Accounting and Management Information Systems
Vol. 12, No. 1, pp. 101–117, 2013

IMPLICATIONS OF THE OPERATIONAL RISK PRACTICES APPLIED IN THE BANKING SECTOR ON THE INFORMATION SYSTEMS AREA

Pavel NĂSTASE and *Simona Felicia UNCHIAŞU*[1]
The Bucharest University of Economic Studies, Romania

ABSTRACT

In financial services organizations, the degree of automation is usually high, while the human intervention low. Banks depend on information technology and information management, complex infrastructure and applications, thus controls are required to support the business processes. Furthermore, the information used by financial institution is often entirely IT generated, managed and controlled, therefore the confidentiality, availability and reliability of financial information is crucial. As such, the risks introduced by the use of information systems play a significant role in the operational risk. The goal of the Basel Committee regulations was to improve the risk management practice, introduce supervisory review of banks' internal capital assessment process and enhance the level of transparency in public reporting. Basel II Accord introduced a new approach to risk within the banking industry as the operational risk was included for the first time. A new framework, Basel III was issued in December 2010, which strengthens the regulation, supervision and risk management of the banking sector. The Basel Accord recommends advanced methods for calculating the risks rating that move towards higher complexity and increased risk sensitivity, so IT re-engineering is necessary in order to better manage data and constantly capture and calculate the different types of risk. This article presents the risks within banking sector as described by the Basel Committee on Banking Supervision and tries to capture the relevance and implications of the recommended practices for the management and supervision of operational risk upon the information systems area.

Basel Accord, Risk management, Operational risk, IT risk, COBIT.

1 *Correspondence address*: Simona Unchiaşu, CISA, CRISC, PhD - Bucharest University of Economic Studies, Romania, email: simonaunchiasu@yahoo.com

INTRODUCTION

Nowadays, the importance of the information systems, hereinafter called IS, cannot be overlooked since their presence is seen everywhere, in the economic, public and social life. Information technology is present in all the activities deployed by an organization, from production, marketing, retail, accounting till management.

The information technology plays a key role in the financial services sector where large volumes of information must be managed. Moreover, technology is used across all areas of financial services, like analysis, modelling, electronic trading and for reporting purposes.

The risk is perceived differently, depending on the forms of business activity. Other types of risk will occur in production facilities and other ones in financial sector.

Theoreticians and practitioners do not give one universal definition to risk, reflecting that risk means different things to different people. In order to put risk in the proper business context, the Committee of Sponsoring Organization of the Treadway Commission (COSO), issued in 2004 the Enterprise Risk Management Integrated Framework (COSO ERM Framework), which defines risk as follows: "Risk is the possibility that an event will occur and adversely affect the achievement of an objective". According to COSO ERM Framework, "enterprise risk management is a process, effected 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 risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (IFAC, 2004).

The current economic environment brings a new spectrum of information technology related risks, such as fraud, disclosure of confidential data; non-availability of services negotiated due to systems downtime, or missed business opportunities caused by a rigid IT infrastructure. A failure in the process of creating a loss event can be tracked down to a technology control that was not designed well or failed to operate. This is the case of the Société Générale's incident which showed inappropriate access to systems as a significant causal factor (Société Générale, 2009). Too often, the IT risk, which is the business risk related to the use of information technologies, is overlooked.

This article presents the risks within banking industry as described by the Basel Committee on Banking Supervision and tries to capture the relevance and implications of the recommended practices for the management and supervision of operational risk upon the information systems area. We started our research with a literature review on the Basel subject and then, based on COBIT framework and our practical experience in IS audit and IS risk management, we analyzed the

influence that the recommended operational risk practices might have on the information technology area.

1. THE BASEL APPROACH TOWARDS MANAGING RISKS

In 2006, the Basel Committee on Banking Supervision published a revised framework of the "International Convergence of Capital Measurement and Capital Standards" paper, known as Basel II Capital Accord, hereinafter called Basel II (BIS, 2006).

The objective of Basel II was to introduce a new approach to risk within the banking industry. The operational risk was included for the first time. The new regulation combined the minimum capital requirements with supervisory review and market discipline in order to impose a stronger risk management practice that will reduce the overall risk exposure of the organizations and therefore the capital charge. The GRC concept, meaning *G*overnance, *R*isk management and *C*ontrol plays a key role in reducing the aforementioned charge (BIS, 2006; ISACA, 2009a).

Basel II makes greater use of assessments of risks provided by the banks' internal systems, copes with new instruments like the credit derivatives and takes into account development in market practices.

Basel II defines the risk categories along with the core business areas found in a banking organization, as follows (Unchiaşu, 2009):

- credit risk is defined as the risk involved in exposures to individual borrowers or counterparties as well as at the portfolio level;
- operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. The operational risk includes the legal risk, defined as the risk of loss because of legally flawed actions of the bank or its employees, ambiguity regarding the requirements and effects of the law itself, relevant inefficiencies of any country's legal system;
- market risk is defined as the risk of potential financial loss due to an adverse change in market variables such as interest or foreign exchange rates;
- interest rate risk includes all material interest rate positions of the bank and considers all relevant repricing and maturity data;
- liquidity risk is the risk that bank will be unable to find assets to meet obligations at reasonable cost or at all;
- reputational risk: reputation is an intangible but highly value asset; is the risk of significant negative public opinion that results in a critical loss of funding or customers.

- strategic risk is the potential of negative impact on the earnings and capital of the bank due to misjudged strategic decisions, inadequacy of the business strategies developed and resources to meet the strategic goals and the lack of responsiveness to industry changes.

A new framework, Basel III was issued in December 2010, which sets higher levels for capital requirements and introduces a new global liquidity framework. Basel III strengthens the regulation, supervision and risk management of the banking sector and aims (BIS, 2010; BIS 2012):

- to improve the banking sector's ability to absorb shocks arising from financial and economic stress, whatever the source is;
- to improve risk management and governance;
- to strengthen banks' transparency and disclosures.

2. REGULATORY ENVIRONMENT

In the EU, Basel II is applied to all internationally banks, regardless of size, via EU directives: EU Directives 2006/48 and 2006/49. The standardised and intermediate approaches for credit and operational risk were available since 1st January 2007, while the advanced approaches were available since January 2008 (BIS, 2006).

Regarding Basel III framework, members of the Basel Committee on Banking Supervision agreed to implement it starting from 1 January 2013, subject to transitional and phase-in arrangements.

At national level, the Romanian Government has issued the Emergency Ordinance (OUG) no. 99 / 2006 on Credit Institutions and Capital Adequacy. As result of the OUG implementation, the National Bank of Romania together with Romanian National Securities Commission has issued several regulations. Among the most recent and significant regulations we quote (NBR, 2012; RNSC, 2012):

- NBR-NSC Regulations no. 20/11/2011 on supplementing NBR-NSC Regulations no. 14/19/2006 and no. 15/20/2006 concerning credit risk treatment using the standardised approach and internal model based approach, respectively;
- NBR-NSC Regulations no. 22/14/2011 on supplementing NBR-NSC Regulations no. 22/27/2006 concerning capital adequacy of credit institutions and investment firms;
- NBR-NSC Regulations no. 29/10/2009 on supplementing NBR-NSC Regulations no. 13/18/2006 concerning the determination of minimum capital requirements for credit institutions and investment firms;
- NBR-NSC Regulation no. 23/28/2006 on technical criteria concerning the organisation and treatment of risks, as well as technical criteria on review and evaluation by the competent authorities;

- NBR-NSC Regulation no. 24/29/2006 concerning calculation of the minimum capital requirements for operational risk of credit institutions and investment firms;
- The aforementioned regulations are applied since 01.01.2008, mainly for the standardised approach;
- NBR Order no. 22/2011 on reporting situations concerning the liquidity indicator and the high liquidity risk. The order is applicable since the beginning of 2012.

3. THE IMPLICATIONS OF BASEL II REQUIREMENTS ON THE INFORMATION SYSTEMS AREA

3.1. Operational Risk and IT Risk

The Basel Committee has defined the operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events".

Operational risk is an inherent element of any business activity, internal procedure, technical infrastructure or corporate governance. It may be found in any stage of a financial product or service design and delivery.

The operational risk presents distinct characteristics and special means to monitor. (Stanciu & Eden, 2008). The operational risk is described by the following components:

- cause: as per definition, operational risk causes include processes, people, systems and external factors;
- event: the incident associated with the risk types;
- consequence: is defined by the bank (e.g. actual loss, potential loss);
- impact: it might be either tangible, like financial impact or intangible, like reputational impact, business efficiency impact;
- control: it could be a process, and IT system, or a policy used to mitigate the risks.

The Basel Committee has identified at least seven dimensions of the operational risk. Based on the literature review (Chorafas, 2001; ITGI, 2007a; Holmquist, 2007; Micallef 2008; Gheorghe *et al.*, 2008, RBA 2009) and our experience, hereinafter we have tried to emphasize the IT dimension of each operational risk area:

a) *Internal fraud* is defined as the losses occurred due to acts intended to defraud, misappropriate property or circumvent regulations by at least one internal party.
   The IT aspects of the internal fraud events are:
   - transactions intentionally not reported or unauthorized;
   - theft of sensitive information;

- extortion;
- malicious destruction of information assets;
- forgery and impersonation;
- deliberate manipulation of programs, hardware, system commands;
- usage of unlicensed or unauthorized software;
- internal circumvention of access privileges.

b) *External fraud* is defined as the losses occurred due to acts intended to defraud, misappropriate property or circumvent the law, which are done by a third party. The IT aspects of the internal fraud events are:
   - theft of sensitive information;
   - robbery, forgery;
   - deliberate changing of data through hacking techniques;
   - external circumvention of access privileges;
   - eavesdropping;
   - viruses.

c) *Employment practices and workplace safety losses* are defined as the losses arisen from acts inconsistent with employment, health or safety laws, from payment of personal injury claims or from discrimination events.
   The IT aspects within the third dimension of operational risk are: weaknesses in the ownership practice for the IT resources, lack of security accountability and misuse of IT resources.

d) *Clients, product and business processes* losses are defined as the losses resulting from an unintentional or negligent failure to meet a professional obligation to certain clients, or from the nature or design of a product.
   The IT dimension is given by the following aspects:
   - disclosure of sensitive information to outside parties by employees, more exactly for the banking environment: retail or corporate customer disclosure violation;
   - breach of privacy;
   - aggressive sales through information systems means, like unsolicited emails;
   - misuse of confidential information like credit cards information, clients' id's numbers;
   - market manipulation using the financial institution systems;
   - exceeding client exposure limits.

e) *Damage to physical assets* are the losses arising from damage to physical assets from natural disaster or other events. The IT dimension is given by the deliberate or accidental damage to the data center or physical IT network infrastructure.
f) *Business disruption and system failure* losses are caused by disruption of business or systems failure.

The IT aspects of the sixth dimension of the operational risk are as follows:

- hardware, software and telecommunications' systems malfunction;
- loss of key IT staff and the absence of a proper implementation of the key IT staff replacement process;
- back-up and recovery processes failure;
- DDOS – distributed denial-of-service attacks.

g) *Execution, delivery and process management* losses are caused by failed transaction processing or process management, from relations with trade counterparties and vendors.

The IT dimension is given by the following aspects:

- data entry errors;
- files maintenance or loading errors;
- missed projects' deadlines;
- failure delivery;
- inaccurate reporting;
- incorrect client records;
- outsourcing, and vendor disputes.

The Basel Committee requires the banking institutions to implement a framework to manage the operational risk. An effective risk management is facilitated by an organization wide risk philosophy, materialized in a set of strategies, processes, enablers and tools used in the business. Through operational risk management, the organization identifies the inherent operational risks, treats them in accordance with its business objectives and monitors the residual risk.

In financial services organizations, the degree of automation is usually high, while the human intervention low. Banks depend on information technology and information management, complex infrastructure and applications, thus controls are required to support the business processes. Furthermore, the information used by financial institution is often entirely IT generated, managed and controlled, therefore the confidentiality, availability and reliability of financial information is crucial. Having this in our mind, it can be said that the risks introduced by the use of information systems play a significant role in the operational risk.

The IT risk is defined by the Information Systems Audit and Control Associations - ISACA as a business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise (ISACA, 2009a).

In practice, the major IT risks relate to inherited and obsolete systems, exposure of sensitive information, outsourcing, the adequacy of major IT investments, business continuity and growth of e-commerce (Guldentops, 2004).

The key for mitigating the risks is to understand them, develop the proper methods to measure and control them and establish accountability. Basel II approach to risk covers the complexity of information technology and information management risks.

3.2 Basel II Operational Risk Principles and their impact on the information systems area

Basel Committee on Banking Supervision has issued in 2003 the "Sound Practices for the Management and Supervision of Operational Risk" document, which provides a framework for the effective management and supervision of operational risk. This document is intended for the use of banks and supervisory authorities when evaluating the operational risk management policies and practices in place (BIS, 2003).

There are ten Basel II principles grouped under categories which:

- establish a framework for the development of an appropriate risk management environment (principles 1-3);
- offer guidance over the risk management process (principles 4-7);
- describe de supervisors' role (principles 8 and 9);
- describe the role of disclosure through principle 10.

Having as starting point the Basel II principles stated in the aforementioned document, their relevance and requirements in terms of information systems is further analyzed.

Principle 1 deals with the board awareness and approval process. The board of directors should approve the implementation of an organization-wide framework for the operational risk as a distinct risk category. The framework should cover the bank's approach to identify, assess, monitor and control the risk.

The IT risk is an important part of the operational risk; therefore IT risk management should be integrated into the overall risk management process. An IT risk management framework should be approved, periodically reviewed and implemented. The IS performance must be assessed based on established key performance indicators – KPI.

Principle 2 introduces the internal audit process. Banks should have in place adequate internal audit coverage. Bank's top management should ensure that the independence of the audit function is maintained and that the frequency and the scope of the audit programme are aligned with the risk exposures.

In Romania, the NBR Regulation no.18/2009 regulates the general framework for the organization and the performance of the internal audit function of financial institutions and the management of material risks. IS external audits are performed when needed, either due to the lack of internal audit expertise or regulations. For example, the Order No. 218/14.06.2004 issued by the Ministry of Communication and Information Technology regarding the procedure for advising the distance payment instruments, like Internet-banking, home-banking or mobile-banking applications states that the audit opinion of a professional holding the CISA - Certified Information Systems Auditor designation is a mandatory document for obtaining the favourable accreditation.

The internal audit plan should include the IS components. The IS audit team should assess the IS universe and perform audits according to the risk ranking. The internal IS audit function should be independent, adequately staffed and skilled. The auditors must have an understanding about the risk assessment techniques, IS control objectives, national and group regulations, in case the bank is part of a worldwide group.

Principle 3 establishes the risk management framework. Management should translate the operational risk framework into specific policies, processes and procedures so as to be implemented by the business units. Senior management should clearly assign responsibilities, authority and reporting relationship to manage the operational risk effectively.

The third principle has profound implications for the implementation of the IT risk management framework. Members of the IT management should have the same responsibilities for implementing the IT risk framework as have members of senior management for implementing the operational risk framework (ITGI, 2007a: 32-37). The framework adopted by the bank should consider the IT risks, and an IT control framework aligned with the GRC framework should be developed. Policies, processes and procedures for managing the IT risks should also be developed, like: IT Governance document, IT Strategy, IT Security Plan, Systems development procedures, Change management procedures, Operation and support procedures, establishment of KPI.

Risk management begins with a clear understanding of the financial organization's appetite for risk, which drives all the risk mitigation efforts and impacts future investments in technology (ITGI, 2005).

Risk management is a process with two components, identification and control. First part means to identify vulnerabilities and threats to the information resources used for achieving the business objectives and the second one, to decide, based on the value of the information resource for the business, what countermeasure to take in reducing risks to an acceptable level.

Principle 4 treats the identification and assessments process. Risk identification is vital for the subsequent development of a successfully operational risk monitoring and control system. An efficient identification process should consider both internal (e.g.: bank's structure, products, activities, organizational changes, staff turnover) and external (e.g.: changes in the market) factors that could adversely impact the achievement of the objectives. Amongst the possible tools recommended in the identification and assessment process there are: self-assessment, risk mapping, establishment of risk indicators and measurement processes.

The information used for operating a bank is entirely generated by the IT systems. Reliability of that information is crucial. Risk assessment should be present in all IT activities (e.g.: program changes and promotion into production, infrastructure changes) that could have a material impact on the bank's business. Users who could be impacted should be involved in the risk assessment process, as well. IT risk assessments results should be integrated with other risk assessments analysis so as to have a global risk assessment view.

The IT risk identification process comprises the following steps (ISACA 2009a, 2009b; ISACA 2011):

- define the universe: gather all the information resources or assets (e.g.: infrastructure, applications, information and data, services, documents, personnel) and their interdependencies. A special attention must be paid in the case of the in-house inherited applications, that usually are not documented, which exist for long time, and the IT staff is so used with them that sometime forgets to perceive them with potential risk.
- identify threats and vulnerabilities: analyze all potential inherent and interdependent threats and vulnerabilities within IT universe. There are different techniques that can be used, like: interviews with managers, focus groups, past experience, scenarios or vulnerability scanning and attack simulation.
- evaluate risk probability: first step is to classify and categorize the risks and then to calculate the risk probability. The evaluation means to estimate through expert judgment or based on historical events the probability of a threat to occur.
- evaluate the cost at risk: estimate the value of the damage if the risk event occurs.

Principle 5 defines the operational risk monitoring process. A regularly monitoring process should be implemented. Regular reporting of significant information to senior management is the prerequisite for proactive management of operational risk. The occurrence of any significant internal or external event should determine the reassessment of the operational risk.

Based on the results of the risk identification and assessment process, the risks are prioritized, as to identify key IT risk indicators (KRI). These indicators should be part of a measurement and monitoring process so as to become an early warning system for the operational risk profile. Nevertheless there are many challenges in establishing successful KRI, such as the KRI are too many, difficult to measure or are too generic. Also it is difficult to aggregate and compare the KRI in a systematic way (ISACA, 2009b).

IT is essential in any reporting and monitoring system; therefore special attention should be paid to the availability, confidentiality, integrity and response time of the information systems involved in the process.

Principle 6 speaks about the necessity of having policies, processes and procedures in place to control or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly.

Since IT risks are an important part of the operational risk, an IT control framework should be developed to mitigate them, as part of an overall control framework. IT policies, processes and procedures should be implemented to support the IT control framework and should be periodically reviewed and formally approved. The IT risks should be reassessed at the occurrence of any significant internal (e.g.: integration of systems, replacement of obsolete applications) or external event.

The control process comprises of the following steps:

- identify risk treatment plan: once risk appetite is defined and risks are identified, strategies for managing risks can be set and responsibilities assigned. Depending on the risk type and its significance, the response may vary, as to Năstase *et al.* (2007) :
  - acceptance: the business decides to live with risk, no further actions are taken other than monitoring it;
  - mitigation: steps are taken in order to mitigate the risk to an acceptable level;
  - avoidance: the business chooses to avoid the risk by stepping out (e.g. avoiding the floods by relocating the disaster recovery site away from the river);
  - transfer: the risk is transferred to the insurance company;
  - eliminate: if possible, remove the source of the risk.
- create a short list of suitable solutions: the proposed solution might be a single control or a combination of controls. According to the IT Governance Institute, control is defined as "the policies, procedures, practices and organizational structures designed to provide reasonable

assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected". Risks tend to be interrelated in complex ways so special attention should be paid in selecting the best solutions.

- calculate residual risk: controls do not always eliminate the risk, thus any remaining risk after a control is implemented, is called "residual risk".
- calculate cost at risk: estimate the value of the damage if the risk event occurs after the implementation of the proposed control. Based on the calculation made, one could estimate the effectiveness of the proposed control.
- cost-benefit analysis: based on the parameters calculated in the previous steps, a cost-benefit analysis should be made. The outcome provides an effective decision mechanism, beyond just controlling the IT risks and leveraging the value towards control.

Principle 7 introduces the contingency subject. 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.

For reasons that may be beyond the bank's control, an unforeseen event may result in the inability of the bank to fulfill its obligations, especially when the IT infrastructure has been damaged. This can result in significant financial losses as well as to the disruption of banking system, due to system down times, e.g. the payment system. Since IT is fundamental for the banking activities, the development of a Disaster Recovery Plan (DRP) and of a Disaster Recovery Site are mandatory. Furthermore, IT continuity plans and procedures should be included in the bank's business continuity plan.

Principle 8 introduces the concept of banking supervision requirements for effective framework. Supervisors should require banks, regardless of size, to develop operational risk management framework consistent with the requirements of the previous principles.

In accordance with the above principle, the IT risk management framework should be aligned with the requirements of the banking supervisors.

Principle 9 brings up the regular independent evaluations topic. Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank's policies, procedures and practices related to operational risks. Supervisors may wish to establish reporting mechanisms in order to receive update information related to operational risk subject.

Based on the aforementioned principle, the IS related regulatory requirements should be integrated with the overall organizational policies and procedures. A mechanism for addressing the supervisor's requirements in a timely manner should be in place.

Principle 10 establishes the public disclosure of information by the banks. Basel Committee considers that banks should make sufficient public disclosure of information in order to allow market participants to assess their approach to operational risk management.

In line with the last principle, the IT management should identify the relevant risks and brings them to the attention of the senior management.

3.3 The IT Road Map to Basel compliance

The implementation of Basel accord is impossible without an IT strategy that will address the business requirements within.

The first pillar within Basel II accord, Minimum Capital Requirements needs the most IT resources since operational and market risk criteria are introduced for measuring risks. The operational risk may be calculated using one of the three approaches recommended: the basic indicator approach, the standardized approach and the advanced measurement approaches (AMA) which are based on internal loss data (Lubbe & Snyman, 2010). For calculating the credit risks, three approaches were also recommended: the standardized approach, the foundation internal ratings based approach (IRB) and the advanced IRB approach.

Currently, most of the banks use the basic or the standardised approach, intending in the next few years to implement the internal ratings approach and the advanced measurement approach which will require additional IT resources. The recommended more advanced methods for calculating the risks rating move towards higher complexity and increased risk sensitivity, so IT re-engineering is necessary in order to better manage data and constantly capture and calculate the different types of risk.

The supervisory review process requires a strong management information system able to provide risk and capital information to the supervisory board on a need basis and in a timely manner. The information must be provided in an easy to understand reports or dashboards. Managers should be able to drill down to the basic numbers and find the deviation causes. There are two supervisory reporting frameworks indicated by the NBR, called COREP – Common solvency ratio reporting framework and FINREP – Financial reporting framework.

The market discipline requirements necessitate the improvement of the management information systems in general and of the reporting system in particular, so as to provide the adequate and accurate reports out to the market in a timely manner. The information must be presented in an easy to understand and friendly form. Based on the information provided, supervisors and other interested parties evaluate the banks' internal capital adequacy assessments and ability to monitor compliance and, if needed, intervene to prevent capital from falling below the minimum levels.

The role of IT re-engineering is to facilitate financial services executives to manage better the data and continuously capture and measure the risks so as to be compliant with the regulations in force. Successful data warehousing and mining of data clears the information burden.

In order to meet Basel accord requirements, the next steps should be followed:

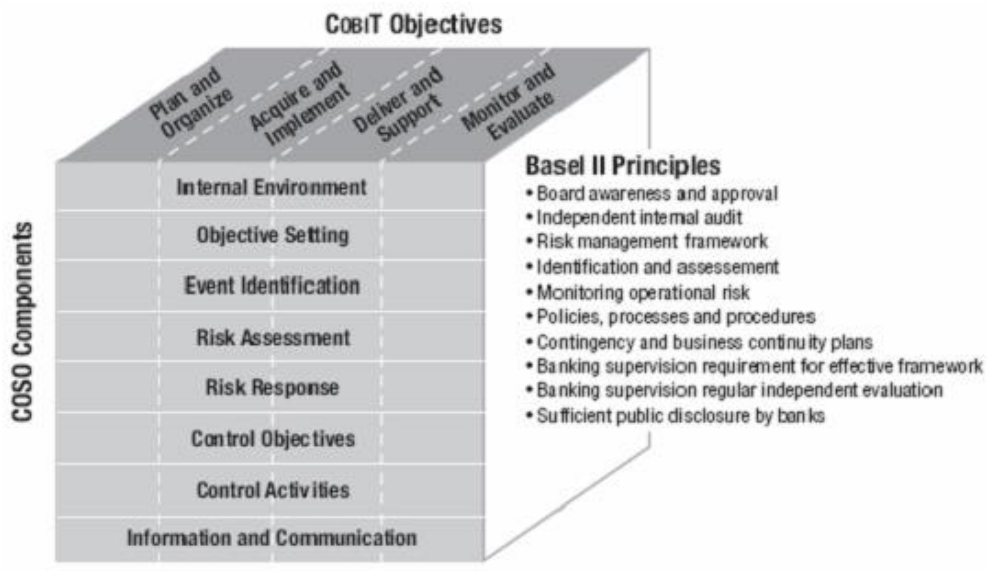
- gather required data for models;
- analyze the existing systems for compatibility with new business needs and technologies;
- evaluate data quality so as to decide if data cleansing is needed;
- evaluate data processing systems for reporting capability;
- map data component;
- create a data warehouse to store data and a history database;
- develop an enterprise wide risk database accessible throughout a single interface;
- develop an application to assist the calculation of estimations per model chosen;
- policy and procedures adjustments;
- parallel run of existing and new approaches;
- set up of a transition period.

The "Control Objectives for Information and related Technology" – COBIT framework, issued by the IT Governance Institute (ITGI 2007b), is a comprehensive framework for the management of IT risk and control, which provides a set of IT processes and controls suited to address the Basel II requirements related to information risk management. COBIT has a business orientation, linking business goals to IT goals, providing metrics and maturity models for their accomplishment and identifying accountability for business and IT process owners. COBIT may assist in defining a standardized control environment by stating the applicable control processes.

As previously mentioned, Basel II has defined ten principles for the management of supervision of operational risk. COSO ERM framework divided the internal control system in eight components, and COBIT has four domains. Figure 1 shows the mapping relationship between the Basel II principles, COSO components and

the specific COBIT domains. As shown in the figure, many COBIT processes have relationship with more than one Basel II principle, due to the nature of general IT control. This multiple relationship expresses the importance of IT controls for a reliable internal control system. It should be mentioned that COBIT provides a set of security related control activities and key risk indicators, however it does not always provide the detailed tools, and therefore professional judgment is necessary.

Figure 1. **Mapping of Basel II principles with COSO ERM and COBIT Frameworks**



Source*:* ITGI, 2007a: 78

CONCLUSIONS

The key message of Basel II or of the upcoming Basel III, is that the capital charge is risk sensitive. Basel Accord forces banks to adopt best practices and align the business with the changing market. The benefits include better market evaluation, lower cost of liabilities, and reduction in provisioning requirements, which all lead to a competitive advantage.

Risk management is not only the job of top management; it is part of every manager's job and should be part of the organizational culture. A successful approach towards managing risk is to understand it, develop the proper methods to measure and control it and to establish accountability.

The risk management requirements of Basel II and Basel III have a significant impact on the IT processes of the banks. Moreover, the information systems related components such as applications, infrastructure and controls are all defined as part of the operational risk. Therefore the IT risk management became an important part of the overall risk management strategy.

The IT Governance Institute and other distinguished publications recommend the mapping of the Basel principles for operational risks against the IT risks, in an effort to support and control them. As such, banks use GRC frameworks to integrate the IT risks within the overall corporate risk management process. However, the frameworks implementation means and the human factor give the trustworthiness and quality of such a risk mapping process.

REFERENCES

BIS (Bank for International Settlements, Basel Committee on Banking Supervision) (2012) "Basel III liquidity standard and strategy for assessing implementation of standards endorsed by Group of Governors and Heads of Supervision", available on line at www.bis.org/press/p120108.htm

BIS (Bank for International Settlements, Basel Committee on Banking Supervision) (2010) "Basel III: International framework for liquidity risk measurement, standards and monitoring", available on line at http://www.bis.org/publ/bcbs188.htm

BIS (Bank for International Settlements, Basel Committee on Banking Supervision (2006) "International Convergence of Capital Measurement and Capital Standards, A revised Framework", available on line at www.bis.org/ publ/bcbs128.htm

BIS (Bank for International Settlements, Basel Committee on Banking Supervision (2003) "Sound Practices for the Management and Supervision of Operational Risk", available on line at www.bis.org/publ/bcbs96.pdf?noframes=1

Chorafas, D. (2001) *Managing Operational Risk – Risk reduction strategies for investment and commercial banks*, Euromoney Books

Gheorghe, M. & Tamaş, I. & Băbeanu, D. (2008) "IT Risks Assessment in Management Information Systems Audit", *Journal of Accounting and Management Information Systems*, Supplement: 684-693

Guldentops, E. (2004) "The IT Dimension of Basel II", *Information Systems Control Journal,* vol. 6: 13- 15

Holmquist, J.(2007) "Implementation of Basel II: Challenges & Opportunities", presentation materials, Institute of International Bankers

IFAC (International Federation of Accountants) (2004) "Enterprise Governance – Getting the Balance Right", available on-line at www.ifac.org/publications-resources/enterprise-governance-getting-balance-right

ISACA (Information Systems Audit and Control Association) (2009a) "The Risk IT Framework", Printed in the United States of America

ISACA (Information Systems Audit and Control Association) (2009b) "The Risk IT Practitioner Guide", Printed in the United States of America

ISACA (Information Systems Audit and Control Association) (2011) "CISA Review Manual", Printed in the United States of America

ITGI (IT Governance Institute) (2005) "Information Risks: Whose Business Are They?", Printed in the United States of America

ITGI (IT Governance Institute) (2007a) "IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance", Printed in the United States of America

ITGI (2007b) "COBIT 4.1", Printed in the United States of America

Lubbe, I. & Snyman, F. (2010) "The advanced measurement approach for banks", *IFC Bulletin no. 33*: 141-149

Micallef, M. (2008) "The New World of Risk-based Regulation - Part 2", *Information Systems Control Journal*, vol.1: 52-56

Năstase, P., Stanciu, V., Năstase, F., Gheorghe, M., Boldeanu, D., Eden, A., Popescu, Ghe., Băbeanu, D. & Gavrilă, A. (2007) *Auditul şi Controlul Sistemelor Informaţionale*, Editura Economică

NBR (National Bank of Romania) and Romanian National Securities Commission regulations (2012) available at http://www.bnr.ro/Reglementari-BNR

RNSC (Romanian National Securities Commission regulations) (2012), available on-line at www.cnvm.ro

RBA (Romanian Banking Association) (2009) "Acord de capital Basel II", http://www.arb.ro/proiecte.php?id=3&c=Aplicarea-prevederilor-noului-acord-de-capital---Basel-II

Societe Generale (2009) "Summary of the Commital Order", available on line at http://www.societegenerale.com/sites/default/files/documents/Summary_of_the_committal_order.pdf

Stanciu, V. & Eden, A. (2008) "Auditing Operational Risk and Security in Banking Institutions", *Journal of Accounting and Management Information Systems*, Supplement: 532 - 536

Unchiaşu, S. (2009) "Information Controls for Basel II Compliance", *Proceedings of the 4th International Conference Accounting and Management Information Systems* - AMIS 2009