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, ISACA® and the authors make no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of any proper procedures and tests or exclusive of any proper procedures and tests or exclusive of other 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
© 2007 IT Governance Institute. Reproduction of selections of this publication for academic use is permitted and must include full attribution of the material’s source. Reproduction or storage in any form for commercial purpose is not permitted without ITGI’s prior written permission. No other right or permission is granted with respect to this work.

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: info@itgi.org
Web site: www.itgi.org

*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
Chris Fox, ACA, 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, Sumitomo Mitsui Banking Corporation, Japan
Robert Stroud, CA Inc., USA
Robert White, CISA, ACA, ING Bank, UK

ITGI Board of Trustees
Everett C. Johnson, CPA, Deloitte & Touche (retired), USA, International President
Georges Ataya, CISA, CISM, CISSP, Solvay Business School, Belgium, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Avinashi Kadam, CISA, CISM, CBCF, CISSP, Miel e-Security Pvt. Ltd., India, Vice President
Jean-Louis Leignel, MAGE Conseil, France, Vice President
Lucio Augusto Molina Focazzi, CISA, Colombia, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Frank Yam, CISA, CIA, CCP, CFE, CFSA, FFA, FHKCS, FH KIoD, Focus Strategic Group, Hong Kong, Vice President
Marios Diamandides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Trustee

IT Governance Committee
Tony Hayes, FCPA, Queensland Government, Australia, Chair
Max Blecher, Virtual Alliance, South Africa
Sushil Chatterji, MBM, MIMC, Edutech, Singapore
Anil Jogani, CISA, FCA, Avon Consulting Ltd., UK
John W. Lainhart IV, CISA, CISM, IBM, USA
Romulo Lomparte, CISA, Banco de Credito BCP, Peru
Michael Schirrmbrand, CISA, CISM, CPA, KPMG LLP, Austria
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada

ITGI Advisory Panel
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Chair
Roland Bader, F. Hoffmann-La Roche AG, Switzerland
Linda Betz, IBM Corp., USA
Jean-Pierre Corniou, Renault, France
Rob Clyde, CISM, Symantec, USA
Richard Granger, NHS Connecting for Health, UK
Howard Schmidt, CISM, R&H Security Consulting LLC, USA
Alex Siow Yuen Khong, StarHub Ltd., Singapore
Amit Yoran, Yoran Associates, USA

Security Management Committee
Emil D’Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJLPD, USA, Chair
Manuel Aceves, CISA, CISM, CISSP, Cerberian, Mexico
John W. Lainhart, CISA, CISM, IBM Business Consulting Services, USA
Yves Le Roux, CISM, Computer Associates, France
Mark Lobel, CISA, CISM, CISSP, PriceWaterhouseCoopers LLP, USA
Takuya Morita, CISA, CISM, CIA, Sumitomo Mitsui Banking Corporation, Japan
Jo Stewart-Rattray, CISA, CISM, Vectra Corporation, Australia
Rolf von Roessing, CISA, CISM, CISSP, FBCI, KPMG Germany, Germany
ITGI Affiliates and Sponsors
ISACA chapters
American Institute of Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association of Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systèmes d’Information
Institute of Management Accountants
ISACA
ITGI Japan
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
CA
Hewlett-Packard
IBM
ITpreneurs Nederlands BV
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Project Rx Inc.
Symantec Corporation
Wolcott Group LLC
World Pass IT Solutions
Table of Contents

Preface ........................................................................................................................................... 7
1. Executive Summary .................................................................................................................. 8
   Scope and Purpose ................................................................................................................... 8
   How to Read This Document ................................................................................................. 8
2. Governance, Risk Management and Compliance Are Top Business Priorities ..................... 10
3. Evolving Regulatory Landscape .......................................................................................... 13
   The New Approach to Managing Risk .................................................................................. 15
5. The Need to Manage Operational Risk ................................................................................ 17
   Risk Management Approaches .............................................................................................. 17
   Framework for Operational Risk Management .................................................................... 18
   Operational Risk Principles and IT Relevance ..................................................................... 22
6. Managing IT Risk ................................................................................................................ 25
   Guiding IT Principles .......................................................................................................... 25
   ITGP1 [Operational Risk Awareness] .................................................................................. 25
   ITGP2 [Internal Audit Requirement] .................................................................................... 26
   ITGP3 [Management Policies, Processes, Procedures] ......................................................... 26
   ITGP4 [Risk Assessment] ..................................................................................................... 27
   ITGP5 [Risk and Loss Monitoring] ...................................................................................... 27
   ITGP6 [Control and Mitigation Policies, Processes, Procedures] ....................................... 29
   ITGP7 [Business Continuity Management] .......................................................................... 29
   ITGP8 [Framework for Risk Control and Mitigation] ........................................................ 30
   ITGP9 [Independent Evaluation] ........................................................................................ 32
   ITGP10 [Disclosure] ........................................................................................................... 34
   Causes of Loss and IT Risk .................................................................................................. 34
   IT Risk Scenario Analysis .................................................................................................... 36
7. Setting Ground Rules for IT Risk Management ..................................................................... 39
   Developing an Appropriate Risk Management Environment ............................................. 39
   Risk Management: Identification, Assessment, Monitoring, and Mitigation/Control ............ 39
   Role of Supervisors ............................................................................................................. 40
   Role of Disclosure .............................................................................................................. 40
8. Applying the COBIT Framework: From Business Processes to IT Risks to IT Controls .......... 43
   The Business Line Approach in Basel II ............................................................................ 43
   Defining IT Risk Using COBIT ........................................................................................... 44
   Process Level Controls ....................................................................................................... 47
   IT General Controls ............................................................................................................ 48
   Entity Level Controls ......................................................................................................... 48
9. Use of Key IT Risk Indicators .............................................................................................. 49
Appendix I—Basel II Summary ................................................................................................. 52
Appendix II—High-level Alignment of COSO ERM and Basel II ............................................ 60
Appendix IV—Table of COBIT Processes Relevant for Basel II ............................................. 64
Appendix V—Basel II Risk Event Types with the Related IT Aspects and Associated COBIT Processes ..................................................................................................................................................................................................................................................................................................................70
Appendix VI—Implementation Road Map Using COBIT ..............................................................................................................................................................................................................................................................................................................71
Appendix VII—References ........................................................................................................................................................................................................................................................................................................................................................................73
Preface

Financial services organizations 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 banking and financial services transactions. In contrast to the first Capital Accord of 1988, information risk and information technology 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, 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, the IT Governance Institute is taking the proactive step of addressing risk in financial services organizations by presenting this first edition of *IT Control Objectives for Basel II*. The publication is intended to give guidance to information risk managers, IT practitioners, and banking experts with tasks and responsibilities in IT. The main objective is to provide clear and unambiguous guidance with regard to 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 as there are many frameworks that might be applied in financial services organizations. The COBIT framework, as a proven and mature set of IT processes and controls, is uniquely suited to address the need for formalization of Basel-related information risk management. As an established governance framework, COBIT has achieved international recognition and is widely regarded as global best practice. Its versatility and simplicity, coupled with ongoing improvement initiatives, have set COBIT apart from proprietary solutions and other frameworks.

*IT Control Objectives for Basel II* has been developed by a committee of senior banking 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 has given additional credibility to the publication. This first edition highlights the need for information risk management and IT controls as seen from the perspective of bankers and financial experts.

ITGI and ISACA welcome any comments on this publication, in order to continuously improve and adapt *IT Control Objectives for Basel II* to the needs of financial services organizations.

Everett Johnson, CPA
International President
IT Governance Institute
1. Executive Summary

Scope and Purpose

*IT Control Objectives for Basel II* provides a framework for managing information risk in the context of Basel II. This document addresses two target groups—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 information technology space. The IT control objectives and management processes outlined address the role of information technology in operational risk, and the resulting tasks for IT practitioners, internal IT auditors, IT risk managers and information security officers.

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

Corporate governance, risk management and regulatory 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 communications and an inadequate understanding of risk, as well as behavior, according to the principles defined by ITGI. Chapter 2 introduces the relevant concepts of corporate governance, risk management, and compliance.

The growing amount of specific regulatory activity, coupled with an increasing level of detail, are evidence to the fact that governance, risk management and compliance are the primary areas of 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 outlines the relevant regulatory components in financial services and IT.

In 2004, the Basel Committee on Banking Supervision published the second capital adequacy framework which introduces a new approach to risk in financial services organizations. The objective of Basel II is 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 in order to reduce the required capital. This 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, and GRC initiatives are an important factor in reducing the charge. Chapter 4 describes the new approach to risk management as defined in the Basel II framework.
Operational risk is regarded as a particularly important risk category, as witnessed by a vast number of incidents and crises over the past decade. The risk intrinsic to banking operations and conducting ordinary business 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 proved 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 provides an overview of operational risk, its relevance for information risk. The chapter further maps Basel principles for operational risk against information technology risk.

In order 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 an integral part of the organization’s GRC framework. Chapter 6 provides a bridge between Basel II and information-related risk, by defining a set of ten guiding principles for information risk management. These guiding principles correspond to the principles of operational risk management as set down in the Basel documents.

Managing information risk in a Basel context requires an adaptation of known IT processes, controls and related activities. These ground rules for managing IT risk are described in Chapter 7. The corporate GRC framework usually consists of many components addressing different parts and objectives of the organization. For information-related risks, the COBIT framework is an optimized set of processes and tools that support the overall GRC framework. Natural links and alignment paths exist between COBIT and many common frameworks for compliance and governance.

Basel II requires a business-driven approach to risk management. In order 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 8 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 should use COBIT to address all Basel-related risks in a step-by-step manner.

Managing risk includes the use of indicators to denote goals, performance, and levels of risk. Chapter 9 introduces the concept of COBIT key risk indicators (KRI) and their use under Basel II. Each KRI supports the ongoing process of risk assessment and risk management in order 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 information risk management framework.
2. Governance, Risk Management and Compliance Are Top Business Priorities

Corporate governance, risk management and regulatory compliance (GRC) have evolved to become 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, for instance:

- 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.

Governance, risk management and compliance cannot exist as separate areas. Organizations addressing each area in a different way are likely to experience significant cost increases and duplication of effort. Taking a reactive, backward-looking approach toward GRC will negatively affect efficiency and prevent proactive, process-driven initiatives.

Good governance is about setting strategy, managing risk, delivering value and measuring performance. A strong corporate governance framework ensures that the interests of stakeholders are adopted and implemented by management and staff 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. Both compliance and risk management are important components of good corporate governance.

Risk management ranks as the top priority for senior executives. 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.

Figure 1—Corporate Governance, Risk Management and Regulations

Compliance has evolved from a tick-box, reactive approach toward 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 to 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, both in terms of 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 toward 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 likely to increase the capital charge on operational risk which is discussed in detail in Chapter 5.
3. Evolving Regulatory Landscape

Laws, regulations, standards and accepted practices in industry all serve one common purpose. In their entirety, they support good corporate governance, compliance and informed, transparent risk management. 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, are evidence of the fact that governance, risk management and compliance are the primary areas of concern for banking and financial services regulators. Over the past few years, there has been a rapid succession of GRC-related regulatory provisions, for instance:

- Basel II
- National laws and regulations (e.g., Sarbanes-Oxley Act 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 geographical spread of financial operations across national borders
- Increased collaboration between regulators across geographical 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

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 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.

Parts of existing regulations and standards will remain rules-based. Organizations are, therefore, required to fully comply with a defined set of requirements, metrics and measurements. With the introduction of Basel II, this normative regulation is extended. Regulation now includes process-based and outcome-based provisions. Financial services organizations are, thus, required to demonstrate their processes and outcomes in order to be compliant with these 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 governance, risk management and compliance in a forward-looking manner, including in previously unregulated areas such as information management, information technology and in related disciplines such as security, business continuity and privacy.

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 a high priority to maintain public confidence in the international financial system.

Within the banking and financial services community, risk, in general, requires categorization in order to create manageable governance, risk management and compliance 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 New Approach to Managing Risk

In 2004, the Basel Committee on Banking Supervision published the second capital adequacy framework which introduces a new approach to risk in financial services organizations. The objective of Basel II is 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 in order 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, and GRC initiatives may be instrumental in reducing this charge. In many cases, financial services organization structure and processes may have to be revisited and reevaluated based on this new perspective on risk and capital requirements.

The new approach to risk is designed to encompass the complexity in information technology and information management. The revised framework, as shown in figure 2, is built on the 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
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 will be 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 in order 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 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.

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 to 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.
5. The Need to Manage Operational Risk

Risk Management Approaches

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. The operational risk category is, therefore, 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. Operational risk may be managed using one of the three fundamental approaches below:

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

In addition to the selection of one of these approaches, financial services organizations must comply with a set of minimum requirements which influence core business and IT. Appendix I outlines the detailed requirements and the approaches listed above.

The second consultation paper 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 banks which could have been avoided if more effective controls and more sophisticated business processes had been in place.

Furthermore, the banks increased dependency on IT, extensive use of the Internet, higher complexity of financial products and the higher number of market channels provide many reasons to recognize and assess the banks’ operational risks.

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.*

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, the banks may use various alternative approaches.

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

Similar to the philosophy behind capital adequacy regulations in connection with credit exposure, the three approaches are moving 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.

Banks 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.

Banks may use the advanced approach for selected individual business lines. The implementation of individual approaches also requires the banks to comply with certain qualifications.

### Figure 3—The Three Approaches to Operational Risk

All banks must comply with the minimum requirements which are defined in the Committee’s guidance notes “Operational Risk Sound Practices.” These include:

- The board of directors and the 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 as witnessed by the vast number of incidents and crises over the past decade. The risk intrinsic to banking 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.

**Figure 4—Framework for Managing Operational Risk**

![Framework for Managing Operational Risk](image)

**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.
**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 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 the advanced measurement approaches (AMA). The need for historic data (including external data) has been a driving force behind 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**
Financial services organizations should assess aspects of operational risk based on key risk indicators (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. Capital modeling 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 as well as external sources.

The Basel Committee explicitly states in its “Sound Practices for the Management and Supervision of Operational Risk” that the growing sophistication of information technology is a factor making the activities of financial services organizations more complex. Six examples of the new and growing risks faced by banks identified in Basel II include, in addition to outsourcing and risk mitigation, four IT-related risks:

- The greater use of more highly automated technology has the potential to transform risks from manual processing errors to system failure risks, as greater reliance is placed on globally integrated systems.
- Growth of e-commerce brings with it potential risks that are not yet fully understood.
- Large-scale acquisitions, mergers, consolidations and divestitures test the viability of new or newly integrated systems.
- The emergence of banks acting as large-volume service providers creates the need for continual maintenance of high-grade internal controls and back-up systems.

The ERM Framework\(^1\) defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) has become the most commonly used framework for establishing a system of internal control and risk management in banks, especially those having to comply with the Sarbanes-Oxley Act 2002 (SOX). SOX and related regulations make reference to the COSO framework as one of the alternatives suggested for implementing an appropriate system of internal controls over financial reporting. COSO has identified a comprehensive set of components essential for effective internal control. The components originally specified in the COSO Integrated Framework 1992 for SOX compliance purposes are still included in the ERM Framework as shown in figure 5.

<table>
<thead>
<tr>
<th>Control Environment</th>
<th>COSO 92</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment</td>
<td></td>
</tr>
<tr>
<td>Control Activities</td>
<td></td>
</tr>
<tr>
<td>Information and Communication</td>
<td></td>
</tr>
<tr>
<td>Monitoring</td>
<td></td>
</tr>
<tr>
<td>Event Identification</td>
<td>COSO ERM Add-Ins</td>
</tr>
<tr>
<td>Objective Setting</td>
<td></td>
</tr>
<tr>
<td>Risk Response</td>
<td></td>
</tr>
</tbody>
</table>

\(^1\) or any other acceptable alternative; for instance, the Combined Code in the UK (“Turnbull”), CoCo, or other national governance frameworks which may be seen as equivalent to the minimum requirements of COSO
The current COSO ERM framework has been extended to cover aspects of governance, risk management and compliance. For organizations that are required to be SOX compliant, the SOX baseline may be used as a starting point for achieving Basel II compliance. Organizations not currently required to be SOX compliant may nevertheless benefit from best practice and experience gained from SOX projects in their country.

The Sarbanes-Oxley Act 2002 requires organizations to introduce a system of internal controls over financial reporting in order to address the risk of financial misstatements. SOX primarily covers financial audit risk, inasmuch as it requires organizations to introduce manual or automated controls that are designed to prevent any significant misstatement in financial accounts. Operational risk is an important component of SOX where an operational impact might ultimately influence the financials of the organization. SOX does not, however, specifically address operational risk as such. SOX only mandates that operational losses be correctly booked and posted to the accounts. For more information about IT aspects of compliance to Sarbanes Oxley see: IT Controls for Sarbanes Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition published by the IT Governance Institute.

In its “Framework for Internal Control Systems in Banking Organisations” (1998), the Basel Committee relies on the definitions and basic elements of internal control systems developed in accordance with COSO. 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 to 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, therefore, an agreed basis for planning, designing and implementing a risk management framework within an organization, covering aspects of financial audit (SOX) risk and operational (Basel) risk. Therefore, the COSO framework reconciles various categories of risk and allows organizations to integrate their GRC initiatives.

The COSO enterprise risk management framework 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, 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 to the requirements of COSO and regulatory drivers. COBIT, therefore, bridges the gap between high-level enterprise risk management and specific IT risk issues.

**Operational Risk Principles and IT Relevance**

Information technology and information management are key elements of a comprehensive strategy to manage GRC and to optimize the capital charge. IT-related components such as applications, infrastructure elements and controls are all defined as parts of operational risk. **Figure 6** shows the guiding Basel II principles on operational risk as well as their relevance and requirements in terms of information management and information technology.
The principles are provided to enable the use and implementation of the *IT Control Objectives for Basel II* within the context of an integrated corporate governance, risk management and regulatory compliance (GRC) framework.

<table>
<thead>
<tr>
<th>Basel Principle</th>
<th>IT Relevance and Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The board of directors should be aware of the importance of operational risk. There is a need for an operational risk management framework.</td>
<td>IT is a critical component of operational risk (systems, processes failure, etc.) and, therefore, must be managed as an operational risk type.</td>
</tr>
<tr>
<td>2. The operational risk management framework is subject to effective and comprehensive internal audit.</td>
<td>The internal IT audit function should be adequately skilled and staffed in line with the IT risk profile, including adequate funding and the use of external specialist resources, where appropriate.</td>
</tr>
<tr>
<td>3. Develop policies, processes and procedures for managing operational risk.</td>
<td>IT should use GRC frameworks (e.g., COSO) to integrate IT-specific risk within the overall corporate risk management process. Information security, business continuity, disaster recover and other relevant policies, procedures and standards should provide a basis for addressing operational risk.</td>
</tr>
<tr>
<td>4. Identify and assess operational risk.</td>
<td>IT should conduct technology-specific risk assessments to identify the potential operational impact of technology-related threats and vulnerabilities. Risk assessment results should be integrated with other risk assessments and incorporated into the GRC framework.</td>
</tr>
<tr>
<td>5. Regularly monitor operational risk profiles and material exposure to losses.</td>
<td>IT should identify acceptable limits of risk and develop metrics to measure performance against these profiles.</td>
</tr>
<tr>
<td>6. Have policies, processes and procedures to control and/or mitigate material operational risks.</td>
<td>The IT risks within operational risk should be subject to an IT risk policy and subsidiary procedures. The policy should in be line with overall GRC policies and procedures.</td>
</tr>
<tr>
<td>7. Have contingency and business continuity plans.</td>
<td>IT should have IT continuity plans and management procedures that link to corporate business continuity and incident response management.</td>
</tr>
<tr>
<td>8. Have framework in place to identify, assess, monitor and control/mitigate material operational risks.</td>
<td>IT should identify relevant parts of the corporate GRC framework, including COSO, and develop an IT-specific risk management framework.</td>
</tr>
<tr>
<td>Basel Principle</td>
<td>IT Relevance and Requirements</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>9. Conduct regular independent evaluation of a bank’s policies, procedures and practices related to operational risk.</td>
<td>IT should document the IT risk profile for the supervisory review process. The external IT audit function should perform reviews of IT-related operational risk management in line with the IT risk profile.</td>
</tr>
<tr>
<td>10. Provide sufficient public disclosure.</td>
<td>IT should identify all relevant risks that constitute a material operational risk in the sense of disclosure as defined by senior management (Annex 13 of the “Basel Sound Practices” paper), escalate where necessary to appropriate stakeholders and take corrective action.</td>
</tr>
</tbody>
</table>
6. Managing IT Risk

Information and information technology 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 Operational Risk Management” lead to a corresponding set of guiding principles for managing information management and information technology risks.

Guiding IT Principles

In order to apply the IT control objectives for Basel II, guiding principles are required for information technology practitioners and financial services experts whose tasks and responsibilities include aspects of information technology. The following principles have been developed using a set of source documents, including:

- The Principles defined in the *Sound Practices for the Management and Supervision of Operational Risk* also published by the Basel Committee in February 2003
- The *Enterprise Risk Management—Integrated Framework* published by the US Committee of Sponsoring Organisations of the Treadway Commission (COSO) in September 2004

**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, the IT component requires definition and in-depth understanding. Awareness should not be restricted to the fact that there is an existing IT risk, and all GRC-related objectives and practices should be aligned with the organizational GRC framework.

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 as well as private settlements. Operational risk specifically excludes strategic and

---

2 More information on the *International Convergence of Capital Measurement and Capital Standards* can be found at www.bis.org/publ/bcbs107.htm.
3 More information on the *Sound Practices for the Management and Supervision of Operational Risk* can be found at www.bis.org/publ/bcbs91.htm.
reputational risk.” 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 may influence information technology, for instance, where incidents or disasters prevent the functioning of critical infrastructures.

Similar rigor should be applied to the management of operational risk as would be expected for the management of other significant banking risks such as credit risk, interest rate risk and liquidity risk. However, operational risk differs from other banking 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 that this affects the risk management process. 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 information technology 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, for instance in credit or market risk. GRC components for IT should, therefore, 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 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 report to the board as appropriate. 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.*

---


6 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.
Managing governance, risk management and compliance requires a clearly defined and documented set of policies, processes and procedures. These should match 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 do not become credit or market risk disciplines. 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 information technology 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.

In order 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 information technology.

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 those risks that fall within their areas of accountability.

**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 are
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, the chief risk officer, the chief information security officer, internal audit and the board risk and audit committees are aware of significant incidents and the risk 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)” paper7 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.

> 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, ensuring its integrity and accuracy, its completeness and its 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

---

7 Published by the Accord Implementation Group’s Operational Risk Subgroup (AIGOR) in October 2006 and focusing 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 Advanced Measurement Approaches.
data upon which that information is built. Entities that treat data as an organizational asset are in a better position to manage it 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, chief executive officer, chief finance officer, chief risk officer and chief information security officer are ultimately accountable for data integrity and its 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 shall be protected by a comprehensive continuity management process. The IT continuity management process shall 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 in order 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. The principles stipulate that an organization shall 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.\textsuperscript{9} 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.\textsuperscript{10} 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.

**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 enterprise risk management (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. The *Enterprise Risk Management—Integrated Framework* published by the US Committee of Sponsoring Organisations of the Treadway Commission (COSO) in September 2004 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, but 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

\textsuperscript{10} cf. ITIL (IT Continuity Management), ISO 27001 and BS PAS 77
It control objectives for Basel II: The importance of governance and risk management for compliance

Exposure Draft

© 2007 IT Governance Institute. All rights reserved. www.itgi.org

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.

Enterprise risk management 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**—Enterprise risk management provides the rigor to identify and select among alternative risk responses—risk avoidance, reduction, sharing, and acceptance.
- **Reducing operational surprises and losses**—Entities gain enhanced capability 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 myriad of risks affecting different parts of the organization, and enterprise risk management 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,” “Recognise and Manage Risk” and “Monitor and Report Risk.”

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

---

11 Each of these components is described in detail in the COSO literature which is available for download for a small price. www.coso.org/publications.htm
In information management and information technology, risk management initiatives and programs should be integrated with the overall GRC approach. This means that ERM as described previously is an important framework for IT risk. 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 COBiT.

**ITGP9 [Independent Evaluation]**

Information management and technology-related risks shall be adequately documented to support the supervisory review process. The external IT audit function should perform reviews of IT-related operational risk management in line with the information risk profile.

Information-related risks require documentation in line with the requirements of the supervisory review process in order 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.
Each component of the ERM framework is assessed against the six “Stages of Control Reliability,” as shown in figure 8:

- **0 Non-existent**—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 standardised 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 not to be working effectively. 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 best 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.

**Figure 8—Stages of Control Reliability**
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 which could potentially undermine the whole ERM framework, such as data quality in monitoring, role clarity, tools and people skills.

**ITGP10 [Disclosure]**

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

Risks, deficiencies and other issues identified within the organization shall 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.” 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 contributing factors to systemic risks is the fact that financial services organizations usually depend on information technology and information management, and that complex infrastructures are required to support core business processes.

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

The definition of operational risk looks very broadly at causes since this provides 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.

**Example 1**

An insider exploiting a programming error in an internal web application should be categorized in the cause category Systems, whereas an intruder obtaining access to a bank’s computer using hacking tools, phishing or malware would 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 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 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 only 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 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 service organizations implementing this risk identification and categorization method should identify additional level II risk categories, using COBIT resources and processes, and 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 sub-categories 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 principle12) that are not working because of a programming error in the banking 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 service organizations using the AMA approach to use scenario analysis and expert opinion in conjunction with external data in order 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 information risk management approach, experienced IT practitioners, information security specialists, business managers and risk management experts as well as IT specialists from internal audit and from the IT compliance function should be brought together to discuss the IT scenarios with a reasonable probability of occurrence and resulting in severe expected losses.

The IT scenarios in figure 9 may be regarded as illustrative, being categorized into A and B according to their importance to the financial services industry.

---

12 The four-eye principle means that all business decisions and transactions need approval from the CEO and CFO. Since the CFO is not reporting to the CEO, there is an independent controlling mechanism in place.
### Figure 9—IT Scenarios

<table>
<thead>
<tr>
<th>Illustrative IT Scenarios</th>
<th>Scenario Definition</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized users perform unauthorized activities</td>
<td>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.</td>
<td>A</td>
</tr>
<tr>
<td>Disruption of service</td>
<td>There is a failure of hardware/software, critical service or environmental systems or data loss, denial of service, capacity planning error.</td>
<td>A</td>
</tr>
<tr>
<td>Incomplete transaction processing</td>
<td>Errors or incomplete transaction processes are not detected resulting in erroneous results.</td>
<td>A</td>
</tr>
<tr>
<td>Misuse of sensitive assets</td>
<td>Those with authorized access misuse access privileges.</td>
<td>A</td>
</tr>
<tr>
<td>Project failure</td>
<td>Project results are not delivered within agreed time frames, budget and quality.</td>
<td>A</td>
</tr>
<tr>
<td>Product failures</td>
<td>There is a failure to identify security requirements or to design security into product selection and implementation activities.</td>
<td>B</td>
</tr>
<tr>
<td>Third-party risk</td>
<td>Risks related to reliance on third-party services are not well defined or are improperly managed.</td>
<td>B</td>
</tr>
<tr>
<td>Theft of sensitive or critical assets</td>
<td>Hardware/software components, devices, system output, data files, notebook computers, portable computing devices, etc., are stolen.</td>
<td>B</td>
</tr>
<tr>
<td>Malicious activity</td>
<td>Hacking, phishing, social engineering or cyber extortion are taking place.</td>
<td>B</td>
</tr>
<tr>
<td>Process failure</td>
<td>There is a lack of integration of security into sensitive business processes.</td>
<td>B</td>
</tr>
</tbody>
</table>

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 is not available.

**Figure 10** shows illustrative risk drivers for the 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 re-assessed by comparing them to actual loss data available over time. This is an essential to ensure the reasonableness of qualitative methods applied to risk management.
<table>
<thead>
<tr>
<th>IT Scenario</th>
<th>Risk Driver for Frequency</th>
<th>Risk Driver for Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized users perform unauthorized activities</td>
<td>• Users with access to sensitive application functions&lt;br&gt;• Lack of supervisory control&lt;br&gt;• Improper definition of access permissions&lt;br&gt;• Excessive access to and use of supervisory capabilities&lt;br&gt;• Improper access to software or systems</td>
<td>• Inadequate monitoring of system exception reports&lt;br&gt;• Lack of management control&lt;br&gt;• Lack of audit review&lt;br&gt;• Inappropriate security policies&lt;br&gt;• Lack of proper security awareness training&lt;br&gt;• Lack of accountability&lt;br&gt;• Inadequate access management</td>
</tr>
<tr>
<td>Disruption of service</td>
<td>• Number of potential damaging incidents which can cause a disruption of service&lt;br&gt;• Susceptibility of hardware and software to damage&lt;br&gt;• Failure to identify interdependencies among systems and applications</td>
<td>• Inability to correctly identify the impact of conditions that can result in a disruption of service&lt;br&gt;• Failure to monitor for events that can result in a disruption of service&lt;br&gt;• Failure to develop and implement incident detection and escalation procedures</td>
</tr>
<tr>
<td>Incomplete transaction processing</td>
<td>• Potential for processing errors to not be detected</td>
<td>• Potential for significant damage resulting from incomplete processing</td>
</tr>
<tr>
<td>Misuse of sensitive assets</td>
<td>• Number of shared user IDs or group accounts&lt;br&gt;• Number of users with access to sensitive applications or application functions&lt;br&gt;• Lack of comprehensive security policies, procedures and standards&lt;br&gt;• Failure to provide security awareness&lt;br&gt;• Lack of monitoring and correction by supervisors&lt;br&gt;• Failure to consider security when defining business procedures and processes</td>
<td>• Lack of monitoring tools or inconsistent use of these tools&lt;br&gt;• Lack of ability to respond to security incidents</td>
</tr>
<tr>
<td>Project failure</td>
<td>• Number of projects&lt;br&gt;• Quality of defined program and project management approach</td>
<td>• Amount of project budget&lt;br&gt;• Number of critical projects</td>
</tr>
</tbody>
</table>
7. Setting Ground Rules for IT Risk Management

The ten principles concentrate on the high-level standards deemed necessary for the management of operational risks. In keeping with the Basel Committee’s goals, the principles are deliberately high level to allow banks to develop approaches suitable to their organizational needs. The ten principles are structured according to the Basel pillar concept in categories and comprise the following aspects.

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 the board should approve and periodically review the bank’s operational risk management framework. The framework should provide a firmwide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.

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.

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 organization, 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.

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.

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.
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.

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.

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.

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.

Role of Disclosure

Principle 10
Banks should make sufficient public disclosure to allow market participants to assess their approach to operational risk management.

Although the ten principles refer to operational risk management as a whole, certain points can be derived for the IT risk management discipline.

Although the ten principles refer to operational risk management as a whole, they form the set of principles that are relevant to IT risk management discipline. As shown in figure 11, COBIT is used to provide a high-level orientation in terms of GRC processes.

COBIT provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT’s good practices represent the consensus of experts. The practices are strongly focused more on control, less on execution. These practices will help optimize IT-enabled investments, ensure service delivery and provide a measure to judge against when things do go wrong.

The process focus of COBIT is illustrated by a process model that subdivides IT into four domains and 34 processes in line with the responsibility areas of plan, build, run and monitor, providing an end-to-end view of IT. Enterprise architecture concepts help identify the resources essential for process success, i.e., applications, information, infrastructure and people.
COBIT offers a dedicated process PO9 *Assess and manage IT risks*. This process satisfies the business requirement for analyzing and communicating IT risks and their potential impact on
business processes and goals by focusing on the development of a risk management framework that is integrated with business and operational risk management frameworks, risk assessment, risk mitigation and communication of residual risk. The planning and organization domain within COBIT may provide further guidance with regard to integrating GRC with general IT management.

Sound operational risk management and heightened transparency are integral components of enhanced GRC and thus of IT governance. COBIT, as an IT governance framework, enables IT governance, especially by using the monitor and evaluate (ME) processes which focus on preparing board reports on IT strategy, performance and risks, and responding to governance requirements in line with board directions. The ME domain within COBIT provides guidance for identifying, measuring and assessing components of an organization’s IT GRC framework, with a view toward improving subsequent GRC steps.

COBIT offers definitions, linkages, and structures as well as a repository of risk mitigation activities and key risk indicators concerning information technology that can be used as building blocks for a framework to manage operational risk, as shown in figure 12.

<table>
<thead>
<tr>
<th>Core Basel principle</th>
<th>IT Relevance</th>
<th>Related COBIT Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Board of directors should be aware of the need for an operational risk management framework.</td>
<td>IT risk management</td>
<td>PO9 Assess and manage IT risk.</td>
</tr>
<tr>
<td>2. Operational risk management framework is subject to effective and comprehensive internal audit.</td>
<td>IT internal audit</td>
<td>ME4 Provide IT governance.</td>
</tr>
<tr>
<td>3. Develop policies, processes and procedures for managing operational risk.</td>
<td>IT risk management</td>
<td>PO9 Assess and manage IT risk.</td>
</tr>
<tr>
<td>4. Identify and assess the operational risk.</td>
<td>IT risk management</td>
<td>PO9 Assess and manage IT risk.</td>
</tr>
<tr>
<td>5. Regularly monitor operational risk profiles and material exposures to losses.</td>
<td>IT risk management</td>
<td>PO9 Assess and manage IT risk.</td>
</tr>
<tr>
<td>6. Have policies, processes and procedures to control and/or mitigate material operational risks.</td>
<td>IT risk management</td>
<td>PO9 Assess and manage IT risk.</td>
</tr>
<tr>
<td>7. Have contingency and business continuity plans.</td>
<td>Ensure continuous service</td>
<td>DS4 Ensure continuous service.</td>
</tr>
<tr>
<td>8. Have framework in place to identify, assess, monitor and control/ mitigate material operational risks.</td>
<td>IT risk management</td>
<td>PO9 Assess and manage IT risk.</td>
</tr>
<tr>
<td>9. Conduct regular independent evaluation of a bank’s policies, procedures and practices related to operational risks.</td>
<td>IT internal audit</td>
<td>ME2 Monitor and evaluate internal control.</td>
</tr>
<tr>
<td>10. Sufficient public disclosure.</td>
<td>IT escalation to management</td>
<td>ME2 Monitor and evaluate internal control.</td>
</tr>
</tbody>
</table>
8. Applying the COBIT Framework: From Business Processes to IT Risks to IT Controls

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.

The Business Line Approach in Basel II

Besides the business line perspective, a bank must also be able to manage risks in a centralized function (e.g., an information technology 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 information technology. 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 which 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 the bank offers services to retail customers; for instance, to purchase shares at the exchange. To use this service, customers must key their orders into an Internet application. On authenticating the order, it is processed by the bank, 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 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 bank, providing not only core application components, but 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 bankwide 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 Using COBIT**

When designing and outlining scenarios for risk evaluation, COBIT may assist in defining a standardized control environment for the scenario under review by stating the applicable control processes. **Figure 13** shows corresponding control objectives for the category A, IT scenarios:

<table>
<thead>
<tr>
<th>IT Scenario</th>
<th>COBIT Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized users perform unauthorized activities</td>
<td>DS5 Ensure systems security.</td>
</tr>
<tr>
<td>Disruption of service</td>
<td>DS4 Ensure continuous service.</td>
</tr>
<tr>
<td>Incomplete transaction processing</td>
<td>AC4 Processing integrity and validity.</td>
</tr>
<tr>
<td>Misuse of sensitive assets</td>
<td>DS5 Ensure systems security.</td>
</tr>
<tr>
<td>Project failure</td>
<td>PO10 Manage projects.</td>
</tr>
</tbody>
</table>

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 a considerable variation in the level of experience, seniority and status of these individuals. In some organizations, the risk manager has senior status and the real ability to challenge 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—an essential requirement of the risk function.

In order to organize the respective roles of compliance, internal audit and risk, some organizations have structured themselves in a Three Lines of Defense Model (see **figure 14**) where risk management provides a second line independent challenge and audit provides assurance that the first two lines are operating as intended.
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 14, based on the COSO ERM framework.

**Figure 14—Lines of Defense—ERM Framework**

- **Objective Setting**
  - Strategic Objectives – Related Objectives – Selected Objectives – Risk Appetite – Risk Tolerances

- **Internal Environment**
  - Risk Management Philosophy – Risk Appetite – Board of Directors – Integrity and Ethical Values – Commitment to Competence – Organizational Structure – Assignments of Authority and Responsibility – Human Resource Standards

- **Tone at the Top**
  - Chief Executive Officer
  - Board
  - Board Risk Committee
  - Board Audit Committee

- **Monitor & Report Risk**
  - Ongoing Monitoring Activities – Separate Evaluations – Reporting Deficiencies

- **Risk Assessment**
  - Inherent and Residual Risk – Establishing Likelihood and Impact – Data Sources – Assessment Techniques – Event Relationships

- **Risk Response**
  - Evaluating Possible Responses – Selected Responses – Portfolio View

- **Control Activities**
  - Integration with Risk Response – Types of Control Activities – Policies and Procedures – Controls over Information Systems – Entity Specific

- **Information & Communication**
  - Information – Communication

- **Integrated Risk Management**
  - Event Identification

- **CORPORATE GOVERNANCE**
  - Tone at the top

- **1 Business Line**

- **2 Risk Management**

- **3 Internal Audit**
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 15. The three lines of defense model distinguishes between 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. The chief executive officer, supported by senior management, has overall responsibility for the management of risks facing the organization. Management and staff 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 rest 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
  - Provides general and specialist support and advice to 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 board audit committee and, ultimately, to the main board.

**Figure 15—Three Lines Concept**

---

13 “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 organisations 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.*
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 general IT controls, assuring that IT applications are developed and operated according to business specification and that users are only permitted access defined by the business.

COBIT control objectives can be used to define the required general and application controls and to 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 (AC) numbers 1 through 6.

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. Errors and irregularities must be detected 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 are performed without compromising original transaction authorization levels. Where appropriate for reconstruction, original source documents should be retained for the appropriate amount of time.

AC3 Accuracy, Completeness and Authenticity Checks
Ensure that transactions are accurate, complete and valid. Validate and edit, or send back for correction, input data 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 the necessary control information is provided and used to enable verification, detection and correction of the accuracy of output.

AC6 Transaction Authentication and Integrity
Before passing transaction data between internal applications and business or operational functions (in or outside the enterprise), check for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.
IT General Controls

For IT general controls, COBIT has defined a recommended set of over 200 control objectives which are either application-specific or applicable throughout the organization. IT general controls usually address summary control objectives that are enablers for process and application level controls. An IT general control such as the access control framework for applications, for instance, 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.

Entity-level Controls

For IT entity level controls as outlined above, COBIT provides a comprehensive set of control objectives with a strategic focus. These objectives 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. The COBIT framework should be applied accordingly. Although illustrative questions may be useful to communicate an overall, high-level understanding of entity level controls, it is the responsibility of managers and information risk specialists to determine the scope and extent of control objectives that is required to obtain reasonable assurance over entity level controls.
9. Use of Key IT Risk Indicators

Risk indicators are parameters tracking operational risk exposure and changes in the operational risk profile. Risk indicators are, therefore, a type of early warning system for the operational risk profile. As opposed to scenario-based risk assessments, indicators track near real-time empirical data, but not estimates of future activities. 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. Threshold levels should always be set (e.g., at green, amber and red with each threshold associated to the related measurable quantifier) to facilitate management response.

Indicators may be detective or preventive in nature. Preventive indicators are designed to stop undesirable transactions, items, events, errors or incidents from occurring (e.g., authorization and approval controls, staff training, automated system calculation and validation, password and access controls). Detective controls are designed to reveal undesirable occurrences promptly so that appropriate corrective action can be taken (e.g., reconciliation or review of exception reports).

The term key risk indicator (KRI) refers to the indicators which track risks especially well or which track very important risks. KRIs are used to manage operational risks and play an important role in operational risk management reporting.

Identifying relevant KRIs can be a complex endeavor since the assumed correlation with actual exposure can only be determined over time using internal loss data. Selection of KRIs is usually done through self assessments and by interviewing executives and managers. Banks may need to combine several primary or directly available indicators to achieve the desired early warning information. To maintain ease of comprehension, many banks have used only a limited set of generic indicators for business units across the bank along with an equally limited set of business line-specific indicators where necessary.

To identify the relevant risk indicators, it is important to identify the risk drivers. When the risk drivers have been identified, they must be made measurable. Risk indicators should be effective, efficient and comparable.

In the banking industry, a library of risk indicator has been developed by the Risk Management Association (RMA), offering a comprehensive collection of risk indicators\(^{14}\) that can be drawn from in the risk indicator definition process. COBIT offers such a library for risk drivers identified in IT control objectives as part of the COBIT\(^{®}\) Control Practices.

COBIT uses two types of metrics:
- Outcome measures or key goal indicators (KGIs) to indicate whether the goals have been met. These can be measured only after the fact and, therefore, are called lag indicators. COBIT KGIs tell management whether an IT process has achieved its business objective, usually expressed in terms of information criteria.

\(^{14}\)www.kriex.org
• Performance drivers or key performance indicators (KPIs) measure how well the process is performing in enabling the process goal to be reached. They are good indicators of capabilities, practices and skills and can be measured before the outcome is clear and, therefore, are called lead indicators. COBIT KPIs measure the activity goals, which are the actions the process owner must take to achieve effective process performance. KPIs indicate whether goals are likely to be met.

The maturity level of a process when measured regularly could also serve as a risk indicator. In addition, the maturity of significant processes should be on a level that ensures ongoing and consistent measurement of KPIs and KGIs, enabling management to base their decisions on a solid basis of indicators.

After defining the relevant risk indicators and the thresholds and action triggers to them, the risk indicators have to be verified at least on an annual basis. This review should be supported through data collections and analysis.

The maturity assessment may, therefore, be documented in accordance with the IT Governance Implementation Guide: Using COBIT® and Val IT®, 2nd Edition, by a Responsible, Accountable, Consulted and Informed (RACI) chart, covering the responsibilities of the board, the board risk and audit committees, and key stakeholders within the ERM three lines of defense, including the business, risk and governance committees, the chief executive officer, chief financial officer, chief risk officer, risk functions and committees, and internal audit.

Finally, it is important to apply the COBIT maturity level assessment and risk indicator approach, including the RACI model, in a uniform manner across the IT scenarios and control processes and objectives. In order to obtain a valid risk indicator, the COBIT model should be applied in a series of steps. This will enable the comparison between KGI/KPI and the resulting measure of risk as required in the context of GRC:
• Identify KGI(s) applying to the control objective
• Measure KPI(s) to obtain the degree of conformity with goal (go beyond a simple yes or no)
• Where maturity is lower than expected, assess the risk:
  - Is it known?
  - Is there an existing risk acceptance?
  - If there is no risk acceptance, does the risk require escalation/disclosure?
• Where KGIs are not matched in performance, and residual risks remain, the gaps should be flagged as key risks. Where the risk is known and accepted, the risk may be present, but it is assumed to be managed.

The use of key risk and key performance indicators will 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. These significant IT weaknesses require quantification. It may be necessary to apply an independent business impact analysis to the IT environment in order to determine the expected loss (weighted) over a given period of time. It should be noted that IT risk in itself is unlikely to cause operational losses that impact the capital charge. It is very likely that IT-induced failures—indirect risks—will have an impact on core business processes that may
lead to severe or catastrophic operational losses (sometimes termed cascading system failures, contagion, ripple-through or domino effect). However, these cannot be quantified in isolation.

There is no Basel specific mandate to use risk indicators. However, KRIIs are an important tool for measuring and evaluating information-related risks. Furthermore, KRIIs provide a detailed view of the relative strength of controls implemented to mitigate and manage individual risks. External loss data and related indicators address the question of probability, and they will provide a view of whether the organization might be under threat from a risk or class of risks. Internal loss data and related indicators will provide a view of internal vulnerabilities. The combination of KGIs, KPIs and key risk indicators with the maturity level model in COBIT will enable the organization to develop remediation and mitigation strategies to close any gaps.
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 then enacted through country legislation\(^{15}\) 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 banking supervision and will cause major changes in the organization of internationally operating banks. The regulators are scheduled to be implemented in a step-by-step approach which started in 2006 and is scheduled to be completed in 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 the 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 Accord is intended to:

- Strengthen the soundness and stability of the international banking system and to maintain the present status of capitalization in the banking system
- Further improve conditions of a level playing field
- Address all risks more comprehensively
- Ensure that the 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 are:

- Regulations are applied to consolidated banking groups rather than only to single institutions.
- Calculation of capital adequacy may be based on banks’ internal rating methods.
- 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.

\(^{15}\) In Europe the standards are initially adopted at a European Union level in the form of an EU Directive.
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 as compared to current rules. However, this is in line with the development of the various business areas and advances in credit risk management of banks.

Banks 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 controlling and risk management among banks. 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 banks’ 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**

Adequate capital for risk-weighted assets alone is not sufficient to stabilize the financial markets. Banks 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 to be further developed as an ongoing process. Banks 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 driven model of banking supervision. The supervisor’s review is considered to be the second pillar of the framework.

The extended disclosure requirements will be 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 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 concern the assessment of credit risk and operational risk. The definition of total capital for regulatory purposes and the calculation of total market risk remain unchanged.

---

16 The following text is based on the document *Basel II Framework* published by the Basel Committee on Banking Supervision, June 2004.
Credit Risk
The Basel Committee uses a risk weighted approach for capital requirements, as shown in figure 16. Participating banks 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 are met as defined by the supervisor.

Figure 16—The Three Approaches to Credit Risk

The Standardized Approach
Basel II continues to use risk weights for credit exposures. However, risk weights should now 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, banks, 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 bank 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 bank 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) will 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.
Internal Ratings Based 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. Banks 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 as set by the supervisor.

Banks must categorize banking-book exposures into 11 classes of exposure with different underlying risk characteristics. The classes of assets are, e.g., corporate, sovereign, bank, retail, and equity. Within these classes the risk components are separately associated with specific (rating based) risk parameters.

For each asset class covered under the IRB framework, there are different regulations to address the individual risk weights. Basically, the banks can choose between two approaches:
- The easier foundation approach
- The advanced approach, which recognizes, to a greater extent, the bank’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 bank has to estimate the probability of default within one year for each category.
- **Exposure at default (EAD)**—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 (LGD)**—In case of default, the loss for the bank depends on the recoverability of any collateral and revenues from the sale of the borrowers’ 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, banks 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, M) are determined by the supervisors. Collateral, warranties, credit derivatives and netting agreements are treated similarly to the standardized approach.
- Under the advanced approach, banks must calculate the effective maturity (M) and are providing their own estimates of the above risk components. To qualify for the advanced approach, banks 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, which concur with the credit portfolio model Credit-Metrics.
To obtain the supervisor’s approval for the IRB approach, banks must comply with the minimum requirements, e.g., a quality rating system and extensive disclosure practices as specified in the third pillar. This should 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, banks should apply stress tests based on their internal models. Such tests should consider at least 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**
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.*

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, the banks may use various alternative approaches.

**Basic Indicator Approach**
Banks using the basic indicator approach (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 is calculated from the sum of interest surplus, and commission surplus, trading result, financial asset result and other income. This broad approach may be used by small banks without a system to control operational risks. The Basel Committee expects international operating banks to use the standardized approach as a minimum.

**Standardized Approach**
The standardized approach (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.

Banks 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 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 the advanced measurement approaches (AMAs) may use actual bank-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 are stating 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 the banks, the supervisor is entitled to determine whether the approach is sound and appropriate. The approval will depend on the presence of various factors the supervisors will want to see properly incorporated in the internal models.

It is imperative that the banks’ approach is based on internal loss data and that the defined but the Committee business lines and loss events are implemented. Furthermore, the banks must fully incorporate the actual risk exposures into their operative and strategic planning. The bank must 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. Banks 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 bank must demonstrate that its operational risk measure meets a sound standard comparable to that of the internal ratings-based 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 banks. The second pillar concentrates on the qualitative aspect of supervisory activities. The national supervisors are responsible for the quality assurance of the banks’ risk management systems. The national supervisors’ duties are as follows:

- 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 the banks. The 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 dialogue 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, which 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.

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.

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 bank 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 bank’s risk profile, the frequency and the amount (core information and supplemental information) of disclosure information can vary. The disclosure requirements comprise four areas:

- **Scope of application**—The name of the top corporate entity in the group should be stated to which the framework applies.
- **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, e.g., paid-up share capital/common stock, reserves and type 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 for each of which separate data have to be disclosed: credit, market, operational and interest rate change risks in the banking book. Basically, the banks 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 should be provided which affect the overall capital requirement and the allocation of economic capital.

**Summary**

- Basel II aims to promote the adoption of advanced risk management practices in financial services organizations.
- Existing systems for management and control of, e.g., credit risk, are being enhanced and operational risk is added as an element to be supported by capital requirement.
- The move to more advanced risk management systems is driven by the possible reward of a reduced capital requirement and comprehensive disclosure requirements.
- Financial services organizations are invited to come forward with their internal risk models and risk management systems and have them reviewed by the supervisors in order to gain their approval.
- The approval will depend on the presence of various factors that the supervisors will want to see properly incorporated in the internal models.
- The more sophisticated the internal models are, the higher is the possible reward of a reduced capital requirement and the higher are the supervisors’ demands on the proven quality of the models.
Appendix II—High-level Alignment of COSO ERM and Basel II

Figure 17—COSO ERM and Basel II High-level Alignment

Board of Directors
- Risk Management Philosophy
- Risk Appetite
- Board of Directors
- Integrity and Ethical Values
- Commitment to Competence
- Organisational Structure
- Assignment of Authority and Responsibility
- Human Resource Standards

Objective Setting
- Strategic Objectives
- Related Objectives
- Selected Objectives
- Risk Appetite
- Risk Tolerances

Risk Management
- Business Line
  - Risk Management
  - Event Identification
- Risk Assessment
  - Inherent and Residual Risk
  - Establishing Likelihood and Impact
  - Data Sources
  - Assessment Techniques
  - Event Interdependencies
- Risk Response
  - Evaluating Possible Responses
  - Selected Responses
  - Portfolio View
- Control Activities
  - Integration with Risk Response
  - Types of Control Activities
  - Policies and Procedures
  - Control over Information Systems
- Information & Communication
  - Information
  - Communication
- Monitoring
  - Ongoing Monitoring Activities
  - Separate Evaluations
  - Reporting Deficiencies

Internal Audit
- Board
- Risk Committee
- Audit Committee

Integrated Risk Management
- Identifying Risks
- Managing Risks
- Monitoring Risks

Board and Senior Management Oversight
A sound risk management process is the foundation for an effective assessment of the adequacy of a bank's capital position. Bank management is responsible for understanding the nature and level of risk being taken by the bank and how this risk relates to adequate capital levels. It is also responsible for ensuring that the formality and sophistication of the risk management processes are appropriate in light of the risk profile and business plan. (para 728)

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;
- A process that relates capital to the level of risk;
- A process that states capital adequacy goals with respect to risk, taking account of the bank's strategic focus and business plan; and
- A process of internal controls, reviews and audit to ensure the integrity of the overall management process. (para 731)

Comprehensive Assessment of Risks
All material risks faced by the bank should be addressed in the capital assessment process. While the Committee recognises that not all risks can be measured precisely, a process should be developed to estimate risks. Therefore, the following risk exposures, which by no means constitute a comprehensive list of all risks, should be considered. (para 732)

Monitoring and Reporting
The bank should establish an adequate system for monitoring and reporting risk exposures and assessing the effect of risk on 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 the level and trend of material risks and their effect on capital levels;
- Evaluate the sensitivity and reasonableness of key assumptions used in the capital assessment measurement system;
- Determine that the bank holds sufficient capital against the various risks and is in compliance with established capital adequacy goals; and
- Assess its future capital requirements based on the bank's reported risk profile and make necessary adjustments to the bank's strategic plan accordingly (para 743)

Internal Control Review
The bank's internal control structure is essential to the capital assessment process. Effective control of the capital assessment process includes an independent review and, where appropriate, the involvement of internal or external audits. 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 risk 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. (para 744)

<table>
<thead>
<tr>
<th>Basel II Pillar II</th>
<th>COSO ERM Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Board and Senior Management Oversight</strong>—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 for 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 to ensure 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.</td>
<td><strong>1. Internal Environment</strong>—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 enterprise risk management, 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.</td>
</tr>
<tr>
<td><strong>2. Sound Capital Assessment</strong>—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.</td>
<td><strong>2. Objective Setting</strong>—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.</td>
</tr>
<tr>
<td><strong>3. Comprehensive Management of Risks</strong>—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.</td>
<td><strong>3. Event Identification</strong>—Management identifies potential events affecting an entity’s ability to successfully implement strategy and achieve objectives. Events with a potentially negative impact represents risks, which require management’s assessment and response. Events with a</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Basel II Pillar II</th>
<th>COSO ERM Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

#### 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 are assessed on both an inherent and a residual basis.

#### 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

<table>
<thead>
<tr>
<th>Basel II Pillar II</th>
<th>COSO ERM Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5. Monitoring and Reporting</strong>—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, the sensitivity and reasonableness of key assumptions used in the capital assessment measurement system, and determine whether the bank holds sufficient capital against the various risks, in line with established capital adequacy goals.</td>
<td><strong>7. Information and Communication</strong>—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 enterprise that enterprise risk management, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream, There is also effective communication with external parties.</td>
</tr>
<tr>
<td><strong>8. Monitoring</strong>—Enterprise risk management is monitored—a process that assesses the presence and functioning of its components over time. This is accomplished through ongoing monitoring activities, separate evaluations of 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. Enterprise risk management deficiencies are reported upstream, with serious matters reported to top management and the board.</td>
<td></td>
</tr>
</tbody>
</table>
Appendix IV—Table of COBIT Processes Relevant for Basel II

<table>
<thead>
<tr>
<th>No.</th>
<th>Goal</th>
<th>Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Respond to business requirements in alignment with the business strategy.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Respond to governance requirements in line with board direction.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Ensure satisfaction of end users with service offerings and service levels.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Optimize the use of information.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Create IT agility.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Define how business functional and control requirements are translated into effective and efficient automated solutions.</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Acquire and maintain integrated standardized application systems.</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Acquire and maintain an integrated and standardized IT infrastructure.</td>
<td>S</td>
</tr>
<tr>
<td>9</td>
<td>Acquire and maintain IT skills that respond to the IT strategy.</td>
<td>S</td>
</tr>
<tr>
<td>10</td>
<td>Ensure mutual satisfaction of third-party relationships.</td>
<td>S</td>
</tr>
<tr>
<td>11</td>
<td>Ensure seamless integration of applications into business processes.</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Ensure proper use and performance of the applications and technology solutions.</td>
<td>S</td>
</tr>
<tr>
<td>14</td>
<td>Account for and protect all IT assets.</td>
<td>S</td>
</tr>
<tr>
<td>15</td>
<td>Optimize the IT infrastructure, resources and capabilities.</td>
<td>S</td>
</tr>
<tr>
<td>16</td>
<td>Reduce solution and service delivery defects and rework.</td>
<td>S</td>
</tr>
<tr>
<td>17</td>
<td>Protect the achievement of IT objectives.</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Establish clarity on the business impact of risks to IT objectives and resources.</td>
<td>S</td>
</tr>
<tr>
<td>19</td>
<td>Ensure that critical and confidential information is withheld from those who should not have access to it.</td>
<td>P</td>
</tr>
<tr>
<td>20</td>
<td>Ensure that automated business transactions and information exchanges can be trusted.</td>
<td>P</td>
</tr>
<tr>
<td>21</td>
<td>Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.</td>
<td>P</td>
</tr>
<tr>
<td>22</td>
<td>Ensure minimum business impact in the event of an IT service disruption or change.</td>
<td>P</td>
</tr>
<tr>
<td>23</td>
<td>Make sure that IT services are available as required.</td>
<td>P</td>
</tr>
<tr>
<td>24</td>
<td>Improve IT’s cost-efficiency and its contribution to business profitability.</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Deliver projects on time and on budget, meeting quality standards.</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Maintain the integrity of information and processing infrastructure.</td>
<td>S</td>
</tr>
<tr>
<td>27</td>
<td>Ensure IT compliance with laws, regulations and contracts.</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.</td>
<td></td>
</tr>
</tbody>
</table>
For selecting controls, there are three options:

- **Bottom-up approach**—Selecting control objectives and processes that might be relevant to manage the scenarios stated in the Basel II annexes.
- **Risk driven approach**—Selecting relevant risk drivers as enumerated in the COBIT Control Practices publication, classifying those risk drivers (critical, important, some impact, no relevancy) and identifying control objectives and processes related to them.
- **Top-down approach**—Identifying IT goals relevant for Basel II and using the guidance provided in the COBIT core content and the IT Governance Implementation Guide: Using COBIT and Val IT.

The top-down approach should be given preference, taking into consideration that:

- The result is driven by the business and IT goals, not by IT capabilities and priorities.
- The bottom-up approach requires thorough knowledge of COBIT content.
- In the second approach, the high number of risk drivers endangers the focus remaining on the major risks.
- The first and second approaches are mainly subjective.

**Figure 19** represents the table of IT goals, as provided in the appendix of COBIT 4.1. The rightmost column indicates whether the IT goal is of primary (P) or secondary (S) relevance for Basel II. IT goals without an entry for relevance are deemed to be less relevant for the purposes of Basel II.

As a result, the selection of processes in **figure 20** should form the basis for the implementation program.

<table>
<thead>
<tr>
<th>COBIT IT Process</th>
<th>No. of Ps</th>
<th>No. of Ss</th>
<th>Overall (Top-down)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO1 Define a strategic IT plan.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO2 Define the information architecture.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO3 Determine technological direction.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO4 Define the IT processes, organization and relationships.</td>
<td>1</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>PO5 Manage the IT investment.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO6 Communicate management aims and direction.</td>
<td>4</td>
<td>1</td>
<td>P</td>
</tr>
<tr>
<td>PO7 Manage IT human resources.</td>
<td>1</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>PO8 Manage quality.</td>
<td>2</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>PO9 Assess and manage IT risks.</td>
<td>2</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>PO10 Manage projects.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AI1 Identify automated solutions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AI2 Acquire and maintain application software.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AI3 Acquire and maintain technology infrastructure.</td>
<td>2</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>AI4 Enable operation and use.</td>
<td>3</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>AI5 Procure IT resources.</td>
<td>2</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>AI6 Manage changes.</td>
<td>1</td>
<td>3</td>
<td>P</td>
</tr>
<tr>
<td>AI7 Install and accredit solutions and changes.</td>
<td>2</td>
<td>2</td>
<td>P</td>
</tr>
<tr>
<td>DS1 Define and manage service levels.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DS2 Manage third-party services.</td>
<td>1</td>
<td>S</td>
<td></td>
</tr>
</tbody>
</table>
**Figure 20—Processes for the Implementation Program**

<table>
<thead>
<tr>
<th>COBIT IT Process</th>
<th>No. of Ps</th>
<th>No. of Ss</th>
<th>Overall (Top-down)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS3 Manage performance and capacity.</td>
<td>1</td>
<td>1</td>
<td>P</td>
</tr>
<tr>
<td>DS4 Ensure continuous service.</td>
<td>3</td>
<td></td>
<td>P</td>
</tr>
<tr>
<td>DS5 Ensure systems security.</td>
<td>3</td>
<td>2</td>
<td>P</td>
</tr>
<tr>
<td>DS6 Identify and allocate costs.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DS7 Educate and train users.</td>
<td>3</td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>DS8 Manage service desk and incidents.</td>
<td>1</td>
<td>1</td>
<td>P</td>
</tr>
<tr>
<td>DS9 Manage the configuration.</td>
<td></td>
<td>3</td>
<td>S</td>
</tr>
<tr>
<td>DS10 Manage problems.</td>
<td></td>
<td>1</td>
<td>S</td>
</tr>
<tr>
<td>DS11 Manage data.</td>
<td></td>
<td>1</td>
<td>P</td>
</tr>
<tr>
<td>DS12 Manage the physical environment.</td>
<td>3</td>
<td></td>
<td>P</td>
</tr>
<tr>
<td>DS13 Manage operations.</td>
<td></td>
<td>2</td>
<td>P</td>
</tr>
<tr>
<td>ME1 Monitor and evaluate IT performance.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ME2 Monitor and evaluate internal control.</td>
<td>1</td>
<td>1</td>
<td>P</td>
</tr>
<tr>
<td>ME3 Ensure regulatory compliance.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ME4 Provide IT governance.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 21** shows the COBIT process risks rated primary (P) or secondary (S).

**Figure 21—Process Risks**

<table>
<thead>
<tr>
<th>Process</th>
<th>Authorized Users Perform Unauthorized Access</th>
<th>Service Disruption</th>
<th>Incomplete Transaction Processing</th>
<th>Misuse of Sensitive Assets</th>
<th>Project Failure</th>
<th>Product Failure</th>
<th>Third-party Risk</th>
<th>Theft of Sensitive or Critical Assets</th>
<th>Malicious Activity</th>
<th>Process Failure</th>
<th>Overall (Bottom-Up)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO1 Define a strategic IT plan.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO2 Define the information architecture.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO3 Determine technological direction.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO4 Define the IT processes, organization and relationships.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO5 Manage the IT investment.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO6 Communicate management aims and direction.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO7 Manage IT human resources.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO8 Manage quality.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO9 Assess and manage IT risks.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Figure 21—Process Risks**

<table>
<thead>
<tr>
<th>COBIT IT Process</th>
<th>Authorized Users Perform Unauthorized Access</th>
<th>Service Disruption</th>
<th>Incomplete Transaction Processing</th>
<th>Misuse of Sensitive Assets</th>
<th>Project Failure</th>
<th>Product Failure</th>
<th>Third-party Risk</th>
<th>Theft of Sensitive or Critical Assets</th>
<th>Malicious Activity</th>
<th>Process Failure</th>
<th>Overall (Bottom-Up)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO10 Manage projects.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>P</td>
</tr>
<tr>
<td>AI1 Identify automated solutions.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>AI2 Acquire and maintain application software.</td>
<td>P P S S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>AI3 Acquire and maintain technology infrastructure.</td>
<td>S S S S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>AI4 Enable operation and use.</td>
<td>P P S S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>AI5 Acquire and maintain technology infrastructure.</td>
<td>S S S S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>AI6 Manage changes.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>AI7 Install and accredit solutions and changes.</td>
<td>P S S S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>DS1 Define and manage service levels.</td>
<td></td>
<td>S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>DS2 Manage third-party services.</td>
<td></td>
<td>S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>DS3 Manage performance and capacity.</td>
<td></td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>DS4 Ensure continuous service.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>DS5 Ensure systems security.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>DS6 Identify and allocate costs.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>DS7 Educate and train users.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>DS8 Manage service desk and incidents.</td>
<td></td>
<td>S P S S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>DS9 Manage the configuration.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>DS10 Manage problems.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>DS11 Manage data.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>DS12 Manage the physical environment.</td>
<td></td>
<td>S P P S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>DS13 Manage operations.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>ME1 Monitor and evaluate IT performance.</td>
<td></td>
<td>S S S S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>ME2 Monitor and evaluate internal control.</td>
<td></td>
<td>P S S S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>P</td>
</tr>
<tr>
<td>ME3 Ensure compliance with external requirements.</td>
<td></td>
<td>S P P P P</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
<tr>
<td>ME4 Provide IT governance.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S</td>
</tr>
</tbody>
</table>

**Figure 22** shows the application process risks.
Figure 22—AC Risks

<table>
<thead>
<tr>
<th>COBIT IT Process</th>
<th>Service Disruption</th>
<th>Incomplete Transaction Processing</th>
<th>Misuse of Sensitive Assets</th>
<th>Project Failure</th>
<th>Product Failure</th>
<th>Third-party Risk</th>
<th>Theft of Sensitive or Critical Assets</th>
<th>Malicious Activity</th>
<th>Process Failure</th>
<th>Overall (Bottom-Up)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC1 Source data preparation and authorization</td>
<td>S</td>
<td></td>
<td></td>
<td>P</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Not applicable, as Application controls are to be implemented into services.</td>
</tr>
<tr>
<td>AC2 Source data collection and entry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC3 Accuracy, Completeness and Authenticity Checks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC4 Processing Integrity and Validity</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td></td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC5 Output Review, Reconciliation and Error Handling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC6 Transaction Authentication and Integrity</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>S</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 23 illustrates the overall process risks.

Figure 23—Overall Process Risks

<table>
<thead>
<tr>
<th>COBIT IT Process</th>
<th>Overall (Top-down)</th>
<th>Overall (Bottom-Up)</th>
<th>Overall (Risk-based)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO1 Define a strategic IT plan.</td>
<td></td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>PO2 Define the information architecture.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO3 Determine technological direction.</td>
<td></td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>PO4 Define the IT processes, organization and relationships.</td>
<td></td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>PO5 Manage the IT investment.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PO6 Communicate management aims and direction.</td>
<td></td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>PO7 Manage IT human resources.</td>
<td></td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>PO8 Manage quality.</td>
<td></td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>PO9 Assess and manage IT risks.</td>
<td></td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>PO10 Manage projects.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AI1 Identify automated solutions.</td>
<td></td>
<td>S</td>
<td>P</td>
</tr>
<tr>
<td>AI2 Acquire and maintain application software.</td>
<td></td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>AI3 Acquire and maintain technology infrastructure.</td>
<td></td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>AI4 Enable operation and use.</td>
<td></td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>AI5 Procure IT resources.</td>
<td></td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>AI6 Manage changes.</td>
<td></td>
<td>P</td>
<td>S</td>
</tr>
<tr>
<td>AI7 Install and accredit solutions and changes.</td>
<td></td>
<td>P</td>
<td>P</td>
</tr>
</tbody>
</table>
As a result it is recommended to:

- Identify control objectives relevant within the processes rated as primary or secondary.
- Ensure a maturity level of at least 3 (defined process) for the processes with a secondary impact and a maturity level of 4 (managed and measured) for the processes with a primary impact.
- Implement controls and control activities for the processes.
- Identify measures, to ensure ongoing and consistent measurement of risks, process outcome and process capabilities.

In addition to the assessment of IT general controls, application control objectives were identified to be of critical impact. Therefore, the IT processes AI2 (responsible for implementation of automated controls) and ME2 (responsible for assessment of controls) should also have a maturity level of 4.
### Appendix V—Basel II Risk Event Types with the Related IT Aspects and Associated COBIT Processes

#### Figure 24—Basel II Risk Event Types and Related ITR Aspects and COBIT Processes

<table>
<thead>
<tr>
<th>Basel II Type</th>
<th>IT Aspects</th>
<th>COBIT Processes</th>
</tr>
</thead>
</table>
| 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 |
| External fraud| • Deliberate changing of system and application data through hacking       | • DS5           |
| Clients, products and business practices | • Disclosure of sensitive information to outsiders by employees  
                                             • Management of third-party suppliers | • PO6  
                                                                           • DS6 |
| 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  
                                           • 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 | • 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 | • AI5  
                                                                           • AI6  
                                                                           • DS5  
                                                                           • DS10 |
Appendix VI—Implementation Road Map Using COBIT

The road map for using COBIT to implement control and governance for Basel II is a generic approach for implementing IT governance. It ensures that the focus is on business needs when improving control and governance of IT processes. The road map is applicable regardless of the size of the initiative, encourages management commitment and involvement and should follow good project management practices. The road map is a continuous improvement approach that is followed iteratively, building a sustainable ‘business as usual’ approach over time. An enterprise implementing IT governance will need to do so in phases based on business priorities and IT risks. The road map achieves this by prioritizing the IT goals and processes (including controls) based on the consideration of business goals and risks.

Given these critical IT goals, the enterprise should identify what must be managed and controlled to ensure successful outcomes. Therefore, management needs to know its current capability and where deficiencies may exist. The road map uses maturity modelling to perform an as-is and to-be capability assessment relative to the controls selected, followed by a gap analysis. The gap analysis is likely to require considerable experience in IT management techniques to develop practical solutions.

Over time, the road map will be followed iteratively while building a sustainable approach to IT governance.
Figure 25—COBIT Implementation Guide Elements

- **Board and Executive**
  - How to define appropriate IT governance practices to define business directions for IT and ensure that value is delivered and risks are managed, using the different COBIT and Val IT components.

- **Business Management**
  - How to define any business requirements for IT governance and ensure that value is delivered and risks are managed, using the different COBIT and Val IT components.

- **IT Management**
  - How to deliver the IT services as required by the business and directed by the board, using the different COBIT and Val IT components.

- **IT Audit**
  - How to use the different COBIT and Val IT components in audit activities to ensure that IT delivers what it needs to deliver.

- **Risk and Compliance**
  - How to use the different COBIT and Val IT components in compliance and risk advisory activities to ensure that IT complies with policies, laws and regulations, and that new risks are identified.

---

<table>
<thead>
<tr>
<th>Identify Needs</th>
<th>Define scope</th>
<th>Define risks</th>
<th>Define requirements and risks matrix</th>
<th>Plan programme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Envision Solution</td>
<td>Define target for improvement</td>
<td>Define significant and identify improvement</td>
<td>Modify/align and identify improvement</td>
<td></td>
</tr>
<tr>
<td>Plan Solution</td>
<td>Define products</td>
<td>Select implementation plan</td>
<td>Implement the improvement</td>
<td>Monitor/management performance</td>
</tr>
<tr>
<td>Implement Solution</td>
<td>Implement the improvements</td>
<td>Monitor performance of the trials</td>
<td>Review programme effectiveness</td>
<td></td>
</tr>
<tr>
<td>Operate/Use Solution</td>
<td>Sustainability</td>
<td>Identify new governance requirements</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix VII—References

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

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


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

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


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