Initial Due Diligence of Information Technology as Risk Identification before Capital Investment in Finance Industry

M.Sc.Boštjan Delak

Nova Ljubljanska banka d.d., Ljubljana
Šmartinska 130, 1520 Ljubljana, Slovenia
bostjan.delak@nlb.si

Abstract. This paper summarizes a research on IT initial due diligence, which I want to submit as a proposal for PhD thesis. The main objective of the research will be to show that based on the experiences with due diligences that I have gained while evaluating tens of companies in financial sector, a general framework for IT due diligence can be developed, which will facilitate evaluation of IT also in other industries. I believe such a framework would be a valuable contribution to the IS community as currently there is no general or widely accepted approach that one could use for initial due diligence of IT. In this proposal I briefly describe various practical concepts, models, frameworks and standards for evaluating IT, which are used worldwide in everyday activities. Then I introduce the approach for an initial IT due diligence that we use in the NLB {Nova Ljubljanska bank[1], Ljubljana, Slovenia}.

Key words: Due Diligence, Information Technology, Information Systems, IT Analysis, IT Research

1 Introduction

Initial due diligence of a financial company is one of the most important activities to be carried out prior to any capital investment. In most cases initial due diligences focus on reviewing liquidity, investments (credit and capital) and risk management. Recently, with an ever growing impact of information systems (IS) on daily company's business support, reviewing this segment of the reviewed company has become very important and vital as well. This is mainly due to large dependency of financial companies on their IS and substantial investments in more quality and up-to-date support ensuring integrity, confidentiality and availability of information.
Initial IT due diligence is a very comprehensive and demanding task, as it covers a wide range of segments, such as information security and operational risk

[1] http://www.nlb.si

assessment. In this paper I describe the research topic that I want to submit as PhD research proposal.

The paper is structured as follows: firstly, the notion of IT due diligence is explained together with comparison between initial IT due diligence, general IT due diligence and IS audit. The next section is dedicated to related work. Several tools, frameworks, standards and methods for IT analysis are briefly described. The third part of the paper gives more details on the research, i.e. the research hypothesis and the research approach.

2 Description of Scientific Area and Related Problems

2.1 Initial IT Due Diligence

One Due Diligence explanation is [1]:

Due diligence in a corporate merger and acquisition close examination of the books to examine the quality of both assets and liabilities of a target company.

The terminology of due diligence emerged or started to be widely used more than 75 years ago, when the US Congress adopted the Securities Act in 1933. In the beginning, pre-merger and acquisition activities focused on legal [2] and financial (bookkeeping) due diligences [3]. As nowadays IS plays a part in almost every process in the modern company, IT due diligence has become a vital part of a complete due diligence process.

Shareholders of the company deciding to make an investment need to get a complete picture of the investments, time required to complete the task and potential risks of all activities and domains of the target company. Generally, initial due diligence is conducted prior to the merger and acquisition of any company, irrespective of the industry or region of the globe. This activity should protect investors and shareholders from making any wrong decisions or underestimating the resources before acquiring the target company. Initial due diligence results and reports represent valuable information for shareholders and negotiators to get adequate data for purchase share value at the final negotiations.

IT due diligence is an IS analysis with the objective to get information about the current status of IT assets, IT resources, company's documentation compliance, compliance with regulation, risk identification, etc. IT due diligence is very similar to general IT audit process [4],[5]. In comparison to general IT due diligence or IS audit, the scope of initial IT due diligence is much wider. Initial IT due diligence must provide valuable information about the current status of IS, risk assessment and estimates of the resources required for harmonization activities during the merger process. Some analyses have shown that information about the value of IT is underestimated. According to the analyses only 15 % of company's market value accounts for tangible assets, whilst 85 % of company's market value consists of intangible assets [6].

Unlike the general IS audit, initial IT due diligence has to provide general risk assessments. There are several types of risks in financial institutions [7]. Operational risks are of particular importance [8]. For banks Basel Committee on

Banking Supervision had issued practices for managing these risks, well known in European banking industry as BASEL II [2] regulations [9]. Internal control on how to manage operational risks has been provided by each national bank [10]. In 2004 IT Governance Institute conducted a questionnaire and its results are available on [11]. Similar to banking industry in EU there are plans to implement restrictive risk management in insurance business - the so-called Solvency II framework. This information can be found at various web pages (e.g. Wikipedia [3], European Commission [4]).
Risk analysis related to the IS risks accounts represents very important information for shareholders and management board in view of their final decisions about potential capital investments - acquisition or merger. Information security is another important segment of initial IT due diligence. Data, information and information assets are the most important supporting components of financial business processes. Information is an asset and has, just like any other business asset, its own value in the company. As such it requires proper protection. These activities refer to safeguarding information against: loss, abuse, disclosure and destruction [12] which is provided through confidentiality, integrity and availability. The objectives of protecting the IS are to assure business continuity and to restrict business losses to the minimum possible level through prevention and security incident effect reduction. Information security can be achieved by implementing adequate controls, which enable compliance with the ISO/ IEC 27001:2005 standard. Information security and utilisation of security metrics is of vital importance in initial IT due diligences [13]

2.2 Initial IT Due Diligence as IS Research

In the last two or three decades information technology has reached the same level of scientific research as other disciplines and a number of studies on information system research have been carried out. Several articles in science magazines describe different approaches to IS research. Design science plays and will play an important role in IS profession also in the future [14]. There is a lively discussion going on in academic circles about IT Artifact and its role [15] and IS work system framework [16].
There is a gap between the IS academic researches and practice waiting to be closed [17]. Therefore it is difficult to determine whether initial IT due diligence is closer to design or behavioural science. The process of initial IT due diligence has similarities with practice driven research, which is explained by Zmud [18]. Initial IT due diligence could be defined as IS work system framework.

[2] http://www.bis.org/publ/bcbsca.htm
[3] http://en.wikipedia.org/wiki/Solvency_II
[4] http://ec.europa.eu/internal_market/insurance/solvency/index_en.htm

3 Motivation

Bhatia explained and confirmed that there is no IT Due diligence framework generally used worldwide [19]. And as there are no worldwide used frameworks and concepts of conducting initial IT due diligences, my objective is to identify the most appropriate concept, define the hypothesis and prove - verify the identified concept by one or more research cases in independent financial institutions outside the banking industry.

4 Related work

This chapter gives a brief description of several methods, models, frameworks, best practices and standards, which are used for conducting different types of IS analyses in a company.

BCM Analysis. One of the most important processes in contemporary companies is Business Continuity Management (BCM) which is also determined by obligatory principle issued by BASEL II. It sets out 10 domains of BCM [20].
One of the tools for the BCM analysis that can provide adequate certification is Publicly Available Specification 56 (PAS56) [5], composed of 6 scorecards representing a complete life cycle of BCM.

COBIT (Control Objectives for Information and related Technology) Model provides good practices across a domain and process framework and presents activities in a manageable and logical structure. These practices will help optimize IT-enabled investments, ensure service delivery and provide a measure against which to judge when things go wrong [6]. For IT to be successful in delivering against business requirements, management should put an internal control system or framework in place.
To govern IT effectively, it is important to appreciate the activities and risks within IT that need to be managed. They are usually ordered into the responsibility domains of: plan, build, run and monitor. Within the COBIT framework these domains are called: Plan and Organize, Acquire and Implement, Deliver and Support, Monitor and Evaluate.
Each of the 34 IT processes has corresponding control objectives. Based on the broader quality, fiduciary and security requirements, seven distinct, certainly overlapping, information criteria are defined (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability). The COBIT framework is well accepted by IS auditors, and they are using it in IT audit activities. According to Bajec [21] the COBIT framework can help you achieve effective and secure usage of information assets in order to meet business objectives.

[5] http://www.pas56.com

CMM (Capability Maturity Model) is used for improvement and quality effectiveness assessments for software development companies. It is a maturity model or framework that helps companies improve their software life-cycle process. The model prevents excessive projects schedule delays and costs overruns by providing the appropriate infrastructure and necessary support to avoid these problems. If a company has defined different levels, CMM can be used as an assessment tool in IS during initial IT due diligence.

INFAUDITOR. Expert systems are also used for evaluation of information systems. INFAUDITOR is one of them. Since information systems assessment is a multi criterion decision, INFAUDITOR methodology structures the audit domains and tests of control as a hierarchical audit tree following an analytic hierarchical process. It is based on several expert systems. The system can be used as a guideline to judge the sufficiency of evidence [22]. INFAUDITOR assists IS auditors in every step of the audit process.

Information Technology Assessment Due Diligence Framework (ITADD) was developed in 2005 as student project at Red McCombs Business School of the University of Texas at Austin (USA). The ITADD framework provides IT managers with a focused method of conducting due diligence assessment of the IT function in companies that are the targets of corporate mergers and acquisitions [23]. ITADD is more than a framework. It is composed of ITADD methodology and ITADD toolkit. Another implication is that ITADD is able to add to IT professionals a framework that is specific to the acquisition of companies and can be used for such processes [24]. The ITADD framework can be successfully used for IT and initial IT due diligences.

IT Balanced Score Cards (BSC) initially developed by Kaplan and Norton is a performance management system that should allow companies to drive their strategies on measurement and follow-up. They proposed a three-layered structure with four perspectives. Each perspective has to be translated into corresponding metrics and measures that assess the current position. Assessments have to be repeated periodically. It is essential that cause and effect relationships are established and that after each measurement performance drivers are clarified. The methodology of BSC is a measurement and management system that is very suitable for supporting IT governance processes [25].

ITIL (Information Technology Infrastructure Library) originated in Europe more than 20 years ago as the collection of best practices for managing IT services based on IT service processes. ITIL is a framework for successful implementation of IT service processes and has become part of the ISO/IEC 20000 standard for IT service management.

IS Risk Assessment is of key importance. There are various assessment methods to be used [12]. An assessor must assess all risks and determine which are of highest importance and which require additional analysis.
The CRAMM program (CCTA Risk Analysis and Management Method) offers several possibilities for quality security risk analysis and management [26].

Val IT is IT governance framework that consists of a set of guiding principles and a number of processes conforming to those principles that are further defined as a set of key management practices. Val IT is based on COBIT. A key lesson of Val IT is that IT investment is no longer about implementing IT solutions but it is about implementing IT enabled changes. Val IT enlarges and supplements COBIT enabling comprehensive control framework for IT management. It focuses on investment decisions (are we doing the right things?) and on realization of benefits (are we getting the benefits?) while COBIT is focusing on the execution (are we doing them the right way and are we getting them done well?). During initial IT due diligence Val IT framework can be effectively used for assessing IS investments and managing them.

NLB Approach. 10 years ago there were no IT due diligence frameworks, models or concepts available. Some consultancy companies were offering such activities but did not share their approaches and protected questionnaires and other documents as their intellectual property. As there were no questionnaires or recipes for initial IT due diligence available on the internet either, I had no choice but to develop my own - NLB approach. Thus on the basis of more than 20 initial IT due diligences in Central and Eastern Europe and over 40 IS analyses (general IT due diligences) conducted in NLB Group within subsidiary companies, internal NLB framework for initial IT due diligences has been developed. This approach allows assessor to collect enough data to get valuable information within a short period of time: on average between 3 and 5 working days on site of the target company. Briefly the NLB approach framework for initial IT due diligence process is divided into the following phases:

- Preparation activities - initial data collecting and preparation/ updating the list of requirements
- Delivery - onsite visit - reviews, data gathering and interviews
- Activities following the onsite visit - collected data analyses and report(s) preparation

Analysis is based on different questionnaires (IS status, transaction statistics, local prices, IT strengths and weaknesses). The most important and valuable are two questionnaires - IS status and the Questionnaire for IT strengths and weaknesses. Information on IS status is collected on the basis of a comprehensive questionnaire (consisting of some 60 pages) which is sent to IT manager of the target company at least one week in advance before assessor's on-site visit.

The content of this document are:

- General Data
- Information System Audit
- Management Planning and Organization of Information Systems
- IT Assets
- Information Security
- Disaster Recovery and BCM
- Business Application Development, Acquisition, Implementation and Maintenance
- Business Process Evaluation and Risk Management
- Other (ITIL, COBIT and ISO 27001:2005 comparison)
- A look in the future

Questionnaire for IS Strengths and Weaknesses is filled during interviews with IT manager / specialists and End User managers - usually also owners of processes. It is advisable to have questionnaires completed by respondents from various organisation units. The questionnaire has more than 50 questions grouped in nine domains:

- Functioning of Data Center
- System Development
- Staff within IT Department
- Quality of the Existing System
- Effective Use of Technology
- Use of Advance Technology
- Co-operation / Partnership with the Business or IT
- Information Security
- Top Management Perspective

The answers are then analyzed using specific procedures. The scope of deviation / correlation in individual questions shows the assessor what the actual state of IT affairs is.
Other questionnaires are also used for assessment of risks and assessment of IT investments / IT costs projection for next five years.

The most important part of the initial IT due diligence comes after a complete analysis of all the documents and questionnaires based on assessor's experience. The assessor has to prepare one or more final reports. The structures of the final reports are predefined for NLB. Usually two reports (a short and a longer) are used. The longer report is prepared when the negotiation activities start, it contains:

- Basis Requirements for the Initial IT Due Diligence
- Management Summary
- Detailed Findings
- Assessor's Opinion

- Recommendations
- Value of IT Assets
- Interviews' Analysis
- SWOT
- Conclusion
    - IS Risks
    - Investment and Cost Estimation for M&A and Harmonization
    - NLB Human Resources Required for M&A and Harmonization

Others. Above mentioned are several alternative approaches that can be used for partial or complete initial IT due diligence. Undoubtedly many other approaches could be found in the theory or in real life worldwide. Aforementioned consultancy companies and world known audit companies have their own methodologies for initial IT due diligences. But they do not share their methods, frameworks and tools. Most probably large global companies have their own methods for due diligence as well.

5 Research Proposal

Almost none of the aforementioned tools, methods, standards and frameworks could easily be used as universal initial IT due diligence framework. At the moment two of them are most convenient: ITADD and NLB Approach. Both approaches share the same goal to capture as much data as possible to provide correct information about the IS current status and its value.

My hypothesis is to prepare a universal initial IT due diligence framework based on NLB Approach framework. I will compare this analysis tool with science research. The framework with an accompanying tool will be verified on real case studies in one or more financial institutions.

6 Research Approach

The framework I would like to develop and prove is based on NLB Approach which has been proven in many initial and general IT due diligences. The experiences I have gained by implementing NLB approach will be the basis for universal initial IT due diligence framework which could generally be used for conducting initial IT due diligences for financial institutions and for other businesses as well.

The initial IT due diligence process will be compared with research methodologies and the parallels with currently known science researches will be documented and presented.

A prototype tool to support defined process will be developed. This tool will help any assessor to repeat processes with the same results.

The new basic initial IT due diligence framework will be documented and practically proven in non banking financial institutions. The confirmed initial IT due diligence framework could then be effectively used almost everywhere.

7 Conclusion

One could say initial IT due diligence is a very simple task. But reality shows that in fact it is a very demanding and complex activity. There are no worldwide used frameworks or standard approaches. Some of the methods, frameworks, standards and best practices have been presented in the document, including the NLB approach, which has shown very good results. At this stage the rough skeleton of universal initial IT due diligence framework is completed with different supporting documents - questionnaires. A corresponding supporting for tool is under development. In the near future a detailed comparison analysis with science research methods will start. I will start looking for potential financial institutions where this framework could be tested, verified and proven.

As mergers and acquisitions are part of daily practice in business, my wishes are for this framework to be used in different business areas.

After all, initial IT due diligence is only ones *due diligence.*

Acknowledgments. I would like to express my thanks to my mentor, assistant professor Marko Bajec, PhD from Faculty of Computer and Information Systems, University of Ljubljana, who has informed me about this event, encouraged me and given me the support.

References

1. Fitch, P.T.: Dictionary of Banking Terms 2nd edition. Barron's Educational Series, page 207 (1993)
2. Mazovec, F.: Legal Due Diligence. NLB internal documentation, Ljubljana (2001), (in Slovene language: Pravni Due Diligence)
3. Podlesnik, B.: Contents Analyses of Commercial Bank Operations. In: 6th Banking Conference - Analysis of Bank Risks, Slovenian Economist Association, Ljubljana (2000), (in Slovene language: Vsebinska analiza poslovanja poslovne banke)
4. ISACA: CISA Review Manual 2005. Information System Audit and Control Association, (2004)
5. ISACA: IS Auditing Procedures IS Risk Assessment Measurements. Information System Audit and Control Association, (2002)
6. ITGI: COBIT 4.1: Control Objectives for Information and Related Technology. IT Governance Institute, (2007)
7. Gornik, R.: Operational Risk Management in Banks. MSc thesis, University of Maribor, Maribor (2004), (in Slovene language: Upravljanje operativnih tveganj v informatiziranih bankah)
8. Gornik, R.: Operational Risk Management in Banking with Capital Accord Basel II. In: 13th International Conference of Auditing and Control of Information Systems, Slovenian Institute for Auditing, pp. 125-148, Ljubljana (2005), (in Slovene language: Upravljanje operativnih tveganj v bankah po novem kapitalskem sporazumu BASEL II)
9. BFIS: Basel Committee on Banking Supervision. Sound Practices for the Management and Supervision of Operational Risk. Bank for International Settlements, (2003)
10. Bank of Slovenia and Slovenian Banks Association: Recommendation for setting up and managing the execution of the system for managing operational risks, Bank of Slovenia, Ljubljana (2005), (in Slovene language: Priporočila za vzpostavitev in izvajanje sistema upravljanja z operativnim tveganjem)
11. Hardy, G.: Information Risks: Whose business are they? IT Governance institute, (2005)
12. Potočnik, M.: Risk Assessments and Risk Analysis Methods for Decision Makers. In: 12th International Conference of Auditing and Control of Information Systems, Slovenian Institute for Auditing, pp. 111-120, Ljubljana (2004), (in Slovene language: Analiza tveganosti za odločanje o ravni varovanja informacij)
13. Gattiker, U.E.: Merger and Acquisition Effective Information Security Depends on Security Metrics. ISACA Information System Control Journal 5, pp. 51-56, (2007)
14. Hevner,A.R., March, S.T., Park, J., Ram, S.: Design Science in Information System Research. MIS Quarterly 28(1), pp. 75-105, (2004)
15. Orlikowski, J.W., Iacono, C.S.: Research Commentary: Desperately Seeking the "IT" in IT Research - A Call to Theorizing the IT Artifact. Information System Research 12(3), pp. 121-134, (June 2001)
16. Alter, S.: 18 Reasons why IT-reliant work system should replace the IT Artifact as the core subject matter of the IS Field. Communications of the Association for Information Systems 12, pp. 366-395, (2003)
17. Benbaset, I., Zmud, W.R.: Empirical Research in Information Systems: The Practice of Relevance. MIS Quarterly 23(1), pp. 3-16, (March 1999)
18. Zmud, W.R.: Conducting and Publishing Practice-Driven Research. In: IFIP Working groups 8.2 and 8.6 joint Working Conference on Information Systems: Current Issues and Future Changes, Helsinki, (December 1998)

19. Bhatia, M.: IT Merger Due Diligence A Blueprint. Information System Control Journal 1, pp. 46-49 (2007)
20. BCI: The ten certification standard for Business Continuity Practitioners, The Business Continuity Institute, (2003)
21. Bajec, M.: Using COBIT as a Model for Delivering a Complete IT Process Review as a Part of the IT/IS Strategy Planning. In: 14th International Conference of Auditing and Control of Information Systems, Slovenian Institute for Auditing, pp. 223-236, Ljubljana (2006), (in Slovene language: Uporaba modela COBIT za celovit pregled IT postopkov v okviru strateškega načrtovanja informatike)
22. Akoka, J., Comyn-Wattiau, I.: A Knowledge-Based System for Auditing Computer and Management Information Systems. A Knowledge-Based System for Auditing Computer and Management Information System 11(3), pp. 361-375, (1996)
23. Sundberg, B., Tan, Z-D., Baublits, T., Stanis, G., Tandriverdi, H.: A Framework for Conducting IT Due Diligence in Mergers and Acquisitions. ISACA Information System Control Journal Online 6, (2006)
24. Baublits, T., Lee, H.H., Stanis, G., Sundberg, B., Tan, Z-D.: Development of an IT Assessment Program for Acquisition. Final Report of the student project in the IT Audit and Security Course at the Red McCombs Business School of the University of Texas at Austin (USA), (2005)
25. VanGrembergen, W.: The Balanced Scorecard and IT Governance. ISACA Information System Control Journal 2, (2000)
26. Umek, M.: Use of Risk Assessment Methods and Tools. In: 12th International Conference of Auditing and Control of Information Systems, Slovenian Institute for Auditing, pp. 99-110, Ljubljana (2004), (in Slovene language: Uporaba metod in orodij pri obvladovanju tveganj)