Holistic Approach for Governing Information System Security

Mario Spremić, *Member, IAENG*

***Abstract*— Over the past decade information system security issues has been treated mainly from technology perspective. That model of information security management was reactive, mainly technologically driven and rarely aligned to business needs. This paper goes a step further and considers it from the governance view, mainly aligning it with the risk management activities and stressing the necessity for a holistic approach in which the executive management should be involved. The main objective of the paper is to stress the importance of implementing information system security governance model as a proactive and holistic approach which aligns security mechanisms, procedures and metrics with governance principles, business drivers and enterprise strategic objectives. Information system security governance model is constructed, explained and discussed. Approaches to for information system security assurance are analysed and the phases and processes of its regular reviews (audits) explained in further details. The standards and legislation activities that help in that sense are evaluated. The holistic model of governing information system security risks as business risks is explained and discussed.**

***Index Terms*— Information System Security Governance Model, IS Auditing, Holistic approach**

I. Introduction

MAIN objective of this paper is to stress the importance of information system security governance. Reactive approach to information systems security was based on technological aspects, but this 'managing' approach proves to be ineffective and obsolete. Therefore in this paper we have particularly focused on holistic – proactive and governance approach (information system security governance), where security issues includes organizational and other non-technical aspects, and the whole model needs to be well aligned with strategic objectives and business drivers.

Information systems (IS) plays very important role in modern business organizations supporting its organizational efficiency or, under certain circumstances, fostering business model innovation and change. IS can influence organization competiveness in two ways:

- supporting operational efficiency (IS as a main infrastructure for the current business), or
- differentiating business through business model innovation and business process change.

In the first role IS enhance conduction of business processes in more efficient, quicker and effective way supporting cost leadership strategy.

F. A. Mario Spremic is full professor Faculty of Economics and Business Zagreb, Department of Informatics, University of Zagreb, Kennedy's sq 6, 10000 Zagreb. CROATIA (e-mail: mspremic@efzg.hr)

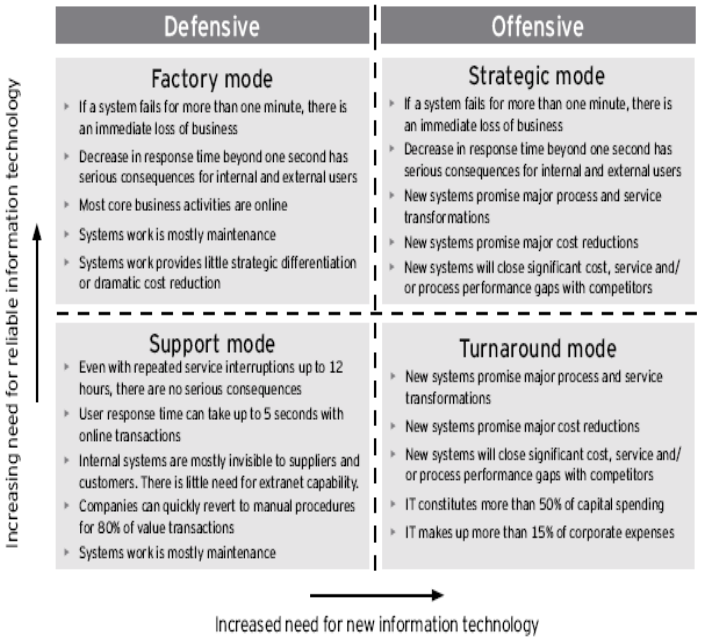

Figure 1. IT Strategic Grid

According to well known McFarlan IT Strategic Grid depicted on figure 1 (Nolan, McFarlan 2005), this is so called defensive role IS might have in the business, with no direct influence on organizational innovativeness, but acting as a strong tool for cutting costs and making business processes conduct faster, efficient and with lower transactional costs. In other mode, IS takes an offensive role to the business, fostering change of business processes and innovation of business model which may result in direct competitive advantage. Innovative IS and underlying information technology (IT) offer so called 'temporary monopoly' to the business mainly through its turnaround and strategic mode. Ernst & Young (2011) reported that 61% of executives believe that IT should focus on driving innovation in business processes.

In either way IS becomes very important to the business and needs to be aligned with strategic objectives in order to justify massive investments. A number of studies (Weill and Ross (2004), Groznik et. al (2003), Spremić (2002)) showed that investments in IS and underlying IT resulted in added business value only if they are truly connected with strategic business objectives.

In that sense proliferation of governance of enterprise IT helps companies manage, or rather, govern IS as a primary business function with executive management involved in making decision about IS and IT. The quality of IT governance is rising with the large number of decisions

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

about IS made by executive management, not IT departments. The more executive management is engaged in making decision about IS and IT, the IT governance is of better quality (Spremic, 2012). Recent researches stands on that point, for example ITGI (2011) reported that important business outcomes of governance of enterprise IT are improved management of IT-related risks, improved communication and relationships between business and IT and improved business competitiveness.

On the other hand, IS and IT becomes inevitable tool for everyday personal activities and pervasive infrastructure for conducting businesses. In fact, environment we working in and information chaos we are living in requires strong governance. ISACA (2012) reported that 6 out of 10 employees aged 18-35 use a personal device for work, security breaches and cybercrime costs are estimated at $ 1 trillion per year and the average costs for a downtime in 2011 was $ 5.000 per minute or 380 billion $ in total in 2011, while by 2020 there will be 24 billion connected devices.

In that sense it is very important to develop holistic business model of governing IS in order to enable executive management involvement in decision making process about IS and IT. It is obvious that IS issues, namely IS security issues are not technical, but business problem that can't be managed at IT department level, but governed at executive level. In this paper we will give a short review of methods, standards and frameworks for IS security and propose a holistic approach to its effective governance.

II. LITERATURE REVIEW ON INFORMATION SYSTEM SECURITY GOVERNANCE

Most organizations in all sectors of industry, commerce and government are fundamentally dependent on their information systems (IS) and would quickly cease to function should the technology (preferably information technology – IT) that underpins their activities ever come to halt. Although, characteristics of IS security incidents and associated risks have dramatically changed in recent decades, IS and underlying IT are still often mistakenly regarded as a separate organization of the business and thus a separate risk, control and security environment. While since 10 or 15 years ago a IS security incident could cause minor 'technical' problems, today it may affect the corporation's competitive position and strategic goals.

In the last 15 years numerous issues have occurred that affect IS security, such as:

- increased internal threats (internal 'wikileaks' incidents, data breaches, malicious attacks from within),
- emergent technologies (for example, cloud computing, web 2.0., mobile technology, social media, RFID, etc.),
- increased external threats (especially due to heavy information connectivity between organizations and vast number of interconnected devices),
- huge data proliferation (average knowledge worker receives 3 terabytes of information per year and the average corporate worker sends and receive 112 e-mails per day (ISACA, 2012),
- extensive use of mobile devices and social media networks and increasingly mobile workforce,
- strong regulation at international and national domain in the area of IS security and data privacy. For example, 65 countries have their own data protection law (ISACA, 2012).

For far too long information security has been operating in a reactive mode. There are a number of evidences where information security professionals have been forced to comply with solutions, frameworks and standards seeing and understanding problem just from technological side. An enterprise would be perfectly compliant with certain security framework and standard but the number of security incidents was not declining and the information security environment was not improved.

According to Ernst & Young 2010 Global Information Security Survey business continuity management is viewed as the most important security risk, followed by compliance and regulatory requirements, data leakage and data loss, information security risk management and identity and access management. According to 2010 Ponemon Institute study, the average total cost per data breach has risen to 7,2 million $, or $204 per incident, compared to $138 in 2005 (Ernst & Young, 2011). Forrester Research Institute calculated the cost per record from $90 to $305, depending on industry and regulatory requirements (Forrester, 2011).

Although, the nature of risks associated to IS security has changed, there are modest research efforts on holistic view at the issue. A number of frameworks and approaches used in practice are mainly oriented to managing IS security risk as a technical problem, with no attention being drawn to executives (governance) layers. Wide range of different evaluation models may be in place (ISO 27001, NIST, SANS, IS3, etc.), but they are used to calculate the technical measure of the associated risks. These calculations and activities need to be part of comprehensive IS security business model who should be aligned with IT Governance rules, policies and procedures. If there is no connection between methods of assessing IS security risk levels and strategic objectives of the business and governance policies (assigning responsibility, defining metrics and risk ownership), measuring IS security risks is technical procedure with no added value to the business, and in fact we are discussing about IS security management activities.

A number of novel researches in the field of IS security management proves the complexity of the problem. Ifinedo (2009) explored IT security concerns in various countries in finance and banking sector, while Caceres and Teshigawara (2010) investigated the security guidelines tool for home users based on international standards and came up to conclusion that automated tools can help users gain information about international standards. IS security issues have been investigating from various perspectives. Von Solms (2006) concluded that information security includes organizational aspects, legal aspects, institutionalization and application of best practice in addition to security technologies. A number of studies (Siponen, 2007; Spremic 2009; Werlinger, et.al. 2009; Abu-Masa, 2010) revealed that research on the non-technical aspects is needed. Hagen et.al (2008) found that technical-administrative measures such as policies, procedures and methods are most commonly implemented organizational information security measures

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

in a sample on Norwegian companies. They concluded that such a practice might be in place to pressure to comply with standards who precisely prescribe measures (security policies, procedures and controls, administration tools, creation and maintenance of security awareness). There are some holistic approached to the problem in the literature, preferably in the area of effectiveness of information security who has been investigating from various perspectives, namely risk management perspective (Singleton, 2012, Spremic, 2008, 2012), economic perspective (Gordon and Loeb, 2002 and their economic model for information security, or ISACA 2010 and their business model for information security) legal and cultural perspective, but there are few methodologies proposed.

We tried to fill that research gap by trying to present and explain a model of the IS security governance as a holistic and structured approach that aligns governance policies, business strategy, management procedures, business processes and operational activities with the purpose of evaluating and managing IS security risk and assign responsibilities and accountability on higher executive levels'.

III. CONSTRUCTING INFORMATION SYSTEM SECURITY GOVERNANCE

IS security management approach proves to be ineffective, because it was mainly oriented to technological part of the problem (tools, hardware, algorithms, infrastructure) and neglected the fact that IS is composed of 'soft' components too, such as people, procedures, processes, politics. So it is obvious that reactive – management approach to IS security is no longer effective and a new, proactive – governance based concept is to be introduced.

Contrary to IS management solutions which uses cause-and-effect pattern and 'need-to-be-compliant' approach no matter of the value added to the business, governance based models for IS security examines the entire enterprise security from business perspective and assist executives in managing IT risks. Main objective of IS security management efforts was to be aligned with the specific standard or framework. Frameworks and standards help organisations to fulfil regulatory requirements and possibly to strengthen security efforts, but they have not provided a holistic solution that examines the entire enterprise and studies how the organisational mission affects the security program and *vice versa* (ISACA 2010).

Therefore, IS security governance model addresses the problem at the strategic and business level with six key outcomes:

- **strategic alignment** with business objectives,
- **risk management** procedures which arises from business perspectives and upon business impact analysis,
- **value delivery** through smart investments in preserving valuable IS resources and allowing businesses to keep running or innovating,
- **resource management** activities which are balancing between people, organization, processes and technology as main resources for IS security governance (due care should be given on managing non-technological resources, preferably people and various organizational aspects such as culture, governance mechanisms, desirable behaviour, politics, etc.),
- **performance management** who should identify appropriate methodologies for measuring the outcomes of IS security efforts and key metrics in every single area with desirable key performance indicators (key risk indicators and key security measures), and
- **assurance process integration** involving regular IS security auditing activities at various levels (internal, external, regulatory, national, international) with proper reporting to executive levels and regulation authorities. IS security assurance and auditing should be done by professionals outside IT department with the main objective of evaluating if the current practice is correct, eventually prescribing control countermeasures needed to be implemented to improve the IS security practice and validating the compliance with required regulations (national, international).

On figure 2 the model for IS security governance is depicted. It is consisted of governance and management layers. Governance layer include business drivers and partly corporate IT governance policies. Management layers include procedures for management IS security on business or functional level and technical activities.

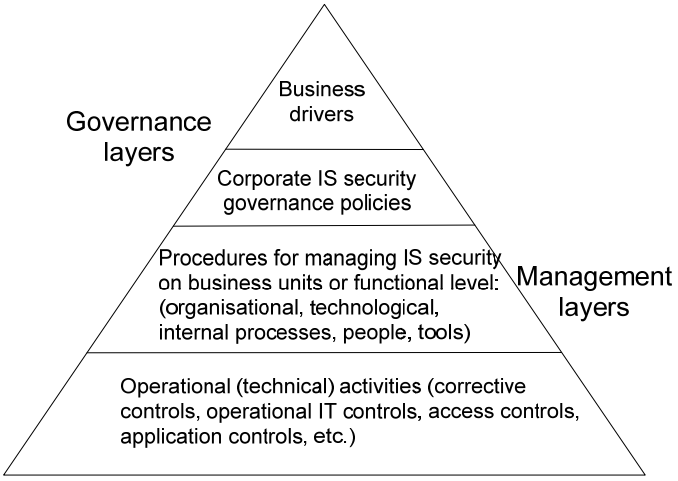

Figure 2. Model for IS security governance

A. Governance layers of the model

Business drivers represent principles for IS security governance which should be aligned with business objectives, regulatory requirements, and board of directors and executive management directives. Board and executive management should set up clear governance principles, accountability and responsibility about IS security. IS security principles should be aligned with the impact of possible incidents to the business processes. Without such alignment, there is the potential for confusion in coordinating various agendas and communicating the overall enterprise IS security vision.

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Corporate governance is a set of responsibilities and practices exercised by the board and executive management with the goal of:

- Providing **strategic direction**
- Ensuring that **objectives** are achieved
- Ascertaining that **risks** are managed appropriately
- Verifying that the **enterprise's resources** are used responsibly.

Therefore, corporate IT risk management (CITRM) process should be set up as a key component of corporate governance which establishes a common methodology and set of processes across the organization for consistent identification, measurement and reporting of risk. Corporate IT Risk Management Model (CITRM) should be a holistic and structured approach that aligns governance policies, business strategy, management procedures, business processes and operational activities with the purpose of evaluating and managing risk and uncertainties the organization faces. The main objective of CITRM model is to align IT resources, IT infrastructure, key resources (data, people, assets, etc.) and business processes with governance policies and management procedures in order to effectively manage IT risk exposure. This in particular means that executive management and Board members become responsible for managing risk associated with using IT in conducting business operations and transactions [20].

Corporate governance policies for managing IS security represent policies that are mandatory at all corporate levels and approved by the highest corporate bodies (Board, executive management). Governance sets the tone at the top and establishes the culture of the organization, including attitude toward risk management and compliance. A governance framework has the benefit of:

- setting business goals for the enterprise and validates enterprise strategy. It ensures growth or mission enhancement with an appropriate amount of risk. It provides focus to strategic initiatives.
- Setting the strategy to support business goals and implementation plan for the strategy. It provides clarity and direction as to how the business goals will be met, and coordinates across the enterprise.
- Aligns spending with business goals. It ensures that spending for the implementation of enterprise initiatives is consistent with its priority level.
- Within these parameters, the mandate for risk and compliance is defined.

Typical examples are:

- defining the 'IS security risk appetite' which commonly represent the corporate rules and policies for IS security risk response strategies (key metrics, Key Security Indicators, Key Risk Indicators - KRIs, Key Performance Indicators - KPIs). This in particular means that the corporation have to define acceptable level of IS security risks as the level of risk which will not affect organisation performance. Acceptable risk level is the intensity of the IT risks which do not negatively affect the conduction of key business processes.
- Corporate policies for analyzing the impact IS security risks may have on the business (quantitative or qualitative measures for conducting a business impact analysis – BIA, metrics for IS security risk validation, IS security risk portfolio).
- Accountability for IS security control activities and framework for the IS security reports (the dynamics of IS security reports, who and to whom they should be presented).
- Establishing committees and other corporate 'bodies' responsible for governing and managing IS security (Audit Committee, IT Governance Committee, IS Security Committee).

Strategies for regulatory compliance and adopting industries best practices.

B. Management layers of the model

Procedures for managing IS security on business units level or functional level. They represent the standards, guidelines and activities which help in implementation of corporate IT governance policies (for example, IS Security Policy, Business Continuity Plan, etc). According to the regulatory requirements and specific area of interest, this usually means the adoption of world-wide standards or frameworks (CobiT, Risk IT, ISO 27005, Sarbanes-Oxley, COSO, Basel II, NIST, SANS, …). Frameworks and standards should not be adopted for their own sake, but rather as part of a process improvement effort. All these activities should be aligned with business drivers and governance policies, or they do not make any sense.

This in fact means that governance layers should defines *mandatory* and *discretionary controls* for business processes. *Mandatory controls* are required for compliance with the certain regulation or act but they will not necessarily meet all control requirements for IT. Most commonly, organizations think of regulatory compliance because laws and regulations are usually mandatory within a country and within an industry.

On the other hand, *discretionary controls* are based on common standards and frameworks are required to reduce risk and improve performance in certain areas, but won't necessarily meet all compliance requirements. Discretionally controls are defined at the governance level, their implementation support business objectives, but not necessarily provide straightforward compliance with a certain standard.

A top-down (identifying mandatory controls) and bottom-up (identifying discretionary controls) approach is required to ensure that the full spectrum of requirements is defined, and that controls can be selected to meet common objectives and avoid duplication. Specifically defined control requirements in laws and regulations should be used as the initial specification for controls.

Finally, periodic internal or external IS security audits are needed to detect the level of compliance with standards and regulatory frameworks. Performing IS audits are necessary in order to detect the priority risk areas, to identify specific IT controls needed, to constantly measure the level of their efficiency and to calculate IS security risk level on regular basis.

Operational (technical) activities, 'driven' by governance policies and management procedures represent the counter-measures, which aim to raise the level of

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

'immunity' on threats or attacks to IT assets. Typical examples of operational IT controls include access controls, application controls, system controls, change controls, data accuracy controls, integrity controls, user rights control, business continuity controls, etc.

IV. REVIEW OF APPROACHES TO INFORMATION SYSTEM SECURITY

For so many years or decades IS and IT area is 'looking for' appropriate, world-wide used, specific, but at the same time general professional standards which will describe the best practices in using IS and IT in the businesses. Prior IT standards (in 1980s and 1990s) were associated with the usage of IT as a technological infrastructure for the business. Such standards (for example OSI reference model for exchanging data, or ITIL v1 – so called 'yellow books') were mainly technologically oriented and showed in further details how certain technology should be used in complex environment. They were rarely connected to business side of the problem and do not question its usage from business perspective. As a matter of fact, in that time there were no use do to so, because IS were used as a technology enabler of the business.

There is no standard that covers every area of IS security management or governance, many standards overlap with each other, and there are some coverage gaps, such as defining the highest-level domains and mechanisms of IT decision making in IT governance. Furthermore, some standards are more like guidelines and assessment methodologies, rather than detailed approaches to IT management. Every standard necessarily leaves room for interpretation, and every active standard is subject to revisions. By treating compliance holistically as a program, rather than as individual projects, an organization can reap savings from more-efficient governance and processes, decreased testing and documentation costs, and reduced capital allocations through rationalization of infrastructure that supports regulated activities.

With the changes in usage of IS in the business, namely through offensive (turnaround and strategic) modes in the business described in the introduction of the paper, a vast number of new, business oriented IT standards emerged with the main objective of aligning IS and IT with strategic business objectives. Many standards and control frameworks (such as ISO 27001/2/5, ISO 15408, ISO 31000, AS/NZS 4360, COSO, NIST, SAS70, CobiT, ITIL and ISO 20000) are useful to guide IT risk and security management programs, but not all are applicable, and not all are practical. The standards such as CobiT, ITIL v3, ISO 27000, Val IT, Risk IT, CMMI, BMIS, ITAF, Prince 2, etc.) aimed at using of IT to add additional value to the business and maximize investments in IT through better business results.

A. COBIT

Developed by ISACA (Information System Audit and Control Association, www.isaca.org) and ITGI (IT Governance Institute, www.itgi.org), **CobiT 5** is the most widely accepted model and an 'umbrella' framework for governing enterprise IT. It is a holistic framework designed for business executives – not just IT leaders consisted of 5 processes for governing enterprise IT and 4 domains with 32 processes for management of enterprise IT. It assumes that enterprise boards, executives and management have to embrace IT like any other significant part of the business and enables information and related technology to be governed and managed in a holistic manner for the whole enterprise.

This is a holistic approach which subdivides IT related practices into two main areas GOVERNANCE (which is further divided into 5 governance processes) and MANAGEMENT (further divided into 4 domains with 32 processes). The GOVERNANCE domain contains five governance processes. Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options; setting direction through prioritisation and decision making; and monitoring performance, compliance and progress against agreed-on direction and objectives. Four MANAGEMENT domains are in line with the responsibility areas of plan, build, run and monitor activities in alignment with the direction set by the governance body to achieve the enterprise objectives. In total, COBIT 5 brings together the five principles that allow the enterprise to build an effective governance and management framework based on a holistic set of seven enablers that optimises information and technology investment and use for the benefit of stakeholders. In new version Risk IT and Val IT frameworks are incorporated in COBIT 5 framework which makes him comprehensive framework for governance of enterprise IT. There a number of principles and processes which are related to IS security (namely Delivery, Service and Support processes such as DSS 01 Manage Operations, DSS02 Manage Service Request and Incidents, DSS03 Manage Problems, DSS04 Manage Continuity, DSS05 Manage Security Services and DSS06 Manage Business Process Controls).

Business Model for Information Security (BMIS) is ISACA's holistic and business-oriented approach to managing information security, and a common language for information security and business management to talk about information protection. The Business Model for Information Security, provides an in-depth explanation to a holistic business model which examines security issues from a systems perspective, and it is very well accompanied by COBIT 5.

4.1. OTHER FRAMEWORKS AND STANDARDS IN INFORMATION SYSTEM SECURITY GOVERNANCE

ISO 27001 standard and **SANS** (www.sans.org), **NIST** (www.nist.org), **(ISC)2** framework (www.isc2.org) and **PCI DSS** (www.pcisecuritystandards.org) may be used to manage the level of **IS security risks.**

ISO/IEC 27000:2005 (The Code of Practice for information Security Management) is the series of standards with a number of guidelines associated with managing information security. ISO 27001:2005 consists of 10 control or risks areas in which about 40 major and 128 detailed IT security controls are offered.

The **PCI DSS** (Payment Card Industry Data Security Standard) is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data and manage IT security and privacy risk in credit card transactions. PCI DSS has 12 requirements (IT control objectives) and more than 50 recommended IT controls.

By adopting industry best practices (e.g. CobiT, ISO 27000, PCI DSS) and adjusting IT infrastructure with high-level executive objectives, companies can lower IT risks, especially security and operational risks. According to the recent IDC white paper (IDC, 2009) implementation of comprehensive IT Governance and IS auditing standards downtime risks may be lower by up to 85%, heavily reducing interruptions to daily data processing and access and supporting business continuity.

V. CONCLUSION

Main objective of this paper was to stress the importance of holistic approach on information system security based on business drivers and balanced between the IS components. IS security issues needs to be managed proactively taking the due care to all IS components (hardware, software, people, processes, organizational culture, procedures, technology and networks). Investigating the current practices and approaches to IS security, we came up to the conclusion that IS security management approach proves to be ineffective, because it was mainly oriented to technological part of the problem (tools, hardware, algorithms, infrastructure). So it is obvious that reactive – management approach to IS security is no longer effective and a new, proactive – governance based concept is to be introduced.

A model of the IS security governance is explained in the paper as a holistic and structured approach that aligns business drivers, governance policies, business strategy, management procedures, business processes and operational activities with the purpose of evaluating and managing IS security risk and assign responsibilities and accountability on higher executive levels'.

Plans for future researches include testing the IS security governance model on wide range of companies from various industries. The difficulties may arise from the fact that the companies in general are not so willing to participate in such researches, case studies or in-depth interviews because they may reveal some vulnerabilities in their businesses and expose to the certain risk.

REFERENCES

[1] Abu-Musa, A.: (2010) "Information security governance in Saudi organizations: an empirical study", Information Management & Computer Security, Vol. 18 Iss: 4, pp.226 – 276

[2] Caceres, G.H.R., Teshigawara (2010): Security guideline tool for home users based on international standards, Information Management & Computer Security, Vol. 18 Iss: 2 pp 101-123.

[3] Caldwell, F. (2009): Selecting and Applying GRC Frameworks and Standards, Gartner Symposium ITExpo, October 2009, Orlando.

[4] Ernst & Young (2011): Into the cloud, out for of the fog, Global Information Security Survey 2011, Ernst & Young, USA

[5] Ernst & Young (2010) Borderless Security, Global Information Security Survey, Ernst & Young, USA

[6] Forrester Wave (2010): Information Security and Risk Consulting Services, Q3 2010, Forrester Research.

[7] Gordon, L.A., Loeb, M.P. (2002) "The economics of information security investment", ACM Transactions on Information and System Security (TISSEC), Vol.5 No.4 pp 438-57.

[8] Groznik, A., Kovačič, A., Spremić, M., (2003): Do IT Investments Have a Real Business Value?, *Applied Informatics*, No. 4, 2003, pp. 180-189.

[9] Hagen, J.M., Albrechten, E., Hovden J. (2008): Implementation and effectiveness of organizational information security measures, Information Management & Computer Security, Vol. 16 Iss: 4 pp 377-397.

[10] Hagen, J.M. (2007) "Evaluating applied information security measures: an analysis of the data from the Norwegian Computer Crime Survey 2006", pp35-48

[11] IDC White Paper (2009): Reducing Downtime and Business Loss: Addressing Business Risk with Effective Technology, IDC, August 2009.

[12] Ifinedo (2009): Information technology security concerns in global finance services institutions: Is national culture a differentiator? Information Management & Computer Security, Vol. 17 Iss: 5 pp 372-387.

[13] ISACA (2010): Business Model for Information Security, ISACA, Rolling Meadows, Illinois, USA.

[14] ISACA (2012): Extracting Value from Information Chaos: Why Good Governance Makes Good Sense, CobiT 5, ISACA, Rolling Meadows, Illinois,USA

[15] ITGI (2011): ITGI Global Status Report on the Governance of Enterprise IT, IT Governance Institute, Rolling Meadows, Illinois, USA

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

[17] Singleton, T. (2012): Evaluating Access Controls Over Data, ISACA Journal, Vol 1, ISACA, Rolling Meadows, Illinois, USA

[18] Siponen, M.T., Oinas-Kukkonen, H. (2007) "A review of information security issues and respective research contributions", The Database for Advances in Information Systems, Vol.38 No.1 pp 60-81.

[19] Spremic, M., Strugar, I. (2002): Strategic Information System Planning in Croatia: Organizational and Managerial Challenges, *International Journal of Accounting Information Systems*, Vol. 3, Num. 3, pp. 183-200.

[20] Spremić, M. (2009): IT Governance Mechanisms in Managing IT Business Value, *WSEAS Transactions on Information Science and Applications*, Issue 6, Volume 6, June 2009, pp. 906-915

[21] 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.

[22] Spremić, M. (2012): Measuring IT Governance Performance: A Research Study on CobiT- Based Regulation Framework Usage, *International Journal of Mathematics and Computers in Simulation*, Volume 1, Issue 6, pp. 17-25

[23] Von Solms, B. (2006) "Information security – the fourth wave", Computers & Security, Vol.25 No.3 pp165-8

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

[25] Werlinger, R., Hawkey, K., Beznosov, K. (2009) "An integrated view of human, organizational, and technological challenges of IT security management", Information Management & Computer Security, Vol. 17 Iss: 1, pp.4 - 19

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)