ISSN 1407-7493 COMPUTER SCIENCE DATORZINĀTNE 2009-7493

APPLIED COMPUTER SYSTEMS
LIETIŠĶĀS DATORSISTĒMAS

INFORMATION SECURITY GOVERNANCE AS KEY PERFORMANCE INDICATOR FOR FINANCIAL INSTITUTIONS

INFORMĀCIJAS DROŠĪBAS PĀRVALDĪBA KĀ FINANŠU INSTITŪCIJU DARBĪBAS RĀDĪTĀJS

Dmitry Kryukov, M.sc.ing., Riga Technical University, Meza 1/3, Riga, LV 1048, Latvia,
dmitrijs.krjukovs@gmail.com

Raimonds Strauss, B.sc.comp., Riga Business School, Skolas 11, Riga, LV 1010, Latvia,
raimonds.strauss@gmail.com

Information security, governance, financial institutions, key performance indicator, KPI

1. Introduction

Financial institutions due to their nature are in constant focus of attention from different stakeholders beginning from owners and investors and ending with government and regulatory agencies. Each stakeholder group according to their functions and interests perform assessment of financial institution's performance using different standards and sets of key performance indicators (KPI) that show different aspects of performance. These sets of KPIs reflect needs of each stakeholder group and measure some specific aspects of financial institution performance whether financial or not – these KPIs reflect ratings, scores and other relative measures of financial or operational strength. Such sets of KPIs in most cases are not interdependent.

At the same time there exist well known public credit rating systems that are developed to provide unified quantitative ratings for financial institution credibility and trustworthiness. Each rating system has publicly available rating methodology behind. Standard & Poor's, Fitch and Moody's ratings are few of the most respectable credit rating systems [1], [2], [3].

Today's economy depends on the secure flow of information within and across organizations. Information security becomes an issue of vital importance. A secure and trusted environment for stored and shared information greatly enhances consumer benefits, business performance and productivity, and national security. Conversely, insecure environment creates the potential for serious damage to corporations and especially financial sector organisations that could significantly undermine their consumers. For companies engaged in critical activities, such as electrical power generation, banking and finance, or healthcare, the stakes are particularly high [4].

During last years the understanding of corporate governance and its role in world's economics is constantly growing [5], [6]. Information security governance in its turn has emerged during last decade and currently takes place as element of corporate governance process [7], [8].

In the same way as each element of corporate governance that influences the institutions financial or operational performance should be measured by rating methodologies, this paper presents and proves hypothesis of information security governance being financial institution key performance indicator in raw with other KPIs and thus should be reflected in rating methodologies.

2. Stakeholders groups, their needs and related sets of KPIs.

Different stakeholder groups might be interested in measuring performance of financial institutions. Stakeholders could be conditionally divided into the following groups according to their interests:

- Shareholders (both minority and majority)

- Creditors
- Board members
- Regulating agencies, institutions and stock exchanges
- Insurance companies providing responsibility insurance services for executives and managers
- Politics
- Financial intermediaries and consultants
- Analysts
- Employees

Although the unified and one-size-fit-all set of KPIs does not exist there are some approaches to definition of KPsI for financial sectors. For instance, during the SPI-Finance project [9] some financial institutions in collaboration have developed the list of key performance indicators and successfully implemented them.

A key performance indicator as a measure designed to provide a quick sign of performance, may be financial or nonfinancial and should be established based on an institution's organizational structure, operating goals and strategies. KPIs will vary from one financial institution to another because of differences in Chief Executive Officers' (CEO) management styles. Regardless, for most community financial institutions there are numerous performance indicators likely to be part of a KPI report. Nevertheless some performance indicators are used in almost every set of KPIs. The most popular and indicative of them according to [10], [11] are:

- **Liquidity ratio indicators** – measures a company's capacity to pay its debts as they come due.
  - **Quick Ratio** is the typical indicator for Liquidity ratio indicators set and is calculated as following: *(Cash+Accounts Receivable + other quick assets) / Current Liabilities*
- **Safety indicators** – indicates a company's vulnerability to risk and the degree of protection provided for the business' debt.
  - **Debt to Equity** (debt to net worth) is the typical indicator for Safety ratio indicator set and is calculated as following: *Total Liabilities (or Debt) / Net Worth (or Total Equity)*
- **Profitability ratios** – measure the company's ability to generate a return on its resources
  - **Gross Profit Margin** is the typical indicator for Profitability ratio indicator set and is calculated as following: *Gross Profit / Total Sales*
- **Efficiency** – evaluates how well the company manages its assets
  - **Accounts Receivable Turnover** is one of the typical indicators for Efficiency ratio indicator set and is calculated as following: *Total Net Sales / Accounts Receivable*
  - **Sales to Total Assets** is one of the typical indicators for Efficiency ratio indicator set and is calculated as following: *Total Sales / Total Assets*

The values for parameters used in calculation of KPIs mentioned above are publicly available from published financial reports for Latvian financial institutions.

The analysis of most popular sets of KPIs for financial institutions shows that although some KPIs may cover some nonfinancial aspects they are nevertheless financially oriented and do not include indicators for corporate governance and information security governance as a part of such. In merger and acquisition (M&A) projects without financial part such KPIs have significant impact also. According to [12] the most relevant are:

- **Managerial Talent**.
- **Share of the industry (market)**.
- **Time being in the industry (market)**.

3. Information security governance assessment methodology

By its own, information security measurement techniques are quite popular and often used by financial institutions and other industry organisations. Methodologies for information security assessment differ and mostly cover governance, technological or process maturity aspects. The following methodologies could be mentioned - IT Governance institute's information governance maturity model, SSE-CMM,

CMMI, IA-CMM, NIST, ISM3, SPMM and IAM [13], [14]. Some researches are made in developing and proposing unified information security assessment methodologies [13].
Taking into account only fully developed and practically implemented models (not only theoretically proposed) for information security assessment the only type of assessment methodologies that fits the objectives of this paper is maturity assessment model types. From maturity models that quantitatively measures information security governance maturity the IT Governance institute's information governance maturity model was chosen as the most appropriate to measure the information security maturity level for financial institutions in scope of this research.

4. Existing researches

Although a lot have been done in information security research field little have been done in research for correlation and interdependences between information security governance and financial institutions' performance measurements. Different scientific and public researches and surveys exist that show latest trends in information security governance for financial sector but little research is done for stages proving information security governance reflecting performance of financial institutions and thus being used as its KPI.
Different researches and papers such as [15], [16], [17] show the high influence of IT and information security on organisation's performance and stress the value provided by them to the business from the theoretical point of view. At the same time these papers do not proof the dependency between level of information security and institutions' performance nor theoretically nor in practice.
From practical point of view there are few global researches and surveys that study a state of information security governance for different corporations and institutions worldwide.
From the latest global publicly available researches regarding information security governance situation and trends for governmental sector (mostly in context of multi-industry research) the following researches could be mentioned:

1. Ernst & Young's annual Global Information Security Survey [18]
2. KPMG Information Security Survey [19]
3. Deloitte Global Technology Media and Telecommunications Security Survey [20]
4. Gartner Information Security Survey and IT Spending Survey [21], [22]

5. Information security governance as KPI for financial institutions

During the performed research that is reflected in this paper the hypothesis for information security governance being key performance indicator for financial institutions has been tested by comparing common financial performance indicators values with information security governance maturity indicators for financial institutions. IT Governance institute's information governance maturity model as described above was chosen for information security evaluation in financial institutions.
For hypothesis testing purposes, the 7 Latvian financial institutions have been chosen which both:

- have financial reports publicly available that contain values for KPI calculation and
- have participated in information security survey covering information security governance issues.

The values for the financial KPIs described above have been calculated from financial institution's public financial report data.
The values for information security governance maturity indicators have been calculated based on these financial institution responses to Ernst & Young Global Information Security Survey [18] questions during their participation in the survey. The Ernst & Young survey [18] contains 32 questions and provides analysis of responses obtained from 16 Latvian organisations representing different industries that have participated in the survey. From the 16 Latvian organisations that have participated in the survey 9 were financial institutions. Authors of the paper have participated in organizing and performing the survey in Latvia thus having deep understanding of the structure of the survey's questionnaire.
The survey questions have been reorganized in the groups below according to information security maturity model [14] to make possible to evaluate maturity of information security governance in the

organizations. Five survey questions were qualified out during reorganization. Regrouping of questions and re-evaluation of survey results were performed by authors of the paper as by experts in information security domain. The questions were reorganized in the following groups:

- **Assignment and supervision of responsibilities** - 8 questions
- **Security organization** - 8 questions
- **Security practices** - 8 questions
- **Security investment management** - 3 questions

In order to ensure confidentiality of organizations which have participated in the survey and have provided responses to the questionnaire the names of the organizations are not disclosured in the paper. Additionally to prevent identification of the financial institutions the absolute values for KPIs and information security governance maturity are not used. Instead the values are ranked according to the scale and principles described below.

The financial performance indicators were calculated for each financial institution. Due to the fact that the range for the values is not defined, that is possible absolute values may differ the calculated absolute values were converted to quantitative indicator values from one to three based on absolute value position on the scale from the minim to the maximum institution's indicator values for each indicator. The Formula 1 for value evaluation is seen below.

$$A'^{m}_{n} = TRUNC(3 * \frac{A^{m}_{n} - MIN(A^{m})}{MAX(A^{m}) - MIN(A^{m})} + 1) \quad (\mathbf{1})$$

where

A^{m} – Set of indicator absolute values for institutions for indicator m

A^{m}_{n} – institution's n absolute value for indicator m

A'^{m}_{n} - institution's n quantitative indicator's value for indicator m

n – institution number from 1 to 7

m – indicator number

For information security governance indicators the range for possible response values for the survey was predefined. There were two types of questions in the survey – multi-choice or single-choice. Each question and its possible responses were rated with absolute numbers. Then the absolute values for the responses were converted to quantitative indicator values based on absolute value position on the scale between the minimum possible and the maximum possible response value for each indicator (see Formula 2).

$$A'^{m}_{n} = TRUNC(3 * \frac{A^{m}_{n} - X}{Y - X} + 1) \quad (\mathbf{2})$$

where

A^{m}_{n} – institution's n absolute value for indicator m

A'^{m}_{n} - institution's n quantitative indicator's value for indicator m

n – institution number from 1 to 7

m – indicator number

X – minimum possible value for survey's question

Y – maximum possible value for survey's question

The research results are shown in the table 1 below. For each financial institution the sum for financial performance indicator and information security governance quantitative values are calculated. Additionally, deviations from ratios calculated and ratio average are expressed in percentage. Therefore, there is relation showed between financial performance and information security governance indicators model.

Table 1

Financial performance and information security governance indicators trend analysis

Indicators	FI1	FI2	FI3	FI4	FI5	FI6	FI7
Financial performance indicators in 2007							
Quick Ratio	2	1	1	1	3	3	1
Debt to Equity	1	3	2	1	3	1	2
Gross Profit Margin	3	1	1	2	1	1	1
Accounts Receivable Turnover	1	1	1	3	2	2	2
Sales to Total Assets	2	1	2	3	2	3	3
Total	**9**	**7**	**7**	**10**	**11**	**10**	**9**
Information security governance indicators							
Assignment and supervision of responsibilities	1.75	1.5	1.75	2.38	2.5	2.63	1.75
Security organization	2.13	1.75	1.88	2.25	1.88	2.63	2
Security practices	2.75	1.63	1.88	2.5	2.38	2.38	2.13
Security investment management	2.33	2	2.33	1.67	2.33	2.33	2
Total	**8.96**	**6.88**	**7.84**	**8.8**	**9.09**	**9.97**	**7.88**
Trend analysis							
Total financial performance indicators to Total information security governance indicators	1.004	1.017	0.892	1.136	1.210	1.003	1.142
Average	1.058						
Deviation from average (%)	5.065	3.838	15.613	7.401	14.372	5.202	7.946

6. Summary and future work

According to the final results presented in the paper there have been identified trends between financial performance indicators and information security governance indicators. Deviation percentage from the average results for the financial institutions under research varies from 3.838 – 15.613%. This variation of percentage can be justified by several aspects, such as:

- Subjectivity factor exposed in the survey. While answering to questions included in the survey each respondent had possibility to influence the results of the particular survey.
- Different survey questions interpretations. Different interpretation of the survey questions among surveyed financial institutions might influence the survey results.

Therefore, authors can conclude that in this particular and proposed model there has been found relatively high relation between these two sets of KPI's. Based on research results authors propose to treat information security governance as one of financial institution KPI's.

Nevertheless, deviation percentage variation shows that model may be improved in the future. Authors have been identified several issues that may be developed further based on the proposed model:

- From financial performance analysis point of view it is recommended to look for financial institutions performance trends in several years period. Therefore, proposed model may be improved using financial performance data provided for time-period that has additional importance in financial performance analysis. This addition could give more precise and realistic input from financial institution's financial performance point of view.
- From information security point of view selected questions and aspects may be more advanced and more detailed in order to cover wider and deeper understanding of information security. Therefore, proposed model may be improved by more qualitative aspects defining information security governance.

Additionally the model could be extrapolated to other industries as well. In such case to verify the hypothesis similar analysis of correlation between financial performance and information security governance sets of KPIs should be performed.

Further research may be performed to determine the influence of information security governance on institution's financial performance. The following hypothesis for such research could be advanced stating that improving information security governance also improves institution's financial and overall performance.

References

1. Standard & Poor`s homepage / Standard & Poor`s, 2008. – www.standardandpoors.com – 02.09.2008.
2. Fitch Ratings homepage / Fitch Ratings, 2008. – www.fitchratings.com – 02.09.2008.
3. Moody's homepage / Moody's, 2008. – www.moodys.com – 02.09.2008.
4. Business Software Alliance. Information Security Governance: Toward a framework for action. – 2005
5. Institute of Internal Auditors. Information Security Management and Assurance: A Call to Action for Corporate Governance. - 2000.
6. Loyd S. Corporate Governance and Information Security. – SANS Institute, 2004
7. Information Technology Governance Institute. Information Security Governance: Guidance for Boards of Directors and Executive Management. - 2006
8. Information Security Forum, "The Standard of Good Practice for Information Security", Version 4, March 2003.
9. SPI-Finance project homepage / SPI-Finance project, 2008 - www.spifinance.com - 02.09.2008.
10. Arnold G. Corporate financial management. – Pearson education limited, 2005.
11. Norman M Scarborough, Douglas L Wilson, Thomas W. Zimmer. Effective Small Business Management. An Entrepreneurial Approach, Ninth Edition. – Pearson education limited, 2009. – P.241-264.
12. Jeff Madura. International Corporate Finance, Ninth Edition – Thomson South-Western, 2008. – P.422-445.
13. Kryukov D. Concept of information security system evaluation model. Scientific proceedings of Riga Technical University. – Riga: RTU, 2008.
14. Chapin, Akridge. How can security be measured. Vol 2. – Information Security Audit and Control association, 2005
15. Information Technology Governance Institute. IT Governance and Process Maturity. – 2008.
16. Kanhere V. Drivinng value from Information security: a governance perspective. Vol 2 – ISACA Journal, 2009
17. UcedaVelez T. Value of IT: beyond the theoretical. Vol 2 – ISACA Journal, 2009
18. Global Information Security Survey – Ernst & Young Global, 2008
19. Information Security Survey 2006 – KPMG EDP Auditors N.V.
20. Global Technology Media and Telecommunications Security Survey 2007 – Deloitte Touche Totmatsu
21. Information Security Survey 2007 – Gartner Inc.
22. IT Spending Survey 2007 – Gartner Inc.

Krjukovs D., Strauss R. Informācijas drošības pārvaldība kā finanšu institūciju darbības rādītājs

Ņemot vērā finanšu institūciju nozīmīgumu gan uzņēmējdarbības, gan valsts, gan ikviena indivīda dzīvē, šo institūciju darbībai un to rādītājiem vienmēr ir pievērsta liela uzmanība no dažādu ieinteresēto pušu grupām. Minētās grupas saskaņā ar savām interesēm izmanto dažādus darbības rādītāju komplektus finanšu institūciju darbības mērīšanai. Piedāvātajā darbā autori izvirza hipotēzi, ka informācijas drošības pārvaldība ir būtisks finanšu institūciju darbības rādītājs. Autori sniedz augsta līmeņa esošās situācijas apskatu finanšu institūciju darbības rādītāju sfērā. Tiek apskatītas pušu grupas, kuras varētu būt ieinteresētas finanšu institūciju darbības mērīšanā. Līdzīgi, kā korporatīvā pārvaldība ir uzskatāma par finansiāli un darbības efektivitāti ietekmējošu un atspoguļojošo faktoru, arī informācijas drošības pārvaldībai, kā korporatīvās pārvaldības sastāvdaļai pēc autoru domām jābūt uztvertai par būtisku finanšu institūcijas darbības rādītāju. Darbā tiek definēti būtiskākie indikatīvie finanšu institūciju finanšu darbības rādītāji un to aprēķināšanas metodes, tiek dots ieskats informācijas drošības novērtēšanas modeļos un pētījumos. Lai pārbaudītu izvirzīto hipotēzi, autori izmantoja

informācijas drošības brieduma modeļa konceptu. Darbā tiek piedāvāta un aprakstīta finanšu darbības rādītāju un informācijas drošības brieduma modeļa rādītāju vērtību aprēķināšanas metodika. Izvirzītā hipotēze tiek pierādīta, veicot korelācijas analīzi starp aprēķinātajiem finanšu darbības rādītājiem un informācijas drošības brieduma modeļa rādītājiem izvēlētajām Latvijas finanšu institūcijām.

Kryukov D., Strauss R. Information security governance as key performance indicator for financial institutions

Due to their nature financial institutions and their performance are in constant focus of attention from different stakeholder groups. These groups according to their functions and interests are implementing different sets of key performance indicators for financial institution performance assessment. In the proposed paper authors present a hypothesis of information security governance being a financial institution key performance indicator. Authors provide high level overview of existing situation in key performance indicator domain for financial institutions. The overview of stakeholder groups interested in financial institution performance management is provided. In the same way as corporate governance is treated as financial and operational performance reflecting and influencing factor, information security governance as a component of corporate governance, according to authors' opinion, should be treated as key performance indicator for financial institutions. In the paper the most indicative financial performance indicators as well as their calculation methods are defined for financial institutions. The paper contains overview of information security assessment models and researches in this field. Authors have chosen information security maturity model to use in testing hypothesis. The paper contains description of calculation methodology for financial performance indicators and information security maturity indicators. The hypothesis has been proved performing analysis of correlation between calculated financial performance indicators and information security governance model indicators for chosen Latvian financial institutions.

Крюков Д., Страус Р. Управление информационной безопасностью как ключевой показатель производительности для финансовых учреждений.

По своей природе к деятельности финансовых учреждений и показателям их производительности всегда привлекается повышенное внимание со стороны различных групп заинтересованных лиц. Эти группы в соответствии со своими интересами используют различные наборы показателей производительности для измерения производительности финансовых учреждений. В предлагаемой работе авторы выдвигают гипотезу о том, что управление информационной безопасностью может являться ключевым показателем производительности для финансовых учреждений. Авторы предоставляют высокоуровневый обзор в сфере показателей производительности финансовых учреждений. Рассматриваются группы лиц, заинтересованных в измерении производительности таких учреждений. Подобно тому, как корпоративное управление рассматривается как фактор, отображающий и влияющий на эффективность финансовой и операционной деятельности, управление информационной безопасностью, как составная часть корпоративного управления, по мнению авторов, должно расцениваться как ключевой показатель производительности финансовых учреждений. В предлагаемой работе определяются наиболее индикативные показатели финансовой деятельности для финансовых учреждений, а также методы для их расчетов. Также предлагается обзор моделей оценки информационной безопасности и исследований в этой сфере. Авторы выбрали модель зрелости информационной безопасности для использования при проверке гипотезы. В предлагаемой работе описывается методика расчета показателей финансовой деятельности и показателей зрелости информационной безопасности. Выдвинутая гипотеза доказывается проведя анализ корреляции между показателями финансовой деятельности и показателями модели зрелости информационной безопасности для выбранных финансовых учреждений Латвии.