APPLICATION CONTROLS

For many of the procedures identified previously for testing application controls, the assurance provider will use sampling methods to select and examine a sub-set of the population of items. To determine the number of items to be selected for a particular sample for a test of controls, the assurance provider considers the desired confidence level, the tolerable rate of deviation from the controls being tested, the likely rate of deviations, and the allowable risk of assessing control risk:

- **Confidence level**—Refers to the degree of assurance to be provided by the sample
- **Tolerable rate of deviation**—Refers to the maximum rate of deviations (i.e., control activity exceptions) the assurance provider is willing to accept in forming a conclusion
- **Likely rate of deviations (or expected error rate)**—Refers to the rate of deviations that are expected to be found within the population. As discussed in chapter 4, application controls can vary in their reliability depending on the attributes of the activity.
- **Allowable risk of assessing control risk (allowable audit risk)**—Refers to false conclusions reached because of the inherent risks in sampling. This includes the risk that the sample of items selected may be too small and does not reflect the actual results in the population taken as a whole.

For additional guidance on sampling internal controls, refer to American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards (SAS) No. 111 Amendment to Statement on Auditing Standards No. 39, Audit Sampling.

Although there are many factors that are considered when selecting sample sizes, **figure 16** represents the common (minimum) sample sizes used by companies and auditors for testing the operating effectiveness of controls.

Figure 16—Guidance for Sample Size Selection

Nature of Control	Frequency of Performance	Minimum Sample Size
Manual	Many times per day	25
Manual	Daily	25
Manual	Weekly	5
Manual	Monthly	2
Manual	Quarterly	2
Manual	Annually	1
Automated	Test one application of each programmed control activity (assumes IT general controls are effective).	
IT General Controls	Follow the guidance above for manual and programmed aspects of IT general controls.	

The guidance in **figure 16** was specifically developed relative to assurance provided for internal controls over financial reporting and the corresponding opinion on the effectiveness of controls at a point in time, and may not be relevant for all circumstances. Final determination of the extent of sampling necessary to support their conclusions requires assurance providers to consider all of the relevant factors and apply their professional judgement. If, for example, it is expected that the sample will include one error, the sample sizes need to be supplemented to reach the same degree of confidence.

For many tests of controls, sampling may not apply. For example, sampling may not apply where there is no documentary evidence of performance or where it may be as efficient for the assurance provider to efficiently examine 100 percent of the available evidence.

Testing Automated Application Controls

In chapter 4, the business value and benefit of automating application controls were discussed. Automated application controls also provide an opportunity for significant savings in assurance costs. **Figure 16** suggests that, where application controls are automated, it may be sufficient to test one application of the control activity to obtain the required assurance (e.g., observe the automated three-way matching process and application of tolerances among the purchase order, goods receipt note and invoice). This can provide significant efficiencies to the assurance provider as the cost of gathering sufficient evidence to support manual control activities grows exponentially with increased size, number and complexity of manual control activities.

This 'test of one' principle is based on the inherent reliability of information systems processing to perform the same way each time until there is some change in the information processing environment that may impact the reliability of processing activity. This requires that the controls within the information processing environment (IT general controls) be evaluated and found to be operating effectively.

Key Message #14

It may be more efficient and cost-effective for assurance providers to rely on automated application controls, where possible, since this may reduce the costs associated with validating the operating effectiveness of manual activities. With effective IT general controls, a benchmarking strategy may further reduce operating effectiveness validation cost and effort.

Benchmarking

Extending this logic further introduces the concept of benchmarking or baselining. Application controls that are entirely automated can be reasonably expected to continue to operate with the same degree of reliability, as long as the computer processing environment in which those application controls operate is appropriately controlled and those controls are operating effectively. Use of this approach as an assurance strategy requires the following:

- The assurance provider needs to establish that the automated application control in question is operating with sufficient reliability. The logic above suggests only that the automated control will continue to operate with the same degree of reliability. If it currently is not operating effectively, it can be reasonably expected to continue to do so (not operate effectively). As such, the assurance provider needs to establish that the automated application control is operating effectively. The activity of establishing that the automated application control is currently effective, is referred to as 'benchmarking' or 'baselining'.
- The assurance provider needs to be able to rely on the design and operating effectiveness of IT general controls that are relevant to the reliable operation of the automated control. Additional guidance on the impact of IT general controls is discussed in the following section. Benchmarking automated application controls can be especially effective for enterprises using purchased software when the possibility of program changes is remote and, therefore, frequent 're-baselining' is not necessary—for example, when the vendor does not allow access or modification to the source code.

Benchmarking has been identified as an acceptable approach for external auditors providing assurance related to internal controls over financial reporting. The following is quoted from the PCAOB's Question and Answer guidance:[20]

> *Automated application controls … will continue to perform a given control (for example, aging of accounts receivable, extending prices on invoices, performing edit checks) in exactly the same manner until the program is changed. Entirely automated application controls, therefore, are generally not subject to breakdowns due to human failure and this feature allows the auditor to 'benchmark,' or 'baseline,' these controls. If IT general controls over program changes, access to programs, and computer operations are effective and continue to be tested, and if the auditor verifies that the automated application control has not changed since the auditor last tested the application control, the auditor may conclude that the automated application control continues to be effective without repeating the prior year's specific tests of the operation of the automated application control. The nature and extent of the evidence that the auditor should obtain to verify that the control has not changed may vary depending on the circumstances, including depending on the strength of the organization's program change controls.*

This statement reinforces the need for IT general controls to be effective for a 'test of one' application control to provide sufficient evidence that the control is operating effectively. If IT general controls are not effective, then a 'test of one' would not necessarily provide sufficient evidence that the application control operated effectively.

In addition to the effectiveness of IT general controls, factors to consider when determining whether a given automated application control is a suitable candidate for a benchmarking strategy and for planning the activities necessary to obtain the desired degree of assurance include:[21]

- The extent to which the automated application control can be matched to a defined program
- The extent to which the application within which the automated application control functions is stable (i.e., there are few changes from period to period)
- Whether a report of the compilation dates of programs placed in production is available and is reliable (This information may be used as evidence that automated application controls within the applications have not changed.)
- The evidence supporting the effectiveness of controls over related files, tables, data and configurable parameters on the consistent and effective functioning of the automated application control (e.g., an automated application for calculating interest income might be dependent on the effectiveness of controls over the continued integrity of a rate table used by the automated calculation)
- How frequently the assurance provider needs to 're-benchmark' the automated application control to continue to have the necessary degree of assurance as to its effectiveness. To determine when to re-establish a benchmark, the assurance provider considers the following factors:
  - The degree of assurance available over the design and operating effectiveness of the IT general control environment, including controls over application and system software acquisition and maintenance, access controls and computer operations
  - An understanding of the frequency and potential cumulative effects of changes, if any, on the specific programs that contain the controls
  - The effectiveness of other related controls
  - The consequences of errors associated with the automated application control that was benchmarked

[20] Public Company Accounting Oversight Board (PCAOB), 'Staff Questions and Answers, Auditing Internal Controls Over Financial Reporting', USA, 15 May 2005
[21] *Ibid.*

IMPACT OF IT GENERAL CONTROL DEFICIENCIES ON APPLICATION CONTROL ASSURANCE

As noted in the previous section, the ability of the assurance provider to obtain assurance over the reliability of automated application controls using a 'test of one' strategy depends on being assured that the IT general controls over the IT processing environment within which those automated application controls operate are, themselves, designed and operating effectively.

The question becomes: What impact do deficiencies in the IT processing environment's IT general controls have on the effective operation of automated application controls?

To answer this question, the assurance provider needs to consider:
- Do the identified IT general control deficiencies relate to the automated application controls in question?
- What is the risk that identified IT general control deficiencies adversely impact the operation of the application or related automated application controls?

Do the Identified IT General Control Deficiencies Relate to the Automated Application Controls in Question?

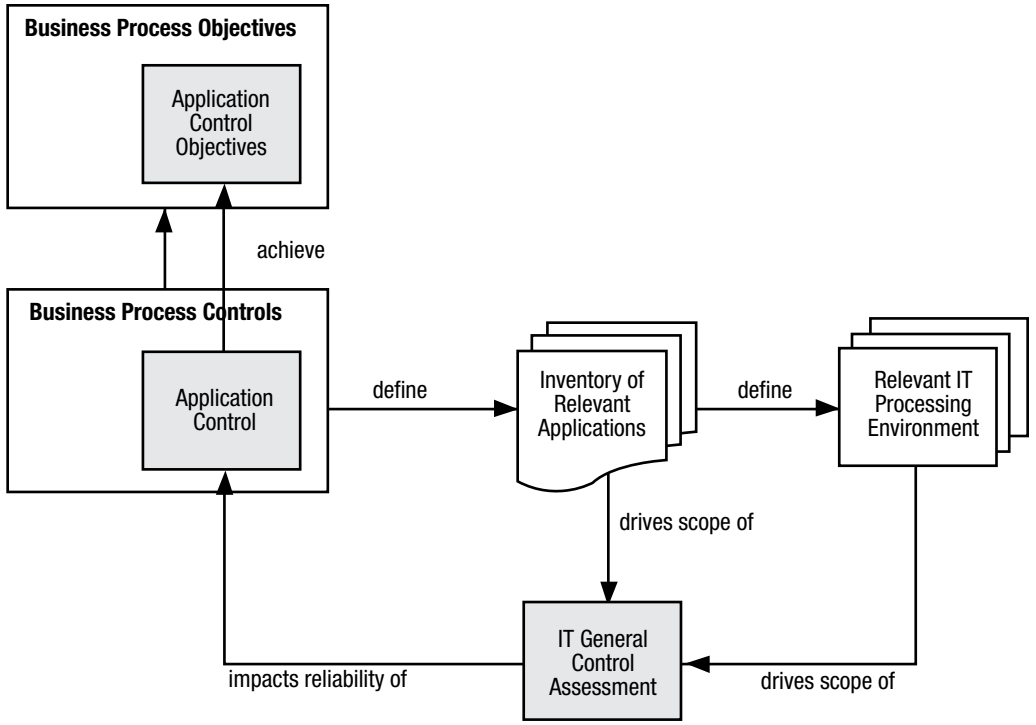
The assurance provider needs to determine whether the identified deficiencies in IT general controls have a connection (or lack thereof) with automated application controls. Establishing this connection, or linkage, can be accomplished by the following:
- The application controls assurance provider needs to identify the specific application within which the automated application control operates. Typically, this can be most efficiently performed when identifying and assessing the design of the automated application controls and may require technical assistance of subject matter experts with detailed knowledge of the application architecture. This identification establishes the inventory of relevant applications upon which the assurance provider requires IT general controls assurance.
- The IT general controls assurance provider can use this inventory of relevant applications to identify the IT processing environments that require assessment of the design and operating effectiveness of IT general controls. Further, the IT general controls assurance provider can use the identified relevant applications in determining an appropriate population from which items are selected to evaluate the effective operation of the IT general controls.
- The IT general controls assurance provider can communicate deficiencies identified in the IT processing environments and the corresponding impacted applications to the application controls assurance provider.

This relationship can be depicted graphically as shown in **figure 17**.

What Is the Risk That IT General Control Deficiencies Adversely Impact the Operation of the Application and Related Automated Application Controls?

Assessing the risk of the IT general control deficiencies adversely impacting the automated application controls requires consideration of the following:
- What is the risk (or error condition) to which the IT general control deficiency is related and how significant is the corresponding impact to achieving the related IT general control objective? Deficiencies identified in IT general controls that are not significant enough to impact whether the related control objective is achieved would normally have no significant impact on related automated application controls.
- Are there other controls within the computer processing environment(s) that are operating effectively and that would compensate for the identified IT general control deficiencies and thus sufficiently reduce the existing risk?
- In the absence of such compensating controls, can further investigative analysis provide sufficient assurance that the automated application controls have not been adversely impacted? For example, if the identified deficiency relates to inappropriate access to the application processing environment by the application developers, an analysis of activity logs (assuming reasonable assurance can be obtained over the completeness of the logs) may provide sufficient assurance that such access was not used to adversely impact the operation of the impacted applications.

Figure 17—Relationship Between IT General Control Deficiencies and Application Control Effectiveness

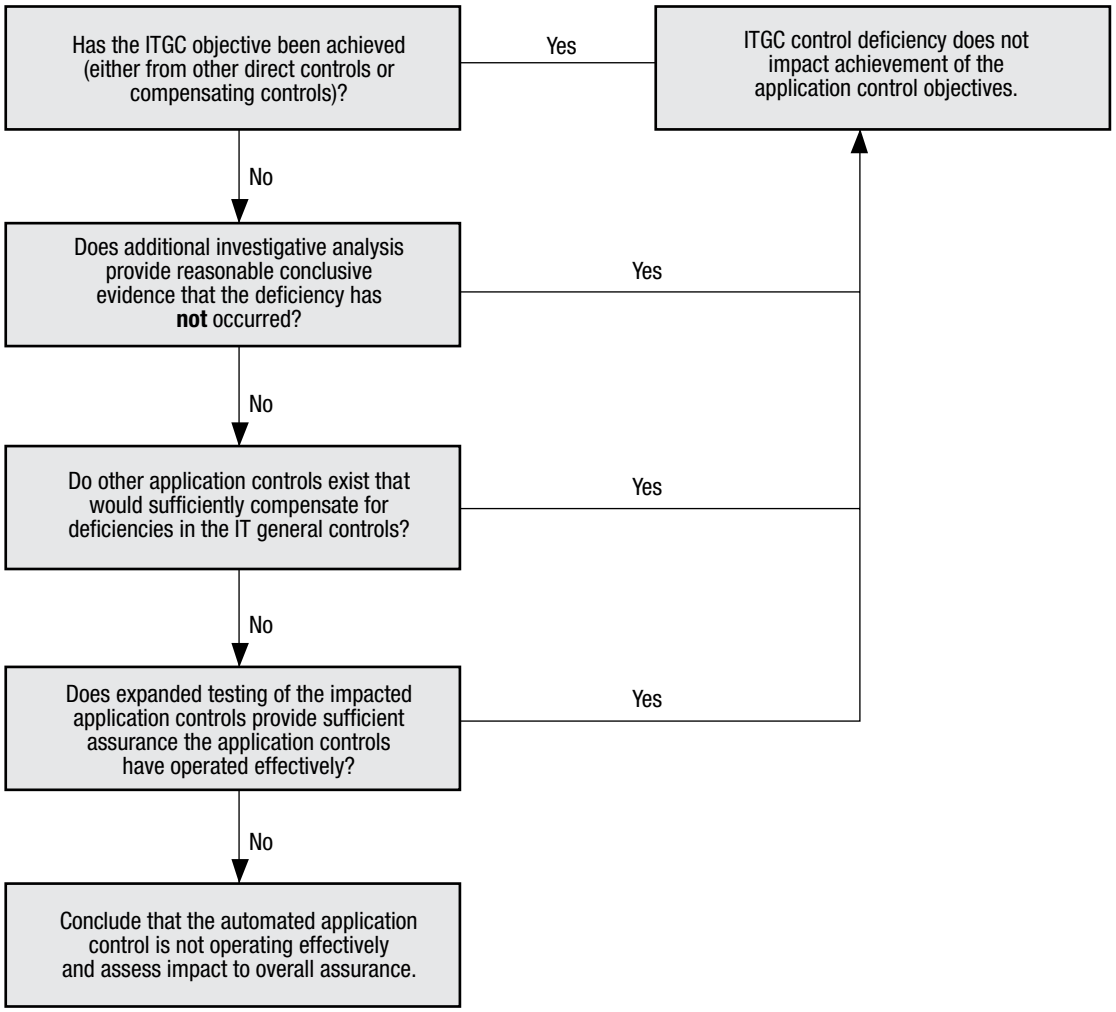


If these activities have not sufficiently reduced the risk of an adverse impact to the automated application controls, the application controls assurance provider should consider the following:

- What is the risk (or error condition) resulting from the potential adverse impact on the automated application control and how significant is the corresponding impact to achieving the application control objective, considering other controls associated with that objective?
- Are there other controls that are operating effectively within the related application and business process controls that could compensate, should the automated application control actually operate ineffectively? For example, manual detective controls may exist that could detect significant failures in automated application controls.
- In the absence of such compensating controls within the other application and business process controls, can further investigative analysis of the application systems and data provide sufficient assurance that the automated control activity has not been adversely impacted? For example, can further testing of the outcomes of the automated activity be performed to provide sufficient assurance that the automated activity has not been adversely impacted by the IT general control deficiency and continues to operate effectively? A decision on the extent of additional testing is a matter of professional judgement. However, if the deficiencies relate to manual IT general controls, additional testing of the application control to the same extent as would otherwise be used if that activity were performed manually (e.g., as outlined in **figure 16**) could provide sufficient evidence that the application control has operated effectively.

The diagram in **figure 18** provides a logic flow that can be used to assist in determining the impact of IT general control deficiencies on application controls.

Figure 18—Impact of IT General Control Weaknesses on Automated Application Controls



It should be noted that, in situations where IT general control deficiencies exist, while there may be other ways the assurance provider can obtain sufficient information relative to the achievement of the application control objectives (such as through the steps outlined previously), this does not imply that management action to correct the IT general control deficiency is not necessary or appropriate.

The relationship between IT general controls and automated application controls demonstrates the importance of timely and effective communication between the application controls assurance provider and the IT general control assurance provider.

APPENDIX A—MAPPING ACTIVITIES RELATED TO APPLICATION CONTROLS TO COBIT 4.1 PROCESSES AND CONTROL OBJECTIVES

Activities associated with the design, implementation, operating and monitoring of automated application controls include responsibilities that are shared between IT management (providing and operating automated solutions and business) and management (running and operating its respective business processes). **Figures 19** and **20** provide a mapping between activities with the respective COBIT 4.1 process and control objectives where additional guidance on process goals, objectives, goals and metrics, maturity models, roles and responsibilities, and control practices can be found. Reference numbers in this table refer to item reference numbers in chapters 4 and 5.

Figure 19—Application Control Design and Implementation: Mapping to COBIT Processes and Control Objectives

Key Activities			Related COBIT Control Objectives
Chapter 4. Design and Implementation of Application Controls	Identify Relevant Control Objectives	Identify key stakeholders and assign application control-related roles and responsibilities.	AI1.1
		Perform an assessment of information-related risks and information processing-related risks.	AI1.2
		Identify and document relevant control objectives.	AI1.1
		For third-party software, include control requirements in the RFP.	AI5.2, 5.3, 5.4
	Design/Build/Configure Application Controls	Review detailed application specification design (including automated application controls).	AI2.1, 2.3
		Evaluate vendor solution (including fit with control requirements).	AI2.2
		Develop future state business process design (including design of manual application controls to meet control objectives).	AI2.1, AI4.1
		Assess and conclude on sufficiency of the design of application controls.	AI2.1, 2.3, 2.4, 2.5
		Code and debug automated application controls as part of software development.	AI2.7
		Install and configure commercial applications, including configurable controls.	AI2.5
	Document Controls and Train Users	Develop/update application control documentation.	AI4.1
		Develop/update user training materials and provide training as required to affected staff.	AI4.2, 4.3, 4.4
		For new employees, provide full training on the application and relevant application controls.	AI4.2, 4.3, 4.4
	Test and Approve Application Controls	Develop, document and approve the test plan.	AI7.2
		Conduct application control testing in accordance with the test plan.	AI7.6
		Identify, log, prioritise and resolve errors and issues identified during testing.	AI7.6
		Document and interpret the final test results, including unresolved issues.	AI7.7
		Approve test results and determine implementation of application control activities.	AI7.7

Appendix A—Mapping Activities Related to Application Controls to CobiT 4.1 Processes and Control Objectives

Figure 20—Operation and Maintenance of Application Controls: Mapping to CobiT Processes and Control Objectives			
Key Activities			Related CobiT Control Objectives
Chapter 5. Operation and Maintenance of Application Controls	Operation of the Automated Solution	Enable effective and reliable operation of automated solutions.	DS13
	Monitor Application Control Effectiveness	Supervise and oversee performance of key manual control activities.	AC1 - AC7
		Supervise and oversee the identification, prioritisation, escalation and resolution of control exceptions, failures and processing errors.	
		Monitor process metrics and key performance indicators.	
		Perform periodic assessments of control effectiveness.	
	Manage Changes to Application Controls	Identify need for change in business processes and underlying automated solutions and define business requirements.	AI6.1
		Assess impact of changes on application controls and define necessary control requirements and changes.	AI6.2
		Design, build, test and implement changes to automated solutions, including automated application controls, based on defined business requirements.	AI2, AI6.3, AI6.4, AI6.5, AI7
		Design, build and implement business process changes, including manual application control procedures based on defined business requirements and changes to automated solutions.	AI4.2
		Manage changes to business information tables, standing data and other 'user managed' configuration tables.	AC1 - AC7
		Manage changes to business rules and other 'IT-managed' configuration tables (see also CobiT control objective AI2.5).	AI2.5, AI6

APPENDIX B—ADDITIONAL GUIDANCE ON TYPES OF APPLICATION CONTROLS

In chapter 4, the need to consider the proximity of controls relative to the occurrence of the risk event was discussed. In the following discussion, further guidance is provided to illustrate the types of controls that may be relevant at various stages in the information processing cycle. These controls are intended to be illustrative and do not necessarily represent a complete listing of relevant control activities.

Controls at each stage in the information processing cycle include:
- Input stage
  - Input validation
  - Input exception reporting and handling
- Processing stage
  - Programming logic
  - Processing validation
  - Processing exception reporting and handling
- Output stage
  - Output verification
  - Output exception reporting and handling
  - Output distribution
  - Output storage and retention
- Processing boundary
  - Information protection and authorisation
  - Segregation of duties
  - Interfaces
- Audit trails and application journalling

Figure 21 provides a mapping of these control types to the COBIT application control objectives.

INPUT STAGE

Controls at the input stage of information processing are used mainly to check the integrity of data entered into a business application, whether the data are entered directly by staff, remotely by a business partner, or through a web-enabled application or interface. They are techniques and procedures used to verify, validate and edit data to ensure that only valid and authorised data are entered into the application and transactions are processed only once.

Input Validation

The goal of input validation controls is to ensure that information entered into the application is valid and complete in the context of what the application was designed to perform. Input validation controls can take many forms, depending on the kind of data that needs to be provided as input and how those data are entered into the application.

For applications that require users to enter information, input validation controls embedded in the applications can verify that mandatory input fields are completed; information is entered in the correct format; input values are valid and/or comply with predefined ranges, limits or other criteria; and the information provided across different input fields is consistent. When creating a new customer in the customer master file, for example, input validation controls can ensure that mandatory information, such as customer name and address, are entered by the user in the correct format (e.g., a specific format for telephone numbers) and

Figure 21—Mapping of Types of Application Controls to Corresponding COBIT Application Control Objectives

Control Types	AC1 Source Data Preparation and Authorisation	AC2 Source Data Collection and Entry	AC3 Accuracy, Completeness and Authenticity Checks	AC4 Processing Integrity and Validity	AC5 Output Review, Reconciliation and Error Handling	AC6 Transaction Authentication and Integrity
Input controls						
Input validation controls	P	S	S			
Input exception reporting and handling	S	P	S			
Processing controls						
Logical controls			P	S		
Processing validation controls			P	P		
Processing exception reporting and handling			P	P		
Output controls						
Output verification controls			S	S	P	
Output exception reporting and handling			S	S	P	
Output distribution controls					P	
Output storage and retention controls					P	
Boundary controls						
Information protection and authorisation controls	P	P	S	P	P	P
Segregation of duties controls	P	P	S	S	S	S
Interface controls			P	S	P	P
Audit trail controls						
Audit trails		S		S	S	S

P = Primary enabler; S = Secondary enabler

consistent (e.g., drop-down list of available information). A range check can also be performed on the specified customer credit limit to ensure that it complies with the company credit policy.

Check digits are also used for validating input. They are useful instruments to detect transpositions or transcription errors in numeric values such as account numbers. A check digit is calculated mathematically and added to the data to ensure that the original data have not been altered or an incorrect, but valid, value substituted. For example, check digits are common practice to confirm the validity of bank account numbers when they are being entered by the user.

For applications that do not require user input (e.g., information is automatically entered in the application via electronic data interchange or an interface), input validation controls can verify the completeness of the information and check for duplicates. For example, control numbers (e.g., invoice numbers) can be used to check whether missing or duplicate records (e.g., invoices for collection) are present in a data file.

Input Exception Reporting and Handling

Input errors should be identified and corrected in a timely and appropriate manner. An input exception reporting and handling control can display a warning message to the user outlining the error and potential resolution or it can stop the process from moving to the next activity if it detects exceptions. What happens will depend on the pre-determined actions, depending on the severity and type of exception. For a control to be effective and efficient, this should be well thought out from design through execution.

For example, a warning message pops up when the e-mail address space for the customer is not filled in during customer creation. However, the user can acknowledge the warning message (without filling in the e-mail address) and create the customer. Conversely, when issuing the customer invoice, the user is prevented from entering a different credit limit than the one configured in the customer master file.

An exception transaction written to an exception file, including an identification of the input errors that were detected, should be generated by the application. The exception transaction is reviewed by a designated individual who will carry out the required activities to correct the errors. The exception file is reviewed by supervisory personnel to ensure that exception transactions are cleared in a timely manner. In addition, the exception file should be reviewed by management to identify persistent exceptions that may require modification of the application controls, application exception messages/documentation or remedial training. This is an example of a hybrid application control.

PROCESSING STAGE

Controls at this stage help ensure the integrity and reliability of application processing.[22] They ensure that application data remain complete and accurate when changed as a result of application processing according to valid processing rules.

Programming Logic

Logic controls are embedded in applications to ensure that the processing of data follows pre-defined (business) logic. For example, consider a purchasing application with three-way functionality for matching purchase orders, goods receipt notes and invoices. Invoices are blocked for posting or payment when differences between the invoice and the corresponding purchase order and/or goods receipt note exceed pre-defined tolerance limits. Once invoices are validated, they can be posted automatically. Invoices with due dates exceeding pre-defined payment limits can then be sent out for management approvals.

Processing Validation

During the processing of data, certain intermediate checks can be performed to ensure that the processing steps are accurately executed. These checks are known as processing validation controls. Two of the existing techniques that can serve this purpose are:

- **Run-to-run totals**—These provide the ability to verify data values through the stages of application processing. Run-to-run total verification ensures that data read into the application were accepted and then applied to the updating process.[23] In a telecom environment, for instance, run-to-run totals might be used in the billing application to ensure that all valid calls are billed.
- **Limit or range checks**—These prevent calculation errors. The calculated amounts can be checked against pre-defined limits or ranges. For example, during the calculation of the monthly salaries of employees in a payroll application, the calculated sub-amounts (e.g., for social contributions or income taxes) can be checked against predefined value ranges. Unusual amounts can result in blocking further processing.

[22] ISACA, *CISA Review Manual 2009*, USA, 2008

[23] Federal Financial Institutions Examination Council (FFIEC), Development and Acquisition Booklet, USA, 2004, *www.ffiec.gov/ffiecinfobase/booklets/d_a/08.html*. This is one in a series of booklets updating the *1996 FFIEC Information Systems Handbook*. The booklet rescinds chapter 12 and provides examiners and financial institutions with guidance for identifying and controlling development and acquisition risks.

Processing Exception Reporting and Handling

Processed transactions or records that fail to meet the controls can be included in a suspended transactions file, typically called a 'rejected items' or 'suspense' file. These rejected transactions can be reprocessed automatically by the application when corrected or reviewed by a designated individual, who may need to make necessary adjustments to the transactions before reprocessing (e.g., purchase orders that were not processed due to stock unavailability).

OUTPUT STAGE

Controls at the output stage ensure that the data delivered by the application are correct (according to the application logic) and will be presented, formatted and delivered in a consistent and secure manner.[24]

Output Verification

The results of application processing can be verified for correctness and validity by using output verification controls. These controls can test the outcome of the processing steps in an application by means of techniques such as:[25]

- **Reasonableness verification**—The processing results are matched against a pre-defined range of reasonable values and can be rejected and submitted for manual review if they fall outside this range. For example, the monthly net salaries calculated by a payroll application can be compared for reasonableness to the previous month. If the current month's figure is not within a certain percent range of the previous month's figure, it will be rejected and submitted for review.
- **Balancing and reconciling**—Control totals are calculated based on input data (e.g., total monetary amount of orders and total number of items to be processed) and compared to output results to ensure completeness and accuracy. This method is particularly useful to verify the results of batch processing. For example, an enterprise automatically balances the total number of transactions entered in its online order entry system to the number of transactions sent to its billing system.

Output Exception Reporting and Handling

Failure to meet the output verification controls can result in the generation of an exception file and report, similar to the files and reports generated for listing input or processing errors. This file/report enables further analysis of the processing results and can require the reprocessing of input data.

The exception file is reviewed by supervisory personnel to ensure that exception transactions are cleared in a timely manner. In addition, the exception file should be reviewed by management to identify persistent exceptions that may require modification of the application controls, application exception messages/documentation or remedial training.

Output Distribution

Output distribution controls help ensure that output reports are distributed according to authorised distribution parameters. Automated distribution lists and access restrictions on information stored electronically or spooled to printers are examples of distribution controls.[26]

Output Storage and Retention

Output storage and retention controls aim to securely store and retain (or destroy) output. For example, a record retention schedule can be used. Applicable governing legal regulations should be included in the retention policy. When the retention period has passed, output should be appropriately destroyed to prevent unauthorised disclosure.

[24] *Op. cit.*, ISACA, *CISA Review Manual 2009*
[25] *Ibid.*
[26] *Op. cit.*, FFIEC, *Development and Acquisition Booklet*

PROCESSING BOUNDARY

Boundary controls are controls that are not related to a specific processing phase in the application (either input, processing or output), but rather act on the boundaries of an application to ensure that information is accurately and completely sent/received and protected from unauthorised access.

Information Protection and Authorisation

Information protection and authorisation controls are commonly used to achieve data confidentiality and integrity as well as data and application availability. These controls are related to the IT general controls concerning information security and consist of three parts:

- **Basic application security**—These are controls related to application authentication mechanisms and password parameters, user time-out settings, etc. For example, the ERP application of an enterprise might require strict password parameters (password length of minimum eight characters, password lifetime of maximum 30 days, complexity enabled, etc.) and session time-out of idle users after 30 minutes.
- **User access to application functionality via authorisation profiles**—Authorisation profiles can be used to limit to a group of authorized individuals the ability of users to input and manipulate data, execute transactions and read output results.
- **Information protection techniques**—Information protection techniques (such as encryption) are commonly used to protect data in transit or stored on computers from unauthorised viewing and manipulation or to ensure the integrity of content.

Authenticity of origin should be ensured when data are exchanged between applications to ensure that data received come from an authorised source, possibly using encryption keys. This risk is rather low when data are handled within the same application, for example, an ERP application type.

Segregation of Duties

Segregation of duties avoids the possibility that a single person could be responsible for diverse and critical functions in such a way that errors or misappropriations could occur and not be detected in a timely manner and in the normal course of (business) processes.[27]

Segregation of duties controls are usually embedded in applications by means of authorisation profiles. Users who are responsible for executing incompatible duties are assigned different authorisation profiles to ensure that they are not able to perform incompatible actions in the application. For example, in a financial application, a user should not have access to all transactions within the expenditure cycle: enter/approve purchase order, post the goods receipt note, post the supplier invoice and perform the cash disbursement. This can be accomplished by assigning different authorisation profiles to users in the expenditure cycle.

Interfaces

Interface controls should be implemented to ensure that data are accurately and completely transferred between applications. For example, this can be accomplished by including control totals in the header details of the interfaced data file. The total number of payments and the total sum of the payment amounts can be included in the header details of a payment file prepared by the purchasing application and transferred to an electronic payment application for execution of the payments. Before processing the payment file, the electronic payment application will recalculate the total number of payments included in the payment file and the total monetary amount, and will compare these values with the values included in the header details of the payment file. If the values do not match, the payment file will be rejected and will not be processed.

[27] *Op. cit.,* ISACA, *CISA Review Manual 2009*

AUDIT TRAILS AND APPLICATION JOURNALLING

Audit trails and journals provide a map to enable reconstruction or to retrace the flow of a transaction. They enable the recreation of the actual transaction flow from the point of origination to its existence on an update file.[28] They provide useful information for investigating and correcting erroneous transactions and facilitating the reconciliation of data. As an example, an accounting application might include the logging of all sensitive transactions performed by users (e.g., maintenance of the accounting period table, creation of general ledger [GL] accounts). The level and degree of application journalling in many application systems has typically been challenging, largely due to the lack of a standardised format that can be universally used for all applications. There are standardised formats for the collection of SYSLOGS, IDS alerts, Web Servers, etc., but no standardised format for application journalling (data and metadata). It is important to have a thorough understanding of the business requirements for application journalling, which should be driven by an integrated (business and technology) risk assessment and analysis of regulatory, security and compliance requirements. These requirements should feed into the application control design and implementation for that application or system.

[28] *Ibid.*

APPENDIX C—SEGREGATION OF DUTIES IN SIGNIFICANT ACCOUNTING APPLICATIONS[29]

Adequate segregation of duties is an important consideration in determining whether an enterprise's control activities are effective in achieving the objectives of internal control. The basic concept underlying segregation of duties is that no employee should be in a position both to perpetrate and to conceal errors or fraud in the normal course of his/her duties. In general, the principal incompatible duties to be segregated are:
- Authorisation or approval of related transactions affecting assets
- Custody of assets
- Recording or reporting of related transactions

Traditional systems of internal control have relied on assigning these duties to different individuals or segregating incompatible functions. Such segregation of duties is intended to prevent one person from having both access to assets and responsibility for maintaining the accountability for such assets. In the IT environment, the segregation of functions is historically considered and tested as a critical component of IT general controls. For example, companies implement controls that restrict the ability to migrate programs to production to authorised individuals. Likewise, enterprises usually segregate duties over requesting and granting access to systems and data.

However, appropriate segregation of duties is also critical at the application/business process level. For instance, in an inventory management system, different individuals are typically responsible for duties such as:
- Initiating or requesting a purchase
- Placing and inputting purchase orders
- Receiving goods
- Ensuring custody of inventories
- Maintaining inventory records and/or authorising adjustments to costs or quantities, including authorising disposal or scrapping
- Making changes to inventory master files
- Performing independent inventory counts
- Following up on inventory count discrepancies
- Authorising production requests and/or material transfers
- Receiving/transferring goods into/from manufacturing
- Shipping goods

A challenge facing many enterprises is identifying incompatible or conflicting duties at the application level. Legacy system environments necessitated and facilitated the segregation of duties because of the predominantly manual control framework surrounding them. The fragmentation of legacy systems also facilitated the segregation of duties since purchasing systems, inventory systems and general ledger systems were separate. However, this traditional notion of segregation of duties needs to be refined in a fully automated ERP system environment. ERP systems have shifted the emphasis to user empowerment, enabling users to have access across business functions or, alternatively, to handle physical assets and record their movements directly into the computing and accounting systems. The notion of segregation of duties control needs to be developed to include a risk management perspective and a trade-off balance. There are various approaches to identifying segregation of duty conflicts at the business process level. What follows are two examples of tools/templates that enterprises might be able to leverage/adapt for their environments. Template 1 in **figure 22** may be more applicable for legacy systems and template 2 in **figure 23** for integrated systems.

[29] Extracted from the IT Governance Institute publication *IT Control Objectives for Sarbanes-Oxley—The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*, USA, 2006. It should be noted that while this discussion focuses on financial applications, segregation of duties applies in other types of applications as well.

Appendix C—Segregation of Duties in Significant Accounting Applications

Figure 22 is an illustration of an approach to highlight conflicting duties performed in relation to a sales application. Similar documents need to be created for other significant applications involved in financial reporting. The template is completed by indicating the name(s) of the individual(s) responsible for each function within the applications listed. If a function is performed by a computer application, 'computer' or 'IT' can be entered as the individual.

Figure 22—Example Segregation of Duties Analysis Matrix: Sales

Sales Application				
	Authorisation	**Custody of Assets**	**Recording**	**Control Activity**
Issues sales orders				
Approves credit and credit terms				
Approves access to credit-related data files				
Authorises shipments				
Initiates shipping documents				
Handles inventories ready for shipment				
Initiates billings				
Verifies accuracy of billings				
Approves access to pricing-related data files				
Approves deviations from standard prices				
Verifies completeness of billings				
Maintains sales records				
Maintains accounts receivable records				
Reconciles shipments to billings				
Reconciles accounts receivable records to the general ledger				

After the form has been completed for each significant application, it is reviewed for any instances where one individual is performing duties that would be considered to be incompatible. Potentially incompatible duties exist if one individual performs duties in more than one category (authorisation or approval, custody or recording/reporting) or if an individual is responsible for performing a control over the same transaction that the individual is responsible for recording/reporting. In addition, when no one performs a duty, it may indicate a weakness in controls. Keep in mind that not all instances where an individual performs duties in more than one column represent a lack of segregation of duties. In addition, companies need to consider that there is the possibility of a lack of segregation of duties within the same category (e.g., the individual who authorises credit also approves the write-off of uncollectible accounts).

Once an individual is identified as performing incompatible duties, all duties performed by that individual should be considered to determine whether the effectiveness of those duties is reduced or eliminated by the lack of segregation of duties. If effectiveness is affected, the next step is to address the effects on the controls over the applications(s) and the risk of error or fraud. If an increase in risk is identified, enterprises should look for other controls that would prevent or detect such risk and assess their effectiveness. If no additional controls are identified, the risk of a reporting error would be greater due to the lack of segregation of duties.

A second approach to evaluating segregation of duties is to utilise a matrix that lists business process functions. Within the matrix, enterprises indicate which functions are compatible and would not create a conflict if performed by the same individual. As part of Sarbanes-Oxley 404 compliance, many enterprises have developed segregation of duties matrices that reflect their risk management perspective and the trade-off between functional access and security. Such templates should be modelled for each business process in the enterprise and appropriate trade-offs made between empowerment and the need to minimise the risk of fraud or unauthorised transactions. **Figure 23** is an example of applying this concept to the purchase-to-pay business function. As illustrated in the example, an 'x' indicates an incompatible function based on management's definition of incompatible duties.

Figure 23—Example Segregation of Duties Analysis Matrix: Purchase to Pay

Control Types	Control Objectives: AC1 Source Data Preparation and Authorisation	AC2 Source Data Collection and Entry	AC3 Accuracy, Completeness and Authenticity Checks	AC4 Processing Integrity and Validity	AC5 Output Review, Reconciliation and Error Handling	AC6 Transaction Authentication and Integrity
Input controls						
Input validation controls	P	S	S			
Input exception reporting and handling	S	P	S			
Processing controls						
Logical controls			P	S		
Processing validation controls			P	P		
Processing exception reporting and handling			P	P		
Output controls						
Output verification controls			S	S	P	
Output exception reporting and handling			S	S	P	
Output distribution controls					P	
Output storage and retention controls					P	
Boundary controls						
Information protection and authorisation controls	P	P	S	P	P	P
Segregation of duties controls	P	P	S	S	S	S
Interface controls			P	S	P	P
Audit trail controls						
Audit trails		S		S	S	S

P = Primary enabler; S = Secondary enabler

Appendix C—Segregation of Duties in Significant Accounting Applications

Specific techniques for automating the testing of segregation of duties are beyond the scope of this publication. However, a starting point is to consider reports that might already be available within the system itself. Software could also be considered to automate as much of the review and testing process as possible. When segregation of duties is tested using automated tools, attention needs to be paid to the completeness of data (i.e., all users, profiles and authorisations are included in the analysis) and accuracy of data (i.e., the appropriate profiles are allocated to users, and authorisations to profiles, respectively).

APPENDIX D—CONTROL PRACTICES, VALUE AND RISK DRIVERS FOR ACHIEVING APPLICATION CONTROL OBJECTIVES

AC1 Source Data Preparation and Authorisation

Control Objective	Value Drivers	Risk Drivers
Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Minimise errors and omissions through good input form design. Detect errors and irregularities so they can be reported and corrected.	• Data integrity • Standardised and authorised transaction documentation • Improved application performance • Accuracy of transaction data	• Compromised integrity of critical data • Unauthorised and/or erroneous transactions • Processing inefficiencies and rework

Control Practices

1. Design source documents in a way that they increase accuracy with which data can be recorded, control the workflow and facilitate subsequent reference checking. Where appropriate, include completeness controls in the design of the source documents.
2. Create and document procedures for preparing source data entry, and ensure that they are effectively and properly communicated to appropriate and qualified personnel. These procedures should establish and communicate required authorisation levels (input, editing, authorising, accepting and rejecting source documents). The procedures should also identify the acceptable source media for each type of transaction.
3. Ensure that the function responsible for data entry maintains a list of authorised personnel, including their signatures.
4. Ensure that all source documents include standard components and contain proper documentation (e.g., timeliness, predetermined input codes, default values) and are authorised by management.
5. Automatically assign a unique and sequential identifier (e.g., index, date and time) to every transaction.
6. Return documents that are not properly authorised or are incomplete to the submitting originators for correction, and log the fact that they have been returned. Review logs periodically to verify that corrected documents are returned by originators in a timely fashion, and to enable pattern analysis and root cause review.

AC2 Source Data Collection and Entry

Control Objective	Value Drivers	Risk Drivers
Ensure that data input is performed in a timely manner by authorised and qualified staff. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.	• Accurate data entry and efficient processing • Errors detected in a timely manner • Sensitive transaction data secured	• Processing inefficiencies due to incomplete data entry • Compromised integrity of critical data • Access control violations • Data entry errors undetected

Control Practices

1. Define and communicate criteria for timeliness, completeness and accuracy of source documents. Establish mechanisms to ensure that data input is performed in accordance with the timeliness, accuracy and completeness criteria.
2. Use only prenumbered source documents for critical transactions. If proper sequence is a transaction requirement, identify and correct out-of-sequence source documents. If completeness is an application requirement, identify and account for missing source documents.
3. Define and communicate who can input, edit, authorise, accept and reject transactions, and override errors. Implement access controls and record supporting evidence to establish accountability in line with role and responsibility definitions.
4. Define procedures to correct errors, override errors and handle out-of-balance conditions, as well as to follow up, correct, approve and resubmit source documents and transactions in timely manner. These procedures should consider things such as error message descriptions, override mechanisms and escalation levels.
5. Generate error messages in a timely manner as close to the point of origin as possible. The transactions should not be processed unless errors are corrected or appropriately overridden or bypassed. Errors that cannot be corrected immediately should be logged in an automated suspense log, and valid transaction processing should continue. Error logs should be reviewed and acted upon within a specified and reasonable period of time.
6. Ensure that errors and out-of-balance reports are reviewed by appropriate personnel, followed up and corrected within a reasonable period of time, and that, where necessary, incidents are raised for more senior attention. Automated monitoring tools should be used to identify, monitor and manage errors.
7. Ensure that source documents are safe-stored (either by the business or by IT) for a sufficient period of time in line with legal, regulatory or business requirements.

AC3 Accuracy, Completeness and Authenticity Checks

Control Objective	Value Drivers	Risk Drivers
Ensure that transactions are accurate, complete and valid. Validate data that were input, and edit or send back for correction as close to the point of origination as possible.	• Data processing errors efficiently remediated • Data accuracy, completeness and validity maintained during processing • Uninterrupted transaction processing • Segregation of duties for data entry and processing	• Processing inefficiencies and reworks due to incomplete, invalid or inaccurate data entry • Compromised integrity of critical data • Data entry errors undetected • Unauthorised data entry

Control Practices

1. Ensure that transaction data are verified as close to the data entry point as possible and interactively during online sessions. Ensure that transaction data, whether people-generated, system-generated or interfaced inputs, are subject to a variety of controls to check for accuracy, completeness and validity. Wherever possible, do not stop transaction validation after the first error is found. Provide understandable error messages immediately such that they enable efficient remediation.
2. Implement controls to ensure accuracy, completeness, validity and compliancy to regulatory requirements of data input. Controls may include sequence, limit, range, validity, reasonableness, table look-ups, existence, key verification, check digit, completeness (e.g., total monetary amount, total items, total documents, hash totals), duplicate and logical relationship checks, and time edits. Validation criteria and parameters should be subject to periodic reviews and confirmation.
3. Establish access control and role and responsibility mechanisms so that only authorised persons input, modify and authorise data.
4. Define requirements for segregation of duties for entry, modification and authorisation of transaction data as well as for validation rules. Implement automated controls and role and responsibility requirements.
5. Report transactions failing validation and post them to a suspense file. Report all errors in a timely fashion, and do not delay processing of valid transactions.
6. Ensure that transactions failing edit and validation routines are subject to appropriate follow-up until errors are remediated. Ensure that information on processing failures is maintained to allow for root cause analysis and help adjust procedures and automated controls.

AC4 Processing Integrity and Validity

Control Objective	Value Drivers	Risk Drivers
Maintain the integrity and validity of data throughout the processing cycle. Ensure that detection of erroneous transactions does not disrupt processing of valid transactions.	• Processing errors detected in a timely manner • Ability to investigate problems	• Insufficient evidence of errors or misuse • Data entry errors undetected • Unauthorised data processing

Control Practices

1. Establish and implement mechanisms to authorise the initiation of transaction processing and to enforce that only appropriate and authorised applications and tools are used.
2. Routinely verify that processing is completely and accurately performed with automated controls, where appropriate. Controls may include checking for sequence and duplication errors, transaction/record counts, referential integrity checks, control and hash totals, range checks, and buffer overflow.
3. Ensure that transactions failing validation routines are reported and posted to a suspense file. Where a file contains valid and invalid transactions, ensure that the processing of valid transactions is not delayed and that all errors are reported in a timely fashion. Ensure that information on processing failures is kept to allow for root cause analysis and help adjust procedures and automated controls, to ensure early detection or to prevent errors.
4. Ensure that transactions failing validation routines are subject to appropriate follow-up until errors are remediated or the transaction is cancelled.
5. Ensure that the correct sequence of jobs has been documented and communicated to IT operations. Job output should include sufficient information regarding subsequent jobs to ensure that data are not inappropriately added, changed or lost during processing.
6. Verify the unique and sequential identifier to every transaction (e.g., index, date and time).
7. Maintain the audit trail of transactions processed. Include date and time of input and user identification for each online or batch transaction. For sensitive data, the listing should contain before and after images and should be checked by the business owner for accuracy and authorisation of changes made.
8. Maintain the integrity of data during unexpected interruptions in data processing with system and database utilities. Ensure that controls are in place to confirm data integrity after processing failures or after use of system or database utilities to resolve operational problems. Any changes made should be reported and approved by the business owner before they are processed.
9. Ensure that adjustments, overrides and high-value transactions are reviewed promptly in detail for appropriateness by a supervisor who does not perform data entry.
10. Reconcile file totals. For example, a parallel control file that records transaction counts or monetary value as data should be processed and then compared to master file data once transactions are posted. Identify, report and act upon out-of-balance conditions.

AC5 Output Handling, Review, Reconciliation and Error Handling

Control Objective	Value Drivers	Risk Drivers
Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient and protected during transmission; that verification, detection and correction of the accuracy of output occur; and that information provided in the output is used.	• Sensitive data output protected • Complete and error-free processing results delivered to the right recipient • Errors detected in a timely manner	• Sensitive transaction data delivered to wrong recipient • Compromised data confidentiality • Inefficient transaction processing • Transaction data output errors undetected

Control Practices

1. When handling and retaining output from IT applications, follow defined procedures and consider privacy and security requirements. Define, communicate and follow procedures for the distribution of output.
2. At appropriate intervals, take a physical inventory of all sensitive output, such as negotiable instruments, and compare it with inventory records. Create procedures with audit trails to account for all exceptions and rejections of sensitive output documents.
3. Match control totals in the header and/or trailer records of the output to balance with the control totals produced by the system at data entry to ensure completeness and accuracy of processing. If out-of-balance control totals exist, report them to the appropriate level of management.
4. Validate completeness and accuracy of processing before other operations are performed. If electronic output is reused, ensure that validation has occurred prior to subsequent uses.
5. Define and implement procedures to ensure that the business owners review the final output for reasonableness, accuracy and completeness, and that output is handled in line with the applicable confidentiality classification. Report potential errors, log them in an automated, centralised logging facility, and address errors in a timely manner.
6. If the application produces sensitive output, define who can receive it, label the output so it is recognisable by people and machines, and implement distribution accordingly. Where necessary, send it to special access-controlled output devices.

AC6 Transaction Authentication and Integrity

Control Objective	Value Drivers	Risk Drivers
Before passing transaction data between internal applications and business/operational functions (in or outside the enterprise), check it for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.	• Straight-through processing • Confidence in validity and authenticity of transactions • Errors and misuse prevented	• Erroneous and/or unauthorised transactions • Transaction errors undetected • Inefficiencies and rework

Control Practices

1. Where transactions are exchanged electronically, establish an agreed-upon standard of communication and mechanisms necessary for mutual authentication, including how transactions will be represented, the responsibilities of both parties and how exception conditions will be handled.
2. Tag output from transaction processing applications in accordance with industry standards to facilitate counterparty authentication, provide evidence of non-repudiation, and allow for content integrity verification upon receipt by the downstream application.
3. Analyse input received from other transaction processing applications to determine authenticity of origin and the maintenance of the integrity of content during transmission.

APPENDIX E—TOOLS FOR DESIGNING AND IMPLEMENTING APPLICATION CONTROLS

DEFINING APPLICATION CONTROL REQUIREMENTS/IDENTIFYING RELEVANT APPLICATION CONTROL OBJECTIVES

Chapter 4 discusses management's responsibilities for identifying relevant application control objectives as part of defining the business requirements for new automated solutions. COBIT Online can be used by management as a tool for determining relevant application control objectives. **Figure 24** is a screen image showing how COBIT Online can be used to identify and assess the importance of the application control objectives for a given automated solution.

Figure 24—MyCOBIT Control Objectives Assessment Form

AC—Application Controls

Process: AC – Application Controls	**Importance to the Enterprise**
	Unimportant ☐ Somewhat Important ☐ Important ☐ Very Important ☐ Critical ☐

	Relevance						**Compliance State** "C"=Current, "P"=Planned							**Evidence**
	Not Relevant	Somewhat	Relevant	Very	Critical	Covered by other objective	Management is not aware	Management is aware	Management is committed to resolve	Implementation is getting started	Implementation is well underway	Solution is implemented	Solution is sustainable	
Control Objective: 1.1. Source Data Preparation and Authorisation														
Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Minimise errors and omissions through good input form design. Detect errors and irregularities so they can be reported and corrected. Expedience: Medium Sustainability: High Effectiveness: High } Contribution: Very High Effort: Very High														

Figure 24—MyCobiT Control Objectives Assessment Form *(cont.)*

AC—Application Controls

Process: AC – Application Controls	**Importance to the Enterprise**
	Unimportant ☐ Somewhat Important ☐ Important ☐ Very Important ☐ Critical ☐

	Relevance						**Compliance State** “C”=Current, “P”=Planned							**Evidence**
	Not Relevant	Somewhat	Relevant	Very	Critical	Covered by other objective	Management is not aware	Management is aware	Management is committed to resolve	Implementation is getting started	Implementation is well underway	Solution is implemented	Solution is sustainable	
Control Objective: 1.2. Source Data Collection and Entry														
Ensure that data input is performed in a timely manner by authorised and qualified staff. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time. Expedience: High Sustainability: High Effectiveness: High } Contribution: Very High Effort: Very High														
Control Objective: 1.3. Accuracy, Completeness and Authenticity Checks														
Ensure that transactions are accurate, complete and valid. Validate data that were input, and edit or send back for correction as close to the point of origination as possible. Expedience: Medium Sustainability: High Effectiveness: High } Contribution: Very High Effort: Very High														

Figure 24—MyCobiT Control Objectives Assessment Form *(cont.)*

AC—Application Controls

Process: AC – Application Controls	**Importance to the Enterprise**
	Unimportant ☐ Somewhat Important ☐ Important ☐ Very Important ☐ Critical ☐

	Relevance						**Compliance State** “C”=Current, “P”=Planned							**Evidence**
	Not Relevant	Somewhat	Relevant	Very	Critical	Covered by other objective	Management is not aware	Management is aware	Management is committed to resolve	Implementation is getting started	Implementation is well underway	Solution is implemented	Solution is sustainable	
Control Objective: 1.4. Processing Integrity and Validity														
Maintain the integrity and validity of data throughout the processing cycle. Ensure that detection of erroneous transactions does not disrupt processing of valid transactions. Expedience: Medium Sustainability: High Effectiveness: High } Contribution: Very High Effort: Very High														
Control Objective: 1.5. Output Review, Reconciliation and Error Handling														
Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient and protected during transmission; that verification, detection and correction of the accuracy of output occur; and that information provided in the output is used. Expedience: Medium Sustainability: Medium Effectiveness: High } Contribution: High Effort: High														

Figure 24—MyCobiT Control Objectives Assessment Form *(cont.)*

AC—Application Controls

Process: AC – Application Controls	**Importance to the Enterprise**
	Unimportant ☐ Somewhat Important ☐ Important ☐ Very Important ☐ Critical ☐

	Relevance						**Compliance State** “C”=Current, “P”=Planned							**Evidence**
	Not Relevant	Somewhat	Relevant	Very	Critical	Covered by other objective	Management is not aware	Management is aware	Management is committed to resolve	Implementation is getting started	Implementation is well underway	Solution is implemented	Solution is sustainable	
Control Objective: 1.6. Transaction Authentication and Integrity														
Before passing transaction data between internal applications and business operational functions (in or outside the enterprise), check it for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport. Expedience: Medium Sustainability: Medium Effectiveness: High } Contribution: High Effort: High														

TEMPLATE FOR DESIGN OF APPLICATION CONTROLS

Figure 25 is an example of a template that may be useful for members of the application solution design team to assist in the design of application controls. This template can be used to capture key elements of designed controls, including their respective attributes, and provides for a conclusion as to whether the controls achieve the respective control objectives. Control information is presented in a way to facilitate management review and approval as part of its responsibilities to ensure the adequacy of design of application controls, as discussed in chapter 4. Control practices in this table have been provided from the *IT Assurance Guide: Using COBIT* and will need to be updated to meet specific requirements of each application solution.

Figure 25—Template for Assisting in the Design of Application Controls

Process/Application Name — **Application Control Design**

Business Process Owner: — **Date:**

Ref	Control Objective and Control Practices Description	Information Objective					Information Criteria							Control Activity Attributes					Design Effectiveness Conclusion
		Completeness	Accuracy	Validity	Authorisation	Segregation of Duties	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Type - Manual - Automated - Hybrid - Configurable	Nature - Preventive - Detective	Frequency - Transaction - Daily - Weekly - Monthly - Annually	Proximity - Point of risk - After risk event - Management review	Performed by - Insert role	
AC1	**Source Data Preparation and Authorisation** Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents.																		
1	Design source documents in a way that they increase accuracy with which data can be recorded, control the workflow and facilitate subsequent reference checking. Where appropriate, include completeness controls in the design of the source documents.																		
2	Create and document procedures for preparing source data entry, and ensure that they are effectively and properly communicated to appropriate and qualified personnel. These procedures should establish and communicate required authorisation levels (input, editing, authorising, accepting and rejecting source documents). The procedures should also identify the acceptable source media for each type of transaction.																		
3	Ensure that the function responsible for data entry maintains a list of authorised personnel, including their signatures.																		

Figure 25—Template for Assisting in the Design of Application Controls *(cont.)*

Process/Application Name | **Application Control Design**

Business Process Owner: | **Date:**

Ref		Control Objective and Control Practices Description	Information Objective					Information Criteria							Control Activity Attributes					Design Effectiveness Conclusion
			Completeness	Accuracy	Validity	Authorisation	Segregation of Duties	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	**Type** - Manual - Automated - Hybrid - Configurable	**Nature** - Preventive - Detective	**Frequency** - Transaction - Daily - Weekly - Monthly - Annually	**Proximity** - Point of risk - After risk event - Management review	**Performed by** - Insert role	
AC1 *cont.*	4	Ensure that all source documents include standard components and contain proper documentation (e.g., timeliness, predetermined input codes, default values) and are authorised by management.																		
	5	Automatically assign a unique and sequential identifier (e.g., index, date and time) to every transaction.																		
	6	Return documents that are not properly authorised or are incomplete to the submitting originators for correction, and log the fact that they have been returned. Review logs periodically to verify that corrected documents are returned by originators in a timely fashion, and to enable pattern analysis and root cause review.																		
AC2		**Source Data Collection and Entry** Establish that data input is performed in a timely manner by authorised and qualified staff. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.																		
	1	Define and communicate criteria for timeliness, completeness and accuracy of source documents. Establish mechanisms to ensure that data input is performed in accordance with the timeliness, accuracy and completeness criteria.																		
	2	Use only prenumbered source documents for critical transactions. If proper sequence is a transaction requirement, identify and correct out-of-sequence source documents. If completeness is an application requirement, identify and account for missing source documents.																		

Figure 25—Template for Assisting in the Design of Application Controls *(cont.)*

Process/Application Name | **Application Control Design**

Business Process Owner: | **Date:**

Ref		Control Objective and Control Practices Description	Information Objective					Information Criteria							Control Activity Attributes					Design Effectiveness Conclusion
			Completeness	Accuracy	Validity	Authorisation	Segregation of Duties	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	**Type** - Manual - Automated - Hybrid - Configurable	**Nature** - Preventive - Detective	**Frequency** - Transaction - Daily - Weekly - Monthly - Annually	**Proximity** - Point of risk - After risk event - Management review	**Performed by** - Insert role	
AC2 *cont.*	3	Define and communicate who can input, edit, authorise, accept and reject transactions, and override errors. Implement access controls and record supporting evidence to establish accountability in line with role and responsibility definitions.																		
	4	Define procedures to correct errors, override errors and handle out-of-balance conditions, as well as to follow up, correct, approve and resubmit source documents and transactions in timely manner. These procedures should consider things such as error message descriptions, override mechanisms and escalation levels.																		
	5	Generate error messages in a timely manner as close to the point of origin as possible. The transactions should not be processed unless errors are corrected or appropriately overridden or bypassed. Errors that cannot be corrected immediately should be logged in an automated suspense log, and valid transaction processing should continue. Error logs should be reviewed and acted upon within a specified and reasonable period of time.																		

Figure 25—Template for Assisting in the Design of Application Controls *(cont.)*

Process/Application Name | **Application Control Design**

Business Process Owner: | **Date:**

Ref		Control Objective and Control Practices Description	Information Objective					Information Criteria							Control Activity Attributes					Design Effectiveness Conclusion
			Completeness	Accuracy	Validity	Authorisation	Segregation of Duties	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	**Type** - Manual - Automated - Hybrid - Configurable	**Nature** - Preventive - Detective	**Frequency** - Transaction - Daily - Weekly - Monthly - Annually	**Proximity** - Point of risk - After risk event - Management review	**Performed by** - Insert role	
AC2 *cont.*	6	Ensure that errors and out-of-balance reports are reviewed by appropriate personnel, followed up and corrected within a reasonable period of time, and that, where necessary, incidents are raised for more senior attention. Automated monitoring tools should be used to identify, monitor and manage errors.																		
	7	Ensure that source documents are safe-stored (either by the business or by IT) for a sufficient period of time in line with legal, regulatory or business requirements.																		
AC3	**Accuracy, Completeness and Authenticity Checks** Ensure that transactions are accurate, complete and valid. Validate data that were input, and edit or send back for correction as close to the point of origination as possible.																			
	1	Ensure that transaction data are verified as close to the data entry point as possible and interactively during online sessions. Ensure that transaction data, whether people-generated, system-generated or interfaced inputs, are subject to a variety of controls to check for accuracy, completeness and validity. Wherever possible, do not stop transaction validation after the first error is found. Provide understandable error messages immediately such that they enable efficient remediation.																		

Figure 25—Template for Assisting in the Design of Application Controls *(cont.)*

Process/Application Name | **Application Control Design**

Business Process Owner: | **Date:**

Ref		Control Objective and Control Practices Description	Information Objective					Information Criteria							Control Activity Attributes					Design Effectiveness Conclusion
			Completeness	Accuracy	Validity	Authorisation	Segregation of Duties	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	**Type** - Manual - Automated - Hybrid - Configurable	**Nature** - Preventive - Detective	**Frequency** - Transaction - Daily - Weekly - Monthly - Annually	**Proximity** - Point of risk - After risk event - Management review	**Performed by** - Insert role	
AC3 *cont.*	2	Implement controls to ensure accuracy, completeness, validity and compliancy to regulatory requirements of data input. Controls may include sequence, limit, range, validity, reasonableness, table look-ups, existence, key verification, check digit, completeness (e.g., total monetary amount, total items, total documents, hash totals), duplicate and logical relationship checks, and time edits. Validation criteria and parameters should be subject to periodic reviews and conformation.																		
	3	Establish access control and role and responsibility mechanisms so that only authorised persons input, modify and authorise data.																		
	4	Define requirements for segregation of duties for entry, modification and authorisation of transaction data as well as for validation rules. Implement automated controls and role and responsibility requirements.																		
	5	Report transactions failing validation and post them to a suspense file. Report all errors in a timely fashion, and do not delay processing of valid transactions.																		
	6	Ensure that transactions failing edit and validation routines are subject to appropriate follow-up until errors are remediated. Ensure that information on processing failures is maintained to allow for root cause analysis and help adjust procedures and automated controls.																		

Figure 25—Template for Assisting in the Design of Application Controls *(cont.)*

Process/Application Name | **Application Control Design**

Business Process Owner: | **Date:**

Ref	Control Objective and Control Practices Description	Information Objective					Information Criteria							Control Activity Attributes					Design Effectiveness Conclusion
		Completeness	Accuracy	Validity	Authorisation	Segregation of Duties	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	**Type** - Manual - Automated - Hybrid - Configurable	**Nature** - Preventive - Detective	**Frequency** - Transaction - Daily - Weekly - Monthly - Annually	**Proximity** - Point of risk - After risk event - Management review	**Performed by** - Insert role	
AC4	**Processing Integrity and Validity** Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions does not disrupt the processing of valid transactions.																		
	1 Establish and implement mechanisms to authorise the initiation of transaction processing and to enforce that only appropriate and authorised applications and tools are used.																		
	2 Routinely verify that processing is completely and accurately performed with automated controls, where appropriate. Controls may include checking for sequence and duplication errors, transaction/record counts, referential integrity checks, control and hash totals, range checks, and buffer overflow.																		
	3 Ensure that transactions failing validation routines are reported and posted to a suspense file. Where a file contains valid and invalid transactions, ensure that the processing of valid transactions is not delayed and that all errors are reported in a timely fashion. Ensure that information on processing failures is kept to allow for root cause analysis and help adjust procedures and automated controls, to ensure early detection or to prevent errors.																		
	4 Ensure that transactions failing validation routines are subject to appropriate follow-up until errors are remediated or the transaction is cancelled.																		

Figure 25—Template for Assisting in the Design of Application Controls *(cont.)*

Process/Application Name | **Application Control Design**

Business Process Owner: | **Date:**

Ref		Control Objective and Control Practices Description	Information Objective					Information Criteria							Control Activity Attributes					Design Effectiveness Conclusion
			Completeness	Accuracy	Validity	Authorisation	Segregation of Duties	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	**Type** - Manual - Automated - Hybrid - Configurable	**Nature** - Preventive - Detective	**Frequency** - Transaction - Daily - Weekly - Monthly - Annually	**Proximity** - Point of risk - After risk event - Management review	**Performed by** - Insert role	
AC4 *cont.*	5	Ensure that the correct sequence of jobs has been documented and communicated to IT operations. Job output should include sufficient information regarding subsequent jobs to ensure that data are not inappropriately added, changed or lost during processing.																		
	6	Verify the unique and sequential identifier to every transaction (e.g., index, date and time).																		
	7	Maintain the audit trail of transactions processed. Include date and time of input and user identification for each online or batch transaction. For sensitive data, the listing should contain before and after images and should be checked by the business owner for accuracy and authorisation of changes made.																		
	8	Maintain the integrity of data during unexpected interruptions in data processing with system and database utilities. Ensure that controls are in place to confirm data integrity after processing failures or after use of system or database utilities to resolve operational problems. Any changes made should be reported and approved by the business owner before they are processed.																		

Figure 25—Template for Assisting in the Design of Application Controls *(cont.)*

Process/Application Name | **Application Control Design**

Business Process Owner: | **Date:**

Ref		Control Objective and Control Practices Description	Information Objective					Information Criteria							Control Activity Attributes					Design Effectiveness Conclusion
			Completeness	Accuracy	Validity	Authorisation	Segregation of Duties	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Type - Manual - Automated - Hybrid - Configurable	Nature - Preventive - Detective	Frequency - Transaction - Daily - Weekly - Monthly - Annually	Proximity - Point of risk - After risk event - Management review	Performed by - Insert role	
AC4 *cont.*	9	Ensure that adjustments, overrides and high-value transactions are reviewed promptly in detail for appropriateness by a supervisor who does not perform data entry.																		
	10	Reconcile file totals. For example, a parallel control file that records transaction counts or monetary value as data should be processed and then compared to master file data once transactions are posted. Identify, report and act upon out-of-balance conditions.																		
AC5		**Output Review, Reconciliation and Error Handling** Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient, and protected during transmission; that verification, detection and correction of the accuracy of output occurs; and that information provided in the output is used.																		
	1	When handling and retaining output from IT applications, follow defined procedures and consider privacy and security requirements. Define, communicate and follow procedures for the distribution of output.																		
	2	At appropriate intervals, take a physical inventory of all sensitive output, such as negotiable instruments, and compare it with inventory records. Create procedures with audit trails to account for all exceptions and rejections of sensitive output documents.																		
	3	Match control totals in the header and/or trailer records of the output to balance with the control totals produced by the system at data entry to ensure completeness and accuracy of processing. If out-of-balance control totals exist, report them to the appropriate level of management.																		
	4	Validate completeness and accuracy of processing before other operations are performed. If electronic output is reused, ensure that validation has occurred prior to subsequent uses.																		

Figure 25—Template for Assisting in the Design of Application Controls *(cont.)*

Process/Application Name | **Application Control Design**

Business Process Owner: | **Date:**

Ref		Control Objective and Control Practices Description	Information Objective					Information Criteria							Control Activity Attributes					Design Effectiveness Conclusion
			Completeness	Accuracy	Validity	Authorisation	Segregation of Duties	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Type - Manual - Automated - Hybrid - Configurable	Nature - Preventive - Detective	Frequency - Transaction - Daily - Weekly - Monthly - Annually	Proximity - Point of risk - After risk event - Management review	Performed by - Insert role	
AC5 *cont.*	5	Define and implement procedures to ensure that the business owners review the final output for reasonableness, accuracy and completeness, and that output is handled in line with the applicable confidentiality classification. Report potential errors, log them in an automated, centralised logging facility, and address errors in a timely manner.																		
	6	If the application produces sensitive output, define who can receive it, label the output so it is recognisable by people and machines, and implement distribution accordingly. Where necessary, send it to special access-controlled output devices.																		
AC6		**Transaction Authentication and Integrity** Before passing transaction data between internal applications and business/operational functions (in or outside the enterprise), check it for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.																		
	1	Where transactions are exchanged electronically, establish an agreed-upon standard of communication, including how transactions will be represented, the responsibilities of both parties, how exception conditions will be handled and mechanisms necessary for mutual authentication.																		
	2	Tag output from transaction processing applications in accordance with industry standards to facilitate counterparty authentication, provide evidence of non-repudiation, and allow for content integrity verification upon receipt by the downstream application.																		
	3	Analyse input received from other transaction processing applications to determine authenticity of origin and the maintenance of the integrity of content during transmission.																		

APPENDIX F—COMMON ISSUES AND CHALLENGES WITH APPLICATION CONTROLS

Figure 26 includes guidance on some of the common risks and challenges associated with application control design, implementation, operation and maintenance, and presents related potential control practices to reduce these risks and challenges.

Figure 26—Risks and Challenges of Application Controls

Type of Application	Application Controls Life Cycle	Risk Indicator (What Could Go Wrong)	Control Practices
Vendor packaged software (as-is, off the shelf)	Identify relevant control objectives and related controls.	The vendor solution does not include key automated application control activities.	Perform gap analysis between application control requirements and vendor solution. Consider alternative control activities that may be required to address control gaps and operational impact. Include assessment of gap analysis in overall solution evaluation.
	Design/build/configure application controls.	Parameter tables are inappropriately configured.	Establish acceptance criteria for configurable control design and operating effectiveness. Measure operating effectiveness prior to implementation.
	Design/build/configure application controls.	There are errors in data transfers between new and legacy applications.	Include interfaces in application control design, implementation, operation and maintenance activities.
	Test application controls.	Vendor solution application controls are not functioning as intended.	Incorporate application controls in test planning and execution. Monitor status of testing errors. Business process owner signs off on test results and acceptance criteria.
	Ensure application control maintenance.	There are unauthorised changes to configuration parameters.	Implement formal change management processes for key configurable controls and configuration parameters. Utilise continuous control monitoring tools.
	Ensure application control maintenance.	There are unauthorised changes to user-managed configuration tables.	Implement approval controls to authorise user-managed table changes. Supervisor reviews table change activity reports.

Figure 26—Risks and Challenges of Application Controls *(cont.)*			
Type of Application	**Application Controls Life Cycle**	**Risk Indicator (What Could Go Wrong)**	**Control Practices**
Custom or in-house developed solutions	Identify relevant control objectives and related controls.	Application control requirements are not defined.	Define roles and responsibilities for application control design. Business process owner approves of application control requirements/ objectives prior to functional design.
	Design/build/configure application controls.	The solution does not include key automated application control activities. Application controls are not functioning as intended.	Define roles and responsibilities for application control design. Require business process owner approval of application control design prior to development. Incorporate application control acceptance criteria during test planning and execution. Business process owner signs off on application control testing.
	Ensure application controls operation and maintenance.	Application control failures are not identified or escalated.	Include assessment of impact to information criteria and escalation protocols as part of incident management processes. Utilise continuous controls monitoring tools.
	Ensure application controls operation and maintenance.	There are unauthorised changes to application controls.	Restrict developer access to production application environment. Implement formal change management processes and controls.
Fourth-generation tool solutions/end-user computing (e.g., Excel, SQL Queries, Cognos)	Design/build/configure application controls.	Relevant control objectives/activities are not incorporated into solutions.	Include fourth-generation tools in roles and responsibilities definitions. Prioritise solutions based on business risks. Segregate incompatible activities of development, testing and operation based on risk assessment of application solution.
	Ensure application controls operation and maintenance.	Changes to fourth-generation solutions introduce undetected errors.	Segregate incompatible activities of development, testing and operation based on risk assessment of application solution. Formalise change management processes for high-risk applications.

APPENDIX G—OVERVIEW OF COBIT

COBIT, developed by the IT Governance Institute, is a governance framework and supporting tool set that IT organisations can use to ensure that IT is working as effectively as possible to minimise risk and maximise the benefits of technology investments. In doing so, it allows an IT function to judge its own efforts against standard industry practices as well as the expectations of management and auditors.

COBIT is a uniquely comprehensive management approach to ensuring that IT is meeting the needs of the business. It is a high-level framework that harmonises more detailed international standards and guidance. Organisations that improve the management of IT based on COBIT benefit from:
- Better quality IT services
- More successful IT projects
- Improved efficiency and optimisation of costs
- Improved information security and privacy
- Easier compliance
- Reduced operational risk
- Improved management confidence and trust

COBIT helps to develop an IT function's processes in a comprehensive, integrated manner based on accepted best practice. COBIT provides management guidance and tools in the following areas:
- Strategic alignment of IT with business goals
- Value delivery of services and new projects
- Risk management
- Resource management
- Performance measurement

COBIT allows management to design IT processes and map the IT-related roles and responsibilities within an enterprise to four main process areas following the Plan, Build, Run and Monitor life cycle. Within these domains the management of IT in an enterprise is organised into processes with clear ownership and responsibilities. Measurement tools enable IT's goals to align to the enterprise's strategic goals.

COBIT provides an end-to-end view of the processes and procedures that are essential for successful management by the enterprise of IT. As such, its adoption is being driven by many executives and CIOs at large and small enterprises around the world. It is accepted by regulators and audit bodies and is mapped to industry standards.

COBIT is freely available for download from *www.isaca.org/cobit.*

COBIT 4.1 includes all of the following:
- Framework—Explains how COBIT organises IT governance management and control objectives, and good practices by IT domains and processes, and links them to business requirements
- Process descriptions—Include 34 IT processes covering the IT responsibility areas from beginning to end
- Control objectives—Provide generic good practice management objectives for IT processes
- Management guidelines—Offer tools to help assign responsibility, measure performance, and benchmark and address gaps in capability
- Maturity models—Provide profiles of IT processes describing possible current and future states

CobiT® and Application Controls

In the years since its inception, CobiT's core content has continued to evolve and the number of CobiT-based derivative works has increased. Following are the publications currently derived from CobiT:

- *Board Briefing on IT Governance, 2nd Edition*—Helps executives understand why IT governance is important, what its issues are and what their responsibility is for managing it
- CobiT® Online—Allows users to customise a version of CobiT for their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys, frequently asked questions, benchmarking and a discussion facility for sharing experiences and questions.
- *CobiT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*—Provides guidance on the risks to be avoided and value to be gained from implementing a control objective, and instruction on how to implement the objective. Control practices are strongly recommended for use with the *IT Governance Implementation Guide: Using CobiT® and Val IT™, 2nd Edition*.
- *IT Assurance Guide: Using CobiT®*—Provides guidance on how CobiT can be used to support a variety of assurance activities and offers suggested testing steps for all of the CobiT IT processes and control objectives. It is also useful for performing self-assessment against the control objectives in CobiT® 4.1.
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*—Provides guidance on how to assure compliance for the IT environment based on the CobiT control objectives
- *IT Governance Implementation Guide: Using CobiT® and Val IT™, 2nd Edition*—Provides a generic road map for implementing IT governance using CobiT and Val IT resources and a supporting tool kit
- *CobiT® Quickstart, 2nd Edition*—Provides a baseline of control for the smaller enterprise and a possible first step for the larger enterprise
- *CobiT® Security Baseline, 2nd Edition*—Focuses on essential steps for implementing information security within the enterprise.
- CobiT® Mappings—Currently posted at *www.isaca.org/downloads*:
  - *Aligning CobiT® 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit*
  - *CobiT® Mapping: Mapping of CMMI® for Development V1.2 With CobiT® 4.0*
  - *CobiT® Mapping: Mapping of ISO/IEC 17799:2000 With CobiT®, 2nd Edition*
  - *CobiT® Mapping: Mapping of ISO/IEC 17799:2005 With CobiT® 4.0*
  - *CobiT® Mapping: Mapping of ITIL With CobiT® 4.0*
  - *CobiT® Mapping: Mapping of ITIL V3 With CobiT® 4.1*
  - *CobiT® Mapping: Mapping of NIST SP800-53 With CobiT® 4.1*
  - *CobiT® Mapping: Mapping of PMBOK With CobiT® 4.0*
  - *CobiT® Mapping: Mapping of PRINCE2 With CobiT® 4.0*
  - *CobiT® Mapping: Mapping of SEI's CMM for Software With CobiT® 4.0*
  - *CobiT® Mapping: Mapping of TOGAF 8.1 With CobiT® 4.0*
  - *CobiT® Mapping: Overview of International IT Guidance, 2nd Edition*
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*—Presents information security in business terms and contains tools and techniques to help uncover security-related problems.

Val IT is the umbrella term used to describe the publications and future additional products and activities addressing the Val IT framework.

Current Val IT-related publications are:

- *Value Management: Getting Started, How to Begin Creating Value Through IT-Enabled Business Investments, An Executive Primer Based on the Val IT Framework*—This publication provides an easy-to-follow guide on getting a value management initiative started for business and IT executives and organisational leaders.
- *Enterprise Value: Governance of IT Investments—The Val IT Framework 2.0*, which explains how an enterprise can extract optimal value from IT-enabled investments and is based on the COBIT framework. It is organised into:
  - Three processes—Value Governance, Portfolio Management and Investment Management
  - IT key management practices—Essential management practices that positively influence the achievement of the desired result or purpose of a particular activity. They support the Val IT processes and play roughly the same role as do COBIT's control objectives.
- *Enterprise Value: Governance of IT Investments—The Business Case*, which focuses on one key element of the investment management process

APPENDIX H—SUMMARY OF KEY MESSAGES

Throughout this publication, several key points have been identified to highlight and reinforce important messages for management's consideration. These key messages are summarised as follows.

CHAPTER 4. DESIGN AND IMPLEMENTATION OF APPLICATION CONTROLS

1. Enterprises regularly consider business and functional requirements as part of application design, but mostly do not explicitly consider 'control' requirements. This can create implementation and operational challenges if necessary controls are not built into the solution from the start and a 'retrofit' of control activities post-implementation is required. In addition to the costs associated with fixing integrity problems, retrofitting controls post-implementation can be very costly. Management should ensure that control requirements are appropriately identified, based on the business risks, and included in functional requirements.
2. Management can optimise the efficiency and effectiveness of its control design through a balance of various attributes, types and nature of control activities. For example:
   - Should a given control activity be a manual activity, automated or some combination of both—a hybrid control? If automated, should the control be designed to be 'configurable' to facilitate changes to business rules over time?
   - Is it more cost-effective/efficient to design the control activity to prevent errors from occurring or to design a procedure that would detect any error situations should they arise?
   - Are the frequency of the control, the proximity of the control activity to the risk event and the role of the individual performing the activity going to be sufficient to reduce the risk of error conditions to an acceptable level?
   - Will the benefits to be realised from reducing a risk outweigh the cost of building, testing and performing the added control activity?
3. Because testing validates whether or not the designed control activities operate as they were intended, it is essential that the systems accreditation activities include testing of these application control activities. Having a clearly documented trail of testing automated application controls and the automated components of hybrid and configurable controls may also provide the necessary evidence to demonstrate the effective operation of these controls. Having a clearly documented trail of testing/validation of manual controls and the manual activities associated with hybrid controls can reinforce their viability and user understanding of the activities.
4. In approving the design and implementation of application controls, management needs to consider the relative efficiency and effectiveness associated with various control design choices and be satisfied that the controls designed are cost-effective and achieve the control objectives, and the relevant information criteria are satisfied.
5. Assessing risks, identifying relevant control objectives and determining the sufficiency of design of application controls are as relevant to existing applications as they are to new applications being acquired/developed and implemented.
6. Automated application controls should be used where possible to provide a more cost-effective and sustainable system of internal controls, but they require effective IT general controls.
7. Responsibility for design and implementation of application controls is shared. Business management is accountable for ensuring that application control requirements have been appropriately designed and implemented to meet the business objectives. IT management is accountable for developing application controls in accordance with business requirements.

CHAPTER 5. OPERATION AND MAINTENANCE OF APPLICATION CONTROLS

8. Ongoing monitoring of application controls is important and necessary to ensure their continuing effectiveness. Key elements for management to consider include:
   - Periodically re-assessing application control effectiveness
   - Monitoring effective operation of manual control activities, including the manual component of hybrid controls
   - Monitoring automated control activities (including the automated component of hybrid controls) to ensure that they continue to operate as intended
   - Monitoring effective operation of application controls delegated and performed by other parties
   - Monitoring business process and application control key performance indicators (KPIs) that may indicate a control failure
9. Continuous controls monitoring (CCM) can be an effective mechanism for management to monitor the ongoing effectiveness of its internal control activities.
10. Responsibility and accountability for operating and maintaining application controls are shared between business management and IT. Business management is accountable for monitoring the ongoing effectiveness of the application controls and for identifying and defining requirements for changes to application controls. IT is accountable for providing a reliable environment for operating the application and related automated application controls and for developing/delivering changes based on user requirements.
11. Periodic assessment of the maturity of application control design, implementation, operation and maintenance processes can be an effective tool to monitor ongoing reliability and identify improvement opportunities.

CHAPTER 6. RELATION AND DEPENDENCIES OF APPLICATION CONTROLS WITH IT GENERAL CONTROLS

12. Application controls, especially automated application controls and the automated components of hybrid and configurable controls, are dependent on the reliable operation of the IT environment in which the application operates. IT general control deficiencies in this environment can impair the operating effectiveness of application controls, while effective IT general controls can provide opportunities to increase reliance on automated application controls.

CHAPTER 7. APPLICATION CONTROLS ASSURANCE

13. The concept of providing assurance is commonly thought of in the context of an auditor (either internal or external) providing assurance to management, the board of directors and the shareholders. However, the concept is increasingly relevant to financial and operational management in terms of providing assurance to relevant stakeholders. Examples where management is providing assurance to stakeholders include CEO/CFO certification of the design and operating effectiveness of internal controls as required by legislation such as Sarbanes-Oxley, and line management (such as the CIO) providing 'sub-certification' to the CEO/CFO on the effectiveness of controls within its operating units.
14. It may be more efficient and cost-effective for assurance providers to rely on automated application controls, where possible, since this may reduce the costs associated with validating the operating effectiveness of manual activities. With effective IT general controls, a benchmarking strategy may further reduce operating effectiveness validation cost and effort.

APPENDIX I—GLOSSARY

Application benchmarking—The process of establishing the effective design and operation of automated controls within an application

Application controls—Policies, procedures and activities designed to provide reasonable assurance that objectives relevant to a given automated solution (application) are achieved

Automated application controls—Controls that have been programmed and embedded within an application

Computer-dependent application controls –See hybrid application controls

Configurable controls—Typically automated controls that are based on and, therefore, dependent on the configuration of parameters within the application system

Control objective—A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process[30]

Detective application controls—Controls designed to detect errors that may have occurred, based on predefined logic or business rules. Detective application controls are usually executed after an action has taken place and often cover a group of transactions.

General computer controls—Controls, other than application controls, that relate to the environment within which computer-based application systems are developed, maintained and operated, and which are therefore applicable to all applications. The objectives of general controls are to ensure the proper development and implementation of applications, as wellas ensure the integrity of program and data files and of computer operations. Like application controls, general controls may be either manual or programmed. Examples of general controls include the development and implementation of an IS strategy and an IS security policy, the organisation of IS staff to separate conflicting duties, and planning for disaster prevention and recovery.[31]

Hybrid application controls—Controls that consist of a combination of manual and automated activities, all of which must operate for the control to be effective; sometimes referred to as computer-dependent application controls

Information criteria—Attributes of information that must be satisfied to meet business requirements. COBIT uses seven information criteria: effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability.

Preventive application controls—Application controls that are intended to prevent an error from occurring. Preventive application controls are typically executed at the transaction level, before an action is performed.

Process—Generally, a collection of activities influenced by the enterprise's policies and procedures that takes inputs from a number of sources, (including other processes), manipulates the inputs and produces outputs. Scope note: Processes have clear business reasons for existing, accountable owners, clear roles and responsibilities around the execution of the process, and the means to measure performance.[32]

[30] *Op. cit.,* IT Governance Institute, COBIT 4.1, p.190
[31] *Ibid.*
[32] *Ibid.*, p.192

Transparency—Refers to an enterprise's openness about its activities and is based on the concepts:
• It is clear to those who are affected by or want to challenge governance decisions regarding how the mechanism functions
• A common vocabulary has been established
• Relevant information is readily available
Scope note: Transparency and stakeholder trust are directly related; the more transparency in the governance process, the more confidence in the governance.

APPENDIX J—REFERENCES AND ADDITIONAL SOURCES OF INFORMATION

American Institute of Certified Public Accountants (AICPA), 'Audit and Accounting Guides', USA, 2008 *www.aicpa.org*

Brancik, Kenneth C.; 'Insider Computer Fraud', Auerbach Publications, USA, 2008

The Committee of Sponsoring Organisations of the Treadway Commission (COSO), *Enterprise Risk Management—Integrated Framework*, USA, 2004, *www.coso.org*

Federal Financial Institutions Examination Council (FFIEC), *Development and Acquisition Booklet*, USA, 2004, *www.ffiec.gov/ffiecinfobase/booklets/d_a/08.html*

FFIEC, 'IT Handbook InfoBase', USA, 2008, *www.ffiec.gov/ffiecinfobase/index.html*

The Institute of Chartered Accountants in England and Wales, *Internal Control Guidance for Directors on the Combined Code* (Turnbull report), UK, 1999, *www.icaew.com/index.cfm/route/120907/icaew_ga/pdf*

Institute of Internal Auditors (IIA), GTAG1—Information Technology Controls, USA, 2005, *www.theiia.org*

IIA, GTAG8—Auditing Application Controls, USA, 2007, *www.theiia.org*

IIA Research Foundation, 'Sarbanes-Oxley Section 404 Work—Looking at the Benefits', USA, 2005, *www.theiia.org*

International Federation of Accountants (IFAC), 'International Standard on Auditing (ISA) 330 (redrafted)', USA, 2006

ISACA, *CISA Review Manual 2009*, USA, 2008, *www.isaca.org*

ISACA, IS Auditing Guideline G14 Application Systems Review, USA, 2008, *www.isaca.org*

ISACA, Houston Chapter, Auxis Management and Technology Solutions, 'Continuous Controls Monitoring', USA, 2007, *www.isacahouston.org*

IT Governance Institute, COBIT® 4.1, USA, 2007, *www.itgi.org*

IT Governance Institute, *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*, USA, 2007

IT Governance Institute, *ITAF™: A Professional Practices Framework for IT Assurance*, USA, 2007, *www.itgi.org*

IT Governance Institute, *IT Assurance Guide: Using COBIT®*, USA, 2007, *www.itgi.org*

IT Governance Institute, *IT Control Objectives for Sarbanes-Oxley, The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*, USA, 2006, *www.itgi.org*

IT Governance Institute, *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition*, USA, 2007, *www.itgi.org*

Kaplan, Robert S.;David P. Norton; *Balanced Scorecard: Translating Strategy Into Action*, Harvard Business School Press USA, 1996

King Committee on Corporate Governance, *King Report on Corporate Governance for South Africa* (King I Report), Institute of Directors in Southern Africa, South Africa, 1992

King Committee on Corporate Governance, *King Report on Corporate Governance for South Africa* (King II Report), Institute of Directors in Southern Africa, South Africa, 2002, *www.iodsa.co.za/king.asp#King%20I%20Report%20-%201994*

National Commission on Fraudulent Financial Reporting (Treadway Commission), Report of the National Commission on Fraudulent Financial Reporting, USA, 1987

Public Company Accounting Oversight Board (PCAOB), 'Staff Questions and Answers on Auditing Internal Control Over Financial Reporting', USA, 15 May 2005

Software Engineering Institute of Carnegie Mellon University, *The Capability Maturity Model: Guidelines for Improving the Software Process* (Also known as the CMM and SW-CMM this title was retired and replaced by the *CMMI®: Guidelines for Process Integration and Product Improvement* in 2003.), Addison-Wesley Professional, USA, 1995

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *info@isaca.org*
Web site: *www.isaca.org*

ISBN 978-1-933284-85-9
90000
9 781933 284859