An Aggregated Information Technology Checklist for Operational Risk Management

Mehmet Zeki Önal*

Abstract

This study addresses the issue of the Information Technology (IT) Governance frameworks and standards that respond to different levels of operational risks, especially those caused by the information systems and technology infrastructure. A requirement analysis regarding Basel II is conducted, a gap analysis between the Information Control Models (ICMs) is performed, and the aggregated IT checklist for Operational Risk Management (ORM) is proposed by mapping the control objectives in ICMs to the operational risk categories described in Basel II as loss event types. The validity and reliability of the study is based on the focus group assessment of the mappings.

Keywords: *Basel II, Operational Risk Management, Information Control Model, Information Technology Governance.*
JEL Classification: *G32, M15, M42*

Özet - Operasyonel Risk Yönetimi İçin Bütünleştirilmiş Bilgi Teknolojileri Kontrol Listesi

Bu çalışma, Bilgi Teknolojileri (BT) Yönetişim çerçevesi ve standartlarının, özellikle bilgi sistemleri ve teknolojileri altyapısından kaynaklanan farklı seviyelerdeki operasyonel risklere cevap vermeleri sorununu vurgulamaktadır. Basel II bağlamında bir gereksinim analizi yapılmış, Bilgi Kontrol Modelleri (BKM) arasında bir farklılık analizi gerçekleştirilmiş ve Basel II'de zarar olay tipleri olarak açıklanan operasyonel risk kategorilerinin BKM'lerdeki kontrol hedeflerine eşleştirilmesi ile Operasyonel Risk Yönetimi (ORY) için bütünleştirilmiş BT kontrol listesi önerilmiştir. Çalışmanın geçerliliği ve güvenilirliği, eşleştirmeler üzerinde yapılmış olan grup değerlendirmesine dayandırılmıştır.

Anahtar Kelimeler: *Basel II, Operasyonel Risk Yönetimi, Bilgi Kontrol Modeli, Bilgi Teknolojileri Yönetişimi.*
JEL Sınıflaması: *G32, M15, M42*

* *CISA; Senior Associate, PricewaterhouseCoopers Turkey*
The views expressed in this paper are solely of the author, and do not necessarily reflect the views of PricewaterhouseCoopers Turkey.

1. Introduction

The business environment is becoming more technologically powered and complex at each heartbeat. New risks and threats are being faced, the needs must be managed, and new opportunities are waiting to be tapped. Operational risk is one of the most significant risks that businesses face in today's complex global economy (Samad-Khan, 2005). For most of the world's leading institutions, it has become more than apparent that implementing an effective Operational Risk Management (ORM) program can help reduce losses, lower costs associated with fixing problems and increase customer and employee satisfaction, thereby improving financial performance and enhancing shareholder value.

All these changes require and produce new regulations for framing and controlling the environment, such as the Basel II capital allocation framework, which requires many actions at different levels in an organization. Basel II has forced banks to review their approach to managing operational risk since it has been effective from January 1st, 2007 in European countries. In addition, the Banking Regulation and Supervision Agency (BRSA) in Turkey announced that the Basel II regulations for the Turkish banking sector will be effective from January 1st, 2009.

However, the methodologies, frameworks, or standards to be referred to as baseline during the ORM regarding the effectiveness of the internal systems have not been discussed in Basel II. Basel II and other regulations such as Sarbanes-Oxley, Law for Security Exchange Commission (SEC) in the USA, and European Directives do not prescribe actual technologies to use for compliance although they give guidance on the implementation of an effective ORM in order to allow local regulators adopting their methodologies. In accordance with this approach, Kane (2001) argues that international regulatory standards are inferior to competition among national regulatory systems, especially in strengthening the banking systems in developing countries. Goldstein (2001) is much more positive about the potential for value-increasing international regulatory standards, especially if flexibility is built into the standards and if the international standards do not reach down into all aspects of the financial system. Therefore, most organizations adopt internal control frameworks as models of best practice for compliance where the most common element of all regulations is a strong set of internal controls (Davidson, 2006).

Responding the need of ORM related to operational risks caused by Information Technology (IT) processes, the Information Technology Governance Institute (ITGI) published the document entitled "Information Technology Control Objectives for Basel II" in October 2007 (ITGI, 2007b) which refers to the Control Objectives for In-

formation and related Technology (CobiT) framework at the sub-domain level. Therefore, the aim of this paper is to assess whether IT Governance frameworks and standards (Information Control Models) are appropriate at the control objective level for controlling the operational risks, and to integrate and harmonize them in order to project an aggregated IT checklist for ORM. In the article, the control objectives in Information Control Models (ICMs) have been evaluated and mapped to the operational risk categories in Basel II which are defined as loss event types, rather than bridging the Basel II principles and CobiT principles, so that the ICMs can be compared against the Basel II requirements' fulfillment.

For such an assessment, following ICMs have been analyzed regarding the Basel II requirements related to ORM:

- CobiT 4th edition (ITGI, 2005),
- Information Technology Infrastructure Library (ITIL) version 2 (OGC, 2004),
- ISO27002:2005 - ISO17799:2005 (BS7799) (BSI, 1999),
- ISO27001:2005 (ISO27001) (ISO, 2005),
- Committee of Sponsoring Organizations (COSO) Enterprise Risk Management (ERM) Integrated Framework (COSO, 2004).

In order to be able to propose a sophisticated IT checklist, the following sections discuss the various definitions of risk, control, operational risk, risk management and measurement, and ORM, in the lights of Basel II ORM requirements and other US and European regulations. Then, Basel II operational risk categories and control objectives in the ICMs are mapped, and the mappings are evaluated by a focus group. Lastly, the aggregated IT checklist for ORM is proposed, which is a best practices approach based on CobiT and structured on COSO. However, the organizations should consider that the aggregated IT checklist for ORM is a framework which supports the whole ORM activities in the organization by excelling the IT related processes and controls in the core IT systems and technologies including the ones used for ORM itself, for example while collecting loss data and calculating the ratios required by Basel II. Thus, the checklist should be considered as a viable part of the ORM and hence corporate governance by sustaining the IT structure.

2. Literature Review

2.1. Operational Risk Management

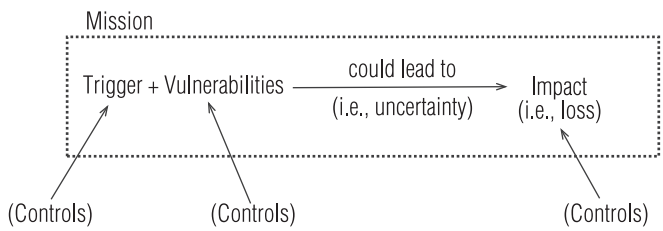
The term risk is used universally, but different audiences often attach slightly different meanings to it (Kloman, 1990). Although there are many variations in how risk is defined,

the following definition succinctly captures its essence: risk is the possibility of suffering loss (Dorofee, 1996). This definition includes two key aspects of risk: (1) some loss must be possible and (2) there must be uncertainty associated with that loss. Thus, risk is subdivided into two types: speculative risks and hazard risks (Young, 2001). With speculative risk, you can realize a gain, improving your current situation relative to the status quo. At the same time, you have the potential to experience a loss. In contrast, hazard risk only has potential losses associated with it and provides no opportunity to improve the current situation.

All forms of risk comprise common elements (Alberts, 2006). These four basic components of risk are: (1) context, (2) action, (3) conditions, and (4) consequence. Context is the background, situation, or environment in which risk is being viewed and defines which actions and conditions are relevant to that situation. The action is the act or occurrence that triggers risk. Whereas the action is the active component of risk, conditions constitute risk's passive element. They are defined as the current state or the set of circumstances that can lead to risk. Conditions, when combined with a specific triggering action, can produce a set of consequences, or outcomes. Consequences, the final element of risk, are the potential results or effects of an action in combination with a specific condition(s).

Figure 1 illustrates how the four elements of risk are translated to operational risk and shows the relationships between controls, triggers and vulnerabilities, and impacts (Alberts, 2006). Controls are the circumstances that propel a process toward fulfilling its mission. They include the policies, procedures, practices, conditions, and organizational structures designed to provide reasonable assurance that a mission will be achieved and that undesired events will be prevented, detected, and corrected (ITGI, 2005). Controls can help reduce risk by eliminating a triggering event, monitoring for the occurrence of a trigger and implementing contingency plans when appropriate, reducing vulnerability, and reducing potential impacts.

Figure 1: Controls and Operational Risk



King (2001) defines operational risk as the risk not related to the way a firm finances its business, but rather to the way a firm operates its business. He offers an alternative definition: operational risk is a measure of the link between a firm's business activities and the

variation in its business results. When the Bankers Trust began its study of operational risks in the early 90's, their definition of operational risks (Hoffman, 2002) was more or less "everything which is not market or credit risk". They decided to define some risk classes such as people, relationship, technology and processing, physical, and other external risks. In addition, Saunders (2000) advocates that the internal sources of the operational risk are employees, technology, customer relationships and capital assets destruction, as the external sources are mainly fraud and natural disasters.

Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events, resulted from an industry study performed by the British Bankers' Association (BBA), the International Swaps and Derivatives Association (ISDA), Risk Management Association (RMA), and PricewaterhouseCoopers (PwC) in 1999 (BBA, ISDA, RMA & PwC, 1999), as affirmed in Basel II (Basel Committee, 2004) and referred by Netter & Poulsen (2005). Beyond the rules and the modeling requirements for measuring the regulatory capital required to cover operational risk properly, the Basel Committee acknowledges a particular attention to the management of this risk by illustrating this concern in the document entitled "Sound Practices for the Management and Supervision of Operational Risk" published by the Bank for International Settlement (BIS) in 2002 referring Basel I (Chapelle, 2005b).

In addition, BRSA (2001) describes the operational risk as the risk of loss arising from errors and omissions caused by breakdowns in the internal controls of the bank, the failure of the bank management and personnel to perform in a timely manner, or mistakes made by the bank management, or breakdowns and failures in the IT system, and events such as major earthquake, major fire or flood. As seen in the definition, the operational risk is detailed by BRSA considering the possible effects of IT processes and controls on the business operations and the trigger effect of the operational risk on other risks such as business risks. BRSA (2006a) lists examples such as that AT&T has experienced a main switch problem in 1998 where many credit cards were out of function for over 18 hours and Imar Bank has built a fraudulent double booking system in 2003, for the operational failures and frauds based on IT. BRSA (2006b) has also published the Regulation on Information Systems Assurance in the Banks for assurance of the information systems. The regulation refers (BRSA, 2006b) to CobiT framework while assuring the IT infrastructure of the banks, and requires that the periodic IT audits including the IT based applications controls within the banking business processes are performed beginning from 2007.

Moreover, the attention has shifted towards the risk management of operational risk because of that events due to operational risk can have a devastating impact on the ope-

rations of banks. Famous cases are Barings' insolvency, the Allied Irish Banks' loss of 750 million dollars due to rogue trading, and the 2 billion dollars settlement of class action lawsuit against Prudential Insurance due to fraudulent sales practices over 13 year (Mürmann & Öktem, 2002). Thus, operational risk has become an important part of financial institution risk management efforts partly because it was highlighted by the Basel Committee and Section 404 of Sarbanes-Oxley, and because of the disruptions associated with the September 11 attacks. Though some still doubt whether it is material or even can be measured, financial institutions increasingly allocate capital to operational risk. For instance, a survey by Oliver Wyman and Company of ten large international banks found that they allocate 53% of their economic capital to credit risk, 21% to market risk and asset-liability rate risks, and 26% to operational and other risks (Carey & Stulz, 2005).

2.2. Basel II and Operational Risk Categories

The fundamental objective of the Basel Committee while revising the 1988 Basel Accord and publishing the Basel II, has been defined as to develop a framework that would further strengthen the soundness and stability of the international banking system while maintaining sufficient consistency that capital adequacy regulation will not be a significant source of competitive inequality among internationally active banks (Basel Committee, 2004). Since the purpose of Basel II was to enhance the way banks cover and manage their risks, the first pillar presents the calculation of the total minimum capital requirements for credit, market, and operational risk (Basel Committee, 2004).

For the purposes of internal ORM, the banks must identify all material operational risk losses consistent with the scope of the definition of operational risk and the loss event including those related to credit risk (Basel Committee, 2004). In addition, the Basel Committee (2004) notes that internal loss data is most relevant when it is clearly linked to a bank's current business activities, technological processes and risk management procedures, and defines seven loss event types. Table 1 (RMG, 2002) represents QIS2 results which detail the operational risk loss information that the 30 contributing banks were able to supply according to the loss event types (Basel Committee, 2004).

Table 1: Frequency Severity Matrix for Basel II Loss Event Types (in percentages)

Loss Event Type	Event Number	Loss Amount
Internal Fraud	2.72	10.66
External Fraud	36.39	20.32
Employment Practices and Workplace Safety	2.71	2.92
Clients, Products & Business Practices	6.39	27.51
Damage to Physical Assets	4.48	3.02
Business Disruption and System Failures	5.32	0.82
Execution, Delivery & Process Management	41.99	34.75

Considering that the technology is seen as one of the internal sources of operational risk by Saunders (2000), that BRSA's (2001) operational risk definition includes the breakdowns and failures in the IT system or any other events which may cause these disruptions, that Hoffman's (2002) definition of operational risks is more or less everything that is not market or credit risk, and the factors that lead the operational risks mentioned above, IT processes and controls are the basic triggers and vulnerabilities which produce the operational risks. These threats are the circumstances that create the potential for harm or loss. Since the operational risk looks into the future, focusing on problems and failures that have not yet occurred, while a problem describes a situation that is presently taking place (Alberts & Dorofee, 2005), the loss event types defined in Basel II are named as operational risk categories because of their natures.

2.3. Information Control Models

These regulations, definitions and attitudes published by Bank for International Settlement (BIS), Banking Regulation and Supervision Agency (BRSA), and other stakeholders lead us to answer whether current ICMs are applicable for controlling the operational risks defined in Basel II. The organizations are increasingly exposed to various operational risks related to the use of IT since IT is now intrinsic to and pervasive within enterprises (ISACA, 2006), e.g. virus attacks, unauthorized access to data, breakdown of infrastructure, system and infrastructure contingency, performance problems. In order to prevent such risks efficiently, the banks are forced to identify, analyze and valuate potential IT related operational risks. They should implement appropriate IT Governance (Jochum, 2006) in order to provide a controlled IT framework to the business processes since IT Governance enables an organization to attain three vital objectives: regulatory and legal compliance, operational excellence, and risk optimization.

The organizations can ease their venture into IT Governance that ensures that the enterprise's IT sustains and extends the organization's strategies and objectives (ITGI, 2005), by leveraging various industry standard frameworks. Champbell (2003) categorizes over fifty ICMs under following subcategories: control objectives communities, principles communities, capability maturity communities, checklists, risk management frameworks, and taxonomies. Most frameworks provide requisite support materials in the form of roadmaps, guides, templates, libraries, and samples. While these are not turn-key methodologies that will embed IT Governance into the organization, the frameworks provide a foundation for creating a governance structure. Therefore, the organizations are arguing to harmonize and integrate the leading frameworks to achieve greater compatibility. The ICMs covered in this study, the-

ir sponsoring organizations, and the numbers of control objectives in each ICM are listed in Table 2.

Table 2: Information Control Models

	Information Control Model	Sponsoring Organizations	Control Objective
1	CobiT	Information Systems Audit and Control Association (ISACA) Information Technology Governance Institute (ITGI)	215
2	BS7799	British Standards Institute (BSI) International Electrotechnical Commission (IEC)	127
3	ISO27001	International Electrotechnical Commission (IEC) International Organization for Standardization (ISO)	133
4	ITIL	United Kingdom's Office of Governance Commerce (OGC)	140
5	COSO	Committee of Sponsoring Organizations of the Treadway Commission (COSO)	39

3. Methodology

3.1. Basel II Requirement Analysis

The improvement of banks' ORM frameworks concerns new requirements addressed in Basel II (Di Renzo & Bernard, 2005). The main sources for the requirement analysis are the publications of the Basel Committee: Basel II (Basel Committee, 2004), and a document entitled "Sound Practices for the Management and Supervision of Operational Risk" (Basel Committee, 2003a). Other important sources were the workshops organized and the documents published by the Basel Committee (2001a, 2001b, 2001c, 2001d, 2002a, 2002b, 2002c, 2003a, 2003b, 2004) where supervisors described their expectations from banks' ORM framework and the assessments' organizational constraints. Then, the descriptions of ICMs and ORM methods and good practices, including loss data analyses, were used. Finally, the articles and case studies structured on the operational failures of the companies were read and interpreted.

Three approaches are proposed in Basel II for the calculation of minimum capital requirements for operational risk: The basic indicator approach (BIA), the standardized approach (SA), and the advanced measurement approach (AMA). So, the requirements were structured along those three approaches. For instance, the requirement that as part of the bank's internal risk assessment system, the bank must systematically track relevant operational risk data including material losses by business lines (Basel Committee, 2004) is essential to the SA. Moreover, these approaches are ranked in increasing order of sophistication. The more advanced approach encompasses the requirements of the less sophisticated approaches. This structure has been adopted for the definition of the categories of requirements. For instance, if a bank adopts an AMA, it will have to meet the following requirement: Any internal risk measurement system must be consistent with the loss event types (Ba-

sel Committee, 2004) in addition to the requirement given above for the SA. This implies a commitment to continuous improvement of ORM, and associated ORM processes, across the organization.

The structure of risk management activities can also be gathered from the requirements. For instance, the requirement that the ORM function must be responsible for developing strategies to identify, assess, monitor, and control/mitigate operational risk (Basel Committee, 2004), indicates activities composing the management of risks. Some requirements refer to a clear assignment of responsibilities and authorities, such as the requirement that the bank must have techniques for creating incentives to improve the management of operational risk throughout the firm (Basel Committee, 2004). This example shows that financial and managerial incentives must be used in order to ensure that each bank employee contributes to the improvement of the operational risk management framework.

Since Basel II requires a supervisory review process including the assessment of the control environment, it is also required that supervisors should consider the quality of the bank's management information reporting and systems, the manner in which business risks and activities are aggregated, and the management's record in responding to emerging or changing risks (Basel Committee, 2004). In addition, Basel II requires that banks should have clear and effective policies, procedures, and information systems to monitor compliance (Basel Committee, 2004), that supervisors should develop detailed review procedures to ensure that banks' systems and controls are adequate to serve (Basel Committee, 2004), and that management must also ensure, on an ongoing basis, that the rating system is operating properly (Basel Committee, 2004). These requirements show that the banks should have a sound ORM structure, and IT related operational risks should be covered in a comprehensive way.

In addition to Basel II itself, ITGI published the document entitled "Information Technology Control Objectives for Basel II" in October 2007 (ITGI, 2007b). ITGI (2007b) is taking the proactive step of addressing risk in financial service organizations considering that information risk and information technology have become decisive factors in shaping modern business, and many financial service organizations have undergone a fundamental transformation in terms of IT infrastructures, applications, and IT related internal controls. Since IT related components such as applications, infrastructure elements and controls are all defined as parts of operational risk, ITGI (2007b) maps Basel II principles for operational risk against information technology risk.

Therefore, ITGI (2007b) defines a set of ten guiding principles for information risk management, where these guiding principles correspond to the principles of ORM as set down in Basel II, and where these risks are related to IT scenarios and controls. These guiding principles are structured by ITGI (2007b) considering Basel II principles and their IT relevance and requirements. Thus, the requirements in Basel II and their impacts on IT are evaluated and a corporate governance, risk management, and regulatory compliance (GRC) framework is established. The core Basel II principles are listed as follows:

1. Board of directors should be aware of the need for an operational risk management framework.
2. Operational risk management framework is subject to effective and comprehensive internal audit.
3. Develop policies, processes and procedures for managing operational risk.
4. Identify and assess the operational risk.
5. Regularly monitor operational risk profiles and material exposures to losses.
6. Have policies, processes and procedures to control and/or mitigate material operational risks.
7. Have contingency and business continuity plans.
8. Have framework in place to identify, assess, monitor and control/ mitigate material operational risks.
9. Conduct regular independent evaluation of a bank's policies, procedures and practices related to operational risks.
10. Sufficient public disclosure.

ITGI (2007b) refers to the CobiT framework at sub-domain level by bridging the Basel II principles and CobiT principles, rather than to the control objective level. In addition, ITGI (2007b) builds an ORM framework, which sets the principles and guides the stakeholders rather than proposing a new ICM for ORM. Instead ITGI (2007b) brings the concepts of risk management, corporate and IT Governance, ICMs, and related regulations, and highlights the importance of GRC. Considering the requirements defined in Basel II in order to have a sound ORM structure, and the control objectives published by ITGI (2007b) in order to have a sound GRC, the organizations should have a comprehensive IT structure which covers all IT systems and technologies and their components which could cause operational risks and hence have impact on financial statements, including also the IT systems for ORM itself. Therefore, an aggregated IT checklist for ORM is proposed in the following

sections, as the methodology used while establishing and designing the checklist is detailed.

3.2. Mapping Information Control Models to Operational Risks

In order to assess the ICMs regarding their ability to cover the operational risks caused by the IT related processes, each and every control objective in ICMs, which are covered in this study, have been mapped to the seven loss event types defined in Basel II (Basel Committee, 2004), which are also operational risk categories (Basel Committee, 2004). In the same way, each and every control objective in ICMs have been mapped to the three control types defined by ITGI (2005): preventive, detective, and corrective. In order to be able to scale the contribution level of each ICM and the penetration level of each control objective smoothly, one-to-one mapping has been performed. However, one-to-one mapping caused an underestimation of the secondary mapping alternatives since control objectives may have an impact on other operational risk categories and additionally on different control types.

While mapping the control objectives, their nature is considered. For example, a control objective may be attained by applying preventive, detective or corrective control at different levels and steps of a process. However, the goal of the control objective is used as the motivation on which the mapping is based, e.g. if the control objective is about monitoring a process, it is mapped to a detective control. In the same way, a control objective may cover the internal fraud or external fraud risk. However, the prior objective of the control objective is used as the motivation on which the mapping is based, e.g. if the control objective is about access rights, it is mapped to internal fraud, rather than considering the access rights of the third parties, since there are different objectives related to relationships with third parties.

Therefore, the loss event type activities exampled in Basel II have been extended in order to cover the context, domains, controls and IT based activities in ICMs so that a guideline for mapping is prepared. Thus, possible operational risks caused by the IT related processes and controls have been exampled. For loss event types, the following activities have been added:

- Internal Fraud: Roles and responsibilities, segregation of duties, data ownership, user account and identity management, promotion to production, logging mechanism.
- External Fraud: Contracted staff security, external network security, external network connections, and exchange of data.
- Employment Practices and Workplace Safety: Organizational structure, staffing, competencies, staff evaluation, training.

- Clients, Products & Business Practices: Policies, procedures and standards, control environment, IT strategy and business practices alignment, IT risk management, IT supervisory and advisory boards, IT budgeting, enterprise IT models (business / technical requirements), portfolio management, value management and delivery, resource management, database management, data classification, data confidentiality.
- Damage to Physical Assets: Site selection and layout, external facilities, offsite storage, media library management, access to physical assets and sensitive documents, disposal.
- Business Disruption and System Failures: Disaster Recovery Plan, Business Continuity Plan, configuration, infrastructure, incident, problem and change management, service desk, development activities, release and distribution, update and upgrade, testing, back-up and recovery.
- Execution, Delivery & Process Management: Service Level Agreements, performance monitoring, key personnel, scheduling, reporting, data integrity, data processing.

3.3. Focus Group Assessment

While mapping the control objectives of CobiT to the operational risk categories in Basel II, a workshop has been organized in order to ensure the reliability of the study. External IT auditors from consultancy services, internal auditors from the business world, and professionals from academic institutions participated in the workshop and served as judges by assessing the proposed mappings between the control objectives in CobiT, operational risk categories and control types. The focus group assessed the CobiT and Basel II mapping which had been proposed before the workshop. Thus, the focus group increased the validity and reliability of the study since the mappings are based on subjective appraisals.

In order to be able to assess the mappings, the focus group was informed about the operational risk categories, the loss event type examples based on IT, and the control types with an invitation letter before the workshop and with a presentation during the workshop. Thus, the focus group had a common understanding of the concepts covered in the aggregated IT checklist.

During the workshop, the focus group discussed each control objective in CobiT and accepted the mapping or rejected it and proposed a new mapping. The control objectives were ordered according to the operational risk categories proposed, and discussed in this order. Therefore, the participants had a wider view of the context

of each operational risk category and a chance to comprehend and compare the control objectives in a specific operational risk category. Additionally, the participants were requested to write down their choice of mappings on the set of documents as evidence.

Table 3 summarizes the differences between the proposed mappings and the focus group assessment results in each operational risk category and control type where applicable.

Table 3: Differences between Proposed Mappings and Workshop Results

Mapping Category		Focus Group Assessment Results	Number of Proposed Mapping
Internal Fraud	Detective	1	3
	Preventive	11	10
External Fraud	Detective	1	1
	Preventive	4	3
Employment Practices and Workplace Safety	Corrective	2	1
	Detective	3	5
	Preventive	12	14
Clients, Products & Business Practices	Corrective	3	6
	Detective	7	6
	Preventive	55	46
Damage to Physical Assets	Detective	0	1
	Preventive	11	10
Business Disruption and System Failures	Corrective	3	8
	Detective	5	6
	Preventive	24	24
Execution, Delivery & Process Management	Corrective	9	15
	Detective	28	31
	Preventive	36	25
Grand Total		215	215

Table 4 presents the consensus within the focus group while mapping the control objectives in CobiT with the decision of the majority or unanimous agreement. The results show us that the focus group generally reached a consensus, especially for the security related issues such as internal fraud, external fraud and damage to physical assets. Since there was a discussion on the IT activities regarding business continuity, whether it should be categorized under business disruption and system failures or execution, delivery & process management, the consensus on these areas are lower than the others. There are seventeen control objectives where the focus group made a majority decision and 198 control objectives where the focus group was unanimous in its decision while mapping the control objectives in CobiT.

Table 4: Workshop Consensus Results

Operational Risk Category	Workshop Results	Number of Control Objective
Internal Fraud	Decision with majority	1
	Decision with unanimity	11
External Fraud	Decision with majority	1
	Decision with unanimity	4
Employment Practices and Workplace Safety	Decision with majority	2
	Decision with unanimity	15
Clients, Products & Business Practices	Decision with majority	2
	Decision with unanimity	63
Damage to Physical Assets	Decision with unanimity	11
Business Disruption and System Failures	Decision with majority	4
	Decision with unanimity	28
Execution, Delivery & Process Management	Decision with majority	7
	Decision with unanimity	66
Grand Total		215

3.4. Gap Analysis

Using the mapping results for CobiT's control objectives, performed during the workshop and mappings between CobiT and other ICMs (ITGI, 2006a and ITGI, 2007a), control objectives in BS7799, ISO27001, ITIL and COSO have been mapped to the operational risk categories and control types. As a result, a gap analysis between ICMs is done by calculating the contribution and penetration levels of each ICM in each operational risk category and control type.

The contribution level is the percentage of the control objectives in an ICM dedicated to a specific operational risk category in Basel II, considering all control objectives in that ICM. The contribution level indicates how many control objectives in an ICM are covering which operational risk category in Basel II. The penetration level is the percentage of the control objectives in an ICM, dedicated to a specific operational risk category in Basel II and to a specific control type, considering all control objectives in that ICM. The penetration level indicates how many control objectives in an ICM are covering which operational risk category in Basel II and in which nature. It is possible to understand which ICM focuses on which operational risk category by interpreting the contribution level. It is possible to understand which ICM focuses on which operational risk category and in which nature of control by interpreting the penetration level.

After mapping the control objectives in ICMs to the operational risk categories and control types, the contribution level of each ICM for each operational risk category has been calculated using the following formula (1):

$$CL_{ICM} = CO_R / COT_{ICM} * 100 \text{ as} \qquad (1)$$

CL_{ICM}: Contribution Level of ICM for the Operational Risk Category

CO_R: Number of Control Objectives in ICM mapped to the Operational Risk Category

COT_{ICM}: Total Number of Control Objectives in ICM.

In the same way, the penetration level of each ICM for each operational risk category and each control type has been calculated using the following formula (2):

$$PL_{ICM} = CO_{RT} / COT_{ICM} * 100 \text{ as} \quad (2)$$

PL_{ICM}: Penetration Level of ICM for the Operational Risk Category and Control Type

CO_{RT}: Number of Control Objectives in ICM mapped to the Operational Risk Category and Control Type

COT_{ICM}: Total Number of Control Objectives in ICM.

4. Findings

4.1. Contribution and Penetration Levels of Information Control Models

The contribution and penetration levels of each ICM are presented in Table 5. These levels show us the characteristics of the control objectives in ICMs considering the operational risk categories and control types. The table points out that the ICMs have mostly preventive control objectives rather than detective and corrective control objectives, e.g. there are no corrective controls for external fraud or damage to physical assets risk categories. These results, the existence of preventive control objectives rather than detective and corrective, are in accordance with the natures of the ICMs since they are based on the control objectives in order to cover the related risks and build a control environment.

The Table 5 shows us that CobiT is the best practice regarding the Employment Practices and Workplace Safety, Clients, Products & Business Practices, and Execution, Delivery & Process Management operational risk categories if we consider that COSO is a risk management framework rather than an IT Governance standard. ISO27001 is the best practice regarding the Internal Fraud and Damage to Physical Assets operational risk categories. BS7799 is the best practice regarding External Fraud, and ITIL is the best practice regarding the Business Disruption and System Failures operational risk category. As a result, the results are in line with the nature of ICM since BS7799 and ISO27001 focus on security and ITIL focuses on change management, availability management, and problem management. In generally, Employment Practices and Workplace Safety operational risk category is not covered with a high contribution level as other operational risk categories. Other categories are covered in different levels by different ICMs.

Table 5: Contribution and Penetration Levels of Information Control Models (in percentage)

Operational Risks	Impact	Control Type	CobiT	BS7799	ISO27001	ITIL	COSO
Internal Fraud	CL	Total	5.58	25.20	26.32	2.14	2.56
	PL	Preventive	5.12	22.05	23.31	2.14	2.56
		Detective	0.47	2.36	2.26	0.00	0.00
		Corrective	0.00	0.79	0.75	0.00	0.00
External Fraud	CL	Total	2.33	18.11	16.54	0.00	0.00
	PL	Preventive	1.86	15.75	13.53	0.00	0.00
		Detective	0.47	2.36	3.01	0.00	0.00
		Corrective	0.00	0.00	0.00	0.00	0.00
Employment Practices and Workplace Safety	CL	Total	7.91	3.15	3.01	2.14	10.26
	PL	Preventive	5.58	2.36	2.26	2.14	10.26
		Detective	1.40	0.00	0.00	0.00	0.00
		Corrective	0.93	0.79	0.75	0.00	0.00
Clients, Products & Business Practices	CL	Total	30.23	13.39	12.78	26.43	56.41
	PL	Preventive	25.58	11.02	10.53	20.00	56.41
		Detective	3.26	2.36	2.26	6.43	0.00
		Corrective	1.40	0.00	0.00	0.00	0.00
Damage to Physical Assets	CL	Total	5.12	15.75	15.79	0.71	0.00
	PL	Preventive	5.12	14.96	15.04	0.71	0.00
		Detective	0.00	0.79	0.75	0.00	0.00
		Corrective	0.00	0.00	0.00	0.00	0.00
Business Disruption and System Failures	CL	Total	14.88	15.75	15.79	41.43	15.38
	PL	Preventive	11.16	9.45	9.77	25.71	5.13
		Detective	2.33	4.72	5.26	12.86	10.26
		Corrective	1.40	1.57	0.75	2.86	0.00
Execution, Delivery & Process Management	CL	Total	33.95	8.66	9.77	27.14	15.38
	PL	Preventive	16.74	4.72	4.51	12.14	0.00
		Detective	13.02	3.94	5.26	10.71	15.38
		Corrective	4.19	0.00	0.00	4.29	0.00

As shown in Table 5, COSO concentrated on the business practices, process management and business disruption. Therefore, COSO (COSO, 2004) emphasizes the responsibilities of management for control, and the key principles for creating an effective risk management process, in order to help businesses and other entities to assess and enhance their internal control systems. Thus, awareness of the management about the internal control environment can be achieved.

CobiT focuses on the employment practices, business practices and process management, as it is an IT Governance framework and has control objectives designed for support and delivery of IT services. CobiT covers the operational risks related to employment practices, business practices and process management considering that it has comprehensive control objectives for planning and organizing IT activities, acquiring and implementing IT systems and technologies, delivering and supporting the IT services, and monitoring and evaluating the IT structure as in its domains. Thus, overall execution of IT processes, ongoing improvement on the process management, employee and business practices, and IT's delivery of value to

the business can be achieved. On the other hand, CobiT does not detail the security related control objectives and hence does not cover the operational risks related to the internal and external fraud. Physical security is not detailed by CobiT since it contains generic control objectives related to security aspects. If the secondary contribution of CobiT is evaluated, the facts show that CobiT has a high contribution on the operational risks related to business disruptions since it is a part of IT Governance.

BS7799 and ISO27001 have similar contribution and penetration levels since they are security standards, and ISO27001 has been developed using BS7799. Therefore, they have higher contribution and penetration levels especially for internal and external frauds, and damage to physical assets. These security standards cover the operational risks related to internal and external frauds, and damage to physical assets considering that they have comprehensive control objectives for logical security including the user account management, physical security, network security, security aspects of system development and maintenance. Thus, unauthorized activities and unauthorized access to the physical and logical systems from internal and external sources can be prevented. On the other hand, these ICMs do not have comprehensive control objectives related to IT Governance and business disruptions since they detail and concentrate on the logical and physical security aspects of an organization. If the secondary contributions of these ICMs are evaluated, the facts show these ICMs have high contributions on the operational risks related to workplace safety since it can also be considered as a security aspect of the business.

ITIL concentrates on the business disruptions since it has specific domains related to incident, problem, availability and change management. ITIL covers the operational risks related to business disruptions considering that it has comprehensive control objectives for infrastructure management, capacity management, availability management, incident management, problem management, change management and release management. Thus, hardware, software, telecommunications, and utility outages/disruptions can be prevented. On the other hand, ITIL does not have any security related control objectives. If the secondary contribution of ITIL is evaluated, the facts show that ITIL has a high contribution on the operational risks related to IT Governance since it also includes the risk appetite of an organization regarding the business disruptions.

Considering that the ICMs covered in this study are assessed according to the contribution and penetration levels on operational risk categories regarding the IT processes and controls, they are not assessed regarding the other sources of operational risks.

4.2. Best Practices Approach Based on CobiT

The gap analysis between the ICMs and the workshop results lead us to recommend an aggregated IT checklist for ORM since the ICMs covered in this study contribute to the operational risk categories at different levels and penetrate into them in different natures considering the control types. Although the importance of IT controls is embedded in the COSO internal control framework, IT management requires more examples to help identify, document and evaluate IT controls (ITGI, 2004). In addition, Public Company Accounting Oversight Board (PCAOB), the regulatory body established by US legislators to oversee companies' (and auditors') compliance with the Sarbanes-Oxley, recommends the COSO framework as a minimum standard (Datardina, 2005). Therefore, we recommend that COSO to be implemented as a starting point by each organization in order to enable the management of operational risks, because COSO is a risk management framework, and companies are starting to move away from considering their risks in isolation, and are looking beyond the traditional hazard and financial risk towards strategic and operational risks (GIRO, 2002).

The COSO approach refers to ERM, which has been viewed as the management of business risk, financial risk, operational risk and risk transfer to maximize a firm's value to owners and customers (Norris & Young, 2005). Risk transfer is the exchange of the unknown financial impact of specified events to a third party for a known financial cost through insurance or securitization (Dowd, 2001). Finally, COSO (2004) itself defines ERM as a process, affected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

In addition to COSO, the CobiT IT Governance framework is recommended as a baseline since effective IT Governance requires control over IT processes (Payne, 2003) as in CobiT, considering that IT processes cover the setting of objectives, giving directions on how to attain objectives and measuring performance in completing these activities (Korac-Kakabadse & Kakabadse, 2001). To improve the overall performance of IT and reduce the failure caused by inappropriate IT activities, there is a need for careful design, planning, acquisition and implementation of IT to manage its various activities and risks (Beaumaster, 2002 & Hardy, 2002). It is important to properly manage IT resources through a set of IT processes that provide

the information which the enterprise needs to achieve its objectives (Payne, 2003). CobiT is based on international best practices from various countries, including the United States of America, Europe, Australia, Canada and Japan; therefore, it serves as a more than appropriate framework on which the comparative framework can be based (Bornman & Labuschagne, 2006). Moreover, CobiT has been regularly accepted and applied by the Turkish banks since 2006 (BRSA, 2006b), and aligns with the spirit of the Sarbanes-Oxley requirement that any framework used be open and generally acceptable (ITGI, 2004). As a result, CobiT bridges the gaps between business risks, control needs, and technical issues. Therefore, it is recommended that CobiT should be a baseline although it is not best practice for each operational risk category in Basel II, referring to that Hardy (1995) defines CobiT as a common framework, which is cumulative instead of exclusive and based on forty-one primary reference materials. Since CobiT is a pervasive ICM, it should be used as a baseline in order to ensure that the organizations have a solid and strong IT governance structure. Hence, other ICMs can easily be adopted in order to improve the related IT related business processes by applying the ICMs in a holistic way, e.g. ICMs for IT risk management, project management, service management, security, system development, change management, service development, etc.

Therefore, it is recommended that the additional control objectives derived from each best practice ICM for each operational risk category should be aggregated with CobiT, where CobiT is not best practice ICM according to the gap analysis performed. While determining the additional control objectives, control objectives assigned to operational risk categories in CobiT have been mapped to the control objectives in each best practice ICM for each operational risk category. Thus, only different control objectives have been added and the overlapping of control objectives has been avoided.

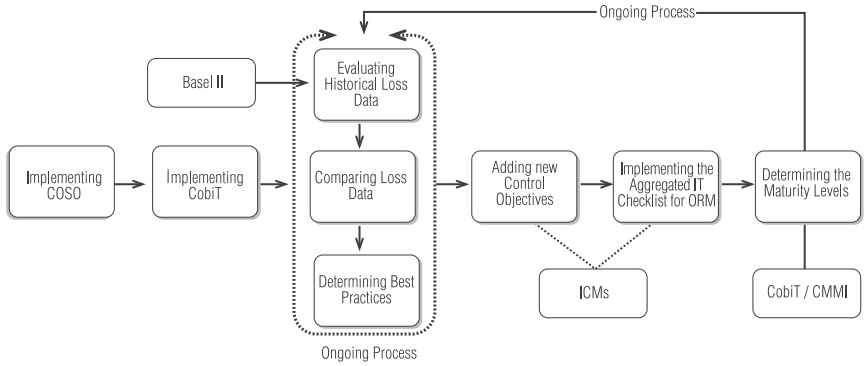
Table 6: Aggregated IT Checklist for Operational Risk Management

Operational Risks	Best Practice	Control Objectives in CobiT	Control Objectives in Best Practice	Additional Control Objectives for CobiT
Internal Fraud	ISO27001	12	35	27
External Fraud	BS7799	5	23	15
Employment Practices and Workplace Safety	CobiT	17	17	N/A
Clients, Products & Business Practices	CobiT	65	65	N/A
Damage to Physical Assets	ISO27001	11	21	12
Business Disruption and System Failures	ITIL	32	58	29
Execution, Delivery & Process Management	CobiT	73	73	N/A

Table 6 shows us the structure of the aggregated IT checklist for ORM. Although COSO is best practice considering the Employment Practices and Workplace Safety, and Clients, Products & Business Practices operational risk categories, CobiT is considered as best practice in these areas since COSO is recommended as a starting point of risk management. For Employment Practices and Workplace Safety, Clients, Products & Business Practices and Execution, Delivery & Process Management, the control objectives of CobiT are appropriate to cover operational risks in these areas. Therefore, there is no need for additional control objectives. For Internal Fraud, twenty-seven additional control objectives from ISO27001 are required in order to able to cover operational risks in this area. In the same way, for External Fraud, fifteen additional control objectives from BS7799 are required, for Damage to Physical Assets, twelve additional control objectives from ISO27001 are required, and for Business Disruption and System Failures, twenty-nine additional control objectives from ITIL are required. Therefore, additional control objectives should be determined according to the needs and priorities of the organizations, considering which operational risk category should be excelled. These objectives should be in accordance with the control objectives of COSO and CobiT, if they are used as a baseline, in order to ensure that the aggregated IT checklist for ORM is a comprehensive checklist and have control objectives in similar context. Thus, additional control objectives should be considered as control objectives which detail the roadmap of the organization in order to have a higher degree of comfort in a specific operational risk category.

As a result, COSO and CobiT serve as the starting point of the aggregated IT checklist for ORM since CobiT relates to COSO at a broad level and it is relatively simple to combine COSO with CobiT at a conceptual level (Panko, 2006). The conceptual framework is illustrated in Figure 2.

Figure 2: Best practices approach based on CobiT



As shown in Figure 2, the assessment of the operational risks categorized in Basel II is performed using a maturity model, which is derived from CobiT or Capability Maturity Model Integration (CMMI). The control objectives in the aggregated IT checklist for ORM are assessed using the maturity levels detailed in CobiT (ITGI, 2005) or in CMMI (SEI, 2002) as shown in Table 7.

Table 7: Maturity Levels

Maturity Level	CobiT	CMMI
0	Non-existent	N/A
1	Initial / Ad-hoc	Initial
2	Repeatable but Intuitive	Managed
3	Defined Process	Defined
4	Managed and Measurable	Quantitatively Managed
5	Optimized	Optimized

This assessment will lead the organizations monitor the ORM activities, update their ORM strategies, and improve their IT structure by evaluating the maturity of the IT related processes and by evaluating the gap between the control objectives in ICMs and their actual implementations in the organization. Maturity model responds to three needs: A relative measure of where the enterprise is, a manner to efficiently decide where to go, and a tool for measuring progress against the goal.

5. Conclusion

As explained above, the aggregated IT checklist for ORM is a combined ICM, which is based on COSO and CobiT and expanded using the control objectives from BS7799, ISO27001, and ITIL where they are best practices in specific operational risk category defined in Basel II. Since organizations may have different frequency and severity matrices regarding each operational risk category, they have a chance to apply the aggregated IT checklist as a whole or separately according to the evaluation of their loss data history by comparing the QIS2 results (RMG, 2002) or later researches and their prioritization of their loss data.

Therefore, it is important to determine which ICM(s) should be applied by the organizations according to their needs and priorities. The organizations should consider that the aggregated IT checklist for ORM is a framework which supports the whole ORM activities in the organization by excelling the IT related processes and controls in the core IT systems and technologies which have impact on financial statements. While adopting the best practices approach based on CobiT, the organizations should concentrate on their needs and apply the best practices for their operations rather than harmonizing all ICMs or the control objectives in ICMs. Thus, the

organizations can avoid the risk of getting lost in the control objectives detailed in different levels in various ICMs, and hence concentrate on the governance structures.

Accordingly, each organization should tailor an IT control approach suitable to its size and complexity, considering the COSO ERM framework (ITGI, 2004), and should develop its GRC (ITGI, 2007b). As a starting point, the organizations should apply the COSO ERM framework and CobiT IT Governance framework in order to be able to manage the operational risks caused by IT processes and controls. The aggregated IT checklist for ORM, which is actually a best practices approach based on CobiT, responds to Basel II ORM requirements by comparing the ICMs at the control objective level regarding their penetration and contribution levels to ORM, rather than offering guidance for ORM steps.

Operational risk managers and internal or external auditors can use this study as an operational risk assessment tool by rating each control objective since Mc Connell (2005) discusses such a measurement need. The assessment of the operational risks categorized in Basel II is performed using a maturity model, which is derived from CobiT. The control objectives in the aggregated IT checklist for ORM are assessed using the maturity levels detailed in CobiT (ITGI, 2005) or in CMMI (SEI, 2002). However, unless all IT systems or processes pose a high risk to the financial statements, not all IT systems or processes need to be included or evaluated to the same extent. In performing a risk assessment, consideration needs to be given to inherent risk rather than residual risk, which is the risk left over after considering the impact of controls (ITGI, 2006b).

For further research, a guideline for assessing the maturity levels of the control objectives coming from CobiT and other ICMs can be prepared in order to evaluate the maturity level of each control objective and to assess the ORM in an organization as a whole. In addition, other ICMs which have not been covered in this article might be evaluated according to the operational risk categories in Basel II, considering that different IT processes need the guidance of various models specified in these areas, e.g. Projects in Controlled Environments (PRINCE2) for project management, CMMI-DEV for product and service development processes, CMMI-ACQ for acquisition and outsourcing processes, IT Grundschutzhandbuch (IT Baseline Protection Manual) for a detailed security configuration. Since the ICMs discussed in this study are updated according to the business world's requirements, such as new editions of ICMs, where CobiT edition 4.1 has been published during the documentation of the study, the study should be revised and updated accordingly.

With so much to do and so little time or resources, the operational risk managers need to prioritize the steps in ORM and apply the 80/20 rule (Lanz, 2002). By focusing on and assigning resources to high-priority risks and exposures, operational risk managers can cost-effectively mitigate risk to an acceptable level for their enterprise. Independently from the methods and models employed during the ORM process, organizations should not forget Hoffman's (2002) statement: all the risk management in the world cannot compensate for a flawed corporate vision and culture.

References

1. Alberts, C. (2006). Common elements of risk. Pittsburgh: *Software Engineering Institute*, Carnegie Mellon University.
2. Alberts, C. ve Dorofee, A. (2005). Mission assurance analysis protocol (MAAP): Assessing risk in complex environments. Pittsburgh: *Software Engineering Institute*, Carnegie Mellon University.
3. Beaumaster, S. (2002). Local government IT implementation issues: a challenge for public administration. Hawaii: *Proceedings of Hawaii International Conference on System Sciences.*
4. Basel Committee. (2001a). The new Basel Capital Accord: an explanatory note. Basel: *The Bank for International Settlements.*
5. Basel Committee. (2001b). Consultative document: operational risk. Basel: *The Bank for International Settlements.*
6. Basel Committee. (2001c). Working paper on the regulatory treatment of operational risk. Basel: *The Bank for International Settlements.*
7. Basel Committee. (2001d). Sound practices for the management and supervision of operational risk. Basel: *The Bank for International Settlements.*
8. Basel Committee. (2002a). Sound practices for the management and supervision of operational risk. Basel: *The Bank for International Settlements.*
9. Basel Committee. (2002b). Overview paper for impact study. Basel: *The Bank for International Settlements.*
10. Basel Committee. (2002c). About the Bank for International Settlements, Basel Committee on Banking Supervision. Basel: *The Bank for International Settlements.*
11. Basel Committee. (2003a). Sound practices for the management and supervision of operational risk. Basel: *The Bank for International Settlements.*
12. Basel Committee. (2003b). The New Basel Capital Accord consultative document. Basel: *The Bank for International Settlements.*
13. Basel Committee. (2004). International convergence of capital measurement and capital standards: A Revised Framework. Basel: *The Bank for International Settlements.*
14. BBA, ISDA, RMA ve PwC. (1999). Operational risk: the next frontier. Philadelphia: British Bankers' Association, the International Swaps and Derivatives Association, Risk Management Association, and PricewaterhouseCoopers.

15. Bornman, W. G. ve Labuschagne, L. (2006). A comparative framework for evaluating information security risk management methods. Auckland Park: Rand Afrikaans University.

16. BRSA. (2001). Regulation on banks' internal control and risk management systems – *Banking Regulation and Supervision Agency*. Turkish Official Gazette, 8 February 2001, 24312.

17. BRSA. (2006a). An attitude of Banking Regulation and Supervision Agency for IT assurance. Istanbul: *IT Audit 2006 Workshops Proceedings.*

18. BRSA. (2006b). Regulation on information systems assurance in the banks - *Banking Regulation and Supervision Agency.* Turkish Official Gazette, 16 May 2006, 26170.

19. BSI. (1999). British Standard: Information security management part1 & part2. London: *British Standards Institute Group (BSI).*

20. Campbell, P. L. (2003). An introduction to information control models. New Mexico: *Sandia National Laboratories.*

21. Carey, M. ve Stulz, R. M. (2005). *The risks of financial institutions*. Columbus: Ohio State University Press.

22. Chapelle, A. (2005b). *The virtues of operational risk management*. Brussels: Université Libre de Bruxelles.

23. COSO. (2004). Enterprise Risk Management – Integrated Framework. Washington: *The Committee of Sponsoring Organizations of the Treadway Commission (COSO).*

24. Datardina, M. (2005). Comparative analysis of IT control frameworks in the context of SOX. Ontario: *Centre for Information Systems Assurance*, University of Waterloo.

25. Davidson, S. (2006). The role of identity management: Moving from compliance to improved business performance. New York: Computer Associates International, Inc.

26. Di Renzo, B. ve Bernard, C. (2005). Operational risk management in financial institutions: Process assessment in concordance with Basel II. Luxembourg: *Centre de Recherche Public Henri Tudor & Commission de Surveillance du Secteur Financier.*

27. Dorofee, A. J. (1996). Continuous risk management guidebook. Pittsburg: *Software Engineering Institute*, Carnegie Mellon University.

28. Dowd, W. (2001). Insurance of operational risk and the New Basel Capital Accord. Boston: *Capital Allocation for Operational Risk Conference Proceedings.*

29. Goldstein, M. (2001). *Comment and discussion on relevance and the need for international regulatory standards.* Washington D.C.: Brookings Institution Press.

30. Hardy, G. (1995). Standards - The need for a common framework. London: Proceedings of COMPSEC International 1995, *12th World Conference on Computer Security, Audit and Control.*

31. Hardy, G. (2002). Make sure management and IT are on the same page: implementing an IT Governance framework. *Information Systems Control Journal*, 3, 14-16.

32. Hoffman, D.G. (2002). *Managing operational risk: 20 firmwide best practice strategies.* New York: Wiley Frontiers in Finance, John Wiley & Sons, Inc.

33. ISACA. (2006). CISA review manual 2007. Rolling Meadows: *Information Systems and Control Association (ISACA).*

34. ISO. (2005). Information technology – Security techniques - Information security management systems – Requirements. Geneva: *International Organization for Standardization (ISO).*

35. ITGI. (2004). IT control objectives for Sarbanes-Oxley 1st edition: The Importance of IT in the design, implementation and sustainability of internal control over disclosure and financial reporting. Rolling Meadows: *IT Governance Institute (ITGI).*

36. ITGI. (2005). COBIT® 4th edition. Rolling Meadows: *IT Governance Institute (ITGI).*

37. ITGI. (2006a). COBIT® mapping: Mapping of ISO/IEC 17799:2005 with COBIT® 4.0. Rolling Meadows: *IT Governance Institute (ITGI).*

38. ITGI. (2006b). IT control objectives for Sarbanes-Oxley 2nd edition: The importance of IT in the design, implementation and sustainability of internal control over disclosure and financial reporting. Rolling Meadows: *IT Governance Institute (ITGI).*

39. ITGI. (2007a). COBIT® mapping: Mapping of ITIL® with COBIT® 4.0. Rolling Meadows: *IT Governance Institute (ITGI).*

40. ITGI. (2007b). IT control objectives for Basel II: The importance of governance and risk management for compliance. Rolling Meadows: *IT Governance Institute (ITGI).*

41. Jochum, C. (2006). IT risk management in the banking industry. Frankfurt am Main: *Institut für Wirtschaftsinformatik.*

42. Kane, E. J. (2001). *Relevance and the need for international regulatory standards.* Washington: Brookings Institution Press.

43. King, J. L. (2001). *Operational risk.* New York: John Wiley & Sons.

44. Kloman, H. F. (1990). Risk management agonists. *Risk Analysis*, 10/2, 201-205.

45. Korac-Kakabadse, N. ve Kakabadse, A. (2001). IS/IT governance: need for an integrated model. *Corporate Governance*, 1/4, 9-11.

46. Lanz, J. (2002). Prioritizing aspects of technology risk assessment and mitigation. *Bank Accounting & Finance*, December 2002, 19-26.

47. Mc Connell, P. (2005). Measuring operational risk management systems under Basel II. Sydney: *Risk Trading Technology.*

48. Mürmann, A. ve Öktem, Ü. (2002). The near-miss management of operational risk. Philadelphia: University of Pennsylvania.

49. Netter, J. M. ve Poulsen, A. B. (2005). Operational risk in financial service providers and the proposed Basel Capital Accord: An overview. Athens: University of Georgia.

50. Norris, V. A. ve Young, L. R. (2005). Risk assessment in Sarbanes-Oxley. Charleston: *Advanced Technology Institute.*

51. OGC. (2004). Information Technology Infrastructure Library v.2. Norwich: *The Office of Government Commerce (OGC).*

52. Panko, R. R. (2006). Spreadsheets and Sarbanes-Oxley: Regulations, risks, and control frameworks. Hawaii: University of Hawaii.

53. Payne, N. (2003). IT Governance and audit. *Accountancy SA*, January 2003, 35.

54. RMG. (2002). The quantitative impact study (QIS) for operational risk: Overview of individual loss data and lessons learned: Report to Basel Committee. Basel: Risk Management Group, *Bank for International Settlements.*

55. Samad-Khan, A. (2005). Why COSO is flawed? Retrieved January 18, 2005, from http://www.operationalriskonline.com

56. Saunders, A. (2000). *Financial institutions management: A modern perspective.* New York: McGraw Hill.

57. SEI. (2002) Capability Maturity Model® Integration (CMMI), version 1.1. Pittsburgh: *Software Engineering Institute*, Carnegie Mellon University.

58. Young, P. C. ve Tippins, S. C. (2001). Managing business risk: An organization-wide approach to risk management. New York: *American Management Association.*