# Using CobiT Methodology in Information System Auditing: Evidences from measuring the level of Operational Risks in Credit Institutions

MARIO SPREMIĆ, Ph.D., Full Professor
MARIJANA IVANOV, Ph.D. Full Professor
BOŽIDAR JAKOVIĆ, M.Sc. Assistant

Faculty of Economics and Business Zagreb, University of Zagreb
Kennedy's sq 6, 10000 Zagreb, CROATIA
e-mail: mspremic@efzg.hr; mivanov@efzg.hr; bjakovic@efzg.hr

*Abstract:*
In this paper we stressed the importance of managing the operational risks in credit institutions by conducting regular information system (IS) audits. Information system audit (IS audit) represents a wide range of audit, managerial, analytical and technological activities with the main objective of thoroughly reviewing the effectiveness of control procedures in various parts of IS, conducting analytical tests and collecting evidences which helps in evaluating the level of operational risks and, finally, recommending company's Board's the corrective counter-measures to lower the unacceptable operational risks. External (CobiT methodology) and especially national regulation framework for conducting IS audits in the Republic of Croatia are explained and analyzed in further details. Also, the methodology for conducting IS auditing is presented and maturity levels explained (5 point scale system with a qualitative marks which range from completely unsatisfactory to completely satisfactory). The results of assessing the level of operational risks in credit institutions in the Republic of Croatia which arises from external IS auditing activities in 2010 were depicted (11 credit institutions satisfactory manage the level of operational risk, 18 partially satisfactory and 2 partially unsatisfactory). Upon the long-lasting (3 years) in-depth case study analysis, we investigate in further details if the practice of managing operational risks in a small credit institution is improving by conducting regular IS audits and obeying to regulatory framework.

*Key-Words:* Information System Audit, IT Governance, IS Maturity, Operational Risk, CobiT

## 1. Introduction

Main objective of this paper is to stress the necessity for measuring the level of various risks the companies are exposed to in financial sector. We particularly focused on methods and frameworks for measuring and managing the level of operational risks in credit institutions. In recent years it became apparent that, if not managed properly, operational risks can make serious negative impact on businesses in financial sector. The operational risk includes the risk of losses resulting from inadequate internal processes including inadequate information system and supported technology in conducting business transactions. For example, any disruption of conducting financial transactions can have direct (losses in revenues) and indirect (reputation risk) negative impact on organizations.

As financial transactions are conducted by support of modern information technology (IT) and information systems (IS), it is clear that risks associated with their usage can't any more be treated as 'technical' (low level) risks, but as 'business' (strategic risks) which needs holistic managerial approach. Gartner [4] stands on that point that IT related risks (operational risks) should be treated as business (strategic) risks and that IT Governance (or rather continuous control monitoring) procedures should be in place to effectively manage it. They report that operational risk acceptance more-properly belongs with the business "owners" of the information assets and business processes.

IT Governance as a relatively new concept introduced in the late 1990s, has gained importance in the 21st century due to well-known collapses (Enron Inc, WorldCom, Parmalat, etc.) and the need for a better reporting and financial disclosure system [10]. International and national regulatory provisions (for example, Sarbanes-Oxley act) helped in understanding control mechanisms in modern IS/IT environment and resulted in further impetus for IT Governance issues world-wide [10]. The primary focus of IT governance is on the responsibility of the board and executive management to control formulation and the implementation of IS strategy, to ensure the alignment of IS and business, to identify metrics for measuring business value of IS and to manage IS related risks in an effective way [13].

ISBN: 978-1-61804-066-4

In this paper we stress the importance of conducting regular information system audit (IS audit) by which the level of operational risks may be assessed. Regulatory framework for conducting IS auditing in credit institutions in the Republic Croatia is explained and discussed, with a detailed analysis of its implications on a sampled credit institution.

## 2. Managing Risks in Credit Institutions

Banks and other credit institutions face a number of risks in their everyday business activities. The credit risk means a possibility that bank borrowers or other counterparties will fail to meet its obligations in accordance with agreed terms. It includes the potential losses arising from credit-sensitive types of bank claims such as loans and debt securities.

The liquidity risk is the possibility that a given securities or other forms of the bank's asset cannot be traded quickly enough in the market to prevent a loss or make the required profit.

Market risks include different types of risks connected with a fall in value of bank portfolio due to changes of interest rates, exchange rates or stock prices on financial markets.

The reputation risk is the possibility of experiencing harms or losses due to negative public perceptions of the particular institution due to which existing and future new business relationships with clients, counterparties, shareholders and investors can be called into question.

The operational risk includes the risk of losses resulting from inadequate internal processes including inadequate information system support for conducting business transactions. There are a lot of operational risk events which can result in a misstatement of bank's risk profile, and expose the institution to significant losses or a reputation risk. In the *Sound Practices for the Management and Supervision of Operational Risk (2003), the* Basel Committee on Banking Supervision has emphasized several typical examples of such events. More detailed they include:

- *Internal frauds* in the forms of an intentional misreporting of positions, employee theft for own account, embezzlement of money for the name of other person, hazardous trading on an employee's own account, conducting the financial transactions against the internal or external regulatory frameworks, insider trading of a corporation's stock or other securities;
- *Misuse and failures in business activities* including a misuse of confidential customer information, improper trading activities on the bank's account, money laundering, financing of terrorism or other forms of crime activities, sale of unauthorized products, tax evasion, issuing and payment of demand drafts over the prescribed limits, failures to meet regulatory requirements;
- *External frauds* like robbery, forgery, cheque kiting, and damage from computer hacking;
- *The negative selection in employment policies and failures in organization of workplace safety* including the violation of employee health and safety rules, discrimination claims etc.;
- *Damages to physical assets* caused by terrorism, vandalism, earthquakes, fires, floods or other forms of environment risks;
- *Business disruptions* like system failures of hardware and software, telecommunication problems, and utility outages;
- *Troubles in execution, delivery and process management* including data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty mis-performance, and vendor disputes.

## 3. Literature Review on Information System Auditing and Assessing The Level of Operational Risks

Information system audit (IS audit) mainly refer to truly analytical part of IT Governance by which the level of IS performance can be measured and IS maturity assessed [9]. IS audit represents a wide range of audit, managerial, analytical and technological activities with the main objective of thoroughly reviewing the effectiveness of control procedures in various parts of IS, conducting analytical tests and collecting evidences which helps in evaluating the level of operational risks and, finally, recommending company's Board's the corrective counter-measures to lower the unacceptable operational risks.

Caldwell [1] reports that enterprise IT security professionals face a complex, even paradoxical situation as the worldwide economic crisis continues. In a period of highly constrained financial and staffing resources, they must manage and mitigate a rapidly changing and expanding risk environment and respond to expanding regulatory and other legally relevant requirements. Dameri [3] analyses the benefits of IS compliance preferably through IT Governance role. Mashour and Zaatreh [9] investigate and validate the positive impact effective IS may have at Jordan Banks. The institute of internal auditors (IIA) [7] issued the guidelines for assessment of IT risk (GAIT) and

ISBN: 978-1-61804-066-4

reported that applying a standard methodology will assist the auditor to focus on what is truly important to meeting the compliance objectives and minimizing operational risk to the organization. Gartner [4] concludes that there is no standard that covers every area of IT Governance and IS audit with many overlapping areas. Singleton [12] argues about the model of IT sophistication according to regulatory provisions and aggregates minimum IT controls composed with IT governance concept to mitigate risks in financial reporting and enhance regulatory compliance. Singleton [11] also states that 'it is becoming increasingly necessary to test more IT controls due to Sarbanes-Oxley requirements, the American Institute of Certified Public Accountants (AICPA)'s Risk Suite requirements and increased reliance on IT controls'.
We can conclude that there are very few evidences in literature review on investigating how IS auditing regulation provisions may help in managing operational risk, so we tried to fill that research gap by questioning its usage and effectiveness.

In following chapters an IS auditing regulatory framework will be explained and analyzed, especially national regulations in the Republic of Croatia. We will investigate if national regulatory provisions in IS auditing help improving IT Governance and operational risk management procedures.

# 4. Regulatory Frameworks in IT Governance and IS Auditing Domain

Main objective of IS auditing activities is to review the company's control procedures associated to IS, collect analytical evidences about possible misuse, evaluate the level of operational risks for different control areas and suggest to company executives corrective control counter-measures. This in particular mean that by engaging in IS auditing companies can periodically measure the IT Governance performance and IS maturity using the world-wide and/or national regulatory framework and well-proved, world-wide frameworks or methods such as CobiT, Risk IT, ITIL, ISO 27001, etc. Such tendencies are mostly motivated by specific regulatory pressures (for example, Sarbanes-Oxley act, Basel II framework, etc.), rather than by IT value-added initiatives.

IT Governance and IS auditing are partly driven by the external regulatory demands like Sarbanes-Oxley act, Basel II, the European 8th Directive and MiFID. Companies operating on multinational markets have to comply with several legal regulations created by public laws on national or international level. For instance, the Sarbanes-Oxley Act (SOX) in the USA and Basel II (the current version is "Basel III") in Europe. "New Capital Accord", also known as Basel II, is a set of recommendations issued by "The Basel Committee on Banking Supervision" regulating the adequacy of banks' capital in relation to risk exposure. Basel II provisions apply to internationally active banks in G10 countries. The European Union adopted a Directive (CAD3) rendering the provisions of the Accord compulsory for all banks in EU member countries by 2007. The Accord deals with requirements for the bank's information system as a part of the operational risk as a whole only through IT Governance principles considering that it is not possible to set strict rules on account of rapid technological changes and differences between banks. The Committee emphasizes the importance of reliability of the IS, particularly in terms of information security and system availability. This means that the stipulations of the Accord have provided banks with great freedom in deciding on the measures for reducing operational risk posed by implementation of IS/IT, but on the same time dictated banks that certain IT Governance activities should be put in practice in order to be compliant.
In recent years various groups have developed world-wide known IT Governance best practices and frameworks to assist management in managing operational risks and measuring the maturity of IS, such as *CobiT, ITIL* or *IT BSC* (IT Balanced Scorecard).

## 4.1. Cobit methodology for conducting IS audits

CobiT (Control Objectives for Information and related Technology) is the widely accepted IT Governance framework organized by key IT control objectives, which are broken into detailed IT controls. Current version 4.1 of CobiT (with a CobiT 5.0 version due in January 2012) divides IT into four key domains which are broken into 34 key IT processes, and then further divided into more than 300 detailed IT control objectives. Developed by ISACA (Information System Audit and Control Association, www.isaca.org) and ITGI [8] (IT Governance Institute, www.itgi.org), CobiT is the widely accepted, an 'umbrella' framework, for implementing IT Governance policies and procedures and for conducting IS auditing. It is a broad and comprehensive de-facto standard which comprises all activities, processes and services which can help companies manage the level of operational (IS/IT related) risks.

ISBN: 978-1-61804-066-4

# 5. National Regulations on IT Governance and IS Auditing in the Republic of Croatia

In the Republic of Croatia the regulatory framework for IS auditing was prescribed by Croatian National Bank (CNB). The main objective of the obligatory regulations is to effectively manage the level of operational risks, namely IS/IT associated risk in credit institutions (banks, etc.). The 'Act about credit institutions' and the 'Decision on adequate information system management' are the cornerstones of the IT governance regulation that obliged every credit institution to perform internal and especially external IS auditing (assessment of operational risks) and to prepare a report for the regulator as well as for company's Board. The regulation itself is CobiT based and concerned to a framework and scope of evaluating the maturity of using IS/IT.

Regulatory framework prescribed the 11 areas and 40 articles which define the scope of information system audit in the credit institutions in Croatia. These areas are as follows:

1. IS security management,
2. IS risk and incident management,
3. User access rights and password management
4. Computer network management and malicious code protection
5. IT outsourcing risk management and third party level agreements
6. IS asset management and physical security management
7. Change management and IS development
8. Business continuity management
9. Back-up, operational and system records
10. Test of IS/IT control procedures in key business processes (payment processing)
11. Implementation of internal act related to IS/IT.

According to the regulatory framework, the Board of every credit institution in Croatia is responsible for mitigating operational risks associated to every single area and to effectively manage the level of the acceptable IS/IT risk. Some detailed and precise regulatory responsibilities include:

- to nominate the member of the Board who is responsible for managing and controlling IS,
- to adopt internal acts for the IT governance and define responsibilities for their supervision,
- to define the criteria and methods for notifying the management and supervisory boards of the relevant facts related to the IS functionality and security,
- to define IS strategy,
- to define clear responsibilities for managing IS,
- to nominate the autonomous CISO function (Chief Information Security Officer),
- to nominate the IT Steering Committee,
- to define the IS risk management methodology,
- management board shall be responsible for establishing the acceptable level of risk to which the IS is exposed (operational risk),
- to classify and protect information,
- to establish the system of user access rights management, comprising the registration, authorisation, identification, authentication and supervision of user access rights,
- changes in the IS's software components need to be recorded and documented in order of occurrence, together with the time of their occurrence,
- Board is responsible to establish the process of business continuity planning (BCP),
- Board is responsible for establishing the process of data recovery which will be stored on the alternative location.

## 5.1. Methodology for Conducting IS Auditing

In Republic of Croatia every single credit institution is obliged to conduct external and internal IS audits with the objective of measuring the level of operational risks. Internal and external IS auditing are conducted according to framework explained in previous chapter. Every single external IS audit should result in comprehensive report which IS auditors are to present to credit institution's Board. Main areas of external IS audit reports are:

- explanation of IS audit methodology and methods for measuring the level of operational risks,
- scope of IS audits (IS control areas and objectives are depending on IS audit assignment)
- results of detailed and thorough review of IS control procedures in chosen audit areas,
- assessment of the level of operational risk for every audit area, with the recommendations to the Board for corrective measures,
- Board's response to IS audits findings,
- summary and review of IS audit documentation.

IS auditors needs to get full and in-depth understanding of control procedures in key business processes and there IS/IT support. As stressed in previous chapters, main objective of IS auditing is to thoroughly review the effectiveness of control procedures in various parts of IS in credit institutions, to measure the level of operational risks and to recommend the corrective measures to Board members. This in particular means that IS auditors need to examine and review the large

ISBN: 978-1-61804-066-4

number of controls inside IS, conduct massive analytical tests (for example, penetration test of computer network, business continuity and disaster recovery tests, test of IS users logical access rights, etc.), collect a number of audit evidences, assess the level of operational risk and prepare the comprehensive IS audit report.
Every single audit area should be thoroughly reviewed with the objective of gathering enough audit evidences which will enable IS auditors to evaluate the efficiency of control procedures. For example, typical key business processes in credit institutions whose IS support needs to be evaluated are:

- Corporate and retail deposits,
- Corporate and retail loans,
- Treasury process,
- Risk management process,
- Payment processing,
- Financial statement close process.

The maturity level of IS management procedures in all 11 audit areas are regularly based on interviews, testing procedures and comprehensive reviews. Maturity levels for all audit areas can be based on CobiT metrics:
0 – Non-existent IS maturity and/or IS control procedures,
1 – Ad hoc / initial IS maturity and/or IS control procedures,
2 – Repeatable but intuitive IS control procedures,
3 – Defined process for IS control procedures,
4 – Managed and measureable IS control procedures,
5 – Optimised IS maturity and/or IS control procedures.

The IS audit report need to be presented to and agreed with the credit institution's Board, while the copy of the report needs to be forwarded to regulatory body (Croatian National Bank and their supervisory units).

### 5.2. The Results of Continuous Quality Control Processes over IS Auditing Reports

Croatian National Bank monitors the whole process, fosters credit institutions to implement IS auditors' recommendation and secure the quality of IS audits. By CNB regulations external IS auditors have to evaluate the maturity of IT Governance practices with following qualitative marks:

- completely unsatisfactory,
- partially unsatisfactory,
- partially satisfactory,
- satisfactory and
- completely satisfactory.

External IS auditors have to present their comprehensive report to bank's Board and CNB authorities. CNB performs quality assurance on these reports and may refuse it and penalize authors while bank's Board have to make formal response to the IS auditors findings. CNB monitors the IS audits and fosters credit institutions to implement IS auditors' recommendation. The assessed level of operational risks in credit institutions in the Republic of Croatia which arises from external IS auditing activities in 2010 were as follows:

- 11 credit institutions **satisfactory** manage the level of operational risk,
- 18 credit institutions **partially satisfactory** manage the level of operational risk and
- 2 credit institutions partially **unsatisfactory** manage the level of operational risk.

Upon the results of external IS audits and according to their internal plan, CNB supervisory unit conduct 'on-site' IS supervisions in which they thoroughly audits the IS of specific credit institutions and give recommendations which credit institutions are lawfully obliged to implement, or they will be fined.
On the other hand, if they do not meet prescribed quality standards, CNB can refuse external IS audit report and mandate the credit institution to, on its additional expense, hire another company to do repeated external IS audit, which is a good mechanisms for regulating and monitoring the IS auditing services and foster quality standards.

## 6. Conclusion

Main objective of this paper was to stress the importance of prescribing IS auditing regulatory framework which helps credit institutions manage the level of operational risk. After analyzing IT Governance and IS auditing terms, we explained external and especially national regulation framework in the Republic of Croatia and present the methodology of conducting IS auditing.
As mentioned in chapter 5. Croatian National Bank (CNB) prescribed IS auditing regulatory framework ('Decision on adequate information system management') upon which regular external and internal IS audits are obligatory for every single credit institution operating in the Republic of Croatia. By this regulation the IT Governance performance (maturity) levels are prescribed (completely unsatisfactory, partially unsatisfactory, partially satisfactory, satisfactory and completely satisfactory).
In 2010 there were only two credit institutions with partially unsatisfactory mechanisms for managing operational risks. The assessed level of operational risks

is associated with the partially unsatisfactory maturity of IS control procedures, which arises from thorough and serious IS audits according to regulatory provisions and world-wide best accepted methodologies (such as CobiT).

We investigate in further details the IT Governance practice in one of the two credit institutions which are partially unsatisfactory managing operational risk. In this small credit institution CIO (Chief Information Officer) reports directly to member of the Board responsible for IS, they have proper IS strategy, autonomous CISO function who reports directly to Supervisory Board, there are a number of cross-functional organizational units who helps to manage IS function (such as IT Steering Committee, Business Continuity Board, IT Change Management Committee). In recent year they prescribe BCP and conduct massive efforts to properly control IS function and associated operational risks.

As mentioned in previous chapters, the main objective of conducting external IS auditing is to assess the level of operational risks, or, in other words, to assess the level of IS Maturity. One can do so by using world-wide accepted standard methodology such as CobiT. CobiT based IS maturity marks for selected small credit institution (scale from 0 to 5) were as follows:

- In a year 2008. - 1.9;
- In a year 2009. - 2.1;
- In a year 2010. - 2.2.

Even the improvement in IS Maturity and IT Governance activities is evident (CobiT is very rigorous methodology), partially unsatisfactory level of managing operational risk stands due to the fact that there still are insufficient control procedures in some key areas of IT Governance (such as BCP, information security, computer network access, IS/IT outsourcing, etc.). On the hand, the bank's management has the clear vision and enough funds to fulfill IS auditor's recommendations and hope for satisfactory level of managing operational risks in 2011.

After explaining the IS auditing regulatory framework in the Republic of Croatia, by presenting the practice of monitoring the quality of IS audits and by conducting long-lasting (3 year) dedicated in-depth interviews in a small bank, we come up to a conclusion that national IS Auditing regulatory framework can help in improving operational risk management practice. The research might be useful because of fact that similar efforts are very rare (if there are any of them) and there are modest evidences how industry best practices and national regulations are used in the real business environment.

*References:*


[1.] Caldwell, F. (2009): Selecting and Applying GRC Frameworks and Standards, Gartner Symposium ITExpo, October 2009, Orlando.

[2.] Champlain, J.J. (2003): Auditing Information Systems, 2nd ed. John Wiley & Sons, SAD.

[3.] Dameri, R.P., (2009): Improving the Benefits of IT Compliance Using Enterprise Management Information Systems, The Electronic Journal Information Systems Evaluation, Volume 12, Issue 1, 2009, pp. 27-38.

[4.] Gartner (2010): Magic Quadrant for Continuous Controls Monitoring, March 2010, Gartner Inc.

[5.] Guldentrops, E. (2004): The IT Dimension of Basel II, *Information System Control Journal*, Volume 6.

[6.] Hunton, J.E., Bryant, S.M., Bagranoff, N.A.: (2004): Core Concepts of Information Technology Auditing, John Wiley &Sons Inc., SAD.

[7.] Institute of Internal Auditors IIA (2008): Case Studies of using GAIT for business and IT Risk to scope PCI compliance, IIA Advanced Technology Committee.

[8.] ITGI (2007): *CobiT 4.1. Framework, Control Objectives and Maturity Models,* IT Governance Institute, Rolling Meadows, Illinois, SAD

[9.] Mashour, A., Zaatreh, Z. (2008): A Framework for Evaluating Effectiveness of Information systems at Jordan Banks: An Empirical Study, Jorunal of Internet Banking & Commerce, April 2008, Vol 13, Num. 1.

[10.] Nicho, M., Cusack, B. (2007): A Metrics Generation Model for Measuring the Contr ol Objectives of Information Systems Audit, Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07), Hawaii, IEEE, January, 2007.

[11.] Singleton, T. (2008): What every IT Auditor Should Know About Access Controls, Information System Control Journal, Vol. 4, ISACA.

[12.] Singleton, T. (2010): The Minimum IT Controls to Assess in a Financial Audit, ISACA Journal, Vol. 2, ISACA.

[13.] Spremić, M. (2009): IT Governance Mechanisms in Managing IT Business Value, *WSEAS Transactions on Information Science and Applications*, Issue 6, Volume 6, June 2009, pp. 906-915

[14.] Spremić, M., Popović, M. (2008): Emerging issues in IT Governance: implementing the corporate IT risks management model, *WSEAS Transaction on Systems*, Issue 3, Volume 7, March 2008, pp. 219-228.

[15.] Weill, P., Ross, J.W., (2004): IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press, 2004.