Methodologies for conducting information system audit: case study of Sarbanes-Oxley compliance

MARIO SPREMIĆ, Ph.D., Associate Professor
Faculty of Economics and Business Zagreb, University of Zagreb
Kennedy's sq 6, 10000 Zagreb, CROATIA
e-mail: mspremic@efzg.hr

MATIJA POPOVIC, M.Sc., CISA
Ernst & Young, Dublin, IRELAND
Senior IT Auditor
e-mail: matija.popovic@ie.ey.com

Abstract

Although information systems (IS) and information technology (IT) are taking significant role in businesses with its innovating and supporting potential, it seems that it is the least understood company asset. Successful organizations manage IT function in much the same way that they manage their other strategic functions and processes. This in particular means that they understand the IT control environment and manage the risks associated with growing IT opportunities, such as increasing regulatory compliance as well as critical dependence of many business processes on IT and vice-versa. They are doing so by engaging in IT Governance and information system audit (IS Audit) activities. In recent years there are a number of world-wide used standard, regulatory frameworks and best practices in IT governance and process management area such as CobiT, ITIL, Basel II Sarbanes-Oxley act (SoX), ISO 27000, which helps management to measure the actual IT performance and comply to regulatory demands. In this paper we present the case study of conducting IT compliance audit according to SoX. After brief explanation of key terms, the methodology of complex SoX compliance audit is given and key performance indicators for major business processes stressed. The IS Audit process resulted in recommendations for business process change.

Keywords: IT Governance, Information System Audit, Business Process Improvements, Case study, Sarbanes-Oxley compliance

Povzetek

Metodologije za izpeljavo revizije informacijskega sistema: študij primera usklajenosti z uredbo Sarbanes-Oxley

Kljub temu da informacijski sistemi (IS) in informacijska tehnologija s svojimi inovativnimi in podpornimi zmožnostmi v poslovnih organizacijah pridobivajo na pomembnosti, se zdi, da so še vedno med najmanj razumljenimi prednostmi podjetij. Uspešne poslovne organizacije namreč upravljajo s svojimi IT-funkcijami približno tako kot z drugimi strateškimi funkcijami in procesi. To v bistvu pomeni, da razumejo okolje nadzora IT in da uravnavajo tveganja, ki izhajajo iz vse večjih zmožnosti IT, kot je vse večja možnost regulatornega usklajevanja ali kritična odvisnost vse več poslovnih procesov od IT in obratno. Tega se lotevajo tako, da vpeljujejo v IT nadzor in revizijske dejavnosti (IS Audit). Zadnja leta so na voljo po vsem svetu znani in na široko uporabljani standardni regulatorni sistemi in dobre prakse na področju IT-nadzora (governance) in upravljanja procesov, kot so CobiT, ITIL, Basel II Sarbanes-Oxley act (SoX), ISO 27000, ki pomagajo menedžmentu izmeriti dejansko učinkovitost (performance) IT in njeno skladnost z regulatornimi zahtevami.

V prispevku obravnavamo študij primera izvajanja revizije in ugotavljanja skladnosti IT z uredbo SoX. Po kratki obrazložitvi ključnih pojmov predstavimo metodologijo kompleksnega ugotavljanja skladnosti s SoX in nato izpostavimo ključne indikatorje uspešnosti glavnih poslovnih procesov. Preskus IS se zaključi s predlaganjem sprememb v poslovnem procesu, ki jih priporočamo podjetju.

Ključne besede: nadzor IT, revizija informacijskega sistema, izboljšave poslovnega procesa, študij primera, uskladitev Sarbanes-Oxley

1 Introduction

In today's highly competitive business environment, effective and innovative use of information technology (IT) has the potential to transform businesses as well as to positively affect organizations' performance. A number of researches showed that technology itself has no inherent value and that IT alone is unlikely to be a source of sustainable competitive advantage (Peppard and Ward, 2004). The business value derived from IT investments only emerges through business process changes and innovations, whether they are product/service innovation, new business models, or process change. Organizations which intensively use IT as a means of improving efficiency and/or as an enabler of

business innovation and competitive advantage need to set-up IT governance processes and start to systematically measure the IT performances. 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 (ITGI, 2007). Nolan and McFarlan (2005) recently pointed out 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'. In recent years various groups have developed world-wide known IT Governance frameworks and/or industry specific regulations (such as CobiT, ITIL, Sarbanes-Oxley act, Basel II, ISO 27000) to assist management in managing risk and measuring the performance of IT initiatives. The main focus of our interest in this paper is the case study of Sarbanes-Oxley IS audit and IT control practices compliance in a large telecommunication company. After brief discussion about the frameworks for conducting IS Audit and IT Governance, the methodologies for conducting Sarbanes-Oxley (SoX) audit compliance are presented in Chapters 3 and 4. In Chapter 5 the description of the 'as-is' business processes in the company is given and according to SoX requirements risks identified and control deficiencies assessed. Chapter 6 refers to IS audit findings on IT control SoX compliance and discussion about the possible changes. The case study results showed how recommendations that arise from a systematic and thorough IS audit may help companies becoming aware of the deficiencies in the control environment and may enable business process change.

2 Emerging issues in IT governance, IS audit and compliance

IT Governance represents 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 (Van Grembergen and Guldentops, 2004; Spremic and Popovic, 2008). A good, or rather, inevitable approach for measuring the performance of IT should include thorough audit of all aspects of IS and IT, including hardware, software, data, networks, organization and key business processes. The primary goal of the information system audit (IT audit) is to identify the key business processes that depend on IT, to systematically and carefully examine their IT controls efficiency, to identify key risk areas and constantly measure the risk level, to warn about possible failures, as well as to offer suggestions to the executive management how to improve current IT risk management practices (Spremic, 2008). Engaging in IT audit is crucial for measuring the performance of IT as well as to manage the IT/business alignment, which makes IT audit the key cornerstone of IT Governance concept. Worldwide or industry specific regulations and IT Governance frameworks (such as CobiT, ITIL, SoX, SAS 70, HIIPA, Basel II, ISO 27000, NIST 800, etc,) help companies assess the level of IT control efficiency compliance and manage the associated risks. Through the information system audit process companies' management become aware of the control deficiencies and the IT auditor recommendations may drive the business process change, in order to mitigate recognized risks and deficiencies.

The need for assurance about the value of IT, the management of IT-related risks and increased requirements for control over information are now understood as key elements of enterprise governance. The issues raised in the control environment component apply throughout an organization. However, IT frequently has characteristics that may require additional emphasis on business alignment, roles and responsibilities, policies and procedures, and technical competence. The following list describes some considerations related to the control environment and IT (ITGI, 2003):

- IT is often mistakenly regarded as a separate organization of the business and thus a separate control environment.
- IT is complex, not only with regard to its technical components but also in how those components integrate into the organization's overall system of internal control.
- IT can introduce additional or increased risks that require new or enhanced control activities to mitigate successfully.
- IT requires specialized skills that may be in short supply.
- IT may require reliance on third parties where significant processes or IT components are outsourced.
- Ownership of IT controls may be unclear, especially for application controls.

Contemporary frameworks for conducting IT Governance and IT Audit are:

- *CobiT* (Control Objectives of Information and related Technology),
- *ISO 27000 'family'* (ISO 27001:2005, ISO 27002:2005), and
- *Sarbanes-Oxley act*,
- *ITIL* (IT Infrastructure Library), etc.

CobiT, for example, is the widely accepted IT governance framework organized by 34 key IT processes (or key IT control objectives), which are broken into more than 300 detailed IT controls. For each of the 34 IT processes 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.

On the other hand, Sarbanes-Oxley Act (SoX), enacted in 2002 by the US Congress in response to series of business failures and corporate scandals (Enron, etc.), represent an internal control framework for financial reporting, prescribed by SEC (US Securities and Exchange Commission) which is obligatory for SEC registrants. The stated purpose of SoX is to protect investors by improving accuracy and reliability of corporate disclosures. If a company wants to do business in USA it has to be SEC registrant. The SEC in its final rules regarding the SoX made specific reference to the recommendations of the Committee of the Sponsoring Organizations of the Treadway Commission (COSO). While there are many sections within the SoX, this paper focuses on section 404, which addresses internal control over financial reporting. Section 404 requires the management of public companies specified by the Act to assess the effectiveness of the organization's internal control over financial reporting and annually report the result of that assessment. It is well known that reliability of financial statements largely depends on information system environment which needs to be adequately controlled, and in compliance with the SoX section 404.[1] Also, all daughter-companies operating all over the world whose parent companies are SEC registrants, need to be SoX compliant, which increases the number of companies obliged to conduct the information systems auditing process.

3 Description of assessment procedures for compliance with Sarbanes Oxley act

Independent auditor is obliged to issue a report regarding internal controls of a company which has to contain assessment of the management's evaluation, and assessment of the design and operating effectiveness of controls over financial reporting. Test procedures are as following:

- assessment of the controls' design effectiveness
- assessment of the controls' operating effectiveness.

In order to 'cover' or rather manage various business risks, assessment of the effectiveness of controls' design relates to reasoning whether the identified control is designed adequately. Operating effectiveness is basically testing controls itself. If the application controls contain both manual, and automated part, i.e. IT dependant manual control, it is necessary to divide them and each part should be assessed separately, bearing in mind that manual part of the control cannot be assessed on a sample of one which is the case with automated part.

After the scope of the review has been defined it is necessary to conduct control assessment. In the following table, SoX assessment plan is described which is used in the case study.

Categorization of deficiencies

While assessing the deficiencies in control environment, the following categorization is possible:

a) No deficiency
b) Deficiency in documentation
c) Control evidence insufficient
d) Control not identified, yet existing
e) Design insufficient
f) Functionality insufficient
g) Both e) and f)

If design is categorized as a) and b), it is proceeded to the next step, which is operating effectiveness assessment.

[1] IT Governance institute (2006): *IT Control Objectives for Sarbanes-Oxley*, IT Governance Institute, Rolling Meadows, Illinois, SAD., pp. 5

Table 1. **Sarbanes-Oxley act compliance process**[2]

Procedure	Step	Question
1. Review of Design Effectiveness	Review Process Documentation	Is the process description complete, plausible, detailed enough and understandable? Additional important points: Sufficient segregation of duties described? Are IT Systems and interfaces completely included?
	Review Control Documentation	Is the control description complete, plausible, detailed enough and understandable? Is the control adequate to achieve the control objective? Additional important points: Is the documentation of control performance sufficient? Is the handling of errors described? Are the control attributes complete and plausible? Are Significant Accounts and Assertions complete and plausible? Are the people performing the control sufficiently qualified?
	Performance of Walkthroughs	Was our understanding of the process, the control design, the involved entities, IT-Systems etc. confirmed? What changes or deviations were noticed compared to the documentation? Are the controls actually implemented or are target controls or processes described?
	Evaluation of Design Effectiveness on Control Level	Summary: Are the controls adequate to cover the control objectives and to prevent misstatements? A categorization of deficiencies (if applicable) has to be done (see Procedure "evaluation of deficiencies") to reach a conclusion ("adequate", "inadequate") and to define the following steps (Testing Operating Effectiveness or additional deficiency evaluation).
	Evaluation of Design Effectiveness on Process Level	Summary: Are all Significant Accounts & Assertions that are relevant for the process covered by controls? Are IT Application controls documented completely?
2. Review of Operating Effectiveness	Development of a Test Plan	Develop a test plan for all controls with adequate control design. Selection of test technique(s) (Inquiry, Observation, Examination, Re performance) taking into account: Kind of control (approval, authorization, segregation of duties, review, system control), control frequency, level of automation, importance of control, security of testing result. Determination of sample size taking into account: Control frequency, level of automation, control complexity, experience of the control performer.
	Perform Independent Testing	Selection of sample size (adequate allocation over period under observation) Testing according to test plan and results (in case of identified exceptions: stop testing or increase the sample size)
	Evaluation of Operating Effectiveness	Does the control operate as described? Is the control able to identify potential errors? Are the control performances and the control results documented adequately?
3. Overall Evaluation on Process Level	Review Summary for Design Effectiveness and Operating Effectiveness	Summary: Are all Significant Accounts & Assertions that are relevant for the process covered by documented and effective controls? If deficiencies were identified: were existing compensating controls considered during evaluation?
4. Evaluation of Deficiencies	Categorization of Deficiencies on Control and Process Level	Identify kind of deficiency: Documentation deficiency, process deficiency, transaction control deficiency, IT General Controls- deficiency.
	Quantitative & Qualitative Evaluation of Deficiencies on Control and Process Level	Classification of affected Significant Accounts & Assertions Determination of likelihood of a misstatement Determination of a potential quantitative magnitude of misstatement (if applicable take into account the adjusted exposure method) Determination of potential qualitative magnitude.
	Definition of the Priority of Deficiencies	Review of the evaluation of deficiencies and predefinition of the priority concerning possible relevance. Discussion of weaknesses!

[2] This is the working material used when conducting IS audit in this case study. The material is particularly based on ITGI (2006) publication (IT Governance Institute (2006): IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition, Rolling Meadows, Illinois, SAD), but has been massively changed and expanded to serve as compliance process model for this particular case study.

Table 2. **Design effectiveness**[3]

Control Design Effectiveness

Results of design testing	Next steps	Assessment	Deficiency categorization*	Detailed deficiency evaluation
No deficiency	Testing Operating Effectiveness	Effective	a)	No
Documentation deficiency*	Testing Operating Effectiveness	Ineffective	b)	No
Not existing control identified in process	No testing, deficiency evaluation	Ineffective	d)	Yes
Design deficiency	No testing, deficiency evaluation	Ineffective	e)	Yes

Table 3. **Operating effectiveness**[4]

Control Operating Effectiveness

Results of operating effectiveness testing	Next steps	Result documentation	Deficiency categorization	Detailed deficiency evaluation needed
No deficiency	-	Effective	a)	-
Exactly 1 Exception identified	New testing by doubling the sample size; deficiency evaluation, if applicable	Effective (no new exception) or Ineffective (further exceptions)	a) or f)	Yes if f)
More then one exception	Stop testing, deficiency evaluation	Ineffective	f)	Yes
Gaps in the control performance documentation, but functionality generally testable throughout period	Deficiency evaluation	Ineffective	c)	No
While performing the walkthrough the auditor encounter the control which management has not identified as a key control	Testing by the auditor, if control is operating effectively. (If the control is effective it should be categorized in issue category d). If the control is not effective the deficiency should be categorized in category f).	Ineffective	d) or f)	Yes
Control not being performed	Deficiency evaluation	Ineffective	f)	Yes

4 Description of the business processes in the company „Happy Phone",[5] before the business process change

In this case study, research objective is the billing process of the local, non interconnection traffic in the large telecommunication company (let's call it 'Happy Phone'). The company is the leading telecommunication provider of both fixed telephony and Internet services, with broad spectrum of services offered to millions of users (voice telephony, data transmission, fast Internet access, digital television, wide range of mobile services, wireless Internet access, etc.). According to the fact that her parent company is listed on USA stock markets, the company was obliged to do conduct the SoX compliance audit. In this chapter business process will be described on a high level, without detailed description of the control points, and in the next chapter control compliance with the SoX will be assessed. For the testing purposes and compliance assessment with the SoX it is necessary to comprehend the process and mapped them. This is the only way how could the potential mitigating controls be understood, and how to confirm the completeness of the management's control identification. During the audit, business processes which are driven by the IT are mapped by information system auditors (IT auditors). The same assumption is adopted in this case study, where integrated audit approach is applied, meaning that interim audit findings can be taken in the consideration during SoX review.

[3] Ibidem.

[4] Ibidem.

[5] Due to complexity and confidentiality of the project, it isn't possible to indicate any other relevant data about the company itself and about the project itself (duration, possible financial savings, the estimation of the risks and damages in current system, etc.). It is important to notice that this is a IS compliance audit project and case study. Despite the fact that the companies rarely engage in them, it appears that the results of IS compliance audit projects may came up with financial savings as well. Unfortunately, further data are not available due to the company's communication policy.

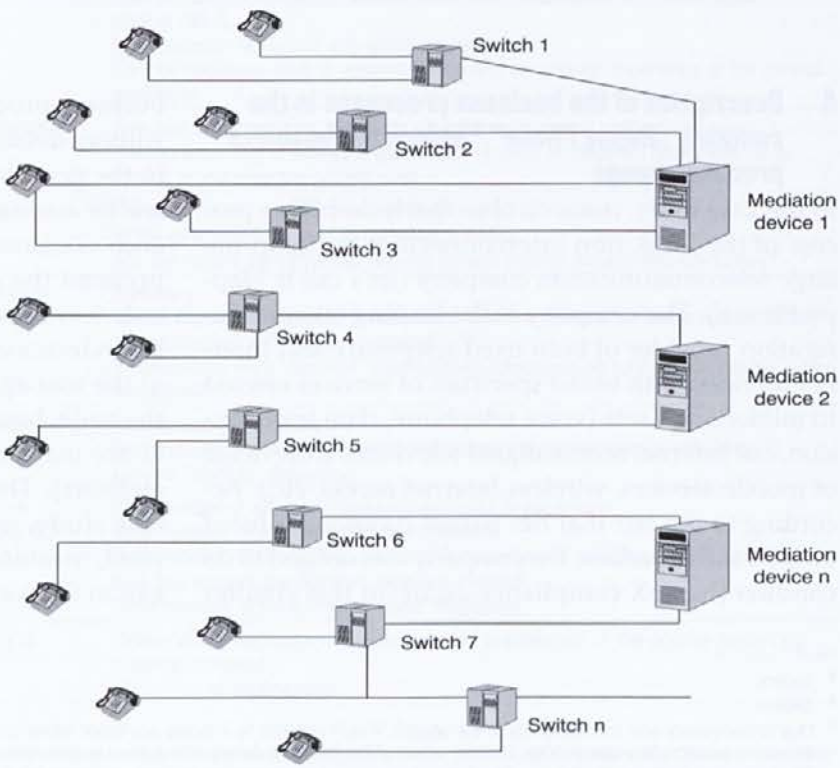
Process which is mapped in the interim audit can be used for understanding the processes during SoX review. Process mapping is performed that one transaction is captured on the beginning of the business process and is traced to its end, which may not always be possible in the IT driven business processes, because in the certain points in the process data is transformed to the format not comparable to the format prior to its transformation.

When the end user of the telecommunication service makes a call, Call Detail Record (CDR) is generated at the switch. CDR contains the following information:

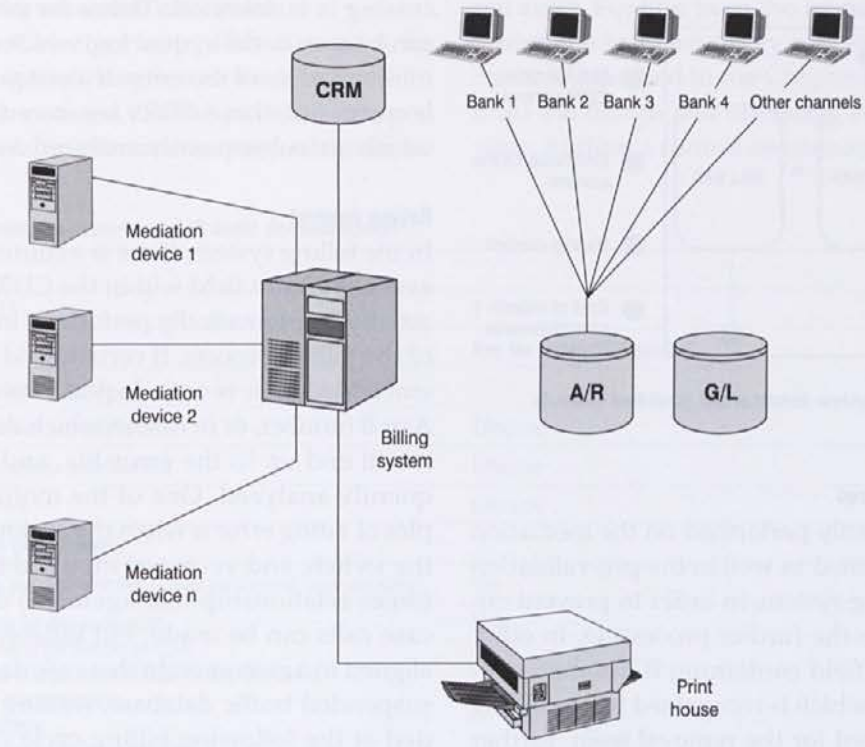
- A Number – Calling number
- B Number – Number that is being called
- Date and time of the Call
- Call duration
- Call route
- Unique call identifier

Every call conducted in the certain moment in the telecommunication network, is according to the caller location, generated and recorded on certain switches. Each call generates at least one CDR. CDRs are according to the geographical and other significant criteria routed to the corresponding mediation devices. In Croatia, there are two types of the switches that are being used. On the switch type one data file, which will be transferred later on to the mediation device, is being filled with the CDRs until defined data threshold volume isn't exceeded, or before defined amount of time elapses. After one of the criteria is met, data file is automatically transferred to the one of the mediation devices. Other type of the switch uses cyclical data file. After defined period of time a pointer is set on the file, and data captured between previous set up of the pointer and the current pointer are packed in the non cyclical data file and is sent to the predefined mediation device. Current pointer becomes point from which data will be captured when next pointer is set. The process is continued likewise until cyclic file doesn't reach its end and CDRs are starting to be overwritten at the beginning of the cyclic file. In addition to the described process of capturing traffic, call can be captured in the pulse counters on the switches as well, now days used for control purposes only. After the data is transferred to the mediation device, data is transformed to the format readable to the billing system. In addition to the mediation devices used for the data transformation, there is a monitoring mediation device, used for managing and monitoring of the traffic on the remaining devices. After the data is transformed to the format readable to the billing system, data from each mediation device are every half an hour transferred to the billing system. In the billing system, the process is performed in 5 steps. Process begins with the data acceptance, followed by the data validation, and with adding the billable amounts to the data. After that billable data is aligned to the end users and finally invoiced.

According to A number, end user is identified to whom invoice will be issued, and based on a B number and call duration in certain CDR value is added to a call, making this a billable data. Information identifying A number is transferred in a real time from the CRM system to the billing system, so that the billable data can be identified to a customer. At the end of the month, in



Picture 1 – **Billing process – Switch mediation connection**



Picture 2 - **Billing process – Billing and ERP system interface**

a dedicated batch processing component, files that are to be sent to the print house, are generated. In the same batch processing billable data are automatically booked on the debit side of accounts receivable account located in the company's ERP system. Accounts receivable are credited by accepting files with payments from various banks, financial agencies that operate in Croatia, post offices and other channels. Files are automatically inputted into the ERP system.

Prior to the end of month batch processing, previous month's calculated penalty interest is transferred to the billing system from the ERP system, in order to be included into new file that is to be sent to a print house. Few days after receiving of the payment files from the banks and other channels, data are transferred from the accounts receivable to the general ledger.

On this roughly described process, which is mapped during the audit, there is a large number of application, manual, and IT dependant manual controls. For each identified application control, IT generals controls are tested as well. Finding obtained during the interim audit, can be used in the integrated audit approach. In the upcoming chapters, a small part of the process will be described in mere details, as well as controls on that part of the process in order to assess their compliance to the SoX.

5 Information system audit findings on control compliance with Sarbanes- Oxley Act in the Happy Phone Company

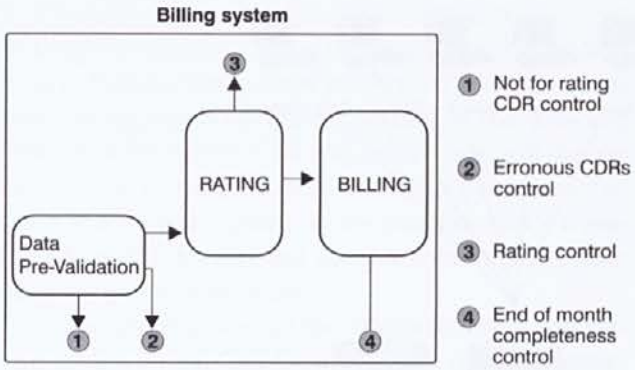
In this chapter, a part of the billing process and related controls are described to which extent do they comply with SoX. Assessment will be conducted based on the procedure described in the Chapter 4 (table 1).

5.1 Controls identified by the Company's management

On the billing process, which is taking place within the Billing system, Company's management has identified following controls as significant:

1. not for rating CDR control,
2. erroneous CDRs control,
3. rating control,
4. end of month completeness control.

Picture 3 shows data flowchart containing the above listed controls on the part of the process that is to be described in details in the following points.



Picture 3 - **Billing system dataflow and identified controls**

Not for rating CDR control

This control is primarily performed on the mediation device, but is performed as well in the pre-validation module of the billing system, in order to prevent entry of such data into the further processing. In other words CDR, in the field containing B number, contains identification, which is recognized by the billing system, and is flagged for the removal from further processing. Such data is continuously stored in the file from which the statistics could be obtained. This control prevents data not meant for billing from being billed, and from charging excessive amounts to the end users.

Erroneous CDRs control

In the billing system there are two types of erroneous CDR validation. First type is that the file carrying CDRs which is sent every half an hour from mediation device to the billing system is duplicated. This error is detected if two received files have same sequential number. Also there is a validation error when there is a gap in the sequentially received files. Error could occur during the transfer from the mediation to the billing system or during the data acceptance in the billing system.

Second type of validation is when mediation device calculates records in the file, and appends checksum at the end of the file. Billing system independently calculates checksum. After the file containing CDRs is transferred to the billing system vie FTP, if the checksums do not match processing is terminated. During the data acceptance, billing system validates sequential order on the level of the records in each file. If there is a duplicate record in a certain file, processing is terminated. The cause of the termination can be seen in the system log, which is used for determining source of the error. If a certain filed in a record is corrupted, these CDRs are stored in the error file, which are subsequently analyzed as well.

Rating control

In the billing system, there is a control point in which ever significant field within the CDR is checked. This activity is automatically performed in the rating phase of the billing process. If certain field according to the embedded logic is not adequate, for example missing A or B number, or in case in which data is unreadable, it will end up in the error file, and could be subsequently analyzed. One of the more common examples of rating error is when the customer is enabled on the switch, and yet is not inputted to the CRM (customer relationship management) database. In that case calls can be made, but billable data cannot be aligned to a customer. In that case data is stored in the suspended traffic database, waiting to be re-suspended at the following billing cycle next month. This loop is repeated until data is successfully re-suspended, or until they are disregarded after defined period of time.

End of month completeness control

Prior to the start of the end of month processing, which results in the customer bill, automatic verification of the critical data is performed. Example of the critical data would be preparedness of the records that is to be included in the end of month processing, conclusion of the dependant components of the batch preceding to the start of the next one, disconnecting link towards the CRM and other. In case that certain batch components haven't been completed processing is stopped, and is re-run.

5.2 Risk identified by the Company's management

Risks identified by the Company's management addressed by the controls which are above mentioned, are the following:

- incorrect and incomplete service billing,
- revenue report is misstated, as a result of incomplete, incorrect or untimely billing,
- correctness of the accounts' receivable analytical data could be tampered, and
- actual traffic is not included in the processing.

5.2.1 Sarbanes Oxley act control assessment

Controls described by the Happy Phone, need to be assessed according to description in the Chapter 4. In this case study it is assumed that the process is mapped by the IS auditors during the interim stage of the financial audit. Finding from the interim audit can be used during the Sarbanes Oxley compliance assessment. All controls described in the Chapter 5.1 are assessed both from the design and operating effectiveness point of view. Auditor's control assessment is the following:

Table 4. **Example of possible reports and IS audit documentation**[6]

Controls information		
1	Control activity ID	**1**
2	Control activity	**Not for rating CDR control**
Self assessment on the control level		
3	Design e ffectiveness assessment	Effective
4	Operating effectiveness assessment	Effective
5	Overall assessment	Effective
Audit assessment on the control level		
6	Was the control self-assessment (CSA) performed appropriately?	Yes
7	If no give reasons for the evaluation Deficiencies of the organization of CSA Documentation of the performed CSA is not sufficient Test techniques inappropriate Sample inappropriate Control deficiencies were not identified Result is not derived properly Other reasons	N/A
8	Audit result of control design assessment	Effective
9	Audit result of control operating effectiveness assessment	Effective
To be reported to the client		
10	Highest category of deficiency related to this control	N/A
11	Explanation of the differences regarding the assessment at the control level and hints for the improvement	N/A

Controls information		
1	Control activity ID	**2**
2	Control activity	**Erroneous CDRs control**
Self assessment on the control level		
3	Design effectiveness assessment	Effective
4	Operating effectiveness assessment	Effective
5	Overall assessment	Effective
Audit assessment on the control level		
6	Was the CSA performed appropriately?	No
7	If no give reasons for the evaluation Deficiencies of the organization of CSA Documentation of the performed CSA is not sufficient Test techniques inappropriate	 yes no no

[6] This material was used in this case study for documenting IS SoX compliance audit findings. It is based on ITGI (2006), but the content and the scope may vary according to the specific tasks. This documentation material may well be the template for similar audit assignments.

	Sample inappropriate	no
	Control deficiencies were not identified	yes
	Result is not derived properly	no
	Other reasons	no
8	Audit result of control design assessment	Ineffective
9	Audit result of control operating effectiveness assessment	Ineffective
To be reported to the client		
10	Highest category of deficiency related to this control	Ineffective design
11	Explanation of the differences regarding the assessment at the control level and hints for the improvement	In control description in the point 3.1.2 the scenario when two files are properly sequentially numbered but have doubled content, isn't described. We confirmed that such control does not exist in practice. In that case files containing double traffic wouldn't be identified and classified as error. Per discussion with the client it is noted that the above mentioned could not be solved by the modification of the existing control yet by implementing a new control on the process. Please see table 3.3.

Controls information		
1	Control activity ID	**3**
2	Control activity	**Rating control**
Self assessment on the control level		
3	Design effectiveness assessment	Effective
4	Operating effectiveness assessment	Effective
5	Overall assessment	Effective
Audit assessment on the control level		
6	Was the CSA performed appropriately?	No
7	If no give reasons for the evaluation	
	Deficiencies of the organization of CSA	No
	Documentation of the performed CSA is not sufficient	Yes
	Test techniques inappropriate	No
	Sample inappropriate	No
	Control deficiencies were not identified	No
	Result is not derived properly	No
	Other reasons	No
8	Audit result of control design assessment	Ineffective
9	Audit result of control operating effectiveness assessment	Effective
To be reported to the client		
10	Highest category of deficiency related to this control	Lack of documentation regarding the design of the control.
11	Explanation of the differences regarding the assessment at the control level and hints for the improvement	Detail documentation should be enclosed to the control testing, to be able to make adequate conclusions.

Controls information		
1	Control activity ID	**4**
2	Control activity	**End of month completeness control**
Self assessment on the control level		
3	Design effectiveness assessment	Ineffective
4	Operating effectiveness assessment	Effective
5	Overall assessment	Ineffective
Audit assessment on the control level		

6	Was the CSA performed appropriately?	Yes
7	If no give reasons for the evaluation Deficiencies of the organization of CSA Documentation of the performed CSA is not sufficient Test techniques inappropriate Sample inappropriate Control deficiencies were not identified Result is not derived properly Other reasons	N/A
8	Audit result of control design assessment	Ineffective
9	Audit result of control operating effectiveness assessment	Effective
To be reported to the client		
10	Highest category of deficiency related to this control	Control not identified yet existing on a process,
11	Explanation of the differences regarding the assessment at the control level and hints for the improvement	Aside from the validation on the CDR level within the file, validation on a level of a file containing defined number of CDRs should be included in a description. Mentioned control is executed on the practice however it is not described in the SOX documentation.

5.3 Assessment of the process compliance with the Sarbanes Oxley Act

Assessment is performed for each significant control on the process, but it has to be performed on a process level as well. If significant control objective cannot be addressed by changing the existing controls, yet by implementation of the new control, as it is in this case study, the process has to be assessed as ineffective.

Table 6. **Assessment of process SoX compliance**[7]

Process		
Process information		
1	Organization	HAPPY@HOME
2	Business unit	HAPPY PHONE
3	Process	Billing
Self-assessment on a process level		
	Management's self assessment	Effective
Audit assessment on a process level		
4	Audit entity	**ABC ltd.**
5	Auditor	XY
6	Date of audit	31.12.2006
7	Self assessment performed appropriately	No
8	If no give reasons for the evaluation Deficiencies of the organization of CSA Documentation of the performed CSA is not sufficient Process deficiencies were not identified Result is not derived properly Other reasons	 Yes No Yes Yes No
9	Audit result on a process level	Ineffective
To be reported to the client		
10	Highest category of deficiency related to this process	Ineffective design and operating effectiveness.
11	Explanation of the differences regarding the self assessment at the process level and hints for the improvement	Process described by the Company's management does not contain control which would prevent erroneous double files, which have correct sequential numbers. Such control should be implemented in order to minimize risk of "Misstatement of the revenue report, as a result of the incomplete, incorrect and untimely billing", which is not completely covered by other controls.

[7] Ibidem.

6 Discussion and possible changes of the process based on the IS auditor's opinion

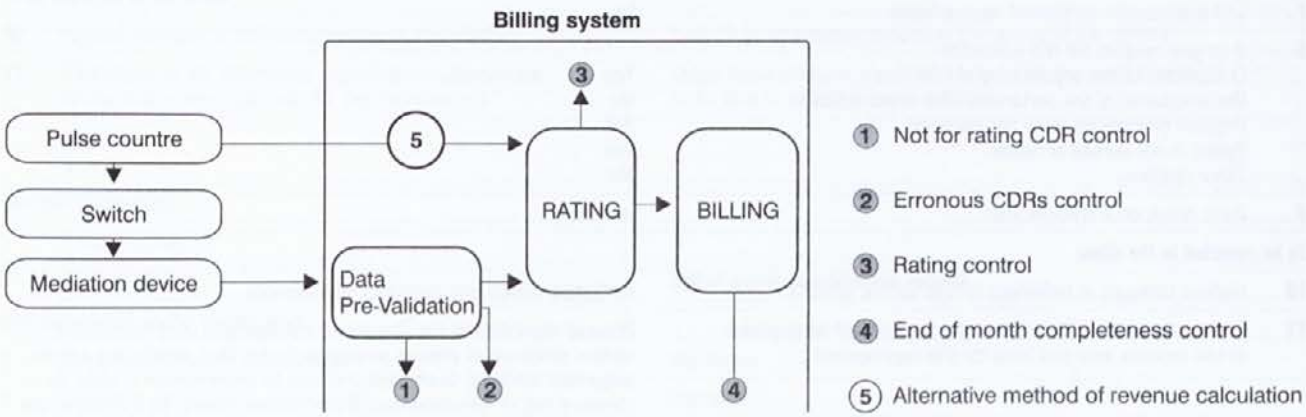
After the company receives a report that the process is inadequate, the organization has an option to implement the recommendation in order to address control objective and cover the risk, or to document lack of a control and disclose that process is ineffective in the self assessment. The most important is that SoX documentation reflects true and fair reflection of the company's control environment. It is more likely that the company will try to address the risk and control objective, due to the fact that once a year, management has to report on the effectiveness of the internal controls over financial reporting according to the Section 404 of the SoX. Furthermore, independent auditor has to issue an opinion about the company's internal controls, which has to contain an opinion regarding management's self assessment and opinion on internal control effectiveness over financial reporting. Therefore it is preferable that the organization looks good in the eyes of its shareholders. If the control framework is strengthening business process risks are minimized. Deloitte & Touche revealed that material ineffectiveness of the internal controls negatively affect the value of the stocks, and reported that a number of companies have experienced 5-10% drop of average stocks value, momentarily after such report is being issued.[8]

[8] Deloitte & Touche (2005): Sarbanes-Oxley 404: Compliance Challenges for Foreign Private Issuers, http://www.iasplus.com/dttpubs/0502soxfpi.pdf, accessed, November 2007.

Auditor's assessment described in the chapter 6.3 is the following:

Process described by the company's management does not contain control which would prevent erroneous double files, which have correct sequential numbers. Such control should be implemented in order to minimize risk of "Misstatement of the revenue report, as a result of the incomplete, incorrect and untimely billing", which is not completely covered by other controls.

This control objective company can achieve utilizing the data gathered from the pulse counters which are already placed on the switches, and by converting pulses to the revenue per call categories. If the amounts received from the pulse information and the amounts captured from the CDRs are compared, using statistical trend analysis deviations can be noticed. It is to be expected that there would be some deviations, but if they are significant, higher then the amount that is to be defined by the company, the causes of deviations would be manually investigated. If the files would have correct sequentially numbering, and yet would be exactly the same, it would be noted by using statistical analysis that two types of measurement give far different output then the one that is to be expected during the regular processing. This control wouldn't be inspecting traffic on a file level. In order to capture statistical trends a month time frame for inspection is more appropriate then inspection on a daily basis. It is important that control is performed prior to the billing cycle



Picture 4 - **Dataflow in the billing system after business process change**

and invoicing. This additional control on the process could cover potential deficiencies of other controls.

Nevertheless in the company's documentation there are also other deficiencies, in no case except the one described, deficiency remediation wouldn't cause the change to the process.

It can be seen on the chart that the control "5, "Alternative method of revenue calculation" is a new control added to the process. Therefore the company has to include this control and perform self assessment in a same manner as it is performed for the rest of the controls. Also, independent auditor has to perform an assessment in a way described in Chapter 4.

7 Conclusion

In this paper we presented a case study of Sarbanes-Oxley compliance audit in a large telecommunication company. Even though the company was obliged to comprise with SoX regulatory requirements, it appears that systematically conducted IT audit may still find certain control deficiencies and propose business process changes.

After understanding the actual business processes in details, after reviewing the process documentation and after conducting tests on processes control effectiveness, an IT (information system) auditor summarizes the findings on the control deficiencies. As presented in this case study, all control deficiencies may be remediated through systematic audits and assessment process. The crucial fact is that an auditor should challenge whether a risk identified by the company's management had been adequately addressed by the existing controls. Moreover, the completeness of the risks identified has to be challenged by the auditor. In this case, it has to be stated in the report that there is no control which completely covers the identified risks, and its implementation should be included in the recommendation. Auditors are not responsible for the design and implementation of the control. An auditor should identify that certain control is missing, and assess it in the next iteration after the company had accepted and implemented the recommendation. Therefore the understanding of the environment is critical for an auditor to practice reasonable assurance during the assessment.

Also, the case study reveals the fact that the nature of business risks has changed and new IT risks emerged. IT risks are risks associated with intensive use of IT to support and improve business processes and business as a whole. They are related to threats and dangers that intensive use of IT may cause undesired or unexpected damages, misuses and losses in whole business model and its environment. Although, traditionally, only the IT departments were responsible for managing IT risks, their importance affects the fact that the number of companies starting to systematically deal with such problems is ever increasing. Thus the issue of managing the IT risks becomes less and less a technical problem, and more and more the problem of the whole organization i.e. a 'business problem', which can be managed by engaging in IT Governance activities and conducting periodic IT Audits.

References

1. Champlain, J. J. (2003): Auditing Information Systems, 2nd ed. John Wiley & Sons, SAD.
2. Epstein, M. J., M. J. Roy, (2004): "How Does Your Board Rate?," *Strategic Finance*, February, p. 25-31, 2004.
3. Hunton, J.E., Bryant, S. M., Bagranoff, N. A.: (2004): *Core Concepts of Information Technology Auditing*, John Wiley & Sons Inc., SAD.
4. IT Governance Institute (2003): *Board Briefing on IT Governance*, 2nd ed., IT Governance Institute, Rolling Meadows, Illinois, SAD.
5. IT Governance Institute (2006): IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition, Rolling Meadows, Illinois, SAD.
6. Nolan, R. and McFarlan, F.W. (2005): Information Technology and Board of Directors, *Harvard Business Review*, October, 2005.
7. 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.
8. 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.
9. Symons, C. (2005): *IT Governance Framework: Structures, Processes and Framework*, Forrester Research, Inc.
10. Van Grembergen, Guldentops, D. R. (2004): *Structures, Processes and Relational Mechanisms for IT Governance*, Idea Group.
11. Venkatraman, N. (1999): *Valuing the IS Contribution to the Business*, Computer Sciences Corporation.

12. Ward, J., Peppard, J. (2002): *Strategic Planning for Information Systems, 3rd ed.*, John Wiley & Sons.

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

Mario Spremić je izredni profesor na Oddelku za informacijske sisteme in upravljalsko informatiko na Ekonomsko-poslovni fakulteti Univerze v Zagrebu. Je tudi programski vodja Ekonomsko-poslovnega mednarodnega programa (EBIB). Diplomiral je iz matematičnih znanosti, magistriral iz menedžmenta informacijskih tehnologij in doktoriral na zagrebški univerzi na področju informacijskih sistemov. Je avtor 8 knjig in več kot 120 člankov v strokovnih revijah, knjigah in zbornikih, v glavnem s področij e-poslovanja, upravljanja z IT, upravljanja s tveganji IT, IS strategijami, kontrolami in revizijami. Predava na številnih podiplomskih študijih na različnih univerzah in je sourednik več strokovnih publikacij.

Matija Popović se je po končanem študiju na Poslovno-ekonomski fakulteti v Zagrebu zaposlil v zagrebški izpostavi družbe Ernst & Young. Kot usposobljen (certificiran) revizor informacijskih sistemov je sodeloval v številnih revizijah IT in svetovalnih projektih na Hrvaškem, Irskem, Slovaškem in v Veliki Britaniji. Po treh letih delovanja v družbi Ernst & Young, Hrvatska, je bil premeščen v izpostavo v Dublinu, kjer se je specializiral kot svetovalec za tveganja. Opravil je magisterij na Poslovno-ekonomski fakulteti v Zagrebu in je avtor dveh člankov.