Macrothink Institute™

Research in Applied Economics
ISSN 1948-5433
2013, Vol. 5, No. 2

Perception of Information Security of Management of Banking and Insurance Companies in Countries of Western Balkans

Edin Osmanbegović[1,*] & Sejfudin Zahirović[1]

[1] Faculty of Economics, University of Tuzla, Univerzitetska 8, Tuzla 75000, Bosnia and Herzegovina

*Corresponding author: Faculty of Economics, University of Tuzla, Univerzitetska 8, Tuzla 75000, Bosnia and Herzegovina. Tel: 387-61-101-741 E-mail: edin.osmanbegovic@untz.ba

Received: March 4, 2013 Accepted: June 6, 2013 Published: June 24, 2013

doi:10.5296/rae.v5i2.3348 URL: http://dx.doi.org/10.5296/rae.v5i2.3348

Abstract

In this paper it is described aspects of standardisation of information security and its implementation in banking and insurance companies in countries of Western Balkans. In terms of approaching the standards of EU, one of the areas that need to be fully justified is the information security. It has been identified and applied a new dual methodology which covers measurement of same variables of information security into two opposite populations. Authors identify banking and insurance sector as a key sector for research due to sensitivity of financial data and information that these companies work with. Key obstacles in implementation of information security come from managers who consider that existing level of information security is on much higher level than it actually is. The authors have identified intensity of perception of information security and gap in perception between managers of financial institutions and auditors, and rank of significant properties of information security. Factor analyses were conducted and four factors were identified which show managers' perception of information security. Also, the authors have identified attributes of marketing aspects of information security and market potential of information security of banking and insurance sector in countries of Western Balkans.

Keywords: information security; perception; managers; standardisation; Western Balkans

1. Introduction

Information technology security is currently one of the most important topics that users and providers of information technology are facing. Organisations are dependent of information technology. This means that they are more vulnerable on information threats. The vulnerability of information systems is increasing as we move towards network computing. There are number of threats within and outside organisation that must be taken into account. These problems are caused by threats such as illegal access, malware, spam mails, and system troubles (Takemura, Osajima and Kawano, 2009). Consequences of these threats can occur in forms of destroying resources, malfunction of applications and data, denial of service, stealing the service and stealing the resources (Seen, 2004).

Information security refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (Statewide Information Systems Policy, 2010). Most common threats against information technology systems can occur on client (user) side, communication lines, corporate servers and corporate systems (Laudon and Laudon, 2005). They can stem from technical, organisational, and environmental factors compounded by poor management decisions. An organisation should build strong safeguards to prevent valuable data being lost, destroyed, or could fall into the wrong hands, revealing important trade secrets or information that violates personal privacy.

In order to get knowledge about state of information security in organisation, it is necessary to research perception of different aspects of information security. As a part of overall information security activities, it can be assumed that perception of attributes of standardisation of information security can indicate the state of information security in companies. Also, this helps to recognize limitations and guidelines for improvement of the information security system. Research described in this paper was conducted in order to discover indicators about perception of information security of management in banking and insurance companies, and information security auditing companies. This can help in improvement of standardisation of information security procedures, as well as finding put knowledge of marketing aspects of information security and market potential of it.

Because of significance of financial sector and vulnerability of the sector, particularly in countries in transition, research was conducted in banking and insurance companies in Western Balkans.

2. Theoretical Frame of Research

In literature it can be found results of different research of influence of information systems and security procedures on overall business and particularly on organisation aspects of business. In context of implementation of information security procedures, the issue of perception of management needs to be researched due to constant and rapid improvement of all aspects of information systems and their security. Framework of this research is based on issues of standardisation of information security. Particular emphasize has been put on ISO

27000 group of standards.

2.1 Theoretical Aspects of Standardisation of Information Security

Information security and control have become crucial nowadays. Organisations may have very valuable information assets to protect. Protection of information resources can be reached mainly through implementation of controls (defence mechanisms) in order to prevent accidental or intentional danger to occur, and detect problems as soon as possible. Important point of protection is to prevent incidents. Defense does not serve anything after an incident has occurred.

One of the most important issues regarding information processing is information security itself. Information security must not be taken as granted. It is an issue of constant work and improvement in any organisation which is dealing with information assets. Some research has shown that 75 percent of companies with information security policies do not keep them up-to-date and that only 9 percent of employees understand these security policies (Laudon and Laudon, 2005). Many organisations lack disaster recovery and business continuity plans, or fail to patch their software routinely against security vulnerabilities. Managers do not appreciate the value of a sound security strategy. Security is a subject most business executives try to avoid since they feel that discussing their business security procedures and policies might increase risk of an attack (Reynolds, 2004). Security threats grow every day, but they are neither predictable nor finite. This makes more difficult to calculate returns on security investments. Unless managers change their attitude about security, security budgets will be inadequate. As standardisation of information security has to be considered within information security as a whole, it can be expected that business executives would try to avoid it.

2.2 Standardisation of Information Security

Standardisation of information security refers to introduction of procedures of protection and allocation of responsibilities in establishment of business recovery procedures. This means that protection of system in case of technical, environmental and management failure should be set as a routine task.

Guidelines for standardisation of information security should be aligned with the business strategy through effective implementation, procurement and integration of the system (Turban, McLean and Wetherbe, 2002). Standardized information security is a set of procedures consisting of hardware, software, lifeware, orgware, netware and dataware support (Hutinski, Sehanović and Zugaj, 2002).

Protection of information resources requires a sound security policy and set of controls. ISO/IEC 27001, an international set of standards for security and control, provides helpful guidelines. It specifies best practices in information systems security and control, including security policy, business continuity planning, physical security, access control, compliance, and creating a security function within the organisation.

There are number of reasons for implementing an information security system that is capable

of being independently certified as compliant with ISO/IEC 27001. A certificate tells existing and potential customers that the organisation has defined and put in place effective information security processes. This helps to create a trusting relationship (Calder and Watkins, 2006).

Protection of information resources requires a well-designed set of controls. Computer systems are controlled by a combination of general controls and application controls, such as following (International Standard ISO/IEC 27001, 2005): security policy, organisation of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, information security incident management, business continuity management and compliance.

Regarding the standardisation of information security, in the last few years there is an increasing number of certified organisations in the world, as it is illustrated in Figure 1. According to International Register if ISMS Certificates (International Register if ISMS Certificates, 2012), 7940 organisation had ISO 27001 standard in July 2012 worldwide. Japan comes on first place with 4152 organisations. United Kingdom comes on the top in Europe with 573 organisations.

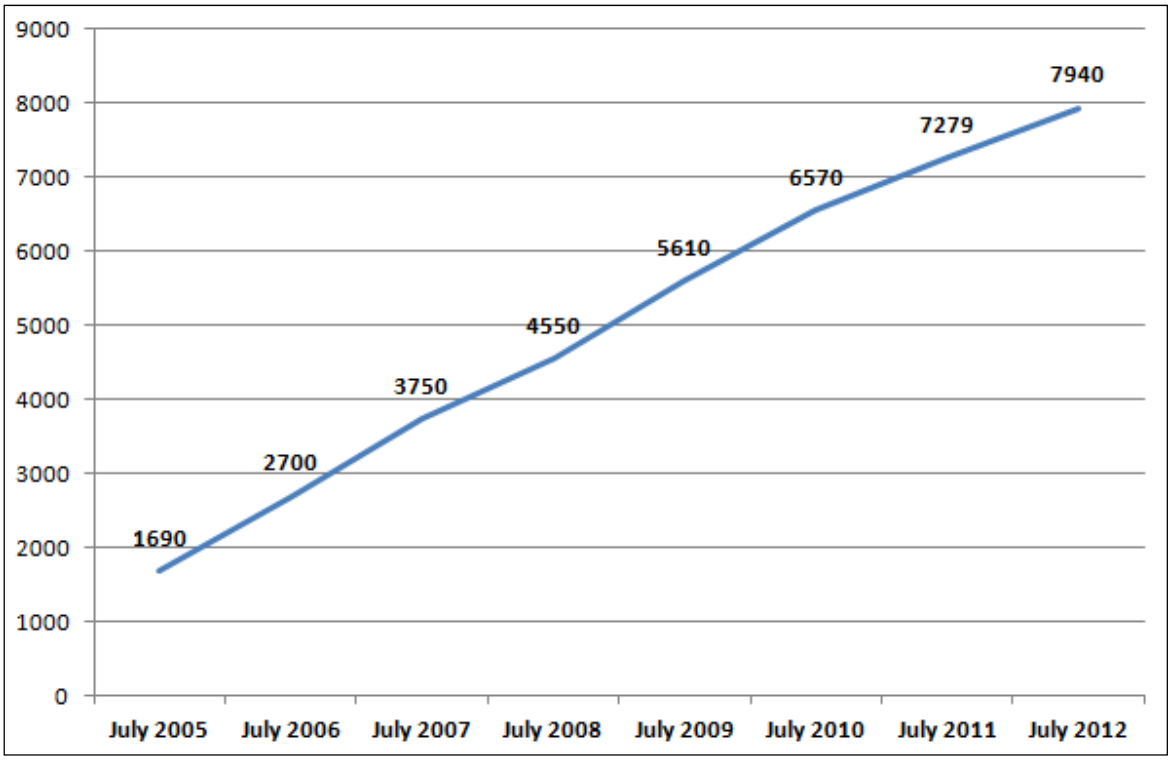

Figure 1: Number of ISO/IEC 27001 Certified Organisations in the World

Considering countries of Western Balkans there were 34 ISO/IEC 27001 certified organisations as following: 27 in Croatia, 2 in Bosnia and Herzegovina, 2 in FYR Macedonia and 3 in Albania, as it is illustrated in Table 1 (International Register if ISMS Certificates, 2012). Also in this region there is registered an increasing number of certified organisations,

in period 2011 – 2012.

Table 1: ISO/IEC 27001 Certified Organisations in Western Balkans

Country	July 2010	July 2011	July 2012
Croatia	6	7	27
Bosnia and Herzegovina	2	2	2
FYR Macedonia	0	2	2
Albania	0	2	3
Serbia	0	0	0
Montenegro	0	0	0
Kosovo under UNSCR 1244/99	0	0	0
Total Western Balkans	8	13	34
% Western Balkans in World	0.12	0.18	0.43

Regardless of growth of certified organisations, it is noticeable that the information security in not adequate in countries of Western Balkans. In some countries there are no ISO/IEC 27001 certified organisations at all (Serbia, Montenegro and Kosovo under UNSCR 1244/99). Therefore, research of perception of management in banking and insurance companies is necessary in order to promote the process if systematic improvement of system of information security.

3. Empirical Research Results of Information Security Procedures in Sectors of Banking and Insurance in Countries of Western Balkans

3.1 Research Methodology and Methods of Analysis

Primary research was conducted with dual methodology applied on two opposite populations with same instrument for measuring of variables, on one side management of banking and insurance companies, and on the other side management of information security auditing companies.

Standardisation of information security is not a compulsory activity in companies and institutions. It is still an optional choice for companies. Organisations from public sector may undertake standardisation activities based on political decision, while commercial sector does it as a measure of business protection as a whole. Banking and insurance companies are commercial companies; therefore they represent a pattern of behaviour for commercial sector.

Research was conducted in four countries: Croatia, Serbia, Bosnia and Herzegovina and Montenegro in period March – June 2012. The field work was conducted by e-mail questionnaire. There were two groups of examinees. First group were managers of banking and insurance companies, and second group were managers of information security auditing companies. Population of banking companies includes 30 in Bosnia and Herzegovina (20

banks in Federation of Bosnia and Herzegovina (Agencija za bankarstvo FBiH, 2012) and 10 banks in Republic of Srpska (Agencija za bankarstvo RS, 2012); 32 in Croatia (Popis hrvatskih banaka, 2012); 32 in Serbia (Spisak banaka Srbije, 2012); 11 in Monte Negro (Udruženje banaka Crne Gore, 2012). Population of insurance companies includes 28 insurance companies in Bosnia and Herzegovina (Agencija za osiguranje u BiH, 2012); 27 in Croatia (HANFA, 2012); 18 in Serbia (Osiguravajuća društva u Srbiji, 2012) and 10 in Monte Negro (Osiguravajuća društva u Crnoj Gori, 2012). Research sample comprised 21 banks companies and 14 insurance companies, which represents 31.34% and 33.33 % of total population, respectively. The second research group was auditing companies. Total population was 7 companies. Four of them took part in research and that represents 57.14 % of population. Information security auditing companies were from Slovenia, Croatia and Serbia, and their market was geographic space of Western Balkans.

The questionnaire was identical for both groups. Variables that were measured cover important aspects of perception of both samples of examinees regarding information security. The focus was on simultaneous analyses of attitudes of both groups (companies and auditors) regarding perception of importance of measured variables, in order to and determine which factors cause covariance between measured variables.

The questionnaire was divided into two parts and comprised 18 questions. First part of the questionnaire covered information security according to ISO/IEC 27001:2005 norm, while second part covered information security barriers and marketing aspects of information security. Perception was expressed with grade of formalisation of procedures of information security in written form and it was measured with 12 variables on Likert scale from 1 to 5 (1 - procedure is not formalized in written form at all, 5 - procedure is fully formalized in written form).

These variables were:

- Information security policy
- Organisation of information security
- Responsibility for Assets
- Information classification
- Human Resources Security
- Physical and Environmental Security
- Communications
- Access Control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business Continuity management

- Compliance.

There were 6 information security barriers defined as following:

- Price of standardisation of information security
- Insufficient number of auditors
- Insufficient knowledge of company managers about information security importance
- Insufficient expertise of company managers in organisational issues
- Inadequate marketing approach by auditors
- Insufficient expertise of IT employees in companies.

Perception of barriers was ranked according to importance of barriers with values from 1 to 6 (1 - highest importance of barrier, 6 - lowest highest importance of barrier). Marketing aspects of standardisation of information security were measured according to auditors' market activities. There were measured auditors approach to the companies and perception of price.

Auditors approach was defined by the following alternatives:

- Sending pricelist and offers to potential clients
- Sending electronic education materials to potential clients
- Sending hard copy education materials to potential clients
- Systematic marketing campaigns from auditors
- Promotion of favourable financial conditions of certification
- Personal contact between auditors and company managers.

Data analysis was carried out using descriptive statistics, Spearman's coefficient of rank correlation, correlation and factor analyses. Factor analysis was conducted for banking and insurance companies.

3.2 Research Results

We present the textual interpretations of the results gathered from 35 banking and insurance companies and 4 information security auditing companies.

Comparative analyses of median value of perception of information security procedures of both samples of respondents are illustrated in the Figure 2.

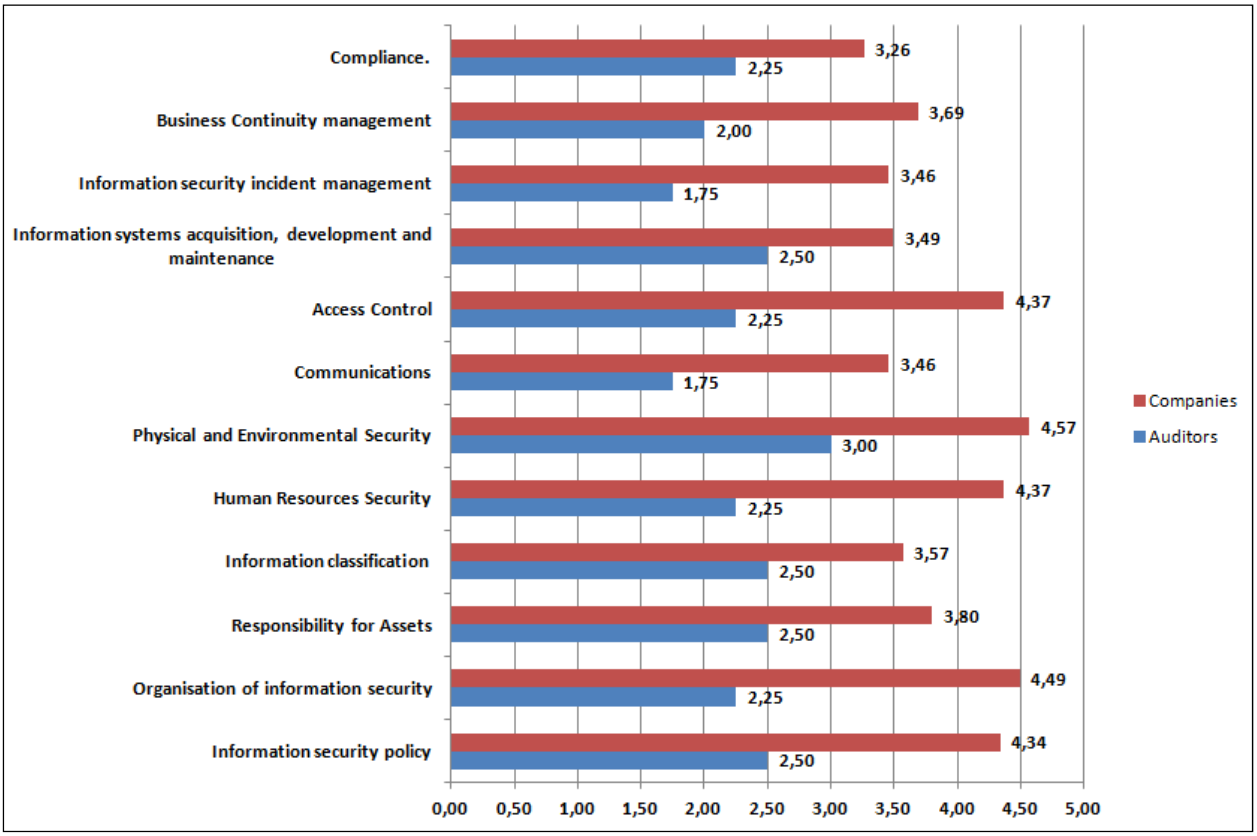

Figure 2: Comparative Analyses of Intensity of Perception of Information Security Procedures

From the Figure 2 it is noticeable that highest graded factor by banking and insurance managers was Physical and environmental security (4.57), while their lowest grade went to factor of Compliance (3.26). Highest graded factor by auditing managers was Physical and environmental security (3.00), and lowest graded were Information security incident management and Communications (both 1.75). The biggest gap in perception was in Organisation of Information Security (2.24) while lowest gap in perception was in Information System Acquisition, Development and Maintenance (0.99).

Generally looking, significant gap is noticeable regarding intensity of perception of information security procedures of respondents from both groups. Managers in organisations gave significantly higher grades to all aspect of information security in companies than auditing managers. It is noticeable that they significantly disagree regarding how good information security procedures are implemented in banking and insurance companies. Also, it can be noticed that managers in organisations underestimate importance of information security in comparison with auditing managers.

Ranking of median values of variables of both groups of respondents are illustrated in Table 2.

Table 2: Ranking of Information Security Procedures

Companies	Information security procedures	Auditors
1	Information security policy	1
2	Organisation of information security	6
3	Responsibility for Assets	7
4	Information classification	8
5	Human Resources Security	2
6	Physical and Environmental Security	3
7	Communications	10
8	Access Control	4
9	Information systems development and maintenance	5
10	Information security incident management	11
11	Business Continuity management	12
12	Compliance	9

Spearman's Rank Correlation Coefficient was calculated to show strength of correlation between groups. Spearman's rank correlation coefficient is a non-parametric measure of statistical dependence between groups. Correlation coefficient of 0.59 indicates that there is rather intense strength of correlation.

3.3 Factor Analyses of Perception of Managers of Banking and Insurance Companies

Factor analysis (Factor analysis was conducted with use of SPSS Statistics 17) was used to determine number of factors which explain relationships between variables and connection of those variables with factors. Based on correlation matrix of 12 variables and testing of null hypothesis that single coefficients of correlation are equal to null (Null hypothesis is accepted for values of significance greater than 0.05), it can be concluded that null hypothesis may accept coefficients of correlation of variable Information security policy and variables Information classification, Human Resources Security, Communications and Access Control; variable Compliance and Physical and Environmental Security, Information security incident management and Business Continuity management; variables Responsibility for Assets and Communications; variable Human Resources Security and variables Communications and Information security incident management; variable Communications and variables Information systems acquisition, development and maintenance and Information security incident management; variable Access Control and variables Information security incident management and Business Continuity management; and variables Information security incident management and Compliance. This means that it cannot be expected that these couples of variables occur together in explanation of single factors. Bartlett's Test of Sphericity is highly significant and indicates a conclusion that there is a significant correlation between variables.

Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO statistics) has value of 0.66 and this confirms justification of application of factor analyses in the research (Factor analyses is

recommended only if KMO statistics is greater than 0.5.). As an Extraction method it was used Principal Component Analysis, while number of factors were determined based on characteristic values (Principal Component Analysis) which were assigned to factors greater than 1. Analyses showed that four factors fulfilled these criteria. Percentage of explained variance for these four factors was 75.96. Rotation was applied using the Varimax rotation method with Kaiser's normalisation. Table 3 shows the results.

Table 3: Results of Factor Analysis after Rotation

Factor	Factor loading	Variables included in the factor	Strength of factors in explaining variance of variables (%)
F_1 (Readiness of employees)	0.827	Access Control	68.4
	0.805	Human Resources Security	64.8
	0.754	Physical and Environmental Security	56.9
	0.674	Information systems acquisition, development and maintenance	45.4
F_2 (Adaptability of organisation)	0.862	Information security policy	74.3
	0.736	Information security incident management	54.2
	0.544	Business Continuity management	29.6
F_3 (Availability of resources)	0.871	Organisation of information security	75.9
	0.768	Responsibility for Assets	59.0
	0.504	Information classification	25.4
F_4 (Normative aspects of security)	0.915	Communications management	83.7
	0.775	Compliance	60.1

The results confirm the justification for using factor analysis when identifying managers' impression about state of information security in banking and insurance companies. Interpretation and explanation of factors is based on weight of factors, specificity of information security research and our assessments.

First factor, F1 - (Readiness of employees), explains 68.4, 64.8, 56.9 and 45.4 percent of the variance of variables Access Control, Human Resources Security, Physical and Environmental Security and Information systems acquisition, development and maintenance. All variables which explain this factor have coefficients of correlation greater than 0.5, with highest coefficient of correlation (0.80) between variables Physical and Environmental

Security and Access Control. The second factor, F2 - (Adaptability of organisation), explains 74.3, 54.2 and 29.6 percent of variables Information security policy, Information security incident management and Business Continuity management. Highest coefficient of correlation (0.51) is between variables Information security incident management and Business Continuity management. Third factor, F3 - (Availability of resources), explains 75.9, 59.0 and 25.4 percent of variables Organisation of information security, Responsibility for Assets and Information classification. Highest coefficient of correlation (0.63) is between variables Organisation of information security and Responsibility for Assets. Fourth factor, F4 - (Normative aspects of security), explains 83.7 and 60.1 percent of variables Communications management and Compliance. Coefficient of correlation between these variables is 0.70.

3.4 Comparative Analyses of Perception of Information Security Barriers

Comparative analyses of perception of information security barriers of both populations of respondents are illustrated in Figure 3.

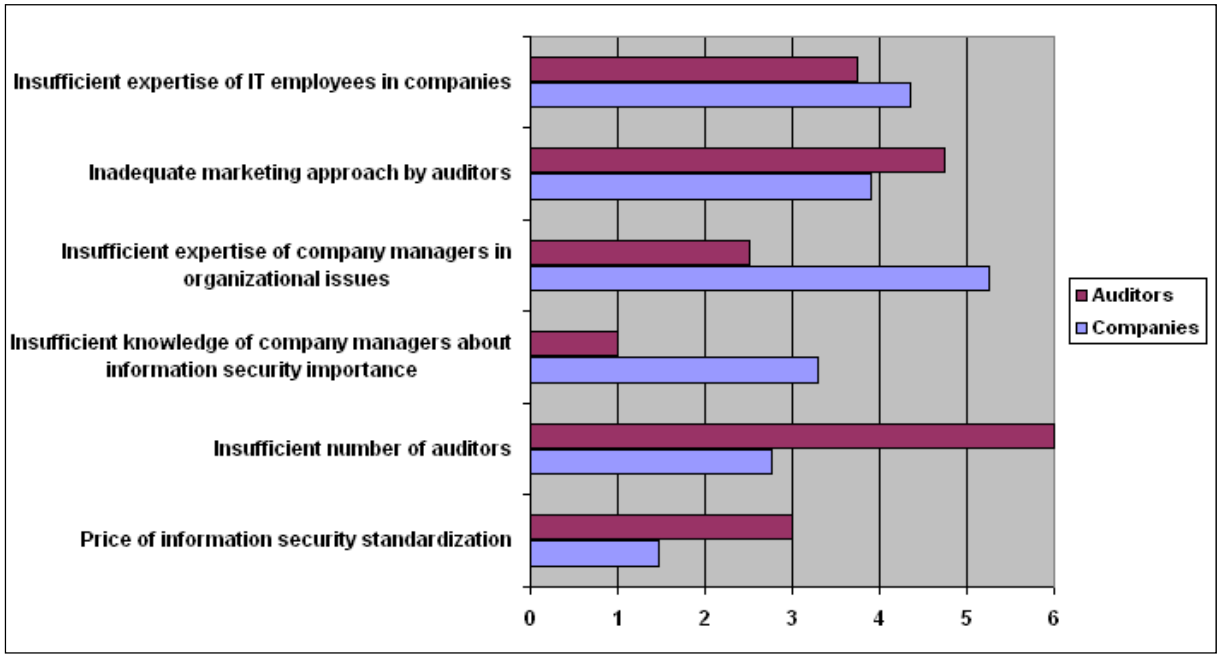

Figure 3: Comparative Analyses of Perception of Information Security Barriers

From the Figure 3 it is noticeable that highest graded barrier in banking and insurance managers was Price of standardisation of information security (1.47), while their lowest grade went to the factor Insufficient expertise of company managers in organisational issues (5.26). Highest graded barrier concerning auditing managers was Insufficient knowledge of company managers about information security importance (1.00), and lowest graded was Insufficient number of auditors (6.00). The biggest gap in perception of information security barriers was insufficient number of auditors (3.24) while lowest gap in perception of barriers was insufficient expertise of IT employees in companies (0.60).

There is a significant gap in perception of information security barriers of respondents from both groups. Managers in companies gave significantly higher importance to the Price of standardisation of information security and insufficient number of auditors than it was graded by auditors. At the same time auditors gave higher importance to insufficient knowledge of company managers about information security importance and insufficient expertise of company managers in organisational issues. It can be noticed that company managers have a perception that biggest information security barriers exist out of their companies, while auditors have a perception that biggest barriers are knowledge and skills of company managers regarding information security importance and organisational issues.

3.5 Analyses of Marketing Aspects of Information Security

Analyses of marketing aspects of information security are illustrated in Table 4. Marketing aspects of standardisation of information security were measured in terms of whether companies were exposed to some of the mentioned types of marketing activities.

Table 4: Marketing Activities of Standardisation of Information Security

Marketing Activity	[%]
Sending pricelist and offers to potential clients	65.22%
Sending electronic education materials to potential clients	95.65%
Sending hard copy education materials to potential clients	21.74%
Systematic marketing campaigns from auditors	39.13%
Promotion of favourable financial conditions of certification	4.35%
Personal contact between auditors and company managers	8.79%

From Table 4 it can be noticed that the most represented way of communication between companies and auditors were Sending pricelist and offers to potential clients (65.22%) and Sending electronic education materials to potential clients (95.65%). Auditors relied mostly on these two marketing activities. It can be observed that Systematic marketing campaigns from auditors (39.13%) and Personal contact between auditors and company managers (8.79%) were lowly presented.

When it comes to the price of standardisation of information security, average price charged by auditors was 22,750.00 €, while average price that companies were ready to pay was 19,964.00 €. The gap was 2,786.00 € or 13.94% with regard to the average price the companies were ready to pay. This gap was not significantly big regarding to the financial potential of banking and insurance companies. These data can serve to calculate market variables such as market potential, market volume, etc. that can be useful to managers of companies and auditors.

4. Conclusion

The research described in this paper lead us to the conclusions that there is a big gap in perception of information security issues of respondents from banking and insurance

companies and auditing managers. In general, banking and insurance managers graded higher all information security issues in own companies than auditing managers did it. These two populations of respondents have different motivation regarding information security. On one hand, mangers of banking and insurance companies do not appreciate the security strategy issues, and they are always trying to spend lesser on it. On the other hand, information security auditing managers have commercial motivation and they are trying to earn more by estimating information security worse than it really is. Real state of information security should lie somewhere between grades of these two populations of respondents.

Ranking the significance of information security variables from groups of respondents has rather high correlation. Although they disagree in terms of real state of information security, they mostly agree concerning significance of particular security procedures. This should be a good starting point which can bring managers together when it comes to implementing information security procedures.

Factor analyses extracted four factors as following: readiness of employees, adaptability of organisation, availability of resources, and normative aspects of security. Mentioned factors have high correlation with belonging variables and simplify the view on standardisation of information security. This should make it easier for banking and insurance managers to appreciate information security and to invest in it more than it has been case so far. The results confirm the justification for using factor analysis to identify managers' impression about state of information security in banking and insurance companies.

Analyses of perception of information security barriers show that there is a significant gap in perception of information security barriers among respondents from both populations. This can help information security auditors in their approach to companies, because they can look on information security issues from company managers perspective.

Analyses of marketing aspects of information security show which marketing activities were mainly presented. This means that information security auditing managers can adapt their marketing approach to banking and insurance companies. This is even more noticeable when it comes to amount of money that managers are ready to invest in standardisation of information security. Investment gap was not significantly big when it comes to the financial potential of banking and insurance companies, therefore big market and financial potential of standardisation of information security in the region of countries of Western Balkans can be exploited with lower barriers than it has been case so far.

Results of this research show that there is necessary to conduct promotion activities of importance of information security in countries of Western Balkans and to give to this aspect of business adequate place in overall business activities in organisations.

In this paper it has been given a new methodology of research of information security which is called "dual methodology". The results of research confirm justification of usage of proposed methodology and statistical procedures within it. Dual methodology proved to be efficient and it can be recommended for research of state of information security in other regional markets.

References

Agencija za bankarstvo FBiH. (2012). Retrieved February 14, 2012 from http://www.fba.ba/index.php?page=27

Agencija za bankarstvo RS. (2012). Retrieved February 14, 2012 from http://www.abrs.ba/banke/banke_lat.htm

Agencija za osiguranje u BiH. (2012). Retrieved February 14, 2012 from http://www.azobih.gov.ba/cms/index.php

Calder, Watkins, (2006). *International IT Governence – An Executive Guide to ISO 17799 / ISO/IEC 27001:2005*. London: Kogan.

HANFA. (2012). Retrieved February 16, 2012 from http://www.hanfa.hr/index.php?AKCIJA=osiguranjaPO&VRSTA=drustva

Hutinski, Sehanovic, Zugaj. (2002). *Informatika za ekonomiste*(1st ed.). Pula: Sveuciliste u Rijeci.

International Register if ISMS Certificates. (2011). Retrieved July 21, 2011 from http://www.iso27001certificates.com/Register%20Search.htm

International Standard ISO/IEC 27001. (2005). Information technology - Security techniques - Information security management systems – Requirements.

Laudon, Laudon, (2005). *Management Information Systems: Managing the Digital Firm* (9th ed.). New Jersey: Pearson Prentice Hall.

Osiguravajuća društva u Crnoj Gori. (2012). Retrieved February 18, 2012 from http://www.portal-crnagora.com/finansije/osiguravajuca-drustva/

Osiguravajuća društva u Srbiji. (2012). Retrieved February 14, 2012 from http://www.portal-srbija.com/banke-i-osiguranja/osiguravajuca-drustva/

Popis hrvatskih banaka. (2012). Retrieved February 16, 2012 from http://www.hnb.hr/supervizija/liste/hlista_banaka.htm

Reynolds, J. (2004). *The Complete E-Commerce Book*(2nd ed.). New York: CMP Books.

Seen J.A. (2004). *Information technology*(1st ed.). Beograd: Edicija Stvarni svet. 834.

Spisak banaka. (2012). Retrieved February 14, 2012 from http://www.kamatica.com/spisak-banaka

Statewide Information Systems Policy. (2010). Statewide Policy: Computer Security Incident Management. Retrieved December 12, 2011 from http://itsd.mt.gov/content/policy/policies/NIST_CF8/Statewide_Policy_Computer_Security_Incident_Management.pdf

Takemura T., Osajima M., & Kawano M. (2009). Positive Analysis on Vulnerability, Information Security Incidents, and the Countermeasures of Japanese Internet Service

Providers. *International Journal of Human and Social Sciences, 4*(15), 1140.

Turban, McLean, Wetherbe, (2002). I*nformation Technology for Management*(3rd ed.). New York. John Wiley & Sons Inc.

Udruženje banaka Crne Gore. (2012). Retrieved February 18, 2012 from http://www.ubcg.info/