IT CONTROL OBJECTIVES FOR BASEL II

THE IMPORTANCE OF GOVERNANCE AND RISK MANAGEMENT FOR COMPLIANCE

IT CONTROL OBJECTIVES FOR BASEL II

THE IMPORTANCE OF GOVERNANCE AND RISK MANAGEMENT FOR COMPLIANCE

IT Governance Institute®
The IT Governance Institute (ITGI™) (*www.itgi.org*) was established in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. Effective IT governance helps ensure that IT supports business goals, optimizes business investment in IT, and appropriately manages IT-related risks and opportunities. ITGI offers original research, electronic resources and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

Disclaimer
ITGI and the author of *IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance* have designed the publication primarily as an educational resource for information risk managers, IT practitioners and banking experts. ITGI and the authors make no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of all proper procedures and tests or exclusive of other proper procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, controls professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or IT environment.

Disclosure

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.606.5700
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*

ISBN 978-1-893209-38-1
IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance
Printed in the United States of America

Acknowledgments

ITGI wishes to recognize:

Principal Contributor
Rolf von Roessing, CISA, CISM, CISSP, FBCI, KPMG Germany, Germany

Focus Group
Urs Fischer, CISA, CIA, CPA, Swiss Life, Switzerland
Christopher Fox, ACA, eDelta, USA
Jimmy Heschl, CISA, CISM, KPMG, Austria
Markus Gaulke, CISA, CISM, KPMG Germany, Germany
Marcelo Gonzalez, CISA, Banco Central Republica Argentina, Argentina
Mario Micallef, CPAA, FIA, National Australia Bank Group, Australia
Masaki Nakamura, CIA, Sumitomo Mitsui Banking Corporation, Japan
Robert Stroud, CA Inc., USA
Robert White, CISA, ACA, ING Bank, UK

ITGI Board of Trustees
Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, PIIA, KPMG LLP, UK, International President
Georges Ataya, CISA, CISM, CISSP, ICT Control sa-nv, Belgium, Vice President
Avinash Kadam, CISA, CISM, CBCP, CISSP, Miel e-Security Pvt. Ltd., India, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Jose Angel Pena Ibarra, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President
Robert E. Stroud, CA Inc., USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP, USA, Vice President
Frank Yam, CISA, FHKCS, FHKIoD, CIA, CCP, CFE, CFSA, FFA, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, Past International President
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Trustee
Tony Hayes, FCPA, Queensland Government, Australia, Trustee

IT Governance Committee
Tony Hayes, FCPA, Queensland Government, Australia, Chair
Max Blecher, Virtual Alliance, South Africa
Sushil Chatterji, Edutech, Singapore
Anil Jogani, CISA, FCA, Avon Consulting Ltd., UK
John W. Lainhart IV, CISA, CISM, IBM, USA
Lucio Molina Focazzio, CISA, Colombia
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada
Michael Schirmbrand, Ph. D., CISA, CISM, CPA, KPMG LLP, Austria
Robert E. Stroud, CA Inc., USA
John Thorp, The Thorp Network Inc., Canada
Wim Van Grembergen, Ph.D., University of Antwerp, University of Antwerp Management School, and IT Alignment and Governance Research Institute (ITAG), Belgium

Table of Contents

Preface 7

1. Executive Summary....9
Scope and Purpose 9
How to Read This Document 9

2. Governance, Risk Management and Compliance: Top Business Priorities....11

3. Evolving Regulatory Landscape 14

4. The Basel II Approach to Managing Risk 16

5. The Need to Manage Operational Risk....19
Risk Management Approaches....19
Framework for Operational Risk Management....21
COSO Components 25
Operational Risk Principles and IT Relevance 32

6. Managing Information Risks 37
IT Guiding Principles....37
Causes of Loss and IT Risk 47
IT Risk Scenario Analysis....50

7. Business Processes to IT Risks to IT Controls: Applying the CobiT Framework 53
Use of Existing Documentation 53
The Business Line Approach in Basel II 53
Defining IT Risk 55
Defining IT Controls....58

8. Use of Key IT Risk Indicators....61

Appendix I—Basel II Summary 63

Appendix II—High-level Alignment of COSO ERM and Basel II....72

Appendix III—High-level Alignment of Basel II Principle 1: The Second Pillar—Supervisory Review Process (June 2006) and COSO ERM—Integrated Framework (September 2004)....73

Appendix IV—The Dependence of the COSO ERM Framework on Data Quality....76

Appendix V—Basel II and COBIT....78

Appendix VI—COBIT Processes....85

Appendix VII—ABC Bank: A Worked Example....96

Appendix VIII—References....102

Preface

Financial services organizations[1] are facing new challenges presented by the Second Capital Accord defined by the Basel Committee on Banking Supervision, colloquially known as Basel II. The Accord builds on an evolving framework for managing risk in financial services transactions. In contrast to the First Capital Accord of 1988, information risk and information technology (IT) have become decisive factors in shaping modern business, and many financial services organizations have undergone a fundamental transformation in terms of IT infrastructures, applications and IT-related internal controls.

The purpose of this publication is to highlight steps toward convergence. Financial services and the financial system have been identified as highly critical infrastructures in a global economy; likewise, operational and information risk management and IT controls are now seen as essentials in good corporate governance. At the highest level of strategy, senior management oversight and good governance over the financial system require that these two worlds be merged into a seamless model.

Following the highly successful publication of *IT Control Objectives for Sarbanes-Oxley*, which is now in its second edition, ITGI is taking the proactive step of addressing risk in financial services organizations by presenting this first edition of *IT Control Objectives for Basel II*. This publication is intended to give guidance to operational and information risk managers, IT practitioners, and financial services organization experts with tasks and responsibilities for IT. The main objective is to provide clear and unambiguous guidance with regard to operational and information risk management, and its application to the requirements and provisions of Basel II as a framework.

There are many reasons for implementing a formal, standardized set of IT controls under Basel II and many frameworks that might be applied in financial services organizations. *Control Objectives for Information and related Technology* (COBIT®),[2] as a comprehensive governance framework for the management of IT risk and control, provides a proven and mature set of IT processes and controls suited to address the need for formalization of Basel II-related operational and information risk management. As an established governance framework, COBIT has achieved international recognition and is widely regarded as a global good practice. Its versatility and simplicity, coupled with ongoing improvement initiatives, have set COBIT apart from proprietary solutions and other frameworks.

[1] As there are a number of organizations that may not be banks, this publication uses the term "financial services organization" rather than "bank," wherever possible.
[2] ITGI, COBIT, USA, 1996-2007, *www.itgi.org*

IT Control Objectives for Basel II has been developed by a committee of senior experts from a wide range of financial services organizations. The rigorous process of challenging assumptions, thoughts and preconceived ideas, and exposing the document to public scrutiny have given additional credibility to the publication. This publication highlights the need for operational and information risk management and IT controls from the perspective of bankers and financial experts.

ITGI welcomes any comments on this publication that will help continuously improve and adapt *IT Control Objectives for Basel II* to the needs of financial services organizations. Comments can be provided at *info@itgi.org*.

Everett Johnson, CPA
Past International President
IT Governance Institute

1. Executive Summary

Scope and Purpose

IT Control Objectives for Basel II provides a framework for managing operational and information risk in the context of Basel II. This document addresses three operational and information risk target groups—information risk managers, IT practitioners and financial services experts. In applying the framework presented in this publication, financial services organizations are able to apply recognized processes and controls to the IT space. The IT control objectives and management processes outlined address the role of information technology in operational risk.

The following chapters present an outline of risk under Basel II, the links between operational risk and IT risk, and an approach for managing information risk.

How to Read This Document

Governance, risk management and compliance (GRC) have evolved as top business priorities. A new evolution in business is being driven by increased stakeholder demands, heightened public scrutiny and new performance expectations. The trend toward improved corporate governance is seen in many initiatives. Good governance is about addressing deficiencies such as poor information flows, bad communication and an inadequate understanding of risk, as well as behavior. Chapter 2, Governance, Risk Management and Compliance: Top Business Priorities, introduces the relevant concepts of GRC.

Growing regulatory activity, coupled with an increasing level of detail, is evidence that GRC is a primary concern for banking and financial services regulators. Over the past few years, there has been a rapid succession of GRC-related regulatory provisions. Regulations of all types have evolved into detailed frameworks covering many aspects of banking and technology. In recent years, national and international regulations have increasingly addressed issues of information management, information technology and specialist disciplines within these fields. Chapter 3, Evolving Regulatory Landscape, outlines the pressures that are intensifying the regulatory focus.

In 2004, the Basel Committee on Banking Supervision published the second capital adequacy framework, which introduced a new approach to risk in financial services organizations. The objective of Basel II was to introduce stronger risk management practices for credit and operational risk and strengthen the link between risk and capital charges. These new regulations provide an incentive for organizations to improve the quality of their risk management frameworks and systems to reduce capital reserve requirements. This provides a competitive advantage to financial services organizations with a strong GRC framework. For each financial services organization, its overall risk exposure will determine the capital charge. GRC initiatives are

an important factor in reducing this charge. Chapter 4, The Basel II Approach to Managing Risk, describes the approach to risk management as defined in the Basel II framework.

Operational risk is regarded as a particularly important risk category. The risk intrinsic to financial services organizations is often more diverse than the comparatively narrow areas covered by other categories, such as interest rate risk. However, identifying and measuring operational risk has proven to be a formidable challenge to banks and financial services organizations. Information technology and information management are key elements in a comprehensive strategy to manage GRC and, thus, optimize the capital charge. IT-related components such as applications, infrastructure elements and controls are all defined as parts of operational risk. Chapter 5, The Need to Manage Operational Risk, provides an overview of operational risk and its relevance for information risk. This chapter further maps Basel II principles for operational risk against IT risk.

To adequately address information-related risks, a business-driven approach is required. Business processes drive the definition of controls and metrics, while the set of IT-related controls are complemented by a set of indicators to measure compliance and maturity. Where an information-related risk has an impact on the business process, steps toward reducing and mitigating the risk are integral parts of the organization's GRC framework. Chapter 6, Managing Information Risks, provides a bridge between Basel II and information-related risk by defining a set of 10 guiding principles for operational and information risk management. These guiding principles correspond to the principles of operational risk management as set down in the Basel II documents.

Basel II requires a business-driven approach to risk management. To apply COBIT as a supporting model for GRC, the set of IT controls must be related to IT risks. IT risks are a subset of business-driven risks that are visible in business processes. Chapter 7, Business Processes to IT Risks to IT Controls: Applying the COBIT Framework, outlines the logical sequence from the business process view to information risk, and then to IT controls. The chapter explains how IT practitioners and risk managers can look to COBIT and its concepts to address many of their Basel II-related risks in a step-by-step manner.

Managing risk includes the use of indicators to denote goals, performance and levels of risk. Chapter 8, Use of Key IT Risk Indicators, introduces the concept of key risk indicators (KRIs) and their use under Basel II. Each KRI supports the ongoing process of risk assessment and risk management to achieve improvements of the overall operational risk. The chapter describes types of indicators, their significance for the overall risk management process, and the definition of KRIs suitable for a comprehensive operational and information risk management framework.

2. Governance, Risk Management and Compliance: Top Business Priorities

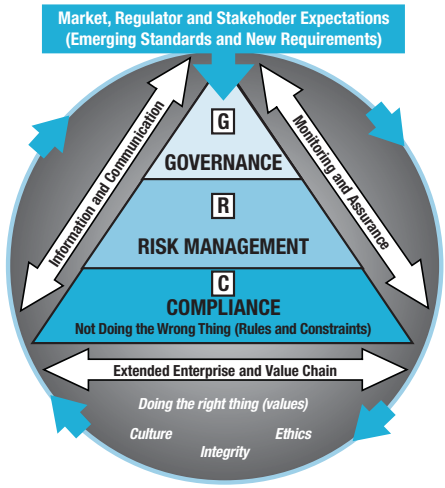
GRC has become a top business priority. The trend toward improved corporate governance is seen in many initiatives, including the following:

- Protecting corporate reputation and brand value
- Meeting the increased demands and expectations of investors, legislators, regulators, customers, employees, analysts, consumers and other key stakeholders
- Driving value and managing performance expectations for governance, ethics, risk management and compliance
- Managing crisis and remediation while defending the organization, its executives and board members against the increased scope of legal enforcement and the rising impact of fines, penalties and business disruption
- Exercising good corporate stewardship and discharging fiduciary duties in a transparent and proactive manner

Organizations are required to address the impact of these initiatives. Some may have had a positive experience in terms of GRC, but are unsure about their ability to maintain their position in a rapidly changing environment. Industry studies show that many organizations believe they are not positioned to effectively meet increased stakeholder demands on a sustainable basis.

Figure 1 outlines the holistic responsibility for corporate governance that reaches all levels of the organization. While GRC is primarily a board responsibility, all organizational units are required to adopt and apply the GRC principles set by management.

Figure 1—Integrity-driven Performance: Managing Risk From the Boardroom to the Mailroom



An integrated approach to GRC should be taken. Organizations addressing each GRC area in a different way are likely to experience significant cost increases and duplication of effort. Taking a reactive, backward-looking approach to GRC could negatively affect efficiency and make the implementation of proactive, process-driven initiatives difficult, if not impossible.

Good governance is about setting strategy, managing risk, delivering value and measuring performance. A strong GRC framework ensures that the interests of stakeholders are adopted and implemented by management and staff members throughout the organization. Such a framework is the foundation of managerial integrity, making the best use of corporate assets and intellectual capital, and understanding and managing risk. All parts of a GRC framework are important components of good corporate governance.

Organizations must address the increased risks associated with geopolitical instability, globalization, aggressive growth targets, increased competition and the information explosion. Risk management has always been a core competency in financial institutions. Today, integrated enterprisewide risk management practices are a regulatory imperative. Entrepreneurial activity and risk are not mutually exclusive. Integrated risk management is an instrument that enables informed managerial decisions and conscious acceptance of tolerable and acceptable level of risk. Therefore, risk management as a part of corporate governance will strengthen stakeholder confidence and provide a clear sense of direction to organizations engaging in entrepreneurial activities.

Compliance has evolved from a tick-box, reactive approach to a forward-looking, proactive discipline that supports good governance. Compliance is now far broader than simply working through a list of all-or-nothing requirements, although rules-based compliance is still an important subset of overall compliance. In most cases, the compliance requirements set down in regulations or standards are maturity-driven and designed for continuous improvement over time. Market practice, benchmarks and new developments in business must be factored into the notion of compliance, given the constant changes and challenges of global business.

GRC is not an afterthought when entering into or operating a business. It is an expression of the need to protect the organization and maintain its integrity—toward external stakeholders, business partners, and internal employees and associates. Legislators with a focus on GRC represent the interests of national and international electorates and constituencies. Laws and statutes reflect a social agreement on the need for good governance. GRC regulations transform this overall agreement into sector- and industry-specific concepts. Industry associations and standards bodies provide consensus on planning, implementing and maintaining concepts relating to GRC.

Basel II and its provisions on risk management reflect the growing focus on building governance structures and frameworks in the financial services industry. The new Capital Accord reaches beyond earlier initiatives and their GRC requirements. The components and building blocks of Basel II cover a wide range of managerial and technical aspects, including challenges to information technology, security and business continuity, thus providing a sense of direction to specialist disciplines within banking and financial services organizations.

Information, the related technologies and challenges to information management are growing in importance. Banking and financial services today are increasingly reliant on complex information technology, in terms of both transacting business and exercising control. As part of GRC, one of the major imperatives is to build a bridge between core business processes and vital supporting technologies. The resulting framework for good governance in information management should not be restricted to control and compliance. The priorities of GRC must be reflected in the overall approach taken to information technology and its potential for supporting business globally. Besides operational losses and reputational damage, deficiencies in the design or effectiveness of the IT governance model, in the context of Basel II, are aspects that could likely contribute to an increase in the capital charge on operational risk which is discussed in detail in Chapter 5, The Need to Manage Operational Risk.

3. Evolving Regulatory Landscape

Laws, regulations, standards and accepted practices in industry all serve one common purpose: in their entirety, they support GRC objectives. In terms of practical applicability and the requisite level of detail expected by the practitioner, national and international regulations form the foundation of GRC, particularly where regulatory provisions are focused on specific industry sectors, such as banking and financial services.

The growth in regulatory activity, coupled with an increasing level of detail required in regulatory responses, is evidence of the fact that GRC is an important area of concern for banking and financial services regulators. Over the past few years, there has been a rapid succession of GRC-related regulatory provisions, including:
- Basel II
- Financial reporting national laws and regulations (e.g., the US Sarbanes-Oxley Act of 2002)
- Prudential standards

Regulations of all types have evolved into detailed frameworks covering many aspects of financial services and technology. In recent years, national and international regulations have increasingly addressed issues of information management, information technology and specialist disciplines within these fields. As a result, both senior management and specialist practitioners are now in a position to transform existing regulations into practical and manageable concepts that support GRC at the organizational level.

The drivers for regulatory change include:
- Growing sophistication of financial technology, leading to more complex activities and risk profiles in financial services organizations
- Globalization of banking and the geographic spread of financial operations across national borders
- Increased collaboration between regulators across geographic jurisdictions, driven by the need for market oversight and supervision
- Widening of compliance requirements into other sectors of the financial services industry, such as anti-money laundering legislation and regulation
- Increased expectations for corporate accountability, emphasizing the importance of enhanced governance, ethics, independence, transparency and rigorous market disclosure
- Increased expectations for the standard of care that directors must exercise in discharging their fiduciary duties, greatly expanding their scope of responsibility and the potential liability of board members and committees
- Heightened public interest and pressure from nongovernmental interest groups, shareholders and the media around governance and risk management, combined with the stronger influence of these groups in regulatory debate

- Internal and external reporting from various applications and databases
- Divergence in compliance standards to satisfy country/host country regulators
- Heavy reliance on the IT infrastructure to provide an efficient and effective service and increased reliance on third parties as a result of developments in the payments and settlements adopted in various jurisdictions

Given the increasing complexity of the global business environment, it is likely that regulation will be more specific in the future, addressing areas not covered in the current regulatory landscape. Although this change in the landscape may be regarded as overregulation, regulators are expected to maintain market confidence, safety and sound practices in financial institutions, including the protection of shareholders, transparency and corporate integrity.

While there is a trend to principles-based regulation, components of regulations and standards will remain rules-based. With the introduction of Basel II, regulation includes process-based and outcome-based provisions. As the onus for regulatory compliance—under the emerging principles-based regulation, as well as the rules-based regulation—now rests with financial services organizations, the respective boards and senior management are required to demonstrate to the satisfaction of their regulators the robustness of their GRC processes and outcomes to be compliant with the extended regulations.

As a result, financial services organizations will have to adapt to the growing extent of regulation and the detailed requirements imposed over time. There is a need to introduce robust business processes to address GRC in a forward-looking manner, including in previously unregulated areas, such as information management and information technology, and in related disciplines, such as security, business continuity and privacy.

4. The Basel II Approach to Managing Risk

Risk, an inherent part of business, has been brought to the attention of a wider public audience as a result of a series of events over the past years. These included incidents of fraud, major credit failures, exploits focused on information technology and many others. Media response and public interest have confirmed that risk management is seen as an important priority to maintain public confidence in the international financial system.

Within the banking and financial services community, risk, in general, requires categorization to create manageable GRC structures. Risk categories are usually defined along the core business areas found in a typical bank or financial services organization. These risk categories include:

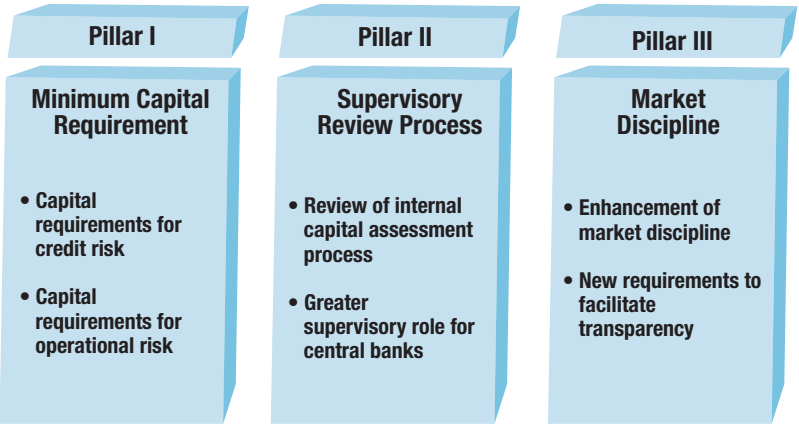
- Credit risk
- Market risk
- Operational risk
- Liquidity risk
- Interest rate risk
- Legal risk
- Strategic risk
- Reputational risk

The Basel Committee on Banking Supervision published the second capital adequacy framework in 2004, which introduced an enhanced approach to risk in financial services organizations. The objective of Basel II was to introduce stronger risk management practices for credit and operational risk, and to strengthen the link between risk and capital charges. The new regulations provide an incentive for organizations to improve the quality of their risk management frameworks and systems to reduce the required capital. This improvement provides a competitive advantage to financial services organizations with a strong GRC framework. For an individual organization, the overall risk exposure will determine the capital charge. GRC initiatives may be instrumental in reducing this charge. Based on this new perspective on risk and capital requirements, many financial service organization structures and processes may have to be revisited and reevaluated.

The Basel II approach to risk is designed to encompass the complexity of information technology and information management. The enhanced framework, shown in **figure 2**, is built on three pillars:

- **Minimum capital requirements**—Refines the Basel I approach to credit risk and introduces a new capital requirement for operational risk
- **Supervisory review process**—Introduces supervisory reviews and self-assessment of the bank's capital adequacy processes, including sound policies and procedures to manage and control capital
- **Market discipline**—Introduces new disclosure requirements to strengthen market discipline and impact market, rating agency and shareholder perceptions

Figure 2—The Three Pillars of the Revised Framework[3]



It is critical that the minimum capital requirements of the first pillar be accompanied by a robust implementation of the second pillar. In addition, the disclosures provided under the third pillar are essential in ensuring that market discipline is an effective complement to the other two pillars.

Financial services organizations may select from a number of approaches for measuring and managing their risks and capital requirements to allow flexibility in the different maturity levels in GRC. Capital charges may be lower for those organizations opting for a more advanced risk management approach. These approaches vary with the category of risk, and it is envisioned that there will be a gradual move toward the more advanced approaches. Organizations may opt for an increased capital charge based on cost-benefit considerations and strategic decisions by senior management, and consciously accept a higher level of overall risk. It should be noted that organizations will have to demonstrate the advanced approach for operational risk prior to implementing the internal ratings-based (IRB) approach for credit risk.

The supervisory review pillar introduces qualitative assurance over GRC in financial services organizations. National supervisory authorities in financial services are required to monitor compliance with minimum capital requirements and to take action in case of inadequacies. Appendix I, Basel II Summary, describes in detail the four principles of supervisory review. The principles and scope of the supervisory process envision an ongoing dialog between financial services organizations and the national supervisory authorities.

[3] This figure shows only the changes in the detailed components in the Basel II framework. More details of each pillar can be found in Appendix I, Basel II Summary.

The market discipline pillar introduces the disclosure of information about risk and GRC. This disclosure is intended to inform all market participants about the overall risk situation and highlight areas of significant potential risk that may exist in individual financial services organizations. As a result, market discipline is enforced and disproportionate risks are reflected in the overall behavior of the market.

The disclosure requirement specifies that potential and actual losses for each type of risk (credit, market, operational, interest rate) must be calculated and disclosed. This specific requirement will allow other market participants to assess the details of an organization's risk profile. Details of the approaches to the types of risk are provided in appendix I, Basel II Summary.

5. The Need to Manage Operational Risk

Operational risk is an important component in determining the minimum capital requirement. Operational risk covers all areas linked to potential failures in the overall operation of a financial services organization and, specifically, the underlying technology and infrastructures. The significance of information technology will have a direct correlation with the associated capital charges on operational risk. Therefore, the operational risk category is much wider than credit, market or interest rate risk. Given the complexity and the scope of operational risk, GRC frameworks and initiatives need to include all areas of an organization that are not directly linked to other risk types.

Risk Management Approaches

Operational risk may be managed using one of the three fundamental approaches:

- The basic indicator approach (BIA)
- The standardized approach (STA)
- Advanced measurement approaches (AMA), which are based on internal loss data

In addition to selecting of one of these approaches, financial services organizations must comply with a set of minimum requirements that influence core business and IT. Appendix I, Basel II Summary, outlines the detailed requirements and the approaches listed in the previous paragraph.

Basel II specifically incorporates operational risks in the calculation of capital adequacy for the first time. The reasons for this move are considerable financial losses in various financial services organizations, which could have been avoided if more effective controls and more sophisticated business processes had been in place.

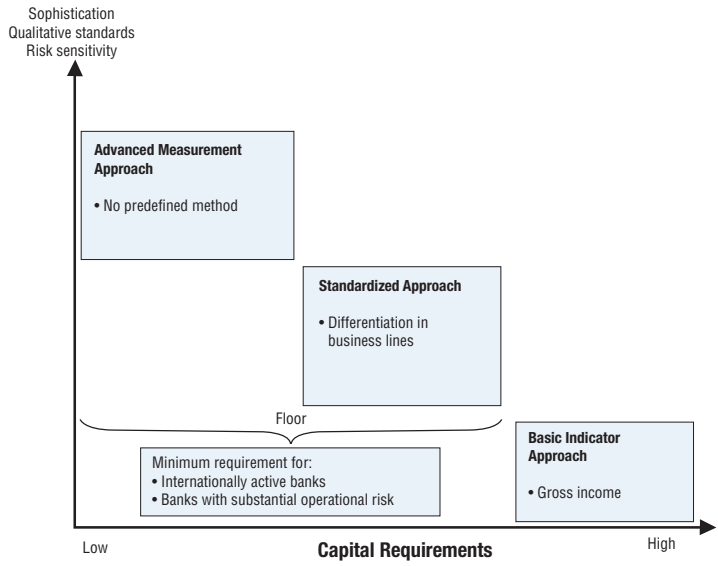
Furthermore, financial services organizations' increased dependency on IT, extensive use of the Internet, higher complexity of financial products and higher number of delivery channels provide many reasons to recognize and assess financial services organizations' operational risks.

The Basel Committee defines operational risk in Basel II as follows: "Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."

The definition includes legal risk but excludes strategic and reputational risk. Currently, operational risk is charged to the capital requirement at 8 percent. To assess the amount of operational risks, banks may use various alternative approaches.

The Basel Committee has provided three approaches—BIA, STA and AMA—to measuring operational risk capital charges in a continuum of increasing sophistication and risk sensitivity, as shown in **figure 3**.

Figure 3—The Three Approaches to Operational Risk



Similar to the philosophy behind capital adequacy regulations in connection with credit exposure, the three approaches move toward higher complexity and provide more risk sensitivity. To qualify for the advanced approach resulting in lower capital requirements, banks have to meet more sophisticated conditions.

Financial services organizations are encouraged to move along the spectrum of available approaches as they develop more sophisticated operational risk measurement systems and practices, as the qualitative and quantitative qualifications for each approach become more demanding. As an incentive, higher capital relief can be obtained with a more sophisticated method.

Financial services organizations may use the advanced approach for selected individual business lines. The implementation of individual approaches also requires financial services organizations to comply with certain qualifications.

All financial services organizations must comply with the minimum requirements, which are defined in the Committee's guidance notes,

"Operational Risk Sound Practices." These requirements include the following:

- The board of directors and executive management must play an active role in the supervision of the management of operational risks.
- The bank must have a functioning, fully implemented and integrated risk management system.
- Whatever approach is chosen, the employee headcount must be sufficient to apply the respective approach.

Framework for Operational Risk Management

Operational risk is regarded as a particularly important risk category. The risk intrinsic to financial services organizations' operations and the conduct of ordinary business is often more diverse than the comparatively narrow areas covered by risk categories such as interest rate risk. Identifying and measuring operational risk has proven to be a formidable challenge for banks and financial services organizations.

Within the operational risk definition, as suggested by regulators and other associations, there is a wide range of individual risk factors that should be taken into consideration prior to integrating the operational component into the wider enterprise risk management framework. Many specific risks in the operational category are linked to broader compliance or corporate governance issues. Others require an in-depth understanding of technology and the infrastructures supporting core business activities.

The Basel Committee requires banks to install a framework to manage operational risk. While the scope and extent of the framework is not specified, the approach in **figure 4** provides a possible way to structure the challenge of managing operational risks.

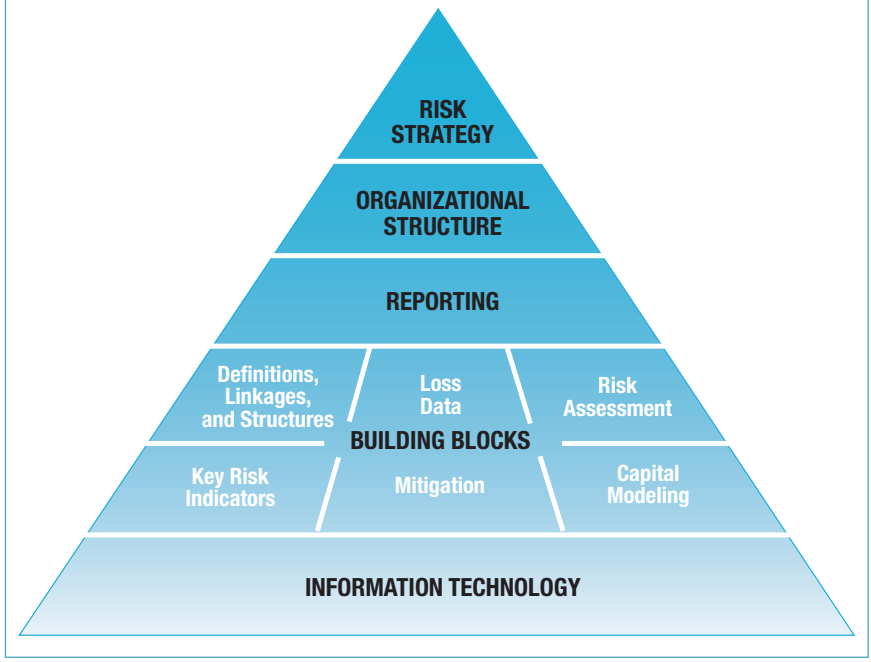
Risk Strategy

Strategies for operational risk drive the other components within the management framework. A comprehensive risk strategy should provide clear guidance on risk appetite or tolerance, policies, and processes for day-to-day risk management.

Organizational Structure

The organizational structure is the organizationwide foundation for all operational risk management activities. Within this context, financial services organizations define and assign centralized and decentralized roles and responsibilities to a wide array of organizational units, functions and, ultimately, individuals.

Figure 4—Framework for Managing Operational Risk



Reporting
Since operational risk affects all business units, operational risk management reporting has a much broader scope than traditional market or credit risk reporting. Such reporting has to cover two distinct aspects:
- Delivery of defined, relevant operational risk information to management and risk control
- Reporting of information combined by risk category to business line management, the board and the risk committee

Definitions, Linkages and Structures
Financial services organizations need a common language for describing operational risk and loss-event types, causes and effects. They also need to map the rules necessary for compliance with regulatory requirements. The development of definitions, linkages and structures enables financial services organizations to efficiently identify, assess and report such operational risk-related information.

Loss Data
A well-structured operational risk framework requires the development of databases to capture loss events attributable to various categories of operational risk. Regulators expect internal loss databases to be comprehensive and to include several years of data prior to formal approval

for use in the risk estimation process. Basel II, specifically, requires a minimum of three years of data for initial implementation and, ultimately, five years for AMA. The need for historic data (including external data) has been a driving force behind the efforts of many financial services organizations to bring their databases into production as soon as possible.

With a common language in place, financial services organizations need a process for collecting, evaluating, monitoring and reporting operational risk loss data. Such a process would be designed to provide the basis for any management decision, from *ad hoc* reporting to regular risk reporting and, ultimately, leading to support quantification models as well as risk assessments.

Risk Assessment
Risk assessment provides financial services organizations with a qualitative approach to identifying potential risks of a primarily severe nature by conducting structured scenarios with representatives of all business units. Risk assessment techniques fill the knowledge gap left by retrospective and often sparse loss data. These techniques attempt to establish risk-sensitive and proactive identification of operational risk.

Key Risk Indicators
As a part of ongoing measurement and monitoring, financial services organizations should assess aspects of operational risk based on KRIs—factors that may provide early warning signals on systems, processes, products, people and the broader environment. Therefore, KRIs are different from risk assessments in that they rely on observable data, not estimates of future activities.

Mitigation
Once the financial services organization has identified and quantified its risks, it can implement a strategy for mitigating them with appropriate policies, procedures, systems and controls.

Capital Modeling
Capital modeling encompasses the calculation of regulatory and economic capital. It involves defining input data (internal and external loss data, scenario data, business environment, and control factors, as well as auxiliary information such as insurance parameters), defining the mathematical/statistical relationships and assumptions for measuring operational risk, the implementation of the model, and the model validation.

Information Technology
Appropriate information technology is the foundation and facilitator of the operational risk management framework. The IT system will need to accommodate a wide variety of operational risk information and interface with a variety of internal systems and external sources.

The Basel Committee explicitly states in its *Sound Practices for the Management and Supervision of Operational Risk*[4] that the growing sophistication of information technology is a factor making the activities of financial services organizations more complex. IT plays an important role in the operation of strategic and managerial information systems. Today, these systems are inseparable from an organization's ability to meet the demands of management, financial services organizations supervisors, market participants and other important stakeholders. With widespread reliance on IT for financial and operational management systems, controls have long been recognized as necessary, particularly for significant information systems.

In its "Framework for Internal Control Systems in Banking Organisations,"[5] the Basel Committee relied on the definitions and basic elements of internal control systems developed in accordance with guidance provided by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) from its Enterprise Risk Management (ERM) framework. Basel II regards this paper as an essential basis for minimum standards and seeks to make the regulatory processes more sensitive to underlying risks and provide incentives to banks with good risk management practices. Improvements in corporate governance, direct accountability of the board and senior management, general controls, and risk management processes are seen as key elements in the sound management of capital.

COSO is a voluntary private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal control and corporate governance. It was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private-sector organization often referred to as the Treadway Commission. The sponsoring organizations include the American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Financial Executives International (FEI), Institute of Internal Auditors (IIA) and Institute of Management Accountants (IMA).

The COSO model does not specifically address information management and information technology. However, IT is an implied part of any system of internal controls, regardless of the type of risk (financial statements, regulatory or operational) and, consequently, forms an important element in organizationwide risk management. The COBIT framework offers a defined and recognized set of IT control processes, objectives and activities designed to adapt IT risk management and is totally aligned with the COSO framework and its concepts. COBIT, therefore, bridges the gap between high-level enterprise risk management and specific IT risk issues. The sections that follow provide further insight into COSO as well as it implications for IT.

[4] Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of Operational Risk*, February 2003
[5] Basel Committee on Banking Supervision, "Framework for Internal Control Systems in Banking Organisations," September 1998

COSO Components

It is important to demonstrate how IT controls support the COSO ERM framework. An organization should have IT control competency in all COSO components. COSO identifies the following eight essential components of effective internal control:

- Internal environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control activities
- Information and communication
- Monitoring

Each of the eight components is described briefly in the following sections. Following that description are high-level IT considerations as they relate to each specific component. The italicized text is taken directly from the COSO ERM framework.

Internal Environment

The internal environment sets the basis for how risk is viewed, including risk management philosophy. It creates the foundation for effective internal control, establishes the "tone at the top" and represents the apex of the corporate governance structure. The issues raised in the internal environment component apply throughout the organization.

However, IT frequently has characteristics that may require additional emphasis on business alignment, roles and responsibilities, policies and procedures, and technical competence. The following list describes some considerations related to the control environment and IT:

- IT is often mistakenly regarded as a separate organization of the business and, thus, a separate control environment.
- IT is complex, not only with regard to its technical components but also in how those components integrate into the organization's overall system of internal control.
- IT can introduce additional or increased risks that require new or enhanced control activities to mitigate successfully.
- IT requires specialized skills that may be in short supply.
- IT may require reliance on third parties where significant processes or IT components are outsourced.
- Ownership of IT controls may be unclear.

The internal environment component relates to Basel II Principles 1, 3, 6 and 10.

Objective Setting

COSO ERM identifies four broad categories of objectives:

- *Operations Objectives—These pertain to the effectiveness and efficiency of the entity's operations, including performance and profitability goals and safeguarding resources against loss. They vary based on management's choices about structure and performance.*

  A financial services organization should identify the operational risk inherent in all IT processes that impact material products, activities, processes and systems. For example, if a key process relied on 24/7 processing and 90 percent availability, the IT risk associated with achieving this objective would need to be assessed.

- *Reporting Objectives—These pertain to the reliability of reporting. They include internal and external reporting, and may involve financial and nonfinancial information.*

  Basel II reporting objectives and related processes are wider in scope than Sarbanes-Oxley reporting objectives. In addition to financial reports, risk management reporting and public disclosure reporting need to be taken into account.

- *Compliance Objectives—These pertain to adherence to relevant laws and regulations. They are dependent on external factors and tend to be similar across all entities, in some cases, and across an industry in others.*

  The IT organization should identify the regulatory requirements with which it needs to comply. These requirements include formal requirements (e.g., the establishment of contingency plans) and less defined requirements (e.g., examiners' expectations of financial services organizations to promote a safe and sound environment).

- *Strategic Objectives—These pertain to the high level goals that are established by management to define what the organization aspires to achieve. Objectives are linked to the organization's operations and reporting procedures, which should directly tie to compliance initiatives and risk management.*

  Departmental goals and reporting procedures need to be tied to management's expectations concerning operational risk. IT is a core component in the implementation and management of basic financial services operations. IT goals need to be aligned with the strategic goals of the organization.

The objective-setting component relates to Basel II Principle 4.

Event Identification
According to the COSO ERM framework:

> *Management identifies potential events that, if they occur, will affect the entity, and determines whether they might adversely affect the entity's ability to successfully implement strategy and achieve objectives. Events with negative impact represent risks, which require management's assessment and response.*

Technology event categories identified in COSO ERM are listed in **figure 5**.

Figure 5—COSO ERM Event Categories

External Factors	Internal Factors
Interruptions	Data integrity
Electronic commerce	Data and system availability
External data	System selection
Emerging technology	Development
	Deployment
	Maintenance

Examples of events mapped to COBIT processes are included in Appendix V, Basel II and COBIT.

The event identification component relates to Basel II Principles 4 and 5.

Risk Assessment
Regarding risk assessment, COSO ERM states:

> *Risk assessment allows an entity to consider the extent to which potential events have an impact on achievement of objectives. Management assesses events from two perspectives—likelihood and impact—and normally uses a combination of qualitative and quantitative methods.*

Risk assessment involves the identification and analysis by management of relevant risks to achieve predetermined objectives, which form the basis for determining control activities. It is likely that internal control risks could be more pervasive in the IT organization than in other areas of the organization. Risk assessment may occur at the entity level (for the overall organization) or at the activity level (for a specific process or business unit).
At the entity level, the following may be expected:
- The responsibilities of the IT planning subcommittee may include:
  - Oversight of the development of the IT internal control strategic plan, its effective and timely execution/implementation, and its integration with the overall risk management plan

– Assessment of IT risks, e.g., IT management, data security, program change and development

At the activity level, the following may be expected:
- Formal risk assessments built throughout the systems development methodology
- Risk assessments built into the infrastructure operation and change process
- Risk assessments built into the program change process

The risk assessment component relates to Basel II Principles 4 and 5.

Risk Response
According to COSO ERM:

> *Risk responses include risk avoidance, reduction, sharing and acceptance. In considering its response, management assesses the effect on risk likelihood and impact, as well as costs and benefits, selecting a response that brings residual risk within desired risk tolerances. Management identifies any opportunities that might be available, and takes an entity-wide, or portfolio, view of risk, determining whether overall residual risk is within the entity's risk appetite.*

Risk responses can be classified into the following categories:
- Avoidance—Exiting the activities giving rise to risk. Risk avoidance may involve moving to a standardized IT infrastructure rather than having multiple "best of breed" architectural components.
- Reduction—Action is taken to reduce risk likelihood or impact, or both. This typically involves any of a wide variety of everyday business decisions, for example, centralization of the program change function.
- Sharing—Reducing risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Common techniques include purchasing insurance products, engaging in hedging transactions or outsourcing an activity.
- Acceptance—No action is taken to affect risk likelihood or impact. For example, if policy requires an eight-digit password and an application will allow only a six-digit password, then a decision may be made to accept this risk.

The risk response component relates to Basel II Principles 6 and 7.

Control Activities
Control activities are the policies, procedures and practices put into place so that business objectives are achieved and risk mitigation strategies are carried out. Control activities are developed to specifically address each control objective to mitigate the risks identified.

Without reliable information systems and effective IT control activities, organizations would not be able to generate accurate financial reports. COSO recognizes this relationship and identifies two broad groupings of information systems control activities: general controls and application controls.

General controls, which are designed so that the financial information generated from an organization's application systems can be relied upon, include the following types:

- Data center operation controls—Controls such as job setup and scheduling, operator actions, and data backup and recovery procedures
- System software controls—Controls over the effective acquisition, implementation and maintenance of system software, database management, telecommunications software, security software and utilities
- Access security controls—Controls that prevent inappropriate and unauthorized use of the system
- Application system development and maintenance controls—Controls over development methodology, including system design and implementation, that outline specific phases, documentation requirements, change management, approvals and checkpoints to control the development or maintenance of the project

Application controls are embedded within software programs to prevent or detect unauthorized transactions. When combined with other controls, as necessary, application controls support the completeness, accuracy, authorization and validity of processing transactions. Some examples of application controls include:

- Balancing control activities—Detect data entry errors by reconciling amounts captured either manually or automatically to a control total. For example, a company automatically balances the total number of transactions processed and passed from its online order entry system to the number of transactions received in its billing system.
- Check digits—Calculate to validate data. A company's part numbers contain a check digit to detect and correct inaccurate ordering from its suppliers. Universal Product Codes (UPCs) include a check digit to verify the product and the vendor.
- Predefined data listings—Provide the user with predefined lists of acceptable data. For example, a company's intranet site might include drop-down lists of products available for purchase.
- Data reasonableness tests—Compare data captured to a present or learned pattern of reasonableness. For example, an order to a supplier by a home renovation retail store for an unusually large number of board feet of lumber may trigger a review.
- Logic tests—Include the use of range limits or value/alphanumeric tests. For example, credit card numbers have a predefined format.

General controls are needed to support the functioning of application controls, and both are needed to support accurate information processing and the integrity of the resulting information used to manage, govern and report on the organization. As automated application controls increasingly replace manual controls, general controls are becoming more important.

This control activities component relates to Basel II Principle 6.

Information and Communication
COSO states that information is needed at all levels of an organization to run the business and achieve the entity's control objectives. However, the identification, management and communication of relevant information represent an ever-increasing challenge to the IT department. The determination of which information is required to achieve control objectives, and the communication of this information in a form and time frame that allow people to carry out their duties, support the other seven components of the COSO framework.

The IT organization processes most financial reporting information. However, its scope is usually much broader. The IT department may also assist in implementing mechanisms to identify and communicate significant events, such as e-mail systems or executive decision support systems.

COSO also notes that the quality of information includes ascertaining whether the information is:
- Appropriate—Is it the right information?
- Timely—Is it available when required and reported in the right period of time?
- Current—Is it the latest available?
- Accurate—Are the data correct?
- Accessible—Can authorized individuals gain access to it as necessary?

At the entity level, the following may be expected:
- Development and communication of corporate policies
- Development and communication of reporting requirements, including deadlines, reconciliations, format and content of monthly, quarterly and annual management reports and public disclosure reporting
- Consolidation and communication of financial information

At the activity level, the following may be expected:
- Development and communication of standards to achieve corporate policy objectives
- Identification and timely communication of information to assist in achieving business objectives
- Identification and timely reporting of security violations

The information and communication component relates to Basel II Principles 3, 5, 6 and 10.

Monitoring
Monitoring, which covers the oversight of internal control by management through continuous and point-in-time assessment processes, is becoming increasingly important to IT management.

In 2006, COSO suggested that effective monitoring should:
- Be integrated, to the extent possible, with operations—Ongoing monitoring is built into the organization's operating activities.
- Provide objective assessments
- Use knowledgeable personnel to perform the evaluations—Evaluators understand the components being evaluated and how they relate to activities supporting the reliability of information.
- Consider feedback—Management, financial services organization supervisors and market participants receive feedback on the effectiveness of internal control over reporting, risk management and compliance.
- Adjust scope and frequency—Management and financial services organization supervisors vary the scope and frequency of separate evaluations depending on the significance of risks being controlled, the importance of the controls in mitigating the risks and the effectiveness of ongoing monitoring.

Increasingly, IT performance and effectiveness are being continuously monitored using performance measures that indicate if an underlying control is operating effectively.

Consider the following examples:
- Defect identification and management—Establishing metrics and analyzing the trends of actual results against metrics can provide a basis for understanding the underlying reasons for processing failures. Correcting these causes can improve system accuracy, completeness of processing and system availability.
- Security monitoring—Building an effective IT security infrastructure reduces the risk of unauthorized access. Improving security can reduce the risk of processing unauthorized transactions and generating inaccurate reports, and should result in a reduction of the unavailability of key systems if applications and IT infrastructure components have been compromised.

An IT organization also has many different types of separate evaluations, including:
- Internal audits
- External audits
- Regulatory examinations
- Attack and penetration studies
- Independent performance and capacity analyses
- IT effectiveness reviews
- Control self-assessments

- Independent security reviews
- Project implementation reviews

At the entity level, the following may be expected:
- Centralized continuous monitoring of computer operations
- Centralized monitoring of security
- IT internal audit reviews (While the audit may occur at the activity level, the reporting of audit results to the audit committee is at the entity level.)

At the activity level, the following may be expected:
- Defect identification and management
- Local monitoring of computer operations or security
- Supervision of local IT personnel

The monitoring component relates to Basel II Principles 2, 8 and 9.

Operational Risk Principles and IT Relevance

Information technology and information management are key elements of a comprehensive strategy to manage GRC and optimize the capital charge. IT-related components such as applications, infrastructure elements and controls are all defined as parts of operational risk. **Figure 6** exhibits the guiding Basel II principles on operational risk and the component of COSO ERM that is addressed, as well as their relevance and requirements in terms of information technology.

The principles are provided to enable the use and implementation of *IT Control Objectives for Basel II* within the context of an integrated GRC framework.

Figure 6—Basel II Principles, COSO Components, and IT Relevance and Requirements

Basel II Principles Note: All italicized text is taken from Basel II.	COSO Components	IT Relevance and Requirements
Developing an Appropriate Risk Management Environment		
Principle 1: *The board of directors should be aware of the major aspects of the bank's operational risks as a distinct risk category that should be managed, and it should approve and periodically review the bank's operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored and controlled/mitigated.*	Internal environment	IT should be integrated into the overall risk management process.

Figure 6—Basel II Principles, COSO Components, and IT Relevance and Requirements *(cont.)*

Basel II Principles Note: All italicized text is taken from Basel II.	COSO Components	IT Relevance and Requirements
Principle 2: *The board of directors should ensure that the bank's operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management.*	Monitoring	The financial services organization's operational risk management framework, including the IT components, should be included in the internal audit plan. The internal IT audit function should be adequately skilled and staffed. Required skills should include an understanding of Basel II, risk management principles, and financial services organizations regulatory and supervisory requirements. The internal IT audit function should be reviewed by the financial services organization's supervisors. External specialist resources should be used where appropriate.
Principle 3: *Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be consistently implemented throughout the whole banking organisation, and all levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all of the bank's material products, activities, processes and systems.*	Internal environment Information and communication	Members of IT management have the same responsibilities as members of senior management. The framework adopted by the bank should be adapted to meet IT requirements (most common GRC frameworks do not address IT in sufficient detail). Consideration could be given to implementing an IT control framework that can be reconciled to the financial services organization's GRC framework. The framework adopted should address areas that would be expected to be addressed by the financial services organization's supervisors and examiners, e.g., IT corporate governance, IT planning and organization, security, systems development, program changes, operations and support, and internal control responsibilities.

Figure 6—Basel II Principles, COSO Components, and IT Relevance and Requirements *(cont.)*

Basel II Principles Note: All italicized text is taken from Basel II.	COSO Components	IT Relevance and Requirements
Risk Management: Identification, Assessment, Monitoring and Mitigation/Control		
Principle 4: *Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems. Banks should also ensure that, before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.*	Objective setting Event identification Risk assessment	Risk assessment should be incorporated in all IT activities that could have a material impact on the bank, e.g., program changes, infrastructure changes and security monitoring. Risk assessments should be integrated into the system development and release management processes. Stakeholders who could be impacted materially should be involved in the risk assessment. Risk assessment results should be integrated with other risk assessments and incorporated into the GRC framework.
Principle 5: *Banks should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.*	Event identification Risk assessment Information and communication	Assessment of operational risk should be incorporated into the annual planning and strategic planning cycle. Operational risk should be reassessed following significant internal and external events, e.g., if an external disaster indicates that the contingency planning strategy should be readdressed. Risk performance metrics should be identified and tracked. If an unfavorable trend is detected, the root cause analysis of the defect should be undertaken and corrective actions implemented.

Figure 6—Basel II Principles, COSO Components, and IT Relevance and Requirements *(cont.)*		
Basel II Principles Note: All italicized text is taken from Basel II.	**COSO Components**	**IT Relevance and Requirements**
Principle 6: *Banks should have policies, processes and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.*	Risk response Internal environment Information and communication Control activities	An IT internal control framework should be in place to mitigate operational risk. The IT internal control framework should be supported by appropriate policies, processes and procedures. Operational risk should be reassessed following significant internal and external events, e.g., if another bank is purchased, consideration should be given to the impact the integration of systems could have on operational risk. IT policies and procedures should be reviewed and formally approved on at least an annual basis.
Principle 7: *Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.*	Risk response	IT should have IT continuity plans and management procedures that link to corporate business continuity and incident response management.
Role of Supervisors		
Principle 8: *Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks as part of an overall approach to risk management.*	Monitoring	IT should implement an IT risk management framework that addresses the requirements of the financial services organization's supervisors.

Figure 6—Basel II Principles, COSO Components, and IT Relevance and Requirements *(cont.)*

Basel II Principles Note: All italicized text is taken from Basel II.	COSO Components	IT Relevance and Requirements
Principle 9: *Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank's policies, procedures and practices related to operational risks. Supervisors should ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at banks.*	Monitoring the financial services	IT senior management should ensure that IT-related regulatory compliance requirements are integrated with the overall organizational policies and procedures addressing operational risk and supervisory requirements, and that deficiencies identified by organization's examiners are addressed in a timely manner. The IT compliance function should be integrated with the financial services organization's compliance function to ensure that the financial services organization's supervisors remain apprised of IT developments.
Principle 10: *Banks should make sufficient public disclosure to allow market participants to assess their approach to operational risk management.*	Internal environment Information and communication	IT should identify all relevant risks that constitute a material operational risk and communicate them to the board and senior management for their consideration.

6. Managing Information Risks

Information and IT management require a specific approach toward GRC. The complexity of an IT environment, its interdependencies with business processes, and the need to identify and address indirect risks are decisive factors in defining and deploying an IT risk framework. Risk evaluation, control and mitigation must be aligned with the overall operational risk approach that the organization has selected under Basel II. The operational risk principles defined in *Sound Practices for the Management and Supervision of Operational Risk*[6] lead to a corresponding set of guiding principles for managing information management and IT risks.

IT Guiding Principles

To apply *IT Control Objectives for Basel II*, guiding principles are required for IT practitioners and financial services experts whose tasks and responsibilities include aspects of information technology. The following IT guiding principles (ITGPs) have been developed using a set of source documents, including:

- The *International Convergence of Capital Measurement and Capital Standards* (Basel II Capital Accord or Basel II) published by the Basel Committee in June 2006[7]
- The Principles defined in the *Sound Practices for the Management and Supervision of Operational Risk* published by the Basel Committee in February 2003[8]
- The *Enterprise Risk Management—Integrated Framework* published by COSO in September 2004[9]

ITGP1 (Operational Risk Awareness)
Information management and technology form a critical part of operational risk management. Practitioners, internal auditors and financial services experts should be aware of the significance of information risk.

As the organization should be aware of operational risks influencing the overall risk position and, thus, the capital charge, so too should it define and gain in-depth understanding of the IT component. Awareness should not be restricted to the fact that there is an existing IT risk. All GRC-related objectives and practices should be aligned with the organizational GRC framework.

[6] Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of Operational Risk*, February 2003
[7] More information on the *International Convergence of Capital Measurement and Capital Standards* can be found at *www.bis.org/publ/bcbs107.htm*.
[8] More information on the *Sound Practices for the Management and Supervision of Operational Risk* can be found at *www.bis.org/publ/bcbs91.htm*.
[9] More information on the *Enterprise Risk Management—Integrated Framework* can be found at *www.coso.org/publications.htm*.

According to Basel II, operational risk is "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk." Legal risk includes, but is not limited to, exposure to fines, penalties or punitive damages resulting from supervisory actions and private settlements. Operational risk specifically "excludes strategic and reputational risk."[10] The definition of operational risk noted previously should be applied to information technology and information management, as many IT-related risks will address systems and related issues in the people or internal process category. External events, such as incidents or disasters that prevent the functioning of critical infrastructures, may influence information technology.

Similar rigor should be applied to the management of operational risk as would be expected for the management of other significant financial services risks, such as credit risk, interest rate risk and liquidity risk. However, operational risk differs from other financial services risks in that it is typically not directly taken in return for an expected reward, but exists in the natural course of corporate activity, and this affects the risk management process.[11] At the same time, failure to properly manage operational risk can result in a misstatement of an institution's risk profile and expose the institution to significant losses.

For the information management and IT area within a financial services organization, this means that operational risks in IT must be managed at a level that is at least as detailed and comprehensive as other GRC components, such as credit or market risk. Therefore, GRC components for IT should be adequately managed in terms of budget, resources, and management attention and support.

ITGP2 (Internal Audit Requirement)
The internal IT audit function should be effective and comprehensive. Skills, resources and funding should be adequate to ensure audit effectiveness.

The importance of internal audit, in general, should be reflected in the setup and functioning of internal IT audit, or operational and information risk audit. The size and complexity of the financial services organization under review should determine the skills, resources and funding of the internal IT audit function. This may include the use of specialist external resources where internal resources cannot provide an adequate level of coverage or effectiveness. Internal IT audit should have ultimate accountability to the organization's audit committee and should report to the board as appropriate.

[10] Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards*, June 2006, paragraph 644

[11] The Basel Committee recognizes that, in some business lines with minimal credit or market risk (e.g., asset management, and payment and settlement), the decision to incur operational risk, or compete based on the ability to manage and effectively price this risk, is an integral part of a bank's risk/reward calculus.

It should be noted that internal IT audit must be impartial and independent with regard to the organization's management.

ITGP3 (Management Policies, Processes, Procedures)
Information management and technology should be governed by an adequate set of policies, processes and procedures for risk management. The guidance given to practitioners, internal auditors and financial services experts should be in line with the organization's GRC framework.

Managing GRC requires a clearly defined and documented set of policies, processes and procedures that matches the overall structure and order of general policies on GRC. IT policies should be specific and targeted in their scope and contents. This guiding principle addresses the requirement for a risk management process, as distinct from risk-related controls (see ITGP6).

Operational risk disciplines relate to the management of operational risks only, as distinct from the risk functions that are responsible for the management of other types of risk. This means that the work done on operational risk by the credit or market risk management functions does not become a credit or market risk discipline. Similarly, an operational risk breakdown within the credit or market risk management functions does not become a credit or market risk breakdown.

This principle is particularly important for the IT function within a financial services organization. IT components are often implemented to manage, control and report credit risk, market risk and other types of core business risk. However, the IT applications and infrastructure elements are still within the operational risk domain, regardless of their specific purpose. As an example, the failure of a credit risk measurement application is an IT failure and, therefore, a systems failure in the sense of operational risk.

ITGP4 (Risk Assessment)
In information management and technology, specific risk assessments should be conducted, using approved methods in line with the organization's GRC framework. Risk assessments should take into consideration the technology-specific complexity and indirect risk factors.

To understand IT risk and related factors, the risk assessment methods selected should provide an in-depth understanding of both direct and indirect risk. Any risk assessment conducted should cover the risks intrinsic to IT and the risks induced by the use of IT.

The organization's risk profile covering its major risks is a prerequisite to effective and efficient risk management. The risk profile should provide an inventory of the organization's major risks and articulate how the business line, risk management, security practitioners, continuity planners and internal audit are fulfilling their accountability in the management of the

risks that fall within their areas of accountability. The structure of an IT organization should include an appropriate segregation of duties.

ITGP5 (Risk and Loss Monitoring)
Losses related to information management and technology should be measured and documented. Specific risk profiles should be monitored.

Technology-related losses should be monitored in line with the overall loss monitoring implemented by the organization. Risk profiles should adequately reflect the complexity of technology and its use within financial services organizations.

The organization must have a clearly defined understanding of its risk appetite, or how much risk the entity is willing to assume. Risks or events falling outside the defined risk appetite should be identified for immediate remedial action. Incident responsibilities need to be assigned in line with the organization's incident management and escalation policies. These policies should also define a process for notification so that the chief executive officer (CEO), the chief risk officer, the chief information security officer (CISO), internal audit, and the board risk and audit committees are aware of significant incidents and the risks they represent.

Compliance under the evolving regulatory regime is focused on accurate reporting. While Basel II data quality is a means to an end rather than an end in itself, the deployment of capital based on risks requires high-quality, high-frequency data. Robust information is at the heart of improved risk management. Inadequate data quality is likely to introduce errors in decision making in an environment in which corporate executives must attest to the accuracy of their financial statements and the quality of internal controls.

The "Observed Range of Practice in Key Elements of Advanced Measurement Approaches (AMA)" paper[12] identified the following challenges relative to data quality:

> *The nature and quality of operational risk data collected by an AMA bank affect not only the outcome of the bank's quantification process but also its operational risk management decisions. As a result, Basel II prescribes certain standards a bank's operational risk data must satisfy before the bank will qualify for an AMA. These standards relate principally to the characteristics of the data, how it is collected and how it is used. The purpose of the standards is to provide some insight into supervisors' minimum expectations regarding data integrity and comprehensiveness, both of which are critical to the effective implementation of an AMA.*

[12] Published by the Accord Implementation Group's Operational Risk Subgroup (AIGOR) in October 2006, the paper focuses on the practical challenges associated with the development, implementation and maintenance of an operational risk management framework to meet the requirements of Basel II, particularly as they relate to the AMAs.

AMA operational risk data has multiple applications, including risk quantification, risk management and accounting and other forms of reporting. Some data are suitable for more than one application, whereas other data are single-purpose.

Data quality requires building processes, procedures and disciplines for managing information and ensuring its integrity, accuracy, completeness and timeliness. The fundamental attributes supporting data quality should include:
- Accuracy
- Integrity
- Consistency
- Completeness
- Validity
- Timeliness
- Accessibility
- Useability
- Auditability

The data quality provided by the various applications depends on the quality and integrity of the data upon which that information is built. Entities that treat data as an organizational asset are in a better position to manage them proactively. Entities that treat data as someone else's problem are constantly dealing with the "garbage in, garbage out" scenario.

The commitment to data quality needs to be driven from the top, with a clear line of accountability threaded throughout the company. Ultimately, the board, CEO, CFO, chief risk officer and CISO are accountable for data integrity and fitness for the purpose of compliance.

ITGP6 (Control and Mitigation Policies, Processes, Procedures) Information management and technology should be governed by an adequate set of policies, processes and procedures for risk control and mitigation. The guidance given to practitioners, internal auditors and financial services experts should be in line with the organization's GRC framework.

For risk control and mitigation, policies, processes and procedures should be implemented as a complement to management policies. This may include specific processes for control and measurement, mitigation procedures for individual risks, and other guidance to provide comprehensive coverage of risks in information management and technology. Risk control and mitigation should be seen as distinct from the overall risk management process (see ITGP3).

In a marketplace where one person can undermine the reputation of a regulated financial institution, all parts of the organization must be aware of and take responsibility for compliance-related risks. Since an organization is as strong or as ethical as its weakest or most unethical employee, the blame for a poor control environment must be shouldered throughout the organization. While the board and senior management must set the tone at the top of the organization for corporate culture, which acknowledges and maintains an effective control environment, each and every person within the organization should be "tuned in" to internal controls. Rules are meaningless in a culture of noncompliance.

ITGP7 (Business Continuity Management)
Information management and technology should be protected by a comprehensive continuity management process. The IT continuity management process should be in line with the organizationwide business continuity management framework.

IT continuity, incident management and recovery are all components of a comprehensive IT continuity management process. It is essential that the management of IT continuity be aligned with overall business continuity to enable the continuation of IT and core business processes under adverse circumstances.

High-level principles of business continuity in financial services organizations have been documented by the Basel Committee.[13] The principles stipulate that an organization should design and implement a business continuity management (BCM) process with senior management responsibility for implementation and monitoring. The high-level principles include elements of an ongoing BCM life cycle, as expressed in other standards and publications.[14] For information management and technology, as well as information-related risks, IT continuity planning, regardless of the method and framework applied, should be aligned with overall enterprisewide BCM. For IT continuity, the design, implementation and monitoring should be adequate and appropriate, as outlined in various sources.[15] IT is one component of a larger BCM capability within the organization. It should be noted that IT continuity at a mature level requires strong business support and interaction with business process owners since IT cannot exist alone or be the subject of an isolated continuity plan.

[13] Joint Forum, "High-level Principles for Business Continuity," 2006
[14] cf. British Standard 25999-1 and the Business Continuity Institute, *Good Practice Guidelines for Business Continuity Management, 3rd Edition*, 2007
[15] cf. ITIL (IT Continuity Management), ISO 27001 and BS PAS 77

ITGP8 (Framework for Risk Control and Mitigation)
Information management and technology should be an integral part of the organization's GRC framework. Control and mitigation of information-related risks should be defined and recognized in the GRC framework.

IT-related risk control and mitigation plans and activities should be designed, implemented and monitored in accordance with the GRC framework. Any technology-related measures should be recognized as a separate and distinct type of risk in the GRC framework. This may include organizational management, individual controls and guidance on compliance.

IT risk control and mitigation are often defined as part of the ERM framework, which is, in turn, a component of organizational GRC. ERM is a fairly broad topic that may have different meanings to different people. COSO states that ERM:
- Is a process—It is a means to an end, not an end in itself.
- Is affected by people—It is not merely policies, surveys and forms; it also involves people at every level of an organization.
- Is applied in setting strategy
- Is applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk
- Is designed to identify events potentially affecting the entity and also manage risk within its risk appetite
- Provides reasonable, but not absolute, assurance to an entity's management and board
- Is geared to the achievement of objectives in one or more separate, but overlapping, categories

The underlying assumption of ERM is that every entity exists to provide value to its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. ERM enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value.

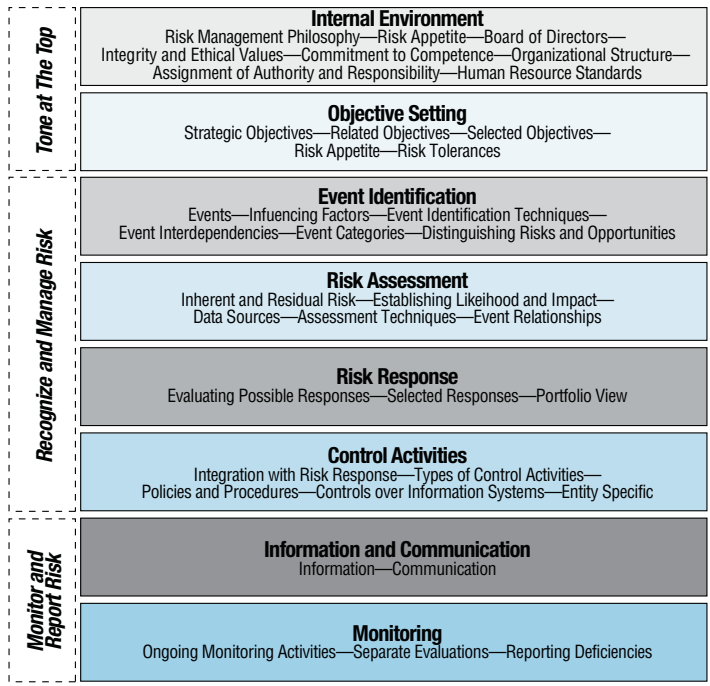
Value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives.

ERM encompasses:
- Aligning risk appetite and strategy—Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives and developing mechanisms to manage related risks.

- Enhancing risk response decisions—ERM provides clear direction to identify and select among alternative risk responses—risk avoidance, reduction, sharing and acceptance.
- Reducing operational surprises and losses—Entities improve their ability to identify potential events and establish responses, reducing surprises and associated costs or losses.
- Identifying and managing multiple and cross-enterprise risks—Every enterprise faces a wide variety of risks affecting different parts of the organization, and ERM facilitates effective response to the interrelated impacts and integrated responses to multiple risks.
- Recognizing opportunities—By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.
- Improving allocation of capital—Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

The COSO ERM framework, illustrated in **figure 7**, consists of eight interrelated components, from internal environment to monitoring, within three distinct domains, i.e., tone at the top, recognize and manage risk, and monitor and report risk.[16]

Figure 7—COSO ERM Framework



[16] Each of these components is described in detail in the COSO literature, which is available for download for a small price at *www.coso.org/publications.htm*.

ERM takes a holistic approach to managing risks on an enterprisewide basis. It is important to note in this context that ERM is not restricted to the downside or risk avoidance; rather, it is about taking risk in an informed and balanced approach. All eight control components must be present and functioning across the organization. This involves identification of the key risks that have an impact on the entity's objectives. These risks are initially assessed on an inherent basis, which involves understanding these risks in the absence of any controls. The residual level of risks is then assessed, taking into consideration the controls in place to manage such risks. Where the residual level is outside the risk appetite, additional controls are implemented to bring the risks into the boundaries set by the level of risk appetite.

The achievement of an entity's objectives is treated as an outcome of the integrated ERM framework and objectives are categorized as:
- Strategic—High-level goals aligned with and supporting the mission
- Operations—Effective and efficient use of resources
- Reporting—Reliability
- Compliance—Applicable laws and regulations

In information management and information technology, risk management initiatives and programs should be integrated with the overall GRC approach. In applying this guiding principle, practitioners should make use of other ISACA/ITGI publications to understand the links between ERM (in accordance with COSO) and IT—using COBIT.

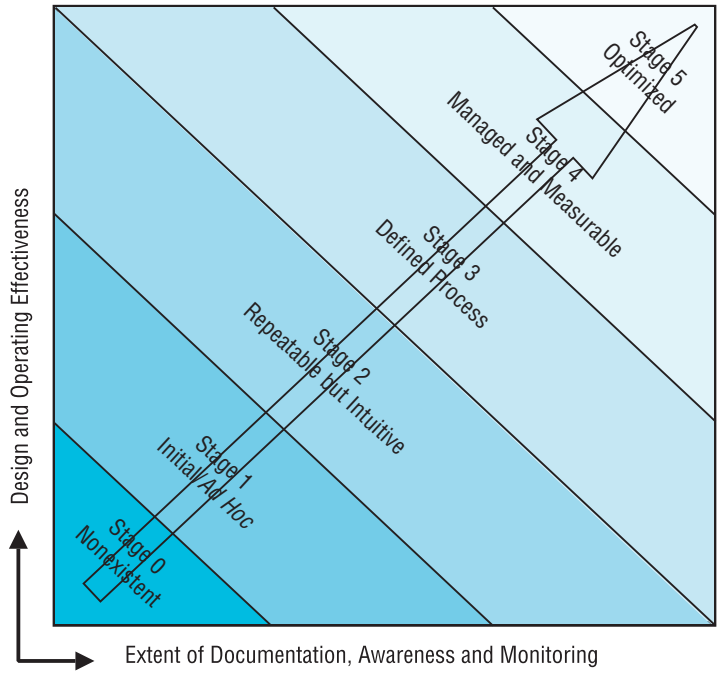
ITGP9 (Independent Evaluation)
Information management and technology-related risks shall be adequately documented to support the supervisory review process. An independent audit function should perform reviews of IT-related operational risk management in line with the operational and information risk profile.

Information-related risks require documentation in line with the requirements of the supervisory review process to enable and support this process. Documentation should be subject to impartial and independent review, including external reviews at regular intervals. Audits and independent reviews of the IT risk documentation should be aligned with the risk profile defined by the organization.

Organizations should adopt a holistic capability maturity assessment of their ERM, where "capability" is how well a discipline or process works and "maturity" is a measure of how far the capability has developed. Processes examined within the context of the maturity model should be at least at stage 4, which requires them to be both managed and measurable.

Each component of the ERM framework is assessed against the six stages of control reliability, as shown in **figure 8**:

Figure 8—Stages of Control Reliability



- **0 Nonexistent**—Absence of risk management processes. The organization has not recognized that issues need to be addressed.
- **1 Initial/*ad hoc***—There is evidence that the organization has recognized that issues exist and need to be addressed. There are no standardized processes, but there may be *ad hoc* approaches tending to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.
- **2 Repeatable but intuitive**—Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.
- **3 Defined**—Procedures have been standardized and documented, and communicated through training. It is, however, left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated, but are the formalization of existing practices.

- **4 Managed and measurable**—It is possible to monitor and measure compliance with procedures and to take action where processes appear to be ineffective. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
- **5 Optimized**—Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modeling with other organizations. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

The organization's ERM capability maturity framework must be assessed and managed bottom-up and top-down. ERM needs to be an integrated framework; therefore, the capability maturity assessment must determine weak points, such as data quality in monitoring, role clarity, tools and people skills, that could potentially undermine the whole ERM framework. See appendix IV, The Dependence of the COSO ERM Framework on Data Quality.

ITGP10 [Disclosure]
Practitioners, internal auditors and financial services experts should identify all information-related risks that may be subject to disclosure. These risks should be communicated to stakeholders as defined by the organization's GRC framework. Corrective action should be taken as appropriate.

Risks, deficiencies and other issues identified within the organization should be evaluated and assessed with regard to their severity and significance. Where an individual risk or more than one risk in combination may lead to operational losses that require disclosure, this information must be communicated to stakeholders as appropriate. This escalation should be clearly defined in the overall GRC framework.

Causes of Loss and IT Risk

Operational risk is easily recognized but difficult to comprehensively define. Risk factors may be found anywhere in the operation of a financial services organization. Potential losses may arise from failures in one or more areas of the organization that would not normally be considered profit centers or value contributors. The Basel Committee has defined operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."[17] This definition includes legal risk but excludes strategic and reputational risk. Specific emphasis is placed on the fact that risks may be interdependent. As a result, "systemic" risk, working across multiple areas or even organizations, should be considered. One of the

[17] Basel Committee on Banking Supervision, "Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework—Comprehensive Version," June 2006

contributing factors to systemic risks is the fact that financial services organizations usually depend on information technology and information management, and complex infrastructures are required to support core business processes.

IT is a significant component of operational risk and, therefore, is a part of the capital charge attributable to operational risk.

The definition of operational risk looks very broadly at causes since they provide an effective mechanism for classifying events. Causes include:
- Processes—Loss events caused from a firm's execution of business operations
- People—Loss events caused by employee errors or misdeeds
- Systems—Loss events resulting from a disruption of service or from technology failures
- External events—Loss events caused by natural and unnatural events that threaten the ability of the firm to continue operations

The strictly causal orientation of the definition is important in the Basel II context since the two other main risk categories—credit risk and market risk—also have clearly distinguishable causes: credit being granted or a market position being entered.

Although banks may choose to adopt their own definitions of operational risks, the definition must consider the full range of material operational risks facing the bank and must capture the most significant causes of potentially severe operational losses.

Cause classification types can be used as a starting point for managing operational risk, especially regarding the mitigation, transfer or avoidance of risk. To provide greater clarity and differentiation that is useful in managing IT risk, the four main types of causes should be broken down into three levels of cause categories. This is especially important since, in practice, risks are often attributed to more than one cause, but should only be allocated to one classification type.

Several brief examples are provided to help clarify the concepts.

Example 1
An insider exploiting a programming error in an internal web application should be categorized in the cause category of systems, whereas an intruder obtaining access to a bank's computer using hacking tools, phishing or malware should be categorized under external events.

Example 2
A fire occurring in the data center destroys IT systems, resulting in IT being unable to support business activities. Taking the Basel II cause and loss event categories, this would be categorized as an external event and the category would be damage to physical assets/disaster.

Looking at the causal chain, the main elements of this risk event would be:
External event (fire)→disaster (fire in the data center)→damage to physical assets (IT system destroyed)→business disruption (business processes not available)

It is apparent that this comparatively simple risk event already links to two Basel II loss event types: damage to physical assets, and business disruption and system failures. The business disruption, in itself, is attributable to the cause category systems, if this loss event type of the chain is addressed. If the fire was caused by an electrician who improperly connected two power cables, a third category would be added: people.

If IT staff members put a new release into production without sufficient testing and without backing up new data elements included in the new release, a fourth category would be added: processes for the release of systems into production, or change management, in general.

This example highlights the difficulties in identifying and weighing the event types to which a chain of risks and resulting losses are attributed. It is further apparent from the example that the cause-oriented definition of operational risk should be applied to information-related risks. Financial services organizations implementing this risk identification and categorization method should identify additional level II risk categories using COBIT resources and processes and should subsequently identify and prioritize the level III risks resulting from their individual qualitative and quantitative risk assessment.

The Basel Committee has identified operational event types with the potential to result in substantial losses:
- Internal fraud
- External fraud
- Employment practices and workplace safety
- Clients, products and business practices
- Damage to physical assets
- Business disruption and system failures
- Execution, delivery and process management

The committee has provided a definition for each loss event type with subcategories and activity examples.

Considering the causes and loss event types, it follows that many operational risks are IT-related, either as direct IT issues (e.g., a fire destroying the data center) or as indirect IT issues [e.g., business process controls (four-eye principle[18]) that are not working because of a programming error in the financial services organization's application].

For IT risk management, the causes and loss event types of Basel II must be detailed further.

For operational risk management, in the sense of identifying, measuring and monitoring/controlling operational risk, the Basel II cause and loss event types may not be sufficiently comprehensive. The multiple causes and resulting events form a network of interdependencies that cannot be fully described. As a result, risk scenarios may be used to provide examples of causal chains and effects. These scenarios are useful tools for illustrating the most common types of IT risks and their consequences for the organization.

IT Risk Scenario Analysis

Basel II requires financial services organizations using the AMA approach to use scenario analysis and expert opinion in conjunction with external data to evaluate their exposure to high-severity, infrequent events. The scenario analysis approach brings experienced business managers and risk management experts together to derive reasoned assessments of plausible severe losses.

For an operational and information risk management approach, experienced IT practitioners, information security specialists, business managers, risk management experts, and IT specialists from internal audit and the IT compliance function should be brought together to discuss the IT scenarios with a reasonable probability of occurring and resulting in severe expected losses.

The IT scenarios in **figure 9** may be regarded as illustrative, being categorized into A and B in terms of importance. These groupings show the relative importance of certain IT scenarios to the financial services industry.

In performing scenario analyses, the frequency and severity of risk drivers should be considered, as the objective of this analysis is to obtain a well-founded expert assessment for further statistical loss distribution. In expert assessments, estimates and expectations based on past experience and market practice may be substituted if operational loss data are not available.

[18] The four-eye principle means that all business decisions and transactions need approval from the CEO and CFO.

Figure 9—IT Scenarios		
Illustrative IT Scenarios	**Scenario Definition**	**Category**
Performance of unauthorized activities by authorized users	Users have access to and misuse functions such as correction capabilities, manipulate software or systems, change application data, circumvent access privileges, or manipulate input data.	A
Disruption of service	There is a failure of hardware/software, critical service or environmental systems or data loss, denial of service, or a capacity planning error.	A
Incomplete transaction processing	Errors or incomplete transaction processes are not detected, resulting in erroneous results.	A
Misuse of sensitive assets	Those with authorized access misuse access privileges.	A
Project failure	Project results are not delivered within agreed-upon time frames, within budget and with appropriate quality.	A
Product failures	There is a failure to identify security requirements or to design security into product selection and implementation activities.	B
Third-party risk	Risks related to reliance on third-party services are not well defined or are improperly managed.	B
Theft of sensitive or critical assets	Hardware/software components, devices, system output, data files, notebook computers, portable computing devices, etc., are stolen.	B
Malicious activity	Hacking, phishing, social engineering or cyberextortion are taking place.	B
Process failure	There is a lack of integration of security into sensitive business processes.	B

Figure 10 illustrates the risk drivers for those that are labeled category A IT scenarios.

Scenario analysis requires that a correlation of multiple scenarios be taken into account; this is essential to identify and evaluate potential losses arising from multiple and simultaneous operational loss events caused by one or more risks. Scenarios should consider internal loss data for evaluating the relative significance of information-related risks and external loss data (where available) for plausibility checks against market and other historic data.

Scenario analyses and risk assessments based on expert opinion should be frequently validated and reassessed by comparing them to actual loss data available over time. This is an essential aid to ensure the reasonableness of qualitative methods applied to risk management.

Figure 10—Illustrative Risk Drivers for Category A IT Scenarios

IT Scenario	Risk Driver for Frequency	Risk Driver for Severity
Performance of unauthorized activities by authorized users	• Users with access to sensitive application functions • Lack of supervisory control • Improper definition of access permissions • Excessive access to and use of supervisory capabilities • Improper access to software or systems	• Inadequate monitoring of system exception reports • Lack of management control • Lack of audit review • Inappropriate security policies • Lack of proper security awareness training • Lack of accountability • Inadequate access management
Disruption of service	• Number of potential damaging incidents that could cause a disruption of service • Susceptibility of hardware and software to damage • Failure to identify interdependencies among systems and applications	• Inability to correctly identify the impact of conditions that can result in a disruption of service • Failure to monitor for events that can result in a disruption of service • Failure to develop and implement incident detection and escalation procedures
Incomplete transaction processing	• Potential for processing errors to go undetected	• Potential for significant damage resulting from incomplete processing
Misuse of sensitive assets	• Number of shared user IDs or group accounts • Number of users with access to sensitive applications or application functions • Lack of comprehensive security policies, procedures and standards • Failure to provide security awareness • Lack of monitoring and correction by supervisors • Failure to consider security when defining business procedures and processes	• Lack of monitoring tools or inconsistent use of these tools • Lack of ability to respond to security incidents
Project failure	• Number of projects • Quality of defined program and project management approach	• Amount of project budget • Number of critical projects

7. Business Processes to IT Risks to IT Controls: Applying the CobiT Framework

The Basel Committee recommends a business line approach to the measurement and management of operational risks. In the standardized approach, gross income by business line is considered to be a broad indicator suitable to serve as a proxy for the scale of business operations and, thus, the likely scale of operational risk exposure within each business line.

Use of Existing Documentation

In most financial services organizations, there is existing documentation that describes business processes. This documentation may include:

- Policies and procedures (especially when required by regulators and kept up to date through the compliance function)
- Business process reengineering documentation
- Financial reporting compliance documentation (e.g., Sarbanes-Oxley)

This documentation can often be used as a basis to begin an analysis of operational risks. For example, Sarbanes-Oxley or any financial reporting, compliance-focused documentation may exist, but the focus is on identifying key controls for financial reporting purposes. In a trading process, the key control is normally the matching and reconciliation process in the back office. It is unlikely that controls in front-end systems would be relied upon. However, for operational risk purposes, front-end systems are very important. Customer limits, trading strategies (particularly in the assessment of risk appetite in determining a trading strategy), security and program change controls all become important when assessing operational risk.

The Business Line Approach in Basel II

Besides the business line perspective, a financial services organization must also be able to manage risks in a centralized function (e.g., an IT department) for an activity that spans more than one business line. In the end, the Basel Committee requires that all banking activities must be mapped to one of the following eight business lines:

- Corporate finance
- Trading and sales
- Retail banking
- Commercial banking
- Payment and settlement
- Agency services
- Asset management
- Retail brokerage

Most business lines will not be able to operate without the support of IT. The level of required support, of course, depends on the nature of the business. Retail brokerage as a function of electronic banking for retail customers obviously requires complex IT systems that must be available on a continuous basis. On the other hand, corporate finance has very different requirements, such as the ability to rapidly develop models and software-based scenarios for product innovation and individual transactions.

The exposure to operational risk should be established by identifying and assessing the operational risk inherent in all material products, activities, processes and systems. In addition to identifying the most potentially adverse risks, banks should assess their vulnerability to these risks. The basis of this assessment may be the systematic and detailed analysis of processes within each line of business. Usually, the product processes are a good starting point since these processes, where a product or service is offered to external customers, are the source of income and revenue.

In retail brokerage, a financial services organization offers services (e.g., purchasing shares at the exchange) to retail customers. To use this service, customers must key their orders into an Internet application. Upon authentication of the order, it is processed by the bank and settled by the exchange, and the settlement is sent to the customers, adding the shares to their portfolio and deducting the money from their accounts. Prior to processing, the identity of customers is authenticated and their profiles are checked to ensure that they have permission to initiate the type of transaction specified. The complete process may be provided through multiple IT systems, both internal and external to the financial services organization, providing not only core application components, but also pricing feeds and exchange settlement.

One way to assess the risk exposure inherent in these processes is to apply scenarios to them. Certain scenarios, such as identity theft in retail brokerage, can be assessed quite accurately, knowing the details of the process outline. Other scenarios that are more financial services organizationwide in nature are more difficult to assess with any degree of certainty.

In a wide range of operational risk scenarios, the business processes controls in place prevent typical risk drivers from becoming too frequent or too severe. These mitigating controls should be considered in addition to other factors, such as internal or external loss data, when evaluating the potential scenario impacts.

Defining IT Risk

When designing and outlining scenarios for risk evaluation, the use of CobiT may assist in defining a standardized control environment for the scenario under review by stating the applicable control processes. **Figure 11** shows corresponding control objectives for category A IT scenarios.

Figure 11—Illustrative Mapping of IT Scenarios Against CobiT Processes

IT Scenario	CobiT Process
Performance of unauthorized activities by authorized users	DS5 Ensure systems security.
Disruption of service	DS4 Ensure continuous service.
Incomplete transaction processing	AC4 Processing integrity and validity
Misuse of sensitive assets	DS5 Ensure systems security.
Project failure	PO10 Manage projects.

At a high level, the risk assessment should consider whether the organization has implemented an adequate control environment consisting of entity- and process-level controls. Entity-level controls typically incorporate the COSO elements:

- Control environment
- Risk assessment
- Information and communication
- Monitoring (in part)

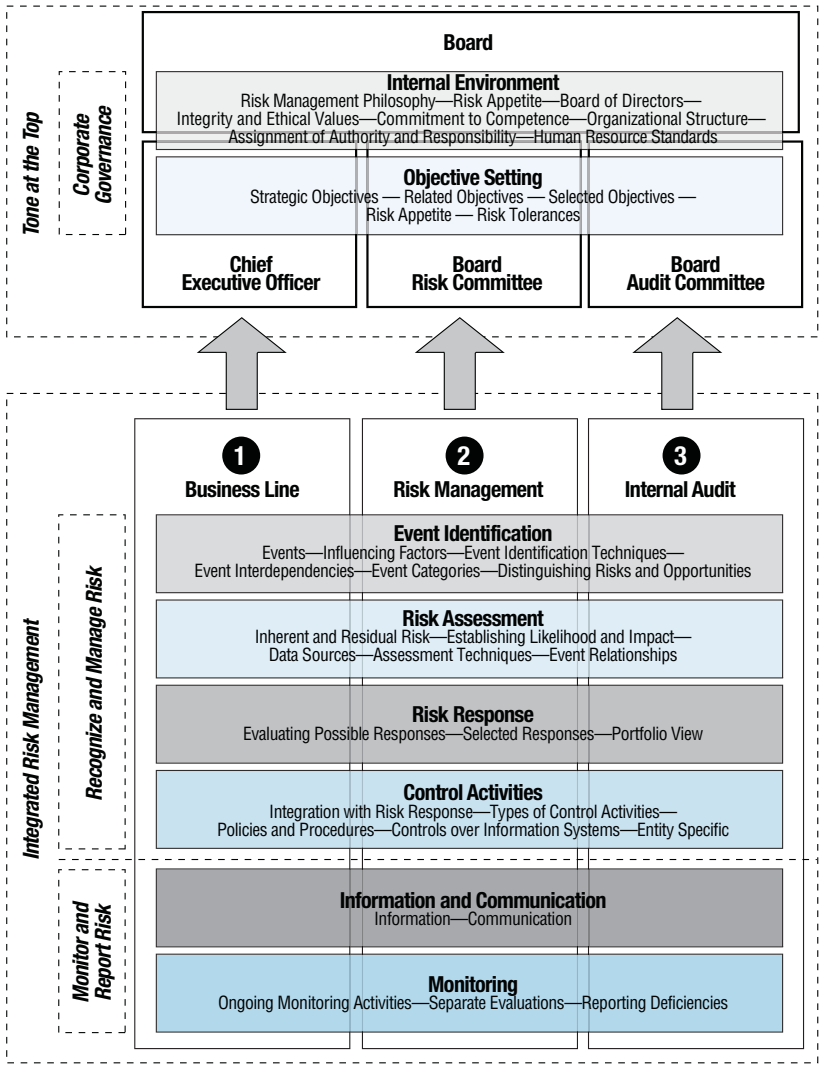
Part of the entity-level controls might include the concept of multiple layers of defense and related responsibilities. A number of firms have appointed risk managers, but there is considerable variation in the level of experience, seniority and status of these individuals. In some organizations, the risk manager has senior status and the ability to challenge decisions and provide an in-depth assessment (e.g., verifying the terms of contracts). In others, the role is limited to the completion of a basic risk assessment without any empowerment to challenge decisions—essential requirements of the risk function.

To organize the respective roles of compliance, internal audit and risk, some organizations have structured themselves in a three lines of defense model[19] (see **figure 12**) where risk management provides a second line independent challenge and audit provides assurance that the first two lines are operating as intended.

[19] The three lines of defense model has been adopted by a number of financial services institutions [refer to the reference to the model in the 2006 Annual Financial Report of the National Australia Bank (Risk Management: Introduction—page 15)].

Within the context of the evolving risk-based, principles-driven regulatory supervision, regulatory compliance has emerged as an outcome of the organization's integrated ERM framework. Effective governance across all risk management disciplines (including credit risk, interest rate risk, liquidity risk and operational risk) is highly dependent on the capability maturity of the three lines of defense model illustrated in **figure 12**, based on the COSO ERM framework.

Figure 12—Lines of Defense: ERM Framework



Control must be exercised through clearly defined and independent lines of defense—the business line, risk management and internal audit—all playing an important function within the integrated ERM, as shown in **figure 13**. The three lines of defense model distinguishes among functions owning and managing risks, functions overseeing risks, and functions providing independent assurance, as follows:

- The board sets the organization's risk appetite, approves the strategy for managing risk and is ultimately responsible for the organization's system of internal control.[20] The CEO, supported by senior management, has overall responsibility for the management of risks facing the organization. Management and staff members within each business have the primary responsibility for managing risk. They are required to take responsibility for the identification, assessment, management, monitoring and reporting of enterprise risks arising within their respective businesses.
- The chief risk officer, supported by the risk functions within the organization, has overall responsibility for the second line of defense. The chief risk officer is accountable to the board risk committee and, ultimately, to the main board. Day-to-day management of risks is not the accountability of the chief risk officer; this rests with the first line of defense. Typically, the risk function:
  - Recommends risk policies to the board for approval; provides objective oversight; and coordinates ERM activities in conjunction with other specialist, risk-related functions

Figure 13—Three Lines Concept

First line	Actions (to manage risk) in line with business objectives, policies, regulation and internal standards
Second line	Objective risk analysis and reporting to support and challenge business objectives, policies, regulations and internal standards
Third line	Confidence that first and second lines are operating in line with policies, regulations and internal standards

[20] "The board of directors should have responsibility for approving and periodically reviewing the overall business strategies and significant policies of the bank; understanding the major risks run by the bank, setting acceptable levels for these risks and ensuring that senior management takes the steps necessary to identify, measure, monitor and control these risks; approving the organisation's structure; and ensuring that senior management is monitoring the effectiveness of the internal control system. **The board of directors is ultimately responsible for ensuring that an adequate and effective system of internal controls is established and maintained**." Source: Basel Committee on Banking Supervision, Principle 1, *Framework for Internal Control Systems in Banking Organisations*.

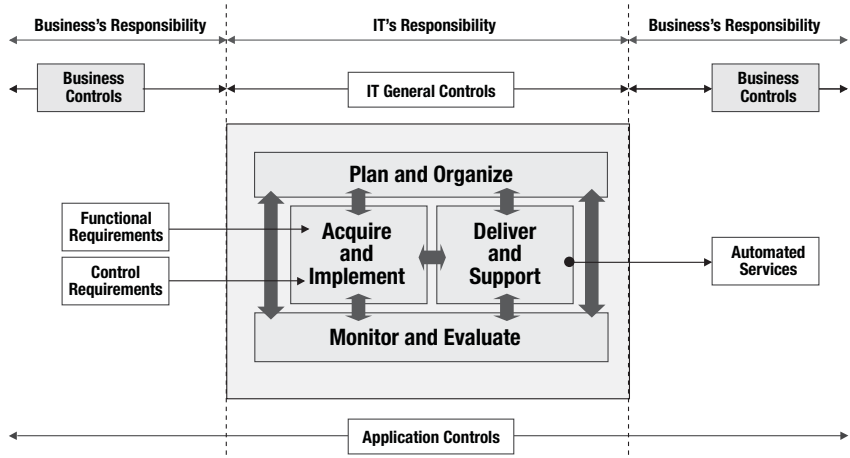
– Provides general and specialist support and advice to members of operating management to assist them with the identification, assessment, management, monitoring and reporting of risks

- The third line of defense—internal audit—provides independent assurance on the effectiveness of the management of enterprise risks across the organization. The internal audit function is accountable to the audit committee and, ultimately, to the main board.

Defining IT Controls

As risk needs to be defined and evaluated from an organizational perspective, progressing through to more detailed process-level considerations, the implementation of controls progresses from an entity perspective to general controls to more specific and detailed process controls. **Figure 14** presents this relationship within the context of a comprehensive business process shared between the business and IT.

Figure 14—Boundaries of Business, General and Application Controls



Entity-level Controls

The use of COBIT provides financial institutions a comprehensive set of control objectives with a strategic focus for entity-level controls. These should be seen in context since the environment of the organization and its business priorities will determine the strategic view on GRC. Senior management may opt for various models to ensure good corporate governance, and the COBIT framework should be applied accordingly. While illustrative questions may be useful to communicate an overall, high-level understanding of entity-level controls, it is the responsibility of managers and operational and information risk specialists to determine the scope and extent of control objectives that are required to obtain reasonable assurance over entity-level controls.

IT General Controls
Control objectives specific to Basel II risk event types are presented in appendix V, Basel II and CobiT. IT general controls usually address summary control objectives that are enablers for process- and application-level controls. For IT general controls, CobiT has defined a set of more than 200 control objectives that are either application-specific or applicable throughout the organization. An IT general control (for instance, the access control framework for applications) sets the scene for more detailed controls in the business workflow. Key controls in the workflow must adhere to the principles and boundaries set by the governing IT general controls. Individual access restrictions in application transactions creating or modifying data must, therefore, follow the direction given in an access control framework.

Key controls implemented as a result of a general control will support the effectiveness of the general control. In an access control scenario, the fact that a key control has been inserted into the workflow confirms that the access control framework (the general control) has been consistently applied to the workflow. Conversely, if an access control framework has not been fully implemented, there will be gaps in access control seen at the workflow level.

Process-level Controls
Process-level controls are often equivalent to application controls. Business processes in banks are often so tightly integrated with IT applications that business process controls are provided within the IT applications supporting that process. For example, within retail brokerage the risk of misselling can be reduced by IT application controls providing plausibility checks for data entered into the IT application.

The IT applications themselves are governed by IT general controls, assuring that IT applications are developed and operated according to business specifications, and that users are permitted access only as defined by the business.

Additionally, if the financial institution is interested, CobiT control objectives can be used to define the required general and application controls and assess the maturity of the controls implemented. For application controls, CobiT has defined a recommended set of six application control objectives. They are identified by application control number (AC):
- AC1 Source Data Preparation and Authorization—Ensure that source documents are prepared by authorized 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 minimized through good input form design. Detect errors and irregularities so they can be reported and corrected.

- AC2 Source Data Collection and Entry—Establish that data input is performed in a timely manner by authorized and qualified staff. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorization levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.
- 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.
- 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.
- AC5 Output Review, Reconciliation and Error Handling—Establish procedures and associated responsibilities to ensure that output is handled in an authorized 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.
- AC6 Transaction Authentication and Integrity—Before passing transaction data between internal applications and business/operational functions (in 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.

8. Use of Key IT Risk Indicators

Risk indicators are parameters tracking operational risk exposure and changes in the operational risk profile. Therefore, risk indicators are a type of early warning system for the operational risk profile. They allow management to document and analyze trends, providing a forward-looking perspective and signaling required actions before the risk becomes a loss. Furthermore, risk indicators help to define risk appetite through the definition of thresholds. As such, key risk indicators (KRIs) should be part of a measurement and monitoring process rather than only a signal of where management intervention is required.

KRIs refer to the indicators that track risks especially well or that track very important risks. KRIs are used to manage operational risks and play an important role in operational risk management reporting.

The use of KRIs could result in the identification of potential operational losses caused by IT-related deficiencies and weaknesses. Some of these may be of a magnitude that may cause a change in capital charge or, at worst, prevent the organization from moving to a more advanced approach.

In the banking industry, a library of KRIs has been developed by the Risk Management Association (RMA)[21]. They can be useful in the risk indicator definition process.

Another source for the identification of risk indicators is the metrics provided by COBIT. Although the COBIT measures focus on performance drivers and outcome measures, the generally accepted means of measuring a process can serve as a basis for identifying risk indicators.

An example of KRIs derived from COBIT process DS 4 *Ensure continuous service* is provided in **figure 15**. The process is measured on three levels: contribution to IT goals, IT processes and activities.

Those measures can serve as risk indicators, and it is good practice to keep the structure of measures as recommended by COBIT. In addition, the maturity of the significant IT process can serve as a risk indicator, as the level of maturity correlates with the level of risk reduction.

[21] *www.kriex.org*

Figure 15—DS4 Metrics	
Measurement of…	**Metric**
IT goal	• Number of hours lost per user per month due to unplanned outages
IT process DS4	• Percent of availability service level agreements (SLAs) met • Number of business-critical processes relying on IT that are not covered by IT continuity plan • Percent of tests that achieve recovery objectives • Frequency of service interruption of critical systems
Activities	• Elapsed time between tests of any given element of IT continuity plan • Number of IT continuity training hours per year per relevant IT employee • Percent of critical infrastructure components with automated availability monitoring • Frequency of review of IT continuity plan

Appendix I—Basel II Summary

Established in the 1930s, the Bank for International Settlements (BIS) has, through its Committee on Banking Supervision, set international prudential standards for the management of banking institutions. The standards are enacted through country legislation[22] and local regulator rulebooks.

The new capital adequacy regulations of Basel II (the revised framework) represent one of the most significant regulatory changes in the financial sector in the past decades. The discussions started in 1998 with the first consultation paper and led to the framework, which the Basel Committee concluded in June 2004. The new regulations represent a significant step forward in financial services organizations supervision and will cause major changes in the organization of internationally operating banks. The national banking regulators around the world are scheduled to implement the Basel II requirements in a step-by-step approach that begun in 2006 and will continue in some countries until 2015 before they are fully implemented. European regulators and banks are leading the implementation with many expected to comply within 2008.

Basel II replaces the capital adequacy framework of 1988, which does not meet modern approaches to risk management and also does not take operational risk into account. The objective of Basel II is to promote the adoption of stronger risk management practices for credit risk and operational risk, and to strengthen the link between banks' financial risks and their capital requirements. The new regulations provide an incentive for banks to move into this direction, i.e., a relaxation of capital requirements in cases of high-quality risk control systems. Consequently, prudent risk management will provide a competitive edge in the market. In addition, capital adequacy requirements should keep pace with market developments and enhancements in risk management practices.

According to the Committee, the Basel II Accord is intended to:
- Strengthen the soundness and stability of the international banking system and maintain the present status of capitalization
- Address all risks more comprehensively
- Ensure that banks' capital is adequate to cover the level of risks resulting from positions taken and other business transactions
- Be equally applicable to banks with varying degrees of complexity and risk appetite

Highlights of the most important changes include the following:
- Regulations are applied to consolidated banking groups rather than to only single institutions.
- Calculation of capital adequacy may be based on banks' internal rating methods.

[22] In Europe, the standards are initially adopted at a European Union (EU) level in the form of an EU Directive.

- There is improved potential to reduce credit exposure by netting against credit collateral.
- A level of operational risk is to be recognized in the determination of capital adequacy.

In addition, standards for supervisory review of the banks' risk assessment systems are specified, requiring extensive regular contacts with banks. Extended disclosure requirements aim to strengthen market discipline.

The focus is minimum capital requirements, and these will have the strongest impact on commercial banks. The new regulations represent a higher level of complexity compared to current rules. However, this is in line with the development of the various business areas and advances in credit risk management of financial services organizations.

Financial services organizations are allowed to select approaches that are most appropriate for their operations to monitor capital requirements of credit, market and operational risks. This option should account for different circumstances of risk control and risk management among financial services organizations. Generally, the assessment of risks and the resulting capital requirement is becoming more risk-sensitive with increasing complexity. At the same time, more challenging qualitative and quantitative requirements have to be met as a condition for application. A relaxation of capital requirements is provided as an incentive to implement a more advanced approach, and to develop and improve financial services organizations' risk management systems.

The revised framework retains key elements of the 1988 capital adequacy regulations: the general requirements for banks to hold total capital equivalent to at least 8 percent of their risk-weighted assets, the basic structure of the 1996 Market Risk Amendment regarding the treatment of market risk, and the definition of eligible capital.

The Three Pillars of the Revised Framework[23]

Adequate capital for risk-weighted assets alone is not sufficient to stabilize the financial markets. Financial services organizations must be able to identify, control and absorb losses from those risks on a continuous basis. This requires advanced risk management systems to be put in place and further developed as an ongoing process. Financial services organizations applying well-developed internal risk control systems may qualify for reduced capital requirements, provided the supervisor approves the soundness and correctness of the systems. In applying this philosophy, the supervisors are moving away from quantitative methods to a more qualitative model of financial services organizations supervision. The supervisory review is considered to be the second pillar of the framework.

[23] The following text is based on the document *Basel II Framework* published by the Basel Committee on Banking Supervision in June 2004.

The extended disclosure requirements are essential in ensuring that market discipline is an effective complement to the other two pillars.

The First Pillar: Minimum Capital Requirements
The minimum capital requirements are defined in Basel II. These are determined by the minimum capital ratio of 8 percent based on the risk-weighted assets, and this percentage remains unchanged. The total risk-weighted assets are determined by multiplying the capital requirements for market risk and operational risk by 12.5 and adding the resulting figures to the sum of risk-weighted assets for credit risk.

The changes focus on the assessment of credit risk and operational risk, while the definition of total capital for regulatory purposes and the calculation of total market risk remain unchanged.

Credit Risk
The Basel Committee uses a risk-weighted approach for capital requirements, as shown in **figure 16**. Participating financial services organizations have the option to apply the standardized approach (normally resulting in a high capital requirement) or their internal model (normally resulting in a lower capital requirement) for calculating their capital requirements for credit risk. Use of the internal model may be approved by the supervisor if certain minimum criteria defined by the supervisor are met.

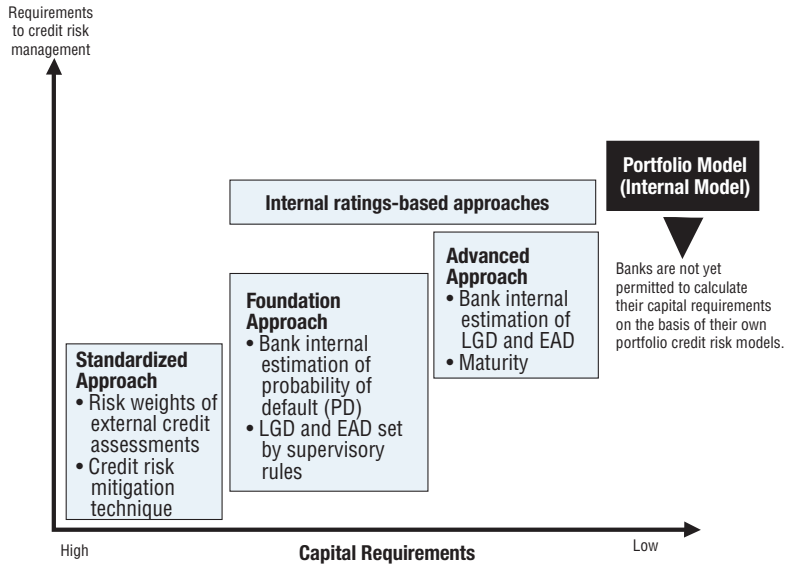
The Standardized Approach[24]
Basel II continues to use risk weights for credit exposures. However, risk weights should be adjusted based on the ratings of external credit assessment institutions (ECAI), e.g., Standard & Poor's or Moody's. National supervisors select and approve ECAIs whose ratings on loans to sovereigns, financial services organizations, corporate clients and securitized loan instruments are used to determine risk weightings.

For the first time, the general regulations also include the treatment of asset-backed securities (ABS). When a financial services organization provides implicit support to a securitization (bank acts as an investor), it must support this with capital according to the rating of the external ECAI. The financial services organizations as originator can reduce the required capital, depending on the scale of direct or indirect credit exposure included in the securitization.

Techniques to minimize credit risks (e.g., collateral, warranties, credit derivatives and netting agreements) become more important when determining risk levels. The catalog of approved collateral has been expanded. The new regulations require adjustments to collateral to account for possible future market price fluctuations.

[24] IT risks will not impact capital charge when using the standardized approach.

Figure 16—The Three Approaches to Credit Risk



Internal Ratings-based (IRB) Approach

Compared to the standardized approach, the IRB approach takes a more appropriate account of banks' individual risk profiles and moves closer to the objective of a risk-weighted capital requirement. Financial services organizations may use their own internal models and estimates of risk components in determining the capital requirement for a given exposure, under the condition that they meet certain minimum criteria set by the supervisor.

Financial services organizations must categorize banking book exposures into 11 classes of exposure with different underlying risk characteristics. The classes of assets are, among others, corporate, sovereign, bank, retail and equity. Within these classes, the risk components are separately associated with specific (ratings-based) risk parameters.

For each asset class covered under the IRB framework, there are different regulations to address the individual risk weights. Basically, financial services organizations can choose between two approaches:

- The easier foundation approach
- The advanced approach, which recognizes to a greater extent the organization's internal model and estimates for risk components

The following risk components are incorporated in the IRB approach:

- Probability of default (PD)—Based on the internal rating, the bank categorizes each borrower into one of the given risk categories. Subsequently, the financial services organization has to estimate the probability of default within one year for each category.

- Exposure at default—An established line of credit does not necessarily determine utilization of the line at a given date. The EAD is an estimate of the outstanding credit at time of default.
- Loss given default—In case of default, the loss for the financial services organization depends on the recoverability of any collateral and revenues from the sale of the borrower's assets. The LGD represents the estimated total net loss at the time of credit default.
- Effective maturity (M)—The effective maturity is the longest possible remaining time before the counterpart is scheduled to meet its obligation and is considered to be a risk factor in the IRB approach. The longer the credit period, the higher the risk of failure is assessed.

To grant access to internal rating methods to a great number of financial institutions, financial services organizations may choose between one of the two IRB approaches:

- The easier foundation approach is based on an internal estimate for losses (PDs) per rating class only. The other risk components (EAD, LGD and M) are determined by the supervisors. Collateral, warranties, credit derivatives and netting agreements are treated similarly to the standardized approach.
- Under the advanced approach, financial services organizations must calculate the effective maturity and provide their own estimates of the risk components. To qualify for the advanced approach, financial services organizations are required to hold an extensive data history and meet advanced minimum requirements. No restrictions regarding credit collateral and warranties apply except for off-balance sheet exposure.

The estimates are based on mathematical functions that concur with the credit portfolio model credit metrics.

To obtain the supervisor's approval for the IRB approach, financial services organizations must comply with the minimum requirements (e.g., a quality rating system and extensive disclosure practices as specified in the third pillar). This helps ensure the integrity of the internal risk assessment systems.

The rating classes assigned to individual customers and the resulting quantitative information are an integral part of the risk assessment system, risk management, pricing and risk provisions. Of course, the information is also used to evaluate capital adequacy. In addition to the previous requirements, financial services organizations should apply stress tests based on their internal models. Such tests should consider the effect of mild recession scenarios.

Market Risk
Market risk is the risk of loss that accrues through the variation of market variables, e.g., interest rates, share prices or foreign currencies. The measurement procedures and the consideration of market risks basically remain the same in Basel II and are not discussed further in the new regulations.

Operational Risk
As noted previously, the Basel Committee defines operational risk as follows: "Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."[25]

The definition includes legal risk but excludes strategic and reputational risk. Currently, operational risk is charged to the capital requirement at 8 percent. To assess the amount of operational risks, financial services organizations may use various alternative approaches.

Basic Indicator Approach
Banks using the BIA must hold capital for operational risk at a fixed percentage (alpha) of the average over the previous three years of positive annual gross income. The annual gross income is used as the exposure indicator (EI), which serves as an indicator for assumed operational risks and is calculated from the sum of interest surplus, commission surplus, trading result, financial asset result and other income. This broad approach may be used by small financial services organizations without a system to control operational risks. The Basel Committee expects financial services organizations that operate internationally to use the standardized approach as a minimum.

Standardized Approach
The STA follows a similar concept, but the different risk sensitivities for each business line defined by the Basel Committee should be considered. A scale of operational risk exposure is defined for each of these business lines, e.g., retail banking. The required capital for each business line is calculated from the value of each business line's risk indicator (e.g., positive annual gross income) multiplied by a factor (beta) assigned to each business line. Diversification factors are not taken into account.

Financial services organizations must comply with further criteria when introducing the standardized approach. These include the existence of a comprehensive process for a permanent reduction of risks and respective monitoring. The board of directors and an independent risk control unit must be actively involved in the controlling and reporting while the internal audit

[25] Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of Operational Risk*, February 2003

function is expected to examine the soundness of the procedures applied. In addition, operational risks data must be supported by statistical data collected from actual transactions, and there should be an appropriate reporting system for the management.

Advanced Measurement Approaches
A bank adopting AMAs may use actual financial services organization-specific data and an allocation mechanism for the purpose of determining the regulatory capital requirement. As an alternative to regulatory-defined business lines with their specific risk indicators, the regulations state seven additional standardized loss events (e.g., legal costs), which represent types of operational risks.

To consider the different methods currently being developed or implemented by financial services organizations, the supervisor is entitled to determine whether the approach is sound and appropriate. The approval will depend on the presence of various factors that the supervisors will want to see properly incorporated in the internal models.

It is important that financial services organizations' approach is based on internal loss data. Furthermore, financial service organizations must fully incorporate the actual risk exposures into their operative and strategic planning. They must also implement a system for the collection of actual losses from operational activities, which ensures a groupwide and reliable collection of perennial historical loss data. An appropriate method should be applied to support, verify or enhance the internal data using information from external sources. Financial services organizations should conduct periodic stress tests and portfolio analysis to review the results.

The Basel Committee does not specify any approach to generate the operational risk measure for regulatory capital purposes. Whatever approach is used, a financial services organization must demonstrate that its operational risk measure meets a sound standard comparable to that of the IRB approach for credit risk (i.e., comparable to a one-year holding period and a 99.9 percentile confidence interval).

Under the AMA, banks are allowed to recognize the risk-mitigating impact of insurance in the measures of operational risk, provided certain criteria are met. The recognition of insurance mitigation should be limited.

The Second Pillar: Supervisory Review Process
The first pillar focuses mainly on the quantitative requirements for financial services organizations. The second pillar concentrates on the qualitative aspect of supervisory activities. The national supervisors are responsible for

the quality assurance of the financial services organizations' risk management systems. The national supervisors' duties are to:
- Monitor the compliance of the minimum requirements, including disclosure requirements
- Promote the development and use of advanced risk management techniques
- Form an opinion on the quality of bank internal risk estimates and the adequacy of the required capital
- Take action in case of inadequate levels of capital

However, the responsibility for implementing and evaluating adequate risk management systems is not meant to be shifted to supervisors. Supervisors should examine the techniques and procedures of financial services organizations. The Basel Committee has identified four key principles of supervisory review:
- Banks should have a process in place for assessing their overall capital adequacy.
- Supervisors should review and evaluate banks' internal capital adequacy assessments and strategies.
- Banks should operate above the minimum regulatory capital ratios.
- Supervisors should seek to intervene at an early stage.

The increased reliance on bank internal methodologies is intended to foster an active dialog between banks and supervisors.

The Third Pillar: Market Discipline
It is the Basel Committee's objective to strengthen the international banking system to soundness and stability. The disclosures provided under the third pillar are considered to be essential in ensuring that market discipline is an effective complement to the other two pillars. The disclosure of bank internal risk data will provide other market participants with specific information about the overall risk situation of the institution. The framework states a general disclosure principle that should be mandatory for all banks:

> *Banks should have a formal disclosure policy approved by the board of directors. As part of this policy, the bank's strategy and objectives, with a view to disclosure of information about the financial situation and profitability, should be specified. In addition, banks should implement a process for assessing the appropriateness of their disclosures.*[26]

This objective is driven by the assumption that well-informed market participants will incorporate the level of risks assumed and the quality of risk management in their investment decisions.

[26] Basel Committee on Banking Supervision, "Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework—Comprehensive Version," June 2006

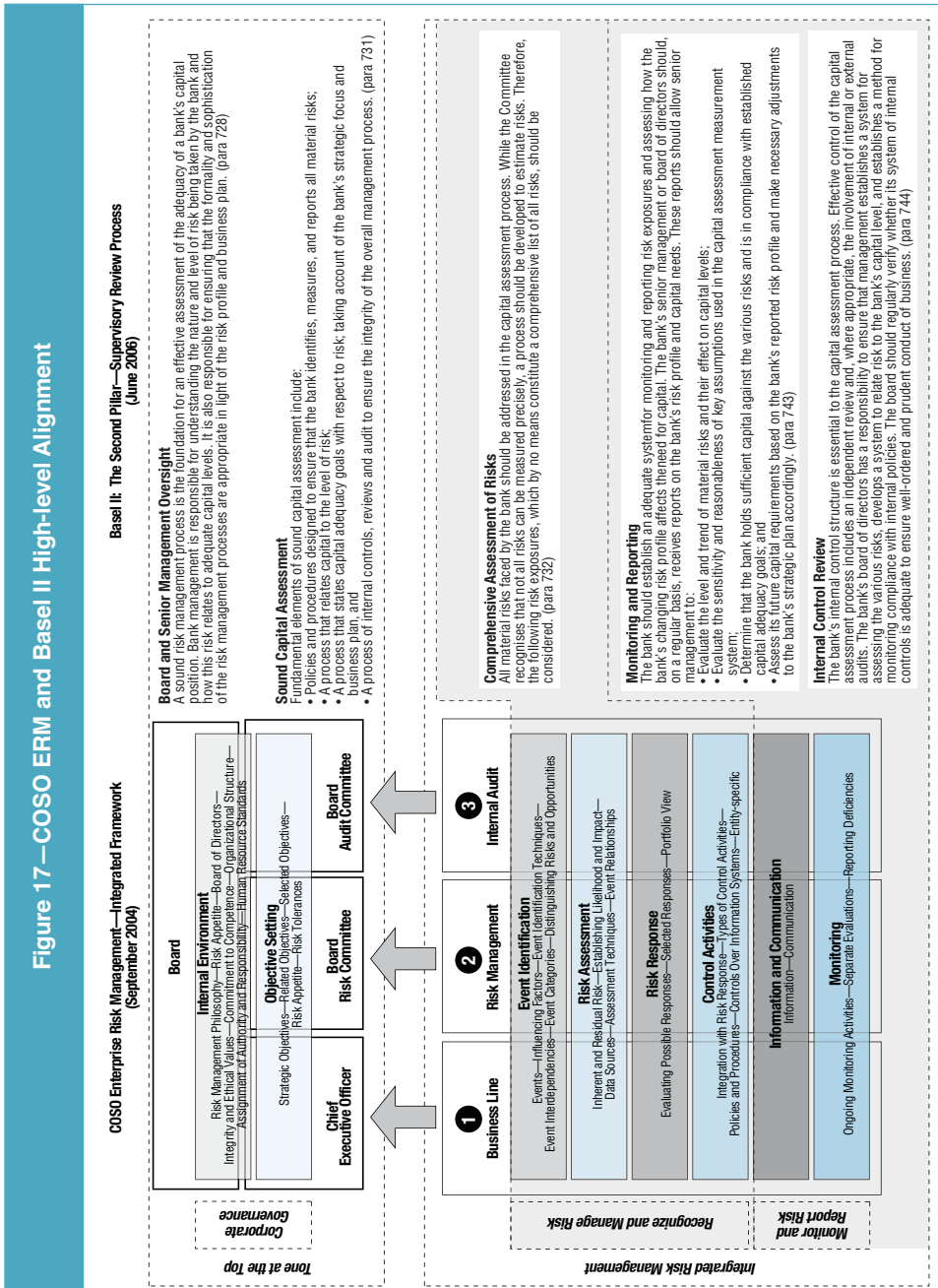
The Basel Committee provides a flexible concept for the amount and frequency of disclosure information. Basically, the proposals are formulated as recommendations. However, the framework represents a binding rule in cases where a financial services organization takes up the option to apply advanced models (i.e., internal ratings) to reduce capital requirements.

Depending on the complexity of the business processes and the financial services organization's risk profile, the frequency and the amount (core information and supplemental information) of disclosure information can vary. The disclosure requirements are composed of four areas:

- Scope of application—The name of the top corporate entity in the group to which the framework applies should be stated.
- Capital structure—A summary of information should be disclosed covering the terms and conditions of the main features of all elements of capital. This includes paid-up shares of capital/common stock, reserves, and types and specifics of innovative capital instruments. The objective is to give market participants the information required to form an opinion on the bank's capacity to withstand financial risks.
- Actual risk and its structure—This is a core area of the third pillar. The four main risks are defined and separate data have to be disclosed for each: credit, market, operational and interest rate change risks in the banking book. Basically, financial services organizations should estimate their potential losses for each type of risk and compare these with actual losses. The result of this comparison should be disclosed. Based on this information, market participants should be able to assess the appropriateness and effectiveness of the risk management system.
- Capital adequacy—The capital requirement equivalent to the assumed risks and the overall capital ratio should be disclosed. Additionally, an analysis of factors that affect the overall capital requirement and the allocation of economic capital should be provided.

Appendix II—High-level Alignment of COSO ERM and Basel II

Figure 17 provides a high-level alignment of COSO ERM and Basel II.



Appendix III—High-level Alignment of Basel II Principle 1: The Second Pillar—Supervisory Review Process (June 2006) and COSO ERM—Integrated Framework (September 2004)

Figure 18 provides a high-level alignment of Basel II, Pillar II and the COSO ERM Framework

Figure 18—Basel II, Pillar II and COSO ERM Framework High-level Alignment

Basel II Second Pillar	COSO ERM Framework
1. Board and senior management oversight—Bank management is responsible for understanding the nature and level of risk being taken by the bank and how these risks relate to adequate capital levels and ensuring that the formality and sophistication of the risk management processes are appropriate in light of the risk profile and business plan. The board of directors has responsibility for setting the bank's tolerance for risks and ensuring that management establishes a framework for assessing the various risks, develops a system to relate risk to the bank's capital level, and establishes a method for monitoring compliance with internal policies.	**1. Internal environment**—The internal environment encompasses the tone of an organization, influencing the risk consciousness of its people, and is the foundation for all other components of ERM, providing discipline and structure. Internal environment factors include an entity's risk management philosophy; its risk appetite and risk culture; oversight by the board of directors; the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; and the way management assigns authority and responsibility and organizes and develops its people.
2. Sound capital assessment—Fundamental elements of sound capital assessment include policies and procedures designed to ensure that the bank identifies, measures and reports all material risks, e.g., a process that relates capital to the level of risk, and a process of internal controls, reviews and audit to ensure the integrity of the overall management process.	**2. Objective setting**—Every entity faces a variety of risks from external and internal sources, and a precondition to effective event identification, risk assessment and risk response in establishment of objectives, linked at different levels and internally consistent. Objectives are set at the strategic level, establishing a basis for operations, reporting and compliance objectives. Objectives are aligned with the entity's risk appetite, which drives risk tolerance levels for the entity's activities.

Figure 18—Basel II, Pillar II and COSO ERM Framework High-level Alignment (cont.)

Basel II Second Pillar	COSO ERM Framework
3. Comprehensive management of risks—All material risks faced by the bank should be addressed in the capital assessment process. While the Accord recognizes that not all risks can be measured precisely, a process should be developed to estimate risks.	**3. Event identification**—Management identifies potential events affecting an entity's ability to successfully implement strategy and achieve objectives. Events with a potentially negative impact represent risks that require management's assessment and response. Events with a potentially positive impact may offset negative impacts or represent opportunities. Management channels opportunities back to the strategy and objective-setting processes. A variety of internal and external factors give rise to events. When identifying potential events, management considers the full scope of the organization. Management considers the context within which the entity operates and its risk tolerances.
4. Internal control review—The bank's board of directors has a responsibility to ensure that management establishes a system for assessing the various risks, develops a system to relate risks to the bank's capital level and establishes a method for monitoring compliance with internal policies. The board should regularly verify whether its system of internal controls is adequate to ensure well-ordered and prudent conduct of business. The bank should conduct periodic reviews of its risk management process to ensure its integrity, accuracy and reasonableness.	**4. Risk assessment**—Risk assessment allows an entity to consider the extent to which potential events might have an impact on achievement of objectives. Management should assess events from two perspectives—likelihood and impact—and normally uses a combination of qualitative and quantitative methods. The positive and negative impacts of potential events should be examined, individually or by category, across the entity. Potentially negative events should be assessed on both an inherent and a residual basis.
5. Monitoring and reporting—The bank should establish an adequate system for monitoring and reporting risk exposures, and how the bank's changing risk profile affects the need for capital. The bank's senior management or board of directors should, on a regular basis, receive reports on the bank's risk profile and capital needs. These reports should allow senior management to evaluate current and future capital requirements and the sensitivity and reasonableness of key assumptions used in the capital assessment measurement system, and enable them to determine whether the bank holds sufficient capital against the various risks, in line with established capital adequacy goals.	**5. Risk response**—Having assessed relevant risks, management determines how it will respond. Responses include risk avoidance, reduction, sharing and acceptance. In considering its response, management considers costs and benefits, and selects a response that brings expected likelihood and impact within the desired risk tolerances. **6. Control activities**—Control activities are the policies and procedures that help ensure that management's risk responses are carried out. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Figure 18—Basel II, Pillar II and COSO ERM Framework High-level Alignment (cont.)	
Basel II Second Pillar	**COSO ERM Framework**
	7. Information and communication—Pertinent information is identified, captured and communicated in a form and time frame that enables people to carry out their responsibilities. Information systems use internally generated data and information about external events, activities and conditions, providing information for managing enterprise risks and making informed decisions relative to objectives. Effective communication also occurs, flowing down, across and up the organization. All personnel receive a clear message from top management that ERM responsibilities must be taken seriously. They understand their own role in ERM, as well as how individual activities relate to the work of others. They have a means of communicating significant information upstream, and there is effective communication with external parties. **8. Monitoring**—ERM is monitored—a process that assesses the presence and functioning of its components over time. This is accomplished through ongoing monitoring activities, separate evaluations and a combination of the two. Ongoing monitoring occurs in the normal course of management activities. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. ERM deficiencies are reported upstream, with serious matters reported to top management and the board.

Appendix IV—The Dependence of the COSO ERM Framework on Data Quality [27]

COSO Components	Data Quality Considerations
Tone at the Top	
Internal Environment—The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.	• Data quality underpins the overall control environment. • Data must be seen as an organizational asset. • Data quality governance and control are clear organizational priorities. • The board, CEO, CFO and CRO are ultimately accountable for data quality exist. • Clear disciplines and accountabilities for data management and information quality exist. • Policies and procedures supporting rigorous data management exist.
Objective Setting—Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.	
Recognize and Manage Risk	
Event Identification—Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.	Poor quality data can: • Result in uninformed decisions adversely impacting the achievement of organizational objectives • Expose the organization to unidentified risks (including operational risk, market risk, credit risk) potentially leading to broader risk implications (e.g., reputational risk, financial risk, regulatory compliance/legal risk and contagion risk)
Risk Assessment—Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.	
Risk Response—Management selects risk responses—avoiding, accepting, reducing, or sharing risk—developing a set of actions to align risks with the entity's risk tolerances and risk appetite.	• If you cannot measure it, you cannot manage it. • Data represent the granular means of control. • Clear disciplines and accountabilities for data management and information quality exist. • Policies and procedures supporting rigorous data management exist.
Control Activities—Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.	

[27] Based on the article "Data Quality: The Hidden Assumption behind COSO," by George Marinos, Partner, PricewaterhouseCoopers.

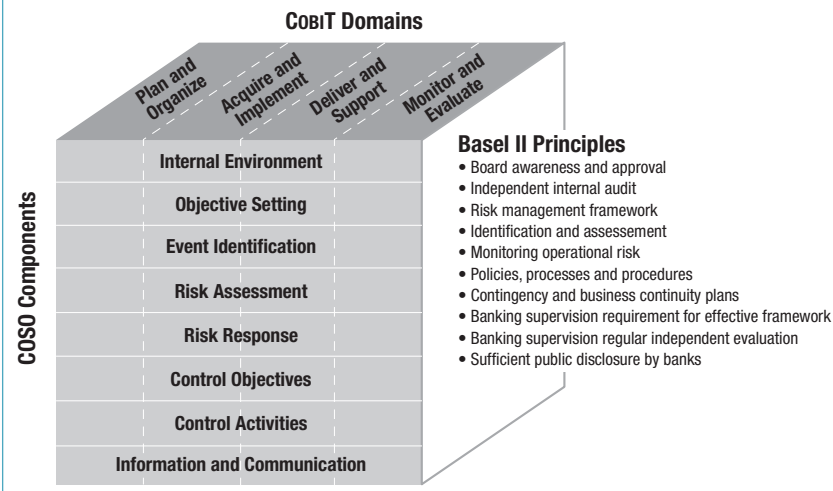
COSO Components	Data Quality Considerations
Monitor and Report Risk	
Information and Communication—Relevant information is identified, captured, and communicated in a form and time frame that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across and up the entity.	• Poor data quality will severely compromise reporting and action. • Pertinent information supporting control functions and responsibilities must be appropriately communicated (content and timeliness) to support responsible officers to carry out their duties.
Monitoring—The entirety of enterprise risk management is monitored and modifications are made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations or both.	• Effective monitoring relies on the fundamental attributes supporting data quality: accuracy, completeness, accessibility, integrity, validity, usability, consistency, timeliness and auditability.

Appendix V—Basel II and CobiT

As noted earlier in the document, Basel II has 10 principles, COSO ERM divides internal control into eight components, and CobiT has four domains. **Figure 19** shows that all of these need to be in place and integrated to achieve Basel II operational risk objectives. CobiT provides similar detailed guidance for IT. The eight components of COSO ERM—beginning with identifying the control environment and culminating in the monitoring of internal controls—can be visualized as the horizontal layers of a three-dimensional cube, with the CobiT objective domains—from Plan and Organize through Monitor and Evaluate—applying to each individually and in aggregate.

Figure 19 illustrates the Basel II principles and maps their relationship to the appropriate COSO component and the specific domains in CobiT. It is immediately evident that many CobiT IT processes have relationships with more than one Basel II and COSO component. This is expected, given the nature of general IT controls as they form the basis for relying on application controls. This multiple relationship attribute further demonstrates why IT controls are the basis for all others and are essential for a reliable internal control program.

Figure 19—Cross-reference of COSO ERM and CobiT



CobiT is a comprehensive framework for management of the governance of risk and control of IT. It is composed of four domains, 34 IT processes and more than 200 control objectives. CobiT includes controls that address all aspects of IT governance, but only those significant to Basel II risk

management objectives have been used to develop this document. CobiT is a freely available framework that aligns with the spirit of the Basel II requirement that any framework used should be easy to access and generally acceptable. CobiT provides both entity-level and activity-level objectives along with associated controls, and it is widely used around the world by organizations as a supplement that provides the IT component to COSO and other governance frameworks.

For selecting relevant IT processes and controls, there are two approaches:
- Risk-driven approach—Selecting relevant risk drivers (ITGI's) *CobiT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*, can assist in facilitating this selection), classifying those risk drivers (critical, important, some impact, no relevancy), and identifying control objectives and processes related to them
- Goal-driven approach—Identifying IT goals relevant for Basel II and using the guidance provided in the CobiT core content and the ITGI publication *IT Governance Implementation Guide: Using CobiT and Val IT, 2nd Edition*

Risk-driven Approach

Within the operational risk definition, as suggested by regulators and other associations, there is a wide range of individual risk factors that can be taken into consideration prior to integrating the operational component into the wider ERM framework.

In general, the following risk-driven strategies have been adopted:
- Identifying the most significant risks and the control objectives and processes related to them—A risk management culture is adopted and an IT risk management framework is used to assist in the management of IT risk. The results of this approach are then integrated into the ERM framework. This approach has the advantage that risk management becomes part of the IT culture and emerging risks are addressed as they are identified.
- Identifying a large number of potential risk event types, assessing controls and mitigating factors, and taking corrective actions where applicable—This approach has the potential disadvantage of being too focused on identified risks and not having the flexibility of reacting to unanticipated risks. If many risk drivers are identified, there is increased risk that the focus on the most significant risks may be reduced.

Figure 20 provides indicative examples of IT event types that address Basel II risk event types and the CobiT processes to address those IT aspects.

Figure 20—Basel II Risk Event Types and Related IT Risk Aspects and CobiT Processes

Basel II Risk Event Types	IT Aspects	CobiT Processes
Internal fraud	•Deliberate manipulation of programs •Unauthorized usage of modification functions •Deliberate manipulation of system instructions •Deliberate manipulation of hardware •Deliberate unauthorized changing of system and application data •Using/copying unlicensed or unauthorized software •Internal circumvention of access privileges	• PO6 • DS5 • DS9 • DS12
External fraud	•Deliberate changing of system and application data through hacking •Outsiders gaining sight of confidential physical or electronic documents •External circumvention of access privileges •Eavesdropping and interception of communication links •Password compromise •Viruses	• DS5
Employment practices and workplace safety	•Misuse of IT resources •Lack of security responsiveness	• PO6 • DS5
Clients, products and business practices	•Disclosure of sensitive information to outsiders by employees •Management of third-party suppliers	• PO6 • DS2
Damage to physical assets	•Deliberate or accidental damage to physical IT infrastructure	• DS12
Business disruption and system failures	•Hardware or software malfunction •Communications failure •Employee sabotage •Loss of key IT staff member(s) •Destruction of software/data files •Theft of software or sensitive information •Computer viruses •Failure to back up •(Distributed) denial-of-service attacks •Configuration control error	• AI7 • DS3 • DS4 • DS5 • DS9 • DS10
Execution, delivery and process management	•Error in handling electronic media •Unattended workstation •Change control error •Incomplete input of transactions •Errors on data input/output •Programming/testing error •Operator error, e.g., in recovery procedural error	• AI3 • AI6 • AI7 • DS5 • DS10

Goal-driven Approach

The goal-driven approach has the advantage that it facilitates the alignment of IT efforts with business goals.

Figure 21 represents the table of IT goals provided in CobiT. The right column indicates whether the IT goal is of relevance for Basel II. IT goals without an entry for relevance are deemed not as relevant for the purposes of Basel II.

Figure 21—CobiT IT Goals

Goal		Relevancy
1	Respond to business requirements in alignment with the business strategy	
2	Respond to governance requirements in line with board direction	●
3	Ensure satisfaction of end users with service offerings and service levels	
4	Optimize the use of information	
5	Create IT agility	
6	Define how business functional and control requirements are translated into effective and efficient automated solutions	
7	Acquire and maintain integrated standardized application systems	
8	Acquire and maintain an integrated and standardized IT infrastructure	●
9	Acquire and maintain IT skills that respond to the IT strategy	●
10	Ensure mutual satisfaction of third-party relationships	●
11	Ensure seamless integration of applications into business processes	
12	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels	●
13	Ensure proper use and performance of the applications and technology solutions	●
14	Account for and protect all IT assets	●
15	Optimize the IT infrastructure, resources and capabilities	●
16	Reduce solution and service delivery defects and rework	●
17	Protect the achievement of IT objectives	
18	Establish clarity on the business impact of risks to IT objectives and resources	●
19	Ensure that critical and confidential information is withheld from those who should not have access to it	●
20	Ensure that automated business transactions and information exchanges can be trusted	●
21	Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster	●

Figure 21—CobiT IT Goals *(cont.)*		
Goal		**Relevancy**
22	Ensure minimum business impact in the event of an IT service disruption or change	●
23	Make sure that IT services are available as required	●
24	Improve IT's cost-efficiency and its contribution to business profitability	
25	Deliver projects on time and on budget, meeting quality standards	
26	Maintain the integrity of information and processing infrastructure	●
27	Ensure IT compliance with laws, regulations and contracts	●
28	Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change	

The selection of IT processes in **figure 22** can form the basis for the implementation program.

Figure 22—Sample IT Processes for Implementation Program CobiT IT Process Overall		
CobiT IT Process		**Overall**
PO1	Define a strategic IT plan.	●
PO2	Define the information architecture.	
PO3	Determine technological direction.	
PO4	Define the IT processes, organization and relationships.	
PO5	Manage the IT investment.	
PO6	Communicate management aims and direction.	●
PO7	Manage IT human resources.	
PO8	Manage quality.	
PO9	Assess and manage IT risks.	
PO10	Manage projects.	
AI1	Identify automated solutions.	
AI2	Acquire and maintain application software.	
AI3	Acquire and maintain technology infrastructure.	
AI4	Enable operation and use.	●
AI5	Procure IT resources.	
AI6	Manage changes.	●
AI7	Install and accredit solutions and changes.	●
DS1	Define and manage service levels.	
DS2	Manage third-party services.	
DS3	Manage performance and capacity.	
DS4	Ensure continuous service.	●
DS5	Ensure systems security.	●
DS6	Identify and allocate costs.	

Figure 22—Sample IT Processes for Implementation Program CobiT IT Process Overall *(cont.)*		
CobiT IT Process		**Overall**
DS7	Educate and train users.	●
DS8	Manage service desk and incidents.	
DS9	Manage the configuration.	●
DS10	Manage problems.	
DS11	Manage data.	●
DS12	Manage the physical environment.	●
DS13	Manage operations.	
ME1	Monitor and evaluate IT performance.	
ME2	Monitor and evaluate internal control.	●
ME3	Ensure regulatory compliance.	
ME4	Provide IT governance.	●

Basel Principles Mapped to CobiT Processes

Figure 23 facilitates the integration of an IT risk management framework with Basel II and the IT guiding principles.

Figure 23—Basel Principles Mapped to CobiT Processes

CobiT IT Processes — Plan and Organize

Basel II and IT Guiding Principles	PO1 Define a strategic IT plan.	PO2 Define the information architecture.	PO3 Determine technological direction.	PO4 Define the IT processes, organization and relationships.	PO5 Manage the IT investment.	PO6 Communicate management aims and direction.	PO7 Manage IT human resources.	PO8 Manage quality.	PO9 Assess and manage IT risks.	PO10 Manage projects.
1				●					●	
2										
3				●		●		●		
4									●	
5									●	
6				●		●		●	●	
7		●								
8				●		●		●	●	
9										
10										

CobiT IT Processes — Acquire and Implement

Basel II and IT Guiding Principles	AI1 Identify automated solutions.	AI2 Acquire and maintain application software.	AI3 Acquire and maintain technology infrastructure.	AI4 Enable operation and use.	AI5 Procure IT resources.	AI6 Manage changes.	AI7 Install and accredit solutions and changes.
1							
2							
3							
4							
5							
6				●			
7							
8							
9							
10							

CobiT IT Processes — Deliver and Support

Basel II and IT Guiding Principles	DS1 Define and manage service levels.	DS2 Manage third-party services.	DS3 Manage performance and capacity.	DS4 Ensure continuous service.	DS5 Ensure systems security.	DS6 Identify and allocate costs.	DS7 Educate and train users.	DS8 Manage service desk and incidents.	DS9 Manage the configuration.	DS10 Manage problems.	DS11 Manage data.	DS12 Manage the physical environment.	DS13 Manage operations.
1													
2													
3													
4													
5													
6													
7	●		●	●									
8													
9													
10													

CobiT IT Processes — Monitor and Evaluate

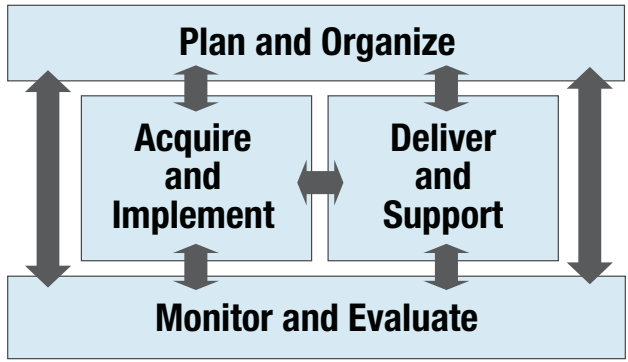
Basel II and IT Guiding Principles	ME1 Monitor and evaluate IT performance.	ME2 Monitor and evaluate internal control.	ME3 Ensure compliance with external requirements.	ME4 Provide IT governance.
1				●
2		●	●	
3	●			
4				●
5	●	●		●
6	●	●	●	●
7	●			
8	●	●	●	●
9		●	●	
10				●

Appendix VI—CobiT Processes

An important part of this publication is to provide IT professionals with guidance on the specific processes that should be considered for compliance with Basel II. As always, IT organizations should consider the nature and extent of their operations in determining which of the control objectives, illustrative controls and tests of controls need to be included in their internal control program.

Basel II does not dictate requirements for such control objectives and related control activities. Such decisions remain the discretion of each organization. Accordingly, organizations should assess the nature and extent of IT controls necessary to support their operational risk on a case-by-case basis.[28] The interrelationships of the four CobiT domains are pictured in **figure 24**.

Figure 24—The Four Interrelated Domains of CobiT



The following control processes have been mapped to a Basel II-related IT goal or a Basel II process.

Plan and Organize

PO2 Define the Information Architecture

The information systems function creates and regularly updates a business information model and defines the appropriate systems to optimize the use of this information.

[28] The ITGI publication *CobiT Control Practices* provides examples of value drivers, risk drivers and control practices supporting the control objectives that underpin the CobiT processes.

This encompasses the development of a corporate data dictionary with the organization's data syntax rules, data classification scheme and security levels.

This process improves the quality of management decision making by making sure that reliable and secure information is provided and that it enables rationalizing information systems resources to appropriately match business strategies.

This IT process is also needed to increase accountability for the integrity and security of data and to enhance the effectiveness and control of sharing information across applications and entities.

PO4 Define the IT Processes, Organization and Relationships
An IT organization is defined by considering requirements for staff, skills, functions, accountability, authority, roles and responsibilities, and supervision.

This organization is embedded into an IT process framework that ensures transparency and control as well as the involvement of senior executives and business management.

A strategy committee ensures board oversight of IT, and one or more steering committees in which business and IT participate and determine the prioritization of IT resources in line with business needs.

Processes, administrative policies and procedures are in place for all functions, with specific attention to control, quality assurance, risk management, information security, data and systems ownership, and segregation of duties.

To ensure timely support of business requirements, IT is to be involved in relevant decision processes.

PO6 Communicate Management Aims and Direction
Management develops an enterprise IT control framework and defines and communicates policies.

An ongoing communication program is implemented to articulate the mission, service objectives, policies and procedures, etc., approved and supported by management.

The communication supports achievement of IT objectives and ensures awareness and understanding of business and IT risks, objectives and direction.

The process ensures compliance with relevant laws and regulations.

PO8 Manage Quality
A quality management system (QMS) is developed and maintained that includes proven development and acquisition processes and standards. This is enabled by planning, implementing and maintaining the QMS by providing clear quality requirements, procedures and policies.

Quality requirements are stated and communicated in quantifiable and achievable indicators.

Continuous improvement is achieved by performing ongoing monitoring and analysis, acting upon deviations, and communicating results to stakeholders.

Quality management is essential to ensure that IT is delivering value to the business, continuous improvement and transparency for stakeholders.

PO9 Assess and Manage IT Risks
A risk management framework is created and maintained.

The framework documents a common and agreed-upon level of IT risks, mitigation strategies and residual risks.

Any potential impact on the goals of the organization caused by an unplanned event is identified, analyzed and assessed.

Risk mitigation strategies are adopted to minimize residual risk to an accepted level.

The result of the assessment is understandable to the stakeholders and expressed in financial terms, to enable stakeholders to align risk to an acceptable level of tolerance.

Acquire and Implement

AI3 Acquire and Maintain Technology Infrastructure
Organizations have processes for the acquisition, implementation and upgrade of the technology infrastructure.

This requires a planned approach to acquisition, maintenance and protection of infrastructure in line with agreed-upon technology strategies and the provision of development and test environments.

This ensures that there is ongoing technological support for business applications.

AI4 Enable Operation and Use
Knowledge about new systems is made available.

This process requires the production of documentation and manuals for users and IT, and provides training to ensure the proper use and operation of applications and infrastructure.

AI6 Manage Changes
All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner.

Changes (including those to procedures, processes and system and service parameters) are logged, assessed and authorized prior to implementation and reviewed against planned outcomes following implementation.

This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

AI7 Install and Accredit Solutions and Changes
New systems are made operational once development is complete.

This requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a postimplementation review.

This assures that operational systems are in line with the agreed-upon expectations and outcomes.

Deliver and Support

DS1 Define and Manage Service Levels
Effective communication between IT management and business customers regarding services required is enabled by a documented definition of and agreement on IT services and service levels.

This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels.

This process enables alignment between IT services and the related business requirements.

DS2 Manage Third-party Services
The need to assure that services provided by third parties (suppliers, vendors and partners) meet business requirements requires an effective third-party management process.

This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance.

Effective management of third-party services minimizes the business risk associated with nonperforming suppliers.

DS3 Manage Performance and Capacity
The need to manage performance and capacity of IT resources requires a process to periodically review current performance and capacity of IT resources.

This process includes forecasting future needs based on workload, storage and contingency requirements.

This process provides assurance that information resources supporting business requirements are continually available.

DS4 Ensure Continuous Service
The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans; utilizing offsite backup storage; and providing periodic continuity plan training.

An effective continuous service process minimizes the probability and impact of a major IT service interruption on key business functions and processes.

DS5 Ensure Systems Security
The need to maintain the integrity of information and protect IT assets requires a security management process.

This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures.

Security management also includes performing security monitoring, conducting periodic testing, and implementing corrective actions for identified security weaknesses or incidents.

Effective security management protects all IT assets to minimize the business impact of security vulnerabilities and incidents.

DS9 Manage the Configuration
Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository.

This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed.

Effective configuration management facilitates greater system availability, minimizes production issues and resolves issues more quickly.

DS10 Manage Problems
Effective problem management requires the identification and classification of problems, root cause analysis, and resolution of problems.

The problem management process also includes the formulation of recommendations for improvement, maintenance of problem records and review of the status of corrective actions.

An effective problem management process maximizes system availability, improves service levels, reduces costs, and improves customer convenience and satisfaction.

DS12 Manage the Physical Environment
Protection for computer equipment and personnel requires well-designed and well-managed physical facilities.

The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities, and designing effective processes for monitoring environmental factors and managing physical access.

Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel.

Monitor and Evaluate

ME1 Monitor and Evaluate IT Performance
Effective IT performance management requires a monitoring process.

This process includes defining relevant performance indicators, reporting performance in a systematic and timely manner, and acting promptly upon deviations.

Monitoring is needed to make sure that the right things are done and are in line with the set directions and policies.

ME2 Monitor and Evaluate Internal Control
Establishing an effective internal control program for IT requires a well-defined monitoring process.

This process includes the monitoring and reporting of control exceptions, results of self-assessments and third-party reviews.

A key benefit of internal control monitoring is to provide assurance regarding effective and efficient operations and compliance with applicable laws and regulations.

ME3 Ensure Compliance With External Requirements
Effective oversight of compliance requires the establishment of a review process to ensure compliance with laws, regulations and contractual requirements.

This process includes identifying compliance requirements, optimizing and evaluating the response, obtaining assurance that the requirements have been complied with, and, finally, integrating IT's compliance reporting with the rest of the business.

ME4 Provide IT Governance
Establishing an effective governance framework includes defining organizational structures, processes, leadership, roles and responsibilities to ensure that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives.

Other control processes defined within CobiT that have not been mapped to either a Basel II-related IT goal or a Basel II process should be considered as part of establishing general IT controls.

Plan and Organize

PO1 Define a Strategic IT Plan
IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities.

The IT function and business stakeholders are responsible for ensuring that optimal value is realized from project and service portfolios.

The strategic plan improves key stakeholders' understanding of IT opportunities and limitations, assesses current performance, identifies capacity and human resource requirements, and clarifies the level of investment required.

The business strategy and priorities are to be reflected in portfolios and executed by the IT tactical plan(s), which specifies concise objectives, action plans and tasks that are understood and accepted by both business and IT.

PO3 Determine Technological Direction
The information services function determines the technology direction to support the business.

This requires the creation of a technological infrastructure plan and an architecture board that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms.

The plan is regularly updated and encompasses aspects such as systems architecture, technological direction, acquisition plans, standards, migration strategies and contingency.

This enables timely responses to changes in the competitive environment, economies of scale for information systems staffing and investments, and improved interoperability of platforms and applications.

PO5 Manage the IT Investment
A framework is established and maintained to manage IT-enabled investment programs and encompasses cost, benefits, prioritization within budget, a formal budgeting process and management against the budget.

Stakeholders are consulted to identify and control the total costs and benefits within the context of the IT strategic and tactical plans, and initiate corrective action where needed.

The process fosters partnership between IT and business stakeholders; enables the effective and efficient use of IT resources; and provides transparency and accountability into the total cost of ownership (TCO), the realization of business benefits and the return on investment (ROI) of IT-enabled investments.

PO7 Manage IT Human Resources
A competent workforce is acquired and maintained for the creation and delivery of IT services to the business.

This is achieved by following defined and agreed-upon practices supporting recruiting, training, evaluating performance, promoting and terminating.

This process is critical, as people are important assets, and governance and the internal control environment are heavily dependent on the motivation and competence of personnel.

PO10 Manage Projects
A program and project management framework for the management of all IT projects is established.

The framework ensures the correct prioritization and coordination of all projects.

The framework includes a master plan, assignment of resources, definition of deliverables, approval by users, a phased approach to delivery, QA, a formal test plan, and testing and postimplementation review after installation to ensure project risk management and value delivery to the business.

This approach reduces the risk of unexpected costs and project cancellations, improves communication to and involvement of business and end users, ensures the value and quality of project deliverables, and maximizes their contribution to IT-enabled investment programs.

Acquire and Implement

AI1 Identify Automated Solutions
The need for a new application or function requires analysis before acquisition or creation to ensure that business requirements are satisfied in an effective and efficient approach.

This process covers the definition of the needs, consideration of alternative sources, review of technological and economic feasibility, execution of a risk analysis and cost-benefit analysis, and conclusion of a final decision to "make" or "buy."

All these steps enable organizations to minimize the cost to acquire and implement solutions while ensuring that they enable the business to achieve its objectives.

AI2 Acquire and Maintain Application Software
Applications are made available in line with business requirements.

This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the development and configuration in line with standards.

This allows organizations to properly support business operations with the correct automated applications.

AI5 Procure IT Resources
IT resources, including people, hardware, software and services, need to be procured.

This requires the definition and enforcement of procurement procedures, the selection of vendors, the setup of contractual arrangements, and the acquisition itself.

Doing so ensures that the organization has all required IT resources in a timely and cost-effective manner.

Deliver and Support

DS6 Identify and Allocate Costs

The need for a fair and equitable system of allocating IT costs to the business requires accurate measurement of IT costs and agreement with business users on fair allocation.

This process includes building and operating a system to capture, allocate and report IT costs to the users of services.

A fair system of allocation enables the business to make more informed decisions regarding the use of IT services.

DS7 Educate and Train Users

Effective education of all users of IT systems, including those within IT, requires identifying the training needs of each user group.

In addition to identifying needs, this process includes defining and executing a strategy for effective training and measuring the results.

An effective training program increases effective use of technology by reducing user errors, increasing productivity and increasing compliance with key controls, such as user security measures.

DS8 Manage Service Desk and Incidents

Timely and effective response to IT user queries and problems requires a well-designed and well-executed service desk and incident management process.

This process includes setting up a service desk function with registration, incident escalation, trend and root cause analysis, and resolution.

The business benefits include increased productivity through quick resolution of user queries.

In addition, the business can address root causes (such as poor user training) through effective reporting.

DS11 Manage Data

Effective data management requires identifying data requirements.

The data management process also includes the establishment of effective procedures to manage the media library, back up and recover data, and properly dispose of media.

Effective data management helps ensure the quality, timeliness and availability of business data.

DS13 Manage Operations
Complete and accurate processing of data requires effective management of data processing procedures and diligent maintenance of hardware.

This process includes defining operating policies and procedures for effective management of scheduled processing, protecting sensitive output, monitoring infrastructure performance, and ensuring preventive maintenance of hardware.

Effective operations management helps maintain data integrity and reduces business delays and IT operating costs.

Appendix VII—ABC Bank: A Worked Example

The objective of this example is to demonstrate the thought process that can occur when assessing and measuring risk. The example is limited to the IT organization and to a single risk. In reality, the risk assessment management process would be organizationwide and would be integrated with the management of other risks and with existing programs.

ABC Bank is addressing the risks associated with internal fraud. It has been determined that the risk tolerance associated with internal fraud is low. While the likelihood of material fraud is considered to be low, the potential impact on the bank's reputation and potential regulatory associated costs are considered to be high. These processes also address risk associated with external fraud, business disruption and system failures that could increase the impact of a control failure.

The IT aspects associated with internal fraud are shown in **figure 25**.

Figure 25—IT Aspects Associated With Internal Fraud

Basel II Event Types	IT Aspects	COBIT Processes
Internal fraud	• Deliberate manipulation of programs • Unauthorized usage of modification functions • Deliberate manipulation of system instructions • Deliberate manipulation of hardware • Deliberate changing of system and application data through hacking • Using/copying unlicensed or unauthorized software • Internal circumvention of access privileges	• PO6 • DS5 • DS9 • DS12

ABC Bank reviewed the COBIT material associated with internal fraud to set goals, consider potential solutions and establish performance metrics as follows.

PO6 Communicate Management Aims and Direction

ABC considers PO6, which states:

> *Management develops an enterprise IT control framework and defines and communicates policies. An ongoing communication programme is implemented to articulate the mission, service objectives, policies and procedures, etc., approved and supported by management. The communication supports achievement of IT objectives and ensures awareness and understanding of business and IT risks, objectives and direction. The process ensures compliance with relevant laws and regulations.*

Consideration was also given to ITGP6 Control and Mitigation Policies, Processes, Procedures, which states:

> *Information management and technology should be governed by an adequate set of policies, processes and procedures for risk control and mitigation. The guidance given to practitioners, internal auditors and financial services experts should be in line with the organization's GRC framework.*

The COBIT maturity levels were reviewed to assist in establishing goals. The aspects of the maturity levels considered to be relevant were:

- Maturity level 3—Defined:
  - A complete information control and quality management environment is developed, documented and communicated by management, and includes a framework for policies, plans and procedures.
  - The policy development process is structured, maintained and known to staff, and the existing policies, plans and procedures are reasonably sound and cover key issues.
  - Management addresses the importance of IT security awareness and initiates awareness programs.
  - Techniques for promoting security awareness have been standardized and formalized.
- Maturity level 4—Managed and Measurable:
  - Management accepts responsibility for communicating internal control policies and delegates responsibility and allocates sufficient resources to maintain the environment in line with significant changes.
  - A positive, proactive information control environment, including a commitment to quality and IT security awareness, is established.
  - A complete set of policies, plans and procedures is developed, maintained and communicated and is a composite of internal good practices.
  - A framework for rollout and subsequent compliance checks is established.
- Maturity level 5—Optimized:
  - The information control environment is aligned with the strategic management framework and vision and is frequently reviewed and updated and continuously improved.
  - Monitoring, self-assessment and compliance checking are pervasive within the organization.
  - Technology is used to maintain policy and awareness knowledge bases and to optimize communication, using office automation and computer-based training tools.

The key characteristics of the communication solution were considered to be the following:
- It had to cover existing good and desired practices (not best practices that could not be achieved).
- It had to be integrated into an overall communications solution.
- It could not be unduly onerous or time consuming.
- It had to demonstrate compliance, i.e., the policy was read and understood.
- Compliance had to be measurable.

The solution considered could include the following components:
- A review of the extent and relevance of existing policies and procedures. Where gaps were identified, policies and procedures were to be updated or new policies and procedures were to be written.
- A policy would be implemented for the annual review and approval of policies and procedures.
- All policies and procedures would be loaded onto the intranet.
- All staff members would be required to undertake an intranet-based update session on changes to policies and procedures. This would include an automated test on the updates and essential policy and procedure components. The test would include a minimum passing grade.

The following measures would be introduced:
- Number of policies and procedures not reviewed and signed off on greater than one month following the annual approval deadline
- Number and percentage of staff members who had not successfully completed the intranet-based update course within two weeks of the compliance deadline
- Test results distributed by the percentage of number of questions answered incorrectly

DS5 Ensure Systems Security

This would be integrated with the overall security plan. The intent of this example is not to show how to implement an integrated security plan. The intent is to show aspects of the thought process.

DS5 states the following:

> *The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents.*

The COBIT maturity levels were reviewed to assist in establishing goals. The aspects of the maturity levels considered to be relevant were:

- Maturity level 4—Managed and Measurable:
  - Responsibilities for IT security are clearly assigned, managed and enforced.
  - IT security risk and impact analysis is consistently performed.
  - Security policies and procedures are completed with specific security baselines.
  - Exposure to methods for promoting security awareness is mandatory.
  - User identification, authentication and authorization are standardized.
  - Security testing is completed using standard and formalized processes, leading to improvements of security levels.
  - IT security processes are coordinated with an overall organization security function.
  - IT security reporting is linked to business objectives.
  - IT security training is conducted in both the business and IT.
  - IT security training is planned and managed in a manner that responds to business needs and defined security risk profiles.
- Maturity level 5—Optimized:
  - IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives.
  - IT security requirements are clearly defined, optimized and included in an approved security plan.
  - Users and customers are increasingly accountable for defining security requirements, and security functions are integrated with applications at the design stage.
  - Security incidents are promptly addressed with formalized incident response procedures supported by automated tools.
  - Periodic security assessments are conducted to evaluate the effectiveness of the implementation of the security plan.
  - Information on threats and vulnerabilities is systematically collected and analyzed.
  - Adequate controls to mitigate risks are promptly communicated and implemented.
  - Security testing, root cause analysis of security incidents and proactive identification of risk are used for continuous process improvements.
  - Security processes and technologies are integrated organizationwide.
  - Metrics for security management are measured, collected and communicated.
  - Members of management use these measures to adjust the security plan in a continuous improvement process.

The solution considered would be comprehensive and beyond the scope of this document. However, the following could be considered:

- The use of ISO 27000 concepts, including certification, independent evaluation and self-assessment

- The development of a security strategy. Realistically, it is not possible to monitor every potential event on all aspects of the IT infrastructure and social infrastructure (e.g., social engineering events). The most important components of the infrastructure and the events to be monitored need to be identified.
- Types of events should be classified. The most important events could be reported by cell phone and e-mail and to centralized operations. Less important events could be reported by e-mail, either individually or as a daily summary report. The least important events may not be recorded, or could be logged and not reported, or could be reported on summary periodic reports to enable trend analysis.
- Monitoring of external events that could be used to facilitate internal fraud, e.g., detection of a flaw in a security package.

COBIT provides the following examples of measures that could be considered; however, the actual measures would be unique to each organization:

- Number of systems where security requirements are not met
- Number and type of suspected and actual access violations
- Number of violations in segregation of duties
- Percent of users who do not comply with password standards
- Number and type of malicious code prevented
- Frequency and review of the type of security events to be monitored
- Number and type of obsolete accounts
- Number of unauthorized IP addresses, ports and traffic types denied
- Percent of cryptographic keys compromised and revoked
- Number of access rights authorized, revoked, reset or changed

These measures would include the measurable goal to be achieved and measurable progress towards that goal.

DS9 Manage the Configuration

DS9 states:

> *Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimises production issues and resolves issues more quickly.*

The COBIT maturity levels were reviewed to assist in establishing goals. The aspects of the maturity levels considered to be relevant were:
- Maturity level 4—Managed and Measurable:
  - The need to manage the configuration is recognized at all levels of the organization, and good practices continue to evolve.
  - Procedures and standards are communicated and incorporated into training, and deviations are monitored, tracked and reported.
  - Automated tools, such as push technology, are utilized to enforce standards and improve stability.
  - Configuration management systems cover most of the IT assets and allow for proper release management and distribution control.
  - Exception analyses, as well as physical verifications, are consistently applied and their root causes are investigated.
- Maturity level 5—Optimized:
  - Baseline audit reports provide essential hardware and software data for repair, service, warranty, upgrade and technical assessments of each individual unit.
  - Rules for limiting installation of unauthorized software are enforced.
  - Asset tracking and monitoring of individual IT assets protect them and prevent theft, misuse and abuse.

The solution considered could include the following components:
- Using/copying unlicensed or unauthorized software—Servers and workstations could be periodically scanned and potentially unauthorized or unlicensed software or file types could be identified.
- Stealing workstations or attaching unauthorized devices—Workstations could be compared to a centralized inventory of workstations and discrepancies could be investigated. Standards could be developed and enforced for all devices attached to the network (e.g., a home computer must have an authorized and current antivirus software package installed).

COBIT provides the following examples of measures that could be considered; however, the actual measures would be unique to each organization:
- Number of business compliance issues caused by improper configuration of assets
- Number of deviations identified between the configuration repository and actual asset configurations
- Percent of licenses purchased and not accounted for in the repository

In addition, the following could be considered:
- Number of licensed products installed
- Number of licensed products installed on workstations that should be used only on servers
- Number of nonstandard, and potentially unlicensed, products installed
- Reporting by geography and department

Appendix VIII—References

Accord Implementation Group (Operational Risk) (AIGOR), "Observed Range of Practice in Key Elements of Advanced Measurement Approaches (AMA)," October 2006

Bank Systems and Equipment, "Basel II Converges With Business Performance," October 2004

Basel Committee on Banking Supervision, Principle 1—*Framework for Internal Control Systems in Banking Organisations*, September 1998

Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards*, June 2006, *www.bis.org/publ/bcbs107.htm*

Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of Operational Risk*, February 2003, *www.bis.org/publ/bcbs91.htm*

BearingPoint, "Basel II Operational Risks," June 2005

BearingPoint, "Data Quality: A Stumbling Block to Basel Compliance," March 2006

British Standards Institution (BSI), BS 25999-1 "Business Continuity Management," 2006

British Standards Institution (BSI), PAS 77 "IT Service Continuity Management," 2006

Business Continuity Institute (BCI), *Good Practice Guidelines for Business Continuity Management, 3rd Edition*, 2007

COSO, *Enterprise Risk Management—Integrated Framework*, September 2004, *www.coso.org/publications.htm*

International Organization for Standardization (ISO), ISO 27001 "Information Security Management Systems—Code of Practice," 2006

IT Governance Institute, COBIT 4.1, USA, 2007 (Source of figure 14.)

IT Governance Institute, *IT Control Objectives for Sarbanes-Oxley, 2nd Edition*, 2006 (Source of figure 8.)

Joint Forum, "High-level principles for Business Continuity," August 2006

KPMG Financial Services, "Basel II—A Closer Look: Managing Operational Risk," 2003 (Source of figures 4 and 13.)

Office of Government Commerce (OGC), IT Infrastructure Library® (ITIL), UK

Paisley Consulting, "The Case for Operational Risk Management," February 2006

PricewaterhouseCoopers, "Basel II: Making It Work for You," March 2004

Symantec, "Risk Management Challenge and Basel II," May 2006

LEADING THE IT GOVERNANCE COMMUNITY

3701 ALGONQUIN ROAD, SUITE 1010
ROLLING MEADOWS, IL 60008 USA
PHONE: +1.847.660.5700
FAX: +1.847.253.1443
E-MAIL: *info@itgi.org*
WEB SITE: *www.itgi.org*