Measuring IT Governance Performance: a Research Study on CobiT- Based Regulation Framework Usage

Mario Spremic, Ph.D., CGEIT, Full Professor

***Abstract*—**After explaining the Information Technology (IT) governance concept and external and national regulation, in this paper we investigate if the prescribed regulatory requirements and regular information system (IS) audits affect the IT Governance initiatives and foster strategic business/IT alignment. External and especially national IT Governance regulation framework in the Republic of Croatia was explained in further details. We constructed the research model around IT Governance components and conducted the research by the series of long-lasting comprehensive in-depth interviews with responsible employees. On the sample of selected Croatian small banks, the organizational position and the role of IT in the business has been investigated, while specific research interest was to get the clear view of the maturity level of IT usage. We hoped that such approach could be useful when trying to answer the posed research question: can national IT Governance regulatory framework help to start to measure IT Governance maturity and are such initiatives helpful in aligning IT and business?

***Keywords*—**IT Governance Performance, IT Maturity, IT Audit, Croatia, CobiT

I. INTRODUCTION

In the early days of implementing IT in the business, it was often seen as a technical support function and was typically managed by finance departments. When evolving from technology providers into strategic partners, IT organizations typically follow a three-stage approach: IT infrastructure management, IT service management and IT business value management (IT Governance) [9]. As the IT initiatives has become far more than a means of improving efficiency and reducing costs and increasingly account for enabler of business innovation, it still seems that it is less understood business resource. One of reason could be that often there is no systematically way of measuring IT performances and implementing IT Governance practices. In this paper we investigated how regulatory framework can affect the level of IT Governance performance and foster measuring IT performance by using world-wide best IT maturity models.

Author is with the University of Zagreb, Faculty of Economics and Business, Department of Informatics, Kennedyev trg 6, 1000 Zagreb, CROATIA (phone: +38512383278; fax: +38512335633; e-mail: mspremic@efzg.hr).

Main objective of this paper is to stress the importance of evolving IT Governance activities.

On the sample of selected Croatian banks and in a form of detailed in-depth interviews with responsible experts (CIOs and Board members), the IT Governance issues were discussed, the organizational position and the role of IT in the business has been investigated, while specific research interest was to get the clear view of the maturity level of IT usage. We hoped that such approach could be useful when trying to answer the posed research question: can national IT Governance regulatory framework help to start to measure IT Governance maturity and are such initiatives helpful in aligning IT and business?

II. KEY IT GOVERNANCE CONCEPTS – LITERATURE REVIEW

IT Governance which was a relatively new concept 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 [7]. 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 [7].

A good theoretical path to IT Governance issues could be found in IT Strategy and IT/Business Alignment literature. Venkatraman [15], for example, illustrates the changes that occur in the perceived contribution of IT by the business during the transformation from Service Provider to Strategic Partner as presented in Table 1.

Table 1: IT as Service provider or as Strategic partner

Service provider	Strategic partner
• IT is for efficiency • Budgets are driven by external benchmarks • IT is separable from the business • IT is seen as an expense to control • IT managers are technical experts	• IT for business growth • Budgets are driven by business strategy • IT is inseparable from the business • IT is seen as an investment to manage • IT managers are business problem solvers

Van Grembergen [14], [15] stands on that point, by pointing out what strategic potential IT initiatives could have if managed (or rather 'governed') properly. When engaging in those changes, IT becomes not only a success factor for survival and prosperity, but also an opportunity for differentiation and achieving competitive advantage. Hunton [4] stress the control focus of IT Governance by defining it as the process for controlling an organization's IT resources, including information and communication systems and technology. Nolan and McFarlan [8] recently stress that 'a lack of board oversight for IT activities is dangerous; it puts the firm at risk in the same way that failing to audit its books would'. Spremic [10] also stressed IT risk management issues as a key part of holistic IT Governance approach. Weill and Ross [16] indicate the performance potential by reporting that companies with effective IT Governance have profits that are 20% higher than other companies pursuing similar strategies. IT Governance Institute [5] focused on the strategic nature of IT governance as well and define it as the responsibility of executives and board of directors, and consists of leadership, organizational structures and processes that ensure that enterprise's IT sustains and extends the organization's strategies and objectives. Van Grembergen [15] stands on that point and defined IT Governance as the organizational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT.

The IT governance relates to IT practices of boards and senior managers. The primary focus of IT governance is on the responsibility of the board and executive management to control formulation and the implementation of IT strategy, to ensure the alignment of IT and business, to identify metrics for measuring business value of IT and to manage IT risks in an effective way (Spremic, [9]).

Figure 1. shows a clear difference between IT governance and IT management. While IT management is mainly focused on the daily effective and efficient supply of IT services and IT operations, IT governance is much broader concept which focuses on performing and transforming IT to meet present and future demands of business and the business' customers. This in particular means that executive management members and corporate governance organizations bodies need to take responsibility for governing IT, which makes IT Governance a key executive function.

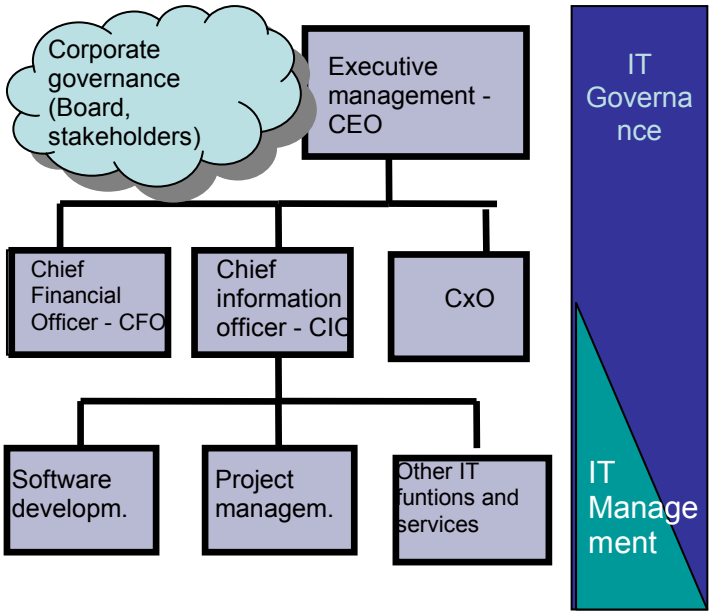

Figure 1. Difference between IT Governance and IT management

III. CONSTRUCTING IT GOVERNANCE COMPONENTS

Having defined IT Governance, it is necessary to understand its most important elements. The IT Governance Institute suggests that fundamentally, IT Governance is concerned about two things [13]:

- IT should deliver value to the business and
- IT risks need to be mitigated.

This leads to the five main focus areas of the IT Governance, all driven by stakeholder value. Two of them are outcomes: value delivery and risk mitigation. Two of them are drivers: strategic alignment and performance measurements. The remaining one refers to IT resource issues. While value delivery is focused on the creation of business value, risk management is focused on the preservation of business value [15].

IT Governance Institute (ITGI) and their partner institution ISACA (Information System Audit and Control Association) stands on that point by proposing that IT Governance should consist of five different components namely [5]:

1. **Business/IT strategic alignment** (IT Governance procedures should ensure linkages of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.
2. **IT value creation and delivery** (ensuring that IT delivers the promised benefits against the strategy).
3. **IT Risk management and/or value preservation** (embedding of IT risk management responsibilities into the organisation, IT risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for IT risk).

4. **Performance measurement in IT** (tracks and monitors IT strategy implementation, IT project completion, resource usage, process performance and service delivery).
5. **IT resource management** (optimal investment in, and the proper management of critical IT resources: applications, information, infrastructure and people).

As shown in Figure 2., IT Governance represent the necessary 'connections' of strategic visions (IT Strategy and IT/Business Alignment initiatives) and the results of their implementation by performing periodic IT Audits with which IT performances could be measured, IT risk identified and IT controls put in place.

Figure 2: IT Governance Components [6]

A. IS auditing as an analytical tool for measuring IT Governance performance

Measuring performance of information systems is a relatively new concept. Although companies are investing heavily in IS and related IT, little attention has been paid to determine formal metrics of IS and IT governance performance.

Information system audit (IT audit) mainly refer to truly analytical part of IT Governance by which the level of IS performance can be measured and information system quality (IS quality) assessed (Spremic, [9]). IS quality is a relative category which measures the current performance of the information system with ideal or required one. The more discrepancy of the actual performance of the information system to ideal (required) one, the system is of less quality and vice-versa. The required level of quality may be defined by regulation frameworks or some business oriented quality criteria should be determined [10].

Actual level of IS quality need to be periodically reviewed by the systematic control activities and the level of its quality is assessed by IT audit. When conducting internal IS control activities companies engage in internal IS audit, while external IS auditing refers to auditing activities performed by external authority (specialised audit company, regulation authority such central bank).

In addition to the term of *information systems auditing*, the term such as *information technology auditing (IT Audit)* is often used. Regardless of different terms being used, main objectives of the information systems audit are:

- to systematically, thoroughly, and carefully examine the IT controls within the business processes that are supported by information systems,
- to identify weak risk areas and to assess the IT related risk level,
- to measure the overall IT performance according to the business requirements
- to warn about possible omissions and risks, and thus examine the quality of the company's information system.

IT auditing is a new profession that extends the concept of control in the form of quality assurance, benchmarking and measurement and it can be also used to implement IT governance [10].

The primary goals of the IT audit are to [12]:

- identify the key business processes that depend on IT or IS,
- to systematically and carefully examine their controls efficiency,
- to identify key risk areas and constantly measure the risk level,
- to warn about possible failures, and
- to offer suggestions to the executive management how to improve current IT risk management practices.

This in particular mean that by engaging in IS auditing companies can periodically measure the IT Governance performance using the 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.

IV. REGULATORY FRAMEWORKS IN IT GOVERNANCE DOMAIN

IT Governance is 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 information system, 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 risk posed by implementation of 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 measuring the maturity of IT. Contemporary IT Governance frameworks are:

- *CobiT* (Control Objectives for Information and related Technology),
- *ISO 27000 'family'* (ISO 27001:2005, ISO 27002:2005),
- *ITIL* (IT Infrastructure Library), or
- IT BSC (IT Balanced Scorecard)

A. CobiT

While ISO 27000 family refers mainly to information security risks issues and surely can't be treated as a comprehensive IT Governance 'tool' (rather as a leading information security norm), 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 divides IT into four domains (Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate), which are broken into 34 key IT processes, and then further divided into more than 300 detailed IT control objectives. ISACA and ITGI [6] defines COBIT as a comprehensive set of resources that contains all the information organizations need to adopt an IT governance and control framework. COBIT provides good practices across a domain and process framework in a manageable and logical structure to help optimize IT-enabled investments and ensure IT is successful in delivering against business requirements. COBIT contributes to enterprise needs by:

- Making a measurable link between the business requirements and IT goals
- Organizing IT activities into a generally accepted process model
- Identifying the major IT resources to be leveraged
- Defining the management control objectives to be considered
- Providing tools for management:
  - Goals and metrics to enable IT performance to be measured.
  - Maturity models to enable process capability to be benchmarked.
  - Responsible, accountable, consulted and informed (RACI) charts to clarify roles and responsibilities.

Developed by ISACA (Information System Audit and Control Association, www.isaca.org) and ITGI (IT Governance Institute, www.itgi.org), CobiT (Control Objective 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 defines:

- performance goals and metrics (for example, RPO, RTO, availability time),
- KRI (Key Risk Indicator), KPI (Key Performance Indicator)
- maturity models (0-5 scale) to assist in benchmarking and decision-making for process improvements,
- a RACI chart identifying who is Responsible, Accountable, Consulted, and/or Informed for specific IT process.

CobiT represent an 'umbrella' framework for implementing IT Governance policies and procedures. It is a broad and comprehensive de-facto standard which comprises all activities, processes and services an IT organization need to manage (or rather govern). Therefore, when engaging in IT Governance activities it is inevitable to use CobiT framework to in details analyze the alignment of current IS and supporting IT infrastructure and business requirements towards it.

If CobiT-based information system audit or any further 'due diligence' come up with the conclusion that an IT organization underperforms in a specific area, an additional project may be opened to assure the compliance and alignment with business requirements. For example:

- ITIL framework may be used to assure better service delivery and service management,
- Val IT framework may be used to assure efficient management of IT investments which may result with additional business value,
- ISO 27000 norm may be used to manage the level of IT security risks,
- Prince 2 and/or PMBOK may be used to bridge the gap in IT project management activities, etc.
- Risk IT framework may be used to help companies manage IT risks.

V. NATIONAL REGULATIONS ON IT GOVERNANCE 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 IT associated risk in credit institutions (namely banks). 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 assessment of IT risks (IS auditing) and to prepare a report for the regulator as well as for company's Board. The regulatory itself is concerned to a framework and scope of evaluating the maturity of using IT. The areas of IT Governance and IS audit are based on CobiT and in line with Basel II requirements and include following areas:

- Framework for IT Governance (IT Governance policy, IS strategy, IT investment plan, IT project management, organizational issues, etc.).
- Information system risk management policy (IT risk management methodology).
- Internal information system auditing.
- Information systems security (IT security policy, logical access to IS, authorisation, operating and system records, incident management).
- Information system maintenance (change management, service providers, outsourcing).
- Business continuity management (policies, disaster recovery plan, data restore and recovery).
- Information system analysis and development and possible outsourcing
- E-banking.

Regulatory framework prescribed the 18 areas and 40 articles which define the scope of every information system audit in the credit institutions in Croatia. These areas are as follows:

1. Managing information system security
2. Managing the risks associated to information systems
3. Managing logical and physical access rights
4. Managing the information systems assets
5. Managing operating and system records
6. Managing back-up and archive
7. Managing the relationships to service providers and outsourcers
8. Managing the relationships to hardware vendors
9. Managing the information system development
10. Managing physical security
11. Managing passwords
12. Configurations management
13. Change management
14. Business Continuity planning
15. Disaster Recovery plan
16. Managing incidents and problems
17. Antivirus policy
18. Documentation and internal acts associated to information systems.

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

- to nominate the member of the Board who is responsible for managing and controlling information system,
- to adopt internal regulations governing the information system management, and define responsibilities for supervising the implementation of these regulations,
- to define the criteria, methods and procedures for notifying the management and supervisory boards of the relevant facts related to the functionality and security of the information system,
- to define information system strategy,
- to define clear and precise responsibilities for managing information system,
- to nominate the autonomous CISO function (Chief Information Security Officer),
- to nominate the IT Steering Committee,
- to define the information system risk management methodology and processes,
- to assess information system risks and to reduce them to acceptable level,
- management board shall be responsible for establishing the acceptable level of risk to which the information system is exposed.
- to classify and protect information,
- internal audit is responsible to conduct information system audits,
- to establish the system of user access rights management, comprising the registration, authorisation, identification, authentication and supervision of user access rights,
- a process of managing the changes in the information system's software components need to be set up (initial versions should be determined, any changes in application software and database environment should be identified and monitored, etc.)
- changes in the information system'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 and management,
- Board is responsible to create the business impact analysis, to accept the business continuity plan, to accept the disaster recovery plan and to test their functionality and effectiveness,
- Board is responsible for establishing appropriate incident management process to ensure a timely and effective response in the event of the violation of security and functionality of the information system

resources supporting the carrying out of the business processes,

- Board is responsible for establishing the process of data recovery which will be stored on the alternative location.

In Croatia, internal and external IS auditing are conducted according to this framework, while Croatian National Bank monitors the whole process and fosters credit institutions to implement IS auditors' recommendation and secure the quality of IS audits. The main objective of such a strong regulation is to strengthen the maturity of IT Governance processes in credit institutions.

By CNB regulations external IS auditors have to evaluate the maturity of IT Governance practices with 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 monitor the IS audits and foster credit institutions to implement IS auditors' recommendation. The main objective of such a strong regulation is to strengthen the maturity of IT Governance processes in credit institutions.

VI. RESEARCH STUDY ON THE IT GOVERNANCE PRACTICES

Very strict and rigorous IT Governance regulations in Croatia may imply that IT Governance procedures are on very mature level in almost all commercial banks operating in the country. In order to be able to answer the posed research questions we decided to conduct a survey followed with a series of comprehensive and in-depth interviews with the key people involved in the IT Governance processes (CIOs and CEOs).

A. Survey instrument

The key objective of the research has been to examine a number of issues regarding IT Governance and therefore we build the research model around 5 different IT Governance components described in chapter 3. The research instrument includes series of in-depth interviews with CIOs and CEOs of selected banks and the research model was constructed around following IT Governance elements:

- do the analyzed companies have IS Strategy aligned with business strategy, IT Steering Committee and IT investment policy (Business/IT strategic alignment focus),
- % of the budget invested in IT (Business/IT strategic alignment focus),
- to whom Chief Information Officer (CIO) reports (IT Risk Management focus)
- do the surveyed companies have IT risk management methodology and policy (IT Risk Management focus)
- do the surveyed companies regularly perform IS audits and measure the IS maturity (Performance measurement focus),
- do the selected companies have Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) (IT Risk Management focus)
- do the surveyed companies have defined metrics to control key IT processes (for example, Recovery Point Objective(RPO) and Recovery Time Objective (RTO) as key metrics for BCP initiatives (Performance measurement focus),
- number of key applications outsourced (IT resource management focus),
- % of the IT staff employed (IT resource management focus), etc.

As all these elements interfere through the IT Governance concepts, we posed the following research questions: can national IT Governance regulatory framework help to start to measure IT Governance maturity and are such initiatives helpful in aligning IT and business?

To address the research's objectives, firstly we draw a survey questionnaire to be able to collect general information about IT Governance practices during years in banks operating in the Republic of Croatia, then we narrow our focus to selected banks around them and finally conduct a series of comprehensive and in-depth interviews with CIOs.

The questionnaire was then sent to CIOs (Chief Information Officers) of small banks operating in the Republic of Croatia. Banks were selected due to very simple reason: the IT Governance regulation described in chapter 5 is obligatory only for banks and credit institution operating in Croatia. Small banks were selected because of fact that there were no questions that large banks with large budgets will be able to meet the regulatory conditions, which is not likely for small ones. The survey has been performed once a year in a period from December 2007 to September 2010 and was conducted by sending questionnaire via e-mail. The survey resulted in important responses which give us the crucial information about the growing maturity of IT Governance initiatives during years. After sending the survey to CIOs every year we pay a visit to 5 selected banks and spent a week or so having in-depth dedicated discussions with CIOs and other responsible employees about IT Governance practices posed in the research model. Such activities are regular IS auditing procedures in which we were engaged.

B. Research Sample

Case study analysis and series of in-depth interviews were performed on a sample of 5 small banks in Croatia during the period 2008-2010. The purpose of the research was to show how regulative body (Croatian National Bank - CNB) and

their regulatory guidelines helped small banks to improve IT Governance practices. All selected banks has from 115 to 150 employees and adequate organizational structure according to its size with IT department as strategic business function directly responsible to CEO and/or Board member responsible for IT. IT departments in all banks typically have three sub-units: application support, system support, business support. Specific functions such as CISO (chief information security manager), internal IS auditor and business continuity manager are extracted from IT department and represent autonomous organizational units.
In bank 1 and bank 3 CEO is the member of the Board responsible for IT, while in other banks this function is controlled by other nominated Board member. All banks have various committees who helps CIO and IT department in IT governance procedures, such as IT Steering Committee (all 5 banks), IT Project Management Committee (bank 3 solely) Business Continuity Board (bank 2 and bank 4), IT Change Management Committee (bank 2 and bank 5).

C. Analyses of research results and the discussion

The analysis of the comprehensive in-depth interviews conducted over the 3 year's time reflects that all the banks in the sample have implemented an IS strategic plan, as a part of overall strategic plan, strengthen the position of CIO as executive manager and nominated the Board member who is responsible for IT. Such results can be explained as direct effect of the regulatory implications because of the fact that results of some comprehensive researches imply that only modest number of Croatian large companies (research have been conducted on a sample of 100 Croatian largest companies) around 46% have proper IS strategy (Spremic, [9]).
Table 2: Selected research results on some IT Governance issues

		CIO respons. to	**CISO respons. to**	**IS internal audit dpt**
Bank 1	**2008**	Board	CIO	No
	2009	Board	Board	Yes
	2010	Board	Board	Yes
Bank 2	**2008**	Board	No CISO	No
	2009	Board	No CISO	No
	2010	Board	Board	Yes
Bank 3	**2008**	CFO	No CISO	No
	2009	Board	Board	No
	2010	Board	Board	Yes
Bank 4	**2008**	Board	Board	No
	2009	Board	Board	Yes
	2010	Board	Board	Yes
Bank 5	**2008**	Board	Board	No
	2009	Board	Board	Yes
	2010	Board	Board	Yes

Table 2 indicates the growing IT Governance maturity on selected set of research criteria. But the IT Governance issues evolve through the years as the banks' Boards realize that they have to improve the current practices to be (stay) competitive as well as to be compliant with regulatory issues. For example, by IT Governance regulations on internal audit was due on 01.01.2009 and stated that internal audit departments are responsible to conduct information system audits (same due time for nominating CISO as an autonomous function outside the IT department).

Also, in the first year of the case study performed (2008), none of the banks did not have a help desk to support IT incidents and problems were handled in in-formal way with no documenting procedures. Rigorous regulations prescribed by CNB resulted in formalizing many procedures and practices (identifying roles and responsibilities within processes, authorizations, logon procedures, outsourcing issues, necessity for archiving system and operating logs, business continuity issues, data recovery procedures, etc.).
Furthermore, majority of the sample banks have approximately 10-14 IT employees (7% to 10% of all bank employees). Discrepancy is noted in one bank (bank 5) which has 19 IT employees (around 15% of all banks employees) due to the fact that they do not use IT outsourcing services in developing and maintaining application for core business processes (they have internal development).

In the first year (2008) of the CNB guidelines and regulation in obligatory usage, in-adequate practice was noted in one out of five banks (bank 3) where CIO was responsible to Chief Finance Officer (CFO) and in three out of five banks (bank 1, 2 and 3) where CISO was responsible to CIO or there was no CISO at all. Also, in the first year of the research conducted (2008), none of the sampled banks had internal IS audit department or had no competent employees to perform IS audit. Internal IS audit was performed on the procedural level with no clear methodology and with much help of the IT department employees which questioned their results and independence. Prescribed regulations raised Boards' awareness of the IS internal audit significance, which in following year(s) resulted in formally appointing qualified IS internal auditor, and defining methodology and framework which helps starting performing internal IS audit. The various IT Governance efforts are very important especially having in mind that small and medium size banks compared to large ones commonly have no huge budget for IT investments. Analyzing the sample banks common practices, following trends in IT investments were noted:

- IT investment budget were increased each year and approximately accounts from 8 to 12% of the total bank budget (or up to 30% of investment budget) and surely help align IT with the business.
- As CNB regulations were due or put into force, more investment in IT is needed especially in business continuity and disaster recovery process.
- IT investments cover all functional areas of IS in banks. Throughout the years there has been constant

increase in number of IT employees for sampled banks, IT investments raised, from 15% to up to 30% of investment budget. At the same time IT outsourcing budget in all banks were (heavily) decreased throughout years, which reflects the fact that on long-term Board and CIOs would like to manage IT by themselves, using in-sourcing strategies.

Table 3. IT policies, procedures and metrics

		IT strategy	IT risk policy	BCP and DRP	RPO and RTO	Applic. outsourcing
Bank 1	**2008**	Yes	No	No	No	Yes
	2009	Yes	Yes	No	No	Yes
	2010	Yes	Yes	Yes	Yes	No
Bank 2	**2008**	Yes	No	No	No	Yes
	2009	Yes	No	Yes	No	Yes
	2010	Yes	Yes	Yes	Yes	Yes
Bank 3	**2008**	No	No	No	No	Yes
	2009	Yes	No	No	No	Yes
	2010	Yes	Yes	Yes	No	Yes
Bank 4	**2008**	No	No	No	No	Yes
	2009	Yes	Yes	No	No	Yes
	2010	Yes	Yes	Yes	Yes	Yes
Bank 5	**2008**	No	No	No	No	Yes
	2009	Yes	Yes	Yes	Yes	No
	2010	Yes	Yes	Yes	Yes	No

Research results depicted in table 3 indicate that banks didn't prescribe some IT Governance procedures prior to mandated regulations. In a series of in-depth interviews performed from 2008 to 2010 on selected banks we confirmed that when approved, these internal acts were successfully implemented.

Business continuity plan (BCP) and disaster recovery plan (DRP) were only IT Governance areas that were last prescribed and implemented in practice. The reason for that may be found in the fact that BCP and DRP are very expensive to implement especially for small banks. Accordingly, all banks have performed business impact analysis (BIA) which showed that regulation is not suitable for small banks but for large ones with higher IT budgets, resources and expertise.

In majority of cases implementation of the procedures and internal acts was not satisfactory in first (2008) and even in the second year (2009) of the research due to the fact that banks prescribe them just to formally fulfill legal obligation. Regular external IS audits, therefore, was the key research instrument to investigate the practice of IT Governance procedure in first two years of the research, with many suggestions for improvements. During the last year of the research (2010) all banks have significantly improved operative effectiveness of the internal acts and procedures in place.

VII. CONCLUSION

In this paper we investigated the practices by which IT can contribute to the business as well as how to measure its maturity. Main objective of this paper was to stress the importance of evolving IT Governance activities. After analyzing IT Governance components and elements we explained external and especially national IT Governance regulation framework in the Republic of Croatia, construct the research model upon the strategic IT/Business alignment and IT Governance issues and conducted the research by the series of long-lasting comprehensive in-depth interviews with responsible employees (CIOs) in selected small banks in Croatia. These activities were regular part of external IS auditing conducted from 2008 to 2010 with the final objective of assessing the level of IT maturity.

As mentioned in chapter 5. Croatian National Bank (CNB) prescribed IT Governance regulatory framework ('Decision on adequate information system management') upon which regular external and internal IT audits are obligatory for every single credit institution operating in the Republic of Croatia. By these regulation and accompanied working instructions the IT Governance performance (maturity) levels are prescribed (completely unsatisfactory, partially unsatisfactory, partially satisfactory, satisfactory and completely satisfactory). The main objective of such a strong regulation is to strengthen the maturity of IT Governance processes in credit institutions. Some results of such approach may be the fact that all credit institutions in Croatia have a CISO (Chief Information Security Officer) as an autonomous person nominated for managing IS security. All of them are conducting IS auditing procedures and every single commercial bank operating in Croatia has to have BCP and DRP integrated into risk management process and IT Governance policies.

In the first year of our research study (2008) IT Governance maturity were evaluated as unsatisfactory in bank 1, bank 2 and bank 4 and partly satisfactory for bank 3 and bank 5. However, despite the fact that CNB regulations are equal for small and for large banks (but small banks eventually do not have enough funds to be in full compliance with all CNB guidelines), IT Governance maturity in 2010 is partly satisfactory in 4 banks and satisfactory in one bank (bank 5).

CobiT maturity marks for selected small banks (scale from 0 to 5) were as follows:

- In a year 2008. - from 2.1 to 2.4;
- In a year 2009. - from 1.9. to 2.9;
- In a year 2010. - from 2.4 to 3.0.

By constructing the research instrument around IT Governance components, by conducting long-lasting (3 year) dedicated in-depth interviews, by implementing IT

Governance best practices (CobiT) and national regulation on a sample of small banks (which are harder to implement them than larger ones), we come up to a conclusion that national IT Governance regulatory framework can help in improving IT Governance maturity and strategically align IT and business and confirm our research question. Research results reveal that when IT and Business are strategically aligned, mainly through IT Governance initiatives, IT investments are high, IT Maturity raise and the IT department is seen as a strategic partner to organization. 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.] Champlain, J.J. (2003): Auditing Information Systems, 2nd ed. John Wiley & Sons, SAD.

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

[3.] Epstein, M.J., M.J. Roy, (2004): "How Does Your Board Rate?," *Strategic Finance*, February, p. 25-31, 2004.

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

[5.] ITGI (2003): *Board Briefing on IT Governance*, 2nd ed., IT Governance Institute, Rolling Meadows, Illinois, SAD.

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

[7.] Nicho, M., Cusack, B. (2007): A Metr ics Gener ation Model for Measur ing 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.

[8.] Nolan, R. and McFarlan, F.W., (2005): Information Technology and Board of Directors, Harvard Business Review, October, 2005.

[9.] 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

[10.] 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.

[11.] Spremić, M., Popović, M. (2007): Towards a Corporate IT Risk Management Model, *Proceedings of the 6th WSEAS International Conference on Information Security and Privacy*, Puerto de la Cruz, Tenerife, Canary Islands, Spain, December 14-16, 2007, pp. 111-117.

[12.] Spremić, M**.,** Žmirak, Z., Kraljević, K. (2008): Evolving IT Governance Model – Research Study on Croatian Large Companies, *WSEAS Transactions on Business and Economics***,** Issue 5, Volume 5, May 2008, pp. 244-253

[13.] Symons, C., (2005): IT Governance Framework: Structures, Processes and Framework, Forrester Research, Inc.

[14.] Van Grembergen, W., (2004): *Strategies for Information Technology Governance*, Idea Group.

[15.] Van Grembergen, Guldentrops, E. (2004): *Structures, Processes and Relational Mechanisms for IT Governance*, Idea Group

[16.] Venkatraman, N., (1999): *Valuing the IS Contribution to the Business*, Computer Sciences Corporation.

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

Mario Spremic is Full Professor and a head of the Department of Informatics at the Faculty of Economics & Business, University of Zagreb, Croatia. He received a B.Sc. in Mathematical Sciences, M.Sc. in IT Management and Ph.D. in Information Systems from the University of Zagreb. He had published 10 books and more than 150 papers in scientific journals, books and conference proceedings mainly in area of e-business, IT governance, IT risk management, IS strategy, IS security, IS control and audit and IT Value.

Mario is an associate editor and a member of Boards and Committees for a number of journals and/or reviewer for various international conferences, full list at www.efzg.hr/mspremic).

Mario is an ISACA member (Information System Audit and Control Association), ISACA Academic Advocate and IIA (Institute of Internal Auditors) member and holds prestigious ISACA's CGEIT international certificate **(**Certificate in Governance of Enterprise IT - www.isaca.org/certification).

As a qualified information system auditor and consultant he has been participating in a number of regulatory-based IS audits and advisory projects and besides scientific, gain in-depth expert knowledge of commonly used standards such as CobiT, ISO 27001, Risk IT, Val IT, Basel II, SoX, ITIL, etc (full reference listing is beneath). Previously he had been working as system analyst, project manager and CIO deputy.