Baltic J. Modern Computing, Vol. 5 (2017), No. 1, 107-123
http://dx.doi.org/10.22364/bjmc.2017.5.1.07

High-Level Self-Sustaining Information Security Management Framework

Laima KAUSPADIENE[1], Antanas CENYS[1], Nikolaj GORANIN[1], Simon TJOA[2], Simona RAMANAUSKAITE[1]

[1]Vilnius Gediminas Technical University, Sauletekio al. 11, LT–10223, Vilnius, Lithuania
[2]St. Poelten University of Applied Sciences, Matthias Corvinus-Str.15, 3100 St. Pölten, Austria

laima.kauspadiene@vgtu.lt, antanas.cenys@vgtu.lt,
nikolaj.goranin@vgtu.lt, simon.tjoa@fhstp.ac.at,
simona.ramanauskaite@vgtu.lt

Abstract. This paper is aimed to provide the inclusive approach of collaborative information security management framework architectural reference model. Integration and performance based design of information security models will be revised in sake to provide integrated holistic methodology for construction of a High-level self-sustaining information security management framework (HISM). In addition, this paper summarizes investigations of existing information security management frameworks and models as well as identifies the advantages of the framework proposed by the authors. Future research directions are discussed.

Keywords: Information security, Information security management, Information security governance, Information security management framework.

1. Introduction

In today's global, digital, interconnected world data becomes one of the most important elements in organizations (Yin et al., 2014). Both internal and external information systems are getting increasingly connected. The emerging "Internet of things" is one of vast examples of hyper connectivity, integrity and complexity. However, problems and security issues in such systems can lead to both cyber and real world damage and loss. Therefore more and more organizations identify its new priority – cyber security. Crucial part of organization's strategy is safeguarding intellectual property, financial information, and its reputation. This is an ongoing process as the cyber risk landscape is very dynamic and threats are increasing in the level of persistence, sophistication and organization. Even if an organization has not experienced an attack yet, it should understand that it could be a cybercrime target, or that its security has already been compromised. Being a victim of cyber-attacks can lead to big looses and troubles. The damage caused by a cyber-attack can severely impact a business (Van Kessel and Allan, 2014): valuable data can be lost, damaged, or altered; computer hardware and/software can be compromised; organization can face financial looses; leadership position or reputation can be destroyed, etc.

Cyber-attacks are targeted at different type of sectors. Critical infrastructure as energy, information and communications technology (ICT), logistics, finance, pharmaceuticals and others are not safe anymore and require even more attention compared to industry. As European Union agency for network and information security (ENISA) reports (WEB, g), in 2014 major changes were observed in top threats: attack complexity increased and successful attacks have been launched on vital security functions of the internet. For example advanced persistent threat (APT) attack (WEB, h) combines a variety of vectors and seeks to steal sensitive data despites the size and authority of the company. One of the APT attacks is named as "Night Dragon" and series of it were performed by Chinese hacks under so called "Operation Aurora" and disclosed by Google hacks on 2010. "Night Dragon" attacks began in 2009 and were targeted mainly at oil, energy, petrochemical and ICT companies (WEB, h). Another cyber-attack campaign "Dragonfly" was launched in 2010, but publicly revealed only in 2014. "Dragonfly" was targeted at industrial control systems and pharmaceutical companies (Langill, 2014) (although initial target was considered as energy sector (WEB, a)) and caused a significant damage. In 2014, disclosed bugs (e.g., Heartbleed, ShellShock) affected many of the world's web users (WEB, f) and the number of breaches is increasing drastically every year (Rutkowski et al., 2010). The annual survey (performed by PricewaterhouseCoopers LLP (WEB, j)), of more than 9,700 security-, IT-, and business executives found that the total number of security incidents detected by respondents climbed to 42,8 million in 2015, an increase of 48% over 2013. That's the equivalent of 117,339 incoming attacks per day, every day (WEB, j). Cybercrime costs the global economy about $445 billion every year, with the damage to business from the theft of intellectual property exceeding the $160 billion loss to individuals from hacking, according to research (WEB, b). In the recent past a number of large scale or high-impact cyber-attacks were performed: over $3.2 million in a period of six months from major U.S. corporations, including the U.S. government and military, and other systems (in total of 25 000) of more than 90 countries including the U.K., Brazil, Mexico, Thailand, Turkey, Saudi Arabia, India, Romania and Canada – all by one hacker, a mid-level criminal, shutting down Israel's Carmel Tunnel. This and many other cases certify that there is no adequate preparation to fend off attacks in the information space. Cyber criminals' target is users of worldwide social networks, such as Skype, Facebook, and Windows using multiple exploits. Web and mobile applications are the new frontiers in the war against cyber-attack (WEB, b).

There exist internationally coordinated operations of law enforcement and security vendor's coordination as well as mobilisation of the cyber community. However, the evidence indicates (WEB, g) that the future cyber threat landscapes will maintain highly dynamic. Understanding this, not only businesses adopt their cyber security plans. Organizations allocate more and more financial resources to protect their assets in terms of information security (WEB, b), but in many cases there is financial resources are used inefficiently due to missing or inadequate Information Security Management (ISM) strategy. Therefore having no suitable management strategy, it is not possible to assure proper information security. For the security of a critical infrastructure and industry, countries adopt cyber security frameworks and strategies. One of the crucial elements of the cyber strategy implementation is its relevant management.

Essential studies in the field of ISM were started by Donn B. Parker in 1976 (Parker, 1976). Proactive analysis and development of frameworks for managing information security were started in the next decade. A substantial contribution to the research of ISM was made by R. von Solms (Solms, 1998a, 1998b, 1999), who was performing an in-depth analysis of standards for ISM.

Since the initial studies, innumerable amount of frameworks and models for ISM were created and developed. There are standardized (ISO 27001, COBIT, etc.), governmental (intended to protect critical infrastructure and similar, of a national and international importance), etc., frameworks for ISM. However, usually specific approaches, aspects, information security levels are discussed and there is no common and general view on what and how should be done in order to ensure unimpeded and resilient processes of ISM. This leads to complications and problems of existing ISM framework or its combination application in real situation.

Current frameworks might not work in real life as Information and Communication Technologies (ICT) are increasingly intertwined across the economies and societies of developed countries and the company might adopt regulations of different parties too. Protecting these technologies from cyber threats requires collaborative relationships for exchanging cyber defence data and an ability to establish trusted relationships. The fact that Communication and Information Systems (CIS) security is an international issue increases the complexity of these relationships (Vázquez et al., 2012). Therefore, simplified isolated organization wide frameworks of ISM are inadequate these days. Cyber defence collaboration among stakeholders in all levels is a must.

The major contribution of this paper is to increase the security level by presenting a high-level self-sustaining information security management framework with a holistic approach to the collaborative information security network defence. This framework will cover all levels and elements of information security management. It will consider all concerned parties and all levels that affect organization's information security management processes as well as will create links between business, academia and government needs in terms of information security. The proposed ISM framework will be unified, holistic and integrated, and will provide open, resilient and collaborative approach to the management of information security.

The rest of the paper is organized as follows. Section 2 presents the background of ISM frameworks. Existing ISM frameworks will be presented and surveyed to answer the research question what elements, links and activities ensure the comprehensive and resilient information security management process. In Section 3 a newly proposed ISM framework is introduced. This is followed by the conclusions of this paper.

2. Existing Information Security Management Frameworks

Currently there exist a large number of ISM frameworks, proposed by scientists, universally accepted organizations, business companies, governmental initiatives for protecting information security and others. All these ISM frameworks concentrate on a specific domain or have its own point of view. The framework selection depends on many factors including industry sector and geography (Van Kessel and Allan, 2014). Therefore, in this section we will provide an overview of some relevant ISM frameworks to form a general view on existing solutions.

2.1. Overview of Information Security Management Frameworks

Eloff and von Solms (2000) proposed a hierarchical framework for various approaches (Figure 1) consisting of three levels, where the top level of the hierarchical framework represents IT in its broadest sense and includes all activities and tools associated with and all approaches adopted to IT in general. This all-covering category is entitled Assessment of Information and Related Technologies. The second level is divided into two areas, namely Information Technology: General and Information

Technology: Security. The area entitled Information Technology: General includes all IT activities and tools that cannot incur any security-related risks. The area entitled Information Technology: Security is divided into the areas entitled Technology and Processes. The area entitled IT: Security Processes is allocated to all IS management actions that should be performed; The area entitled IT: Security Technology is reserved for all the 'visible' aspects involved in IT security, such as the controls that are put into place to prevent possible damage by malicious software. The areas IT: Security Processes and IT: Security Technology is mapped onto third level of the framework. Going down IT: Security Processes are divided into four terms (fourth level): (1) guidelines, code of practice, (2) standards, (3) legislation, (4) benchmarking. The area of IT: Security Technology consists of the same terms except of legislation, as it is replaced by evaluation. At the fifth level of the framework, some of the above terms are subdivided further as being either internal or external. Internal guidelines are dictated by the specific in-house requirements of an organization. It should be noted, that in terms of the framework, international standards, as endorsed by an international standards organization, are classified as being external standards.

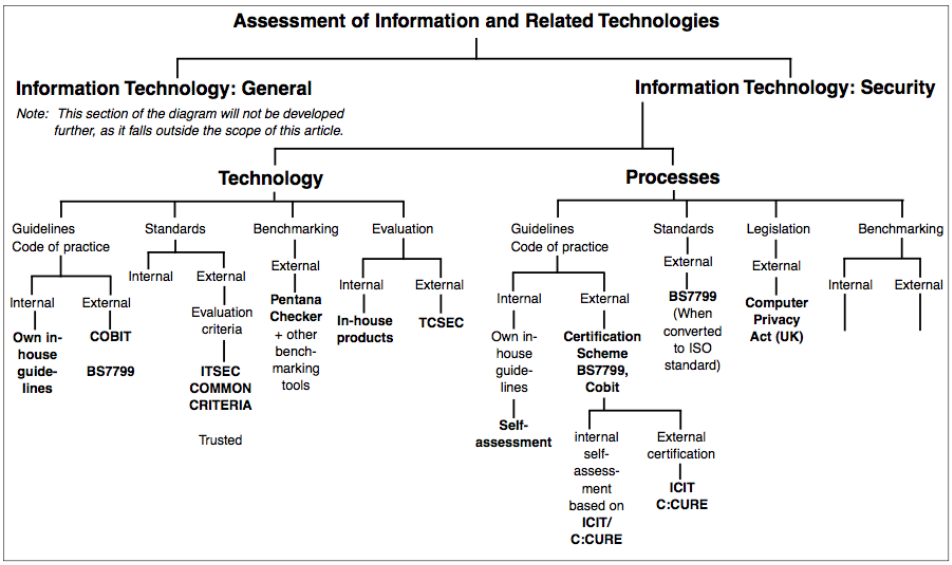

Figure 1. A hierarchical framework for IS management (Eloff and von Solms, 2000)

Trček (2003) proposed an integral framework for information systems security management based on layered multi-panes (Figure 2). The author declares that in order to protect information, an organization has to start with the identification of threats related to business assets. Based on threats analysis, he proposed a layered multi-plane approach. The first plane is focused on interactions, starting with security mechanisms and therefore deploying security services, which are linked to human-machine interactions. Finally, human interactions have to be covered. Thus, in parallel, to make things operational, scientist proposes to address another perspective, which includes technological, organizational and legislative planes.

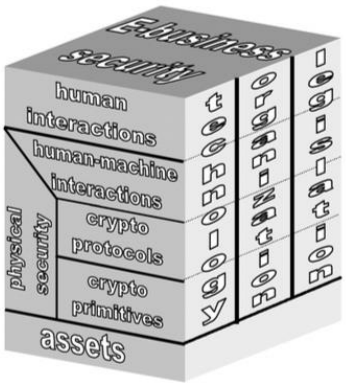

Figure 2. Layered multi-panes model for information systems security (Trček, 2003)

Bradley and Josang (2004) propose an open framework for enterprise security management. This framework is intended to be a technology-dependent, and comprises an information repository, manager programs, and configuration agents. The information repository stores network and security policy information. Manager programs are technology-domain-specific, and act as expert systems querying the repository and communicate with configuration agents. Configuration agents provide the required expert system functionality. The study proposes a technical solution to information security management problem. Since the proposed framework is technology-dependent, it would not provide the type of flexibility that may be required in certain cases.

Sherwood et al. (2005) represented SABSA (Sherwood Applied Business Security Architecture) framework for Enterprise Security Architecture. SABSA is intended for developing risk-driven enterprise information security and information assurance architectures and for delivering security infrastructure solutions that support critical business initiatives. It is an open standard, comprising a number of frameworks, models, methods and processes. The SABSA Model covers the life cycle of operational capabilities and comprises six layers. For each horizontal layer there is a vertical analysis based on the six questions: What (assets)? Why (motivation)? How (process and technology)? Who (people)? Where (location)? When (time)? This leads to a six-by-six cell matrix called the SABSA Master Matrix. The sixth layer, the service management layer, is overlaid on the other five layers and further vertically analysed to produce the five-by-six cell SABSA Service Management Matrix. Some of the key features of the SABSA are: it can be implemented incrementally, may be used in any industry sector and in any organization whether privately or publicly owned, can be used for the development of architectures and solutions at any level of granularity of scope, enables relevant existing standards to be integrated under the single SABSA framework, enabling joined up, end-to-end architectural solutions, is continually maintained and developed and up-to-date versions are published from time to time.

SABSA is a generic architectural development framework that can be used for the operational-risk-based development and maintenance of operational capabilities in any type of business organization (WEB, c). It provides a holistic approach to information security and is baselined against the Security Architecture' standard ISO 7498-2:1989[1]. Five layer SABSA framework answers the what, why, how, who, where and when questions for security architecture. Five layers of SABSA are (see Figure 3): Contextual

1 http://www.iso.org/iso/catalogue_detail.htm?csnumber=14256

Architecture, Conceptual Architecture, Logical Architecture, Physical Architecture and Component Architecture. A sixth layer is added for Service Management Architecture and is synonymous with Operational Security Architecture.

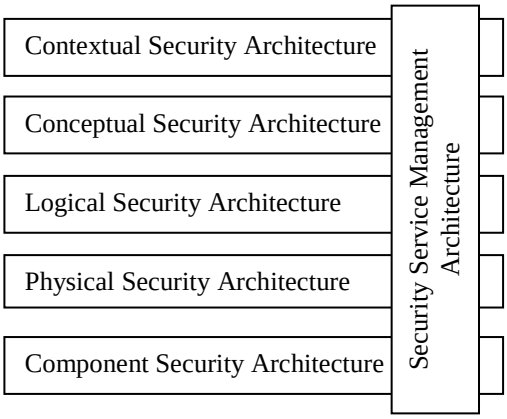

Figure 3. SABSA model (WEB (c))

Suter (2007) introduced a Generic National Framework for Critical Information Infrastructure Protection (CIIP). CIIP is universally acknowledged as a vital component of national security policy. In order to protect their critical infrastructure, countries establish sophisticated and comprehensive CIIP organizations and systems, involving governmental agencies from different ministries, with a variety of initiatives. In the paper, the author offers a few building-blocks for a functional CIIP unit and states, that by concentrating on top priorities, cooperation between various stakeholders, flexibility and adaptability, relatively inexpensive solutions can be developed to meet country-specific needs. Essential tasks of CIIP author arranges in a "Four-Pillar Model". The four pillars of this model are: prevention and early warning; detection; reaction; and crisis management. While the aim of Prevention and early warning is to reduce the number of information security breaches; the aim of Detection is to discover threats as quickly as possible, Reaction includes the identification and correction of the causes of a disruption, Crisis management aims at minimizing the effects of any disruptions. In the paper essential partners of the framework, organizational structure of CIIP unit are also discussed, as well as case study provided.

Ho (2008) represented a solution and procedures of coordinated defence. In the paper, the nature of attacks has been analysed and countermeasures of coordinated defence have been provided, the weakest link (the human element) in the layered defence has been identified. This paper contributes to the information systems security by providing a framework for approaching coordinated defence. It benefits research into information systems security by introducing the evolutional concept of coordinated defence. According to the author, his solution of a coordinated defence framework aims to protect information as assets by technologies, policy, and best management practices for defending against coordinated attacks. In addition, it is noted that the framework forms unique characteristics of an information security culture for the organization. Layered defence covers all aspects of defence including social and technical aspects. Building security mechanisms and infrastructure comprise the first layer of this defence strategy. Secondly, a fundamental "deny all unless specified" access control security policy is proposed for implementation. The third layer in the coordinated defence model should conduct infrastructure threat analysis and intrusion forecasts. The fourth layer in

the coordinated defence model would be to monitor and detect intrusion. In the framework sensor technology at an infrastructure level, or systems level are built to detect and monitor activities. In addition, human (physical) activities could be monitored. Finally, an overarching layer of the defence emphasizes the resiliency and sustainability of the defence infrastructure, where the damage assessment and impact analysis lead to the rebuilding of recovery and response mechanisms.

Ma et al. (2009) propose an integrated framework for ISM (Figure 4), in which ISM is conceptualized as a continuous decision-making process. The rationale of this framework is based on four guiding principles: (1) have goal in mind, (2) align security goals with business strategy, (3) ISM is a multivariate system and (4) ISM is a dynamic process. Key components of the proposed ISM framework include the following steps: assess the organizational environment, establish information security objectives, analyse information security requirements, develop information security controls, and train/evaluate information security controls. The authors define ISM as a continuous improvement process intended to assure business continuity, customer confidence, and protection of business information assets and the minimization of damage to the business by preventing or minimizing the impact of security incidents. They declare, that the framework is beneficial, because it serves as a common ground for integrating all types of information security functions, helps answer questions of how to react to information security issues and it helps identify what are the important components involved in establishing and maintaining information security initiatives.

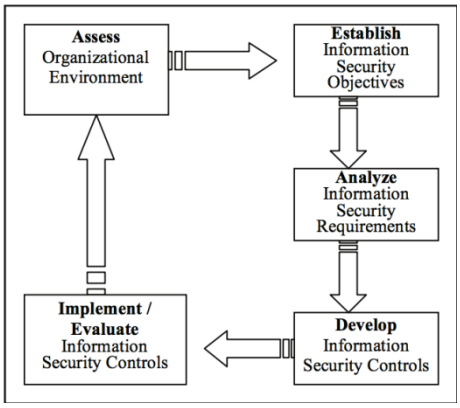

Figure 4. Information security management framework (Ma et al., 2009)

An organizational-level process model in Information security policy was proposed by Knapp et. al (2009). The model (Figure 5) suggests that a security governance program together with the organization's information security office, an ongoing process of interrelated policy management activities, and the proper gauging of key external and internal influences together contribute greatly to the success of an organization's information security policies. The model provides unique value through its comprehensive, real-world representation of an information security policy process in modern organizations. The data used in the development of the model is rooted in the broad-based experiences of those who have been most active in developing and implementing organizational information security policies. Thus, this model provides a more complete, practice-based framework that informs organizations and researchers concerning the interactions of key processes and influences that form an effective information security policy process. In the model, information security governance is an

overarching category directly affecting the entire policy management process. The organization information security office is depicted as a category supporting the policy management phases. The internal and external influences are depicted as general influences on the entire policy management process. Internal influences include senior management support, organization culture, technology architecture, etc. External double arrows illustrate the two-way interaction between the policy management processes and the internal and external influences. External influences include economic sector, industry standards, legal and regulatory requirements, etc. The central part of the model pictures the entice process of organization's security policy – it is a continuous cycle, affected by internal and external factors, where key elements are policy approval, training, implementation, monitoring, enforcement, review, risk assessment and, finally, policy development.

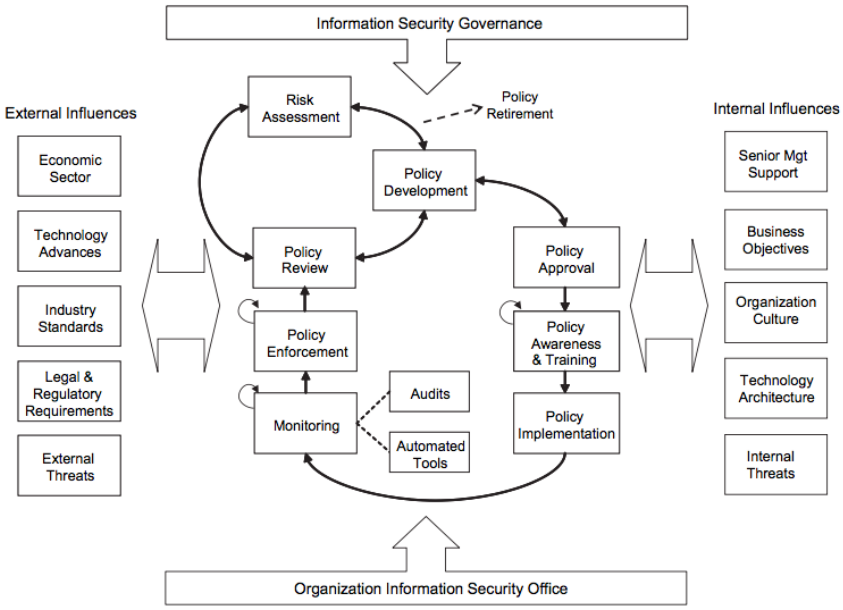

Figure 5. Comprehensive information security policy process model (Knapp et al., 2009)

In September 2014, the Government of South Australia approved the Information Security Management Framework (WEB, d), which provides maximum coverage for control and risk management objectives by providing a wide array of risk management controls and is not purely mapped directly to the most recent standards publications, but refers to a suite of publications in order to provide government agencies with a comprehensive set of risk controls in order to appropriately protect their information and support their business undertakings. This framework references a set of policies, standards, guidelines and control mechanisms for South Australian Government Agencies to use in developing their information security capabilities. It has been designed as a practical, useable framework, which can be implemented readily by South Australian Government Agencies and Suppliers to the Government of South Australia.

2.2. Comparison of Information Security Management Frameworks

To compare the surveyed frameworks defined characteristics (features) had to be used. For this reason, we decided to use the logic modelling theory (WEB, g) as security strategy of the enterprise has the same principles as national cyber security is. ENISA presented number of general and specific security objectives (WEB, g), while we grouped them into five more abstract characteristics. All presented frameworks were evaluated by the following defined characteristics: application of standards (C1), implementation or performance model provided (C2), whether the framework is a process (C3) or goal (C4) oriented, framework integration regarding different approaches and/or ISM levels (C5). C1 refers to application, implementation or reference to standards, such as ISO 27000 series, COBIT and others, into the framework proposed. For a successful framework adoption, it is very important to have in place all the steps, participants and relations among them, therefore, implementation or performance model (C2) of the framework is among features in evaluating the ISM frameworks. Characteristics C3 and C4 are essential in order to discern whether framework is developed for managerial purposes of organization whether to assure the main aspects of the information security – confidentiality, integrity and availability. Value added is provided for the framework when one or more approaches (e.g., Plan-Do-Check-Act cycle, Command and Control system, etc.) are applied and different levels, from operations/service managing to international matters, are covered.

Thinking on the application of information security framework, it is important to have high level view as well as detailed framework implementation specification. The high level view gives a solution to understand the overall area of information system management while detailed level is needed in order to implement it in real situation. However, in order to implement the framework successfully, the overall area understanding is a must. As well it is important to take into account as wide area as possible in order to introduce all possible stakeholders. Therefore, we add two more characteristics for the comparison of ISM frameworks: framework presentation in high level abstraction concepts (C6) and different type stakeholder presentation in the framework (C7). C6 is meet if the framework provides a basic architecture of information security management framework which can be used for information security management area understanding. While “four Ps of Service Design” (Clinch, 2009) should have an analogue in the ISM framework to meet C7.

We evaluated all overviewed ISM frameworks according to the chosen characteristis (does it apply (+) to the framework fully, partially (+-), or not apply at all (-)) and the results are presented in Table 1.

Table 1. A summary of ISM frameworks' comparison results

Author	Framework	Purpose	C1	C2	C3	C4	C5	C6	C7
Eloff et. al (2000)	Hierarchical framework for various approaches	Framework aims to unite and integrate issues of certification, benchmarking, guidelines, codes of practice and IS management approaches widely accepted in the international arena.	+	-	+	-	+	+	-
Trček (2003)	An integral framework for information systems security management	Author proposes a layered multi-plane approach based on identification of threats to e-business assets. Framework focuses on physical security and human interactions. Technological, organizational and legislative perspectives are addressed.	+	+	-	+	+	-	+-
Bradley and Josang (2014)	An open framework for enterprise security management	The aim of the framework is to turn the black art of enterprise security management into a reproducible, automatable science.	-	-	+	-	-	-	-
Sherwood et al. (2005)	Sherwood Applied Business Security Architecture (SABSA)	This framework is designed for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives.	+	+	+	-	+	+	-
Suter (2007)	Generic National Framework for Critical Information Infrastructure Protection (CIIP)	Framework provides concrete solutions to meet country-specific needs in protecting critical information infrastructure by concentrating on top priorities and cooperation between various stakeholders, flexibility and adaptability.	-	+	+	-	+	-	+
Ho (2008)	Coordinated defense framework	Framework aims to protect information as assets through the use of technologies, policy, and best management practices for defending against coordinated attacks.	+	-	+	-	+	+	+
Ma et al. (2009)	An integrated framework for ISM	Framework is intended to serve as a common ground for integrating all types of information security functions. It helps answer questions of how to react to information security issues.	-	+	-	+	-	+	-
Knapp et al. (2009)	An organizational-level process model	The purpose is to provide a more complete, practice-based framework that informs organizations and researchers concerning the interactions of key processes and influences that form an effective information security policy process.	+	+	+	-	-	-	-
Government of South Australia (WEB, d)	Information security management framework (ISMF)	Among many objectives of the ISMF, the main is to support the attainment and realization of three information security objectives across Government: Confidentiality, Integrity and Availability of information.	+	+	+	-	+	+	+

The results showed most of the analysed solutions are internal-level (organizational or information security system) ISM frameworks. This proves the idea there is a lack of ISM framework which would take into account the complexity of nowadays enterprise, organization or system as relationships between different stakeholders are ignored.

During the comparison of analyzed ISM frameworks we noted some of the ISM frameworks can be applicable to a particular part of the organization, e.g. – to the operational level, while others are intended to be applied to the entire organization but in very abstract approach, not considering integration, partnership, external communication.

The balance between abstract level presentation and implementation step definition in achieved in Sherwood Applied Business Security Architecture (SABSA) model by Sherwood et al. (2005) and Information security management framework (ISMF) by Government of South Australia (WEB, d). These frameworks present a main architecture of the framework as well as provide guidelines for framework implementation. The difference between those two frameworks is application area as SABSA is organization oriented, while ISMF is government oriented framework. This makes ISMF harder to apply in small or even medium size organizations. Meanwhile SABSA framework does not involve all 4 P's from ITIL (Clinch, 2009), which means it is not holistic and do not present enough wide organization security management area.

In overall it can be said that analyzed ISM frameworks does not meet all depicted characteristics. Frameworks take into account theoretical and conceptual approaches for managing information security, and there is a lack of attention, committed to ensure the unimpeded and resilient process of ISM as some important stakeholders are not taken into account.

3. High-Level Self-Sustaining Information Security Management Framework

The second generation (Solms, 1996) ISM framework must take into account the nature of nowadays enterprise. Today business has multiple partners, uses collaborative systems, outsourcing and other third parties, which requires a broader view into organization security management. Maynard et. al (2011) identify 9 stakeholder categories in organization security policy development while European security Trends and Threats In Society (ETTIS) (WEB, e) uses the broader concepts of security and identifies 7 stakeholder categories in global security area. We used a classification of 7 stakeholder categories (see Table 2) to define high level stakeholder categories, which acts in today's enterprise and have to be taken into account to ensure organizations security.

Most ISM frameworks have no list of default stakeholders and require an identification of stakeholders as every situation can be unique and require different type of stakeholders to include. However, this approach is stakeholder identification knowledge and practice dependent. If one or more important stakeholders would be missed, the final security management result can be crucial as this is a base for other information security management elements. Our proposed approach has 7 top level stakeholder categories, which can be divided into smaller, more specific ones. Therefore, the stakeholder identification, specification process starts from these top level categories to think of and leads to smaller probability to miss some important stakeholders.

Table 2. HISMF stakeholder categories and its relation to organization oriented and global security oriented stakeholder taxonomies (invented by authors)

Stakeholders Category	**Description**	**Interest/ Responsibilities**	**Maynard Category** (Maynard et al., 2011)	**ETTIS Category** (WEB, e)
Corporate governance	Ensuring the security of critical infrastructure	Critical infrastructure security	Business Unit Representatives	Think tanks
Legislative bodies	Ensures Cyberspace monitoring	Cyber space monitoring	Legal & Regulatory	Government
Professionals	Ensures the management of information security in a system-level	Information security management	ICT Specialists; Security Specialists	Industry
IT Enterprises	Enterprises, that provides physical infrastructure	Physical infrastructure		
Developers	Software development	Software	Executive Management; Human Resources	
Academia	Prepare expertise human resource for performing the processes of information security management	Human resources		Academia/ research institutions
External parties	Collaborates with the organization, by changing different information, tools, services, etc.	Information and resource exchange	Public Relations; User Community; External Representatives	Civil Society Organisations; The media; The public

The proposed framework has main information security management components too. In Figure 6, essential elements in performing information security management are shown. It is a matter-of-course that the uninterrupted and resilient processes are the gist of information security management performance.

Information security management processes are performed by professionals - an expertise human element, e.g., CISO (Chief Information Security Officer), that are prepared by academia and science institutions. This is the core of the proposed framework as presents the organization level. The organization has multiple processes (internal as well as external) which are the engine of the company. The organization enables a command to manage, and installs a control to perform a monitoring of these processes. For a continuous development, a best-practice based processes optimization should be organized. However, all innovations and optimizations have to be audited and confirmed by certain control in order to meet organization needs, regulatory compliance and security requirements. All the production (or services the organization provide) is dependent on organization, processes and optimization elements, while command and control (C2) denotes the set of organizational and technical attributes and processes by which an enterprise marshals and employs human, physical, and information resources to solve problems and accomplish tasks (Vassiliou et al., 2014). Military system C2 should be applied for the monitoring and management of the processes (see Figure 6). This is required as the human factor is the weakest link of any security system and the biggest attention in security management should be given to the processes, performed by

people. Cyber warfare command and control system demonstrates that defence-in-depth can be taken to a new level that is active and anticipatory rather than passive and reactive (Howes et al., 2004).

Figure 6. Core elements (organization level) of HISMF (invented by authors)

The Deming cycle Plan-do-check-act (PDCA) is another approach which was integrated as a must in the framework (see Figure 7). Based on application criteria, certain standards and methodologies should be applied to the ISM of organization (Methods section, Figure 7). According to the security standards and technologies, security actions are planned and later integrated to the information security platform. The information security platform is a set of physical tools used for information security implementation. Usually the information security platform depends on organizations technical capabilities and professionals, which are capable to use those tools properly and to obtain clear evidence on the efficiency of implemented security tools. This includes an analysis of organization information, its compliance to certain controls, and acting according a certain situation, defined in standards and methodologies.

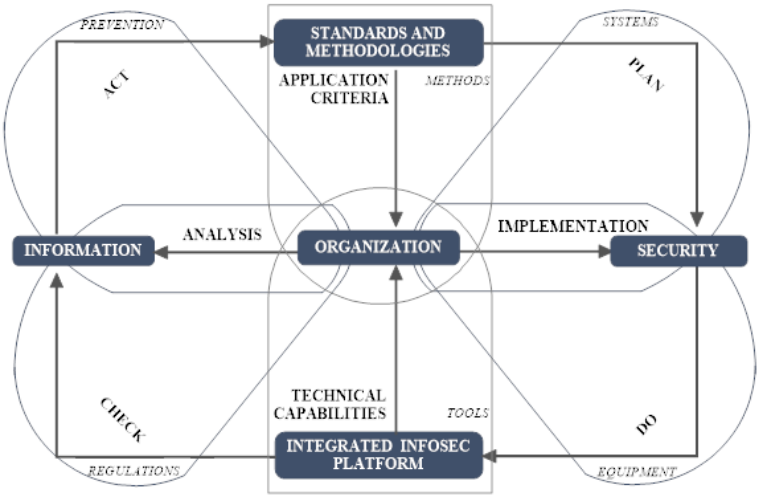

Figure 7. Main components of organization security level (invented by authors)

To understand the relations between components of organization security level and ISM shareholders and responsabilities or functions they perform (see Table 2), four additional sections are identified (Figure 8): (1) *prevention* is done by cyber space monitoring in the software level, according regulations, issued by the legislative bodies,

and involves control and information elements, as the control of information plays one of the major roles in IS prevention, weather it is data leakage, fraud, etc.; (2) *regulations* are issued by legislative bodies and implemented at the cyber space monitoring and physical infrastructure levels, and involves control and information elements due to ensure processes compliance to national as well as international law (personal data protection, audit procedures, laws of cyber space, etc.); (3) *systems* (at the software level provided by the developers community) and (4) *equipment* (at the hardware – physical infrastructure - level, provided by IT enterprises) serves to the corporate government by assuring the security of critical infrastructure, whereas the security is implemented under the commands given by organization.

When organization is growing, the continuous improvement loop - PDCA cycle - turns around bringing new informational security management challenges that influence stakeholders' demands. To provide more clear guidance we mapped the PDCA cycle to security level as well as associated all elements of the HISMF to certain top level stakeholder category or its responsibility (see Figure 8). As external parties can be of very different type and purpose they can act in different responsibility areas, however they should be treated as external level and separated from the organizational or even security level. Therefore, partners are linked to the elements of standards and methodology, security, integrated security platform and information.

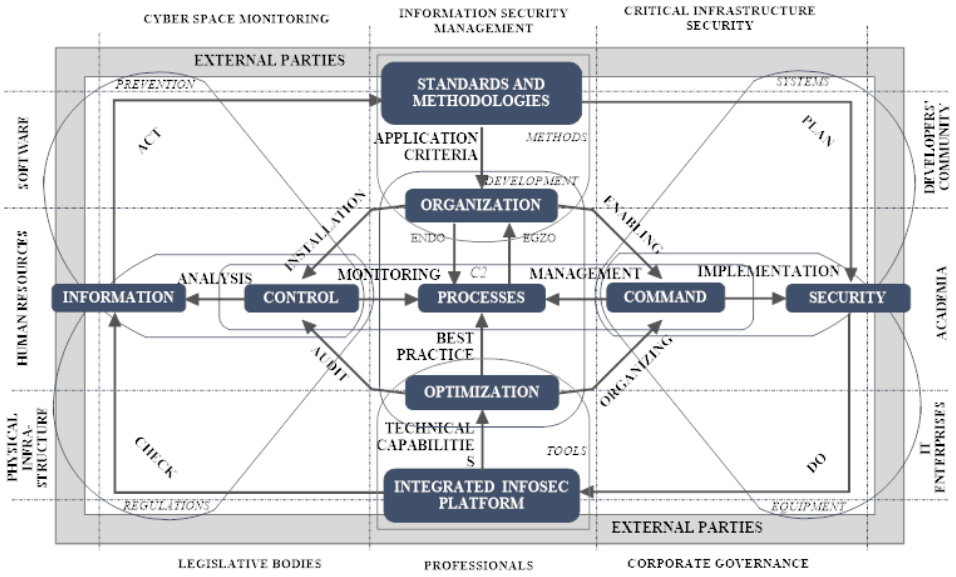

Figure 8. High-level self-sustaining Information Security Management Framework (invented by authors)

Self-responsive cyber security network, generated by High-level information security management framework, is based on five resilience principles (Vries, 2010): self-merging, robustness, viability, flexibility and interoperability. Instructional design of self-sustainable components of high-level information security management framework is arranged to form a self-organizing system. Self-referingness on demand, based upon distributed stakeholders' initiative, enables system to self-awareness.

The high-level information security management framework represents holistic approach to collaborative information security network defence. This framework

represents security processes demystification paradigm, based upon embed systems participate development. Four sections of the model correspond to viable resilient cyber security system that is based upon interlinked participate network. Cyber security demand is fulfilled in this system as co-working crowd source based IT system integration pattern in complex self-repellent environment. Various challenges, as provision of skills and competencies, are conglomerated as general PDCA model acts upon supervision of framework stakeholders' superiority. Superior forces of self-referencing development of technological capabilities are fulfilled by using foremost open-source tools of self-referring standards that are proclaimed as best practice based knowledge assets.

The framework provides new approach to organization informational security management challenge and can be suitable for any type of organization. Emerging organization growth is considered in high-level information security management framework – processes are controlled on demand using C2 paradigm, utilizing PCDA cycle collaborate stakeholders grid efforts.

4. Conclusions

This paper presented the findings of an exploratory study that revealed there is a lack of attention, committed to ensure the unimpeded and resilient process of ISM. Analyzed ISM framework sometimes lack of an abstract level information security management area presentation, where all type stakeholders would be taken into account. As organizations are not isolated the stakeholder identification by including both internal and external resources, actors is a must in order to manage information security properly.

Based on the analysis results and existing information security management paradigms a new high level self sustaining ISM framework was designed and presented. This framework provides evolutionary approach to organization informational security management challenge and can be suitable for any type of organization, as none of existing and analyzed frameworks meet all features necessary for nowaday organization to ensure its security. Emerging organization growth is considered in High-level information security management framework – processes are controlled on demand using Command and Control paradigm, utilizing Plan-Do-Check-Act cycle collaborate stakeholders grid efforts.

Provided framework represents holistic approach to the collaborative information security network defence. In addition, this framework represents security processes demystification paradigm, based upon embed systems participate development. In the framework, there are defined stakeholders of a whole system of Information security management. Stakeholders are: Legislative bodies (ensure cyberspace monitoring), Corporate governance (ensure the security of critical infrastructure), Universities (provision of expertise human resource), IT enterprises (provides physical infrastructure), Professionals (management of information security in a system-level) and Developers' community (software development), External parties (all external communications). These stakeholder categories ensure a wide area of information security management will be analyzed by leaving no space for stakeholders influence no estimation.

This paper contributes to the information systems security by providing a framework for coordinated, collaborative defence. Inter alia, the High-level information security management framework can serve practitioners as guidelines for development of an overall information security plan or program in their organizations.

References

Bradley, D., Josang, A. (2004). Mesmerize - an Open Framework for Enterprise Security Management. Second Australasian Information Security Workshop (AISW2004). 32, pp. 37-42. Dunedin, New Zealanf: CRPIT.

Clinch, J. (2009). ITIL V3 and Information Security. Retrieved 11.15.2015 from http://itsmf.cz/wp-content/uploads/2014/04/itilv3_and_information_security_white_paper_may09.pdf

Eloff, M. M., von Solms, S. H. (2000). Information security management: a hierarchical framework for various approaches. *Computers & Security*, *19*(3), 243-256.

Ho, S. M. (2008). A Framework of Coordinated Defence. Proceedings of the Second International Conference on Computational Cultural Dynamics (pp. 39-44). Association for the Advancement of Artificial Intelligence (*www.aaai.org*).

Howes, N. R., Mezzino, M., Sarkesain, J. (2004). Cyber Warfare Command and Control Systems. Ninth International Command and Control Research and Technology Symposium.

Knapp, K. J., Jr., R. F., Marshall, T. E., Byrd, T. A. (2009). Information security policy: An organizational-level process model. Computers & Security , 28 (7), 493–508.

Langill, J. T. (2014). Defending Against the Dragonfly Cyber Security Attacks. Retrieved 11.15.2015 from http://info.belden.com/ab-cyber-security-dragonfly-bc-lp

Ma, Q., Schmidt, M. B., Pearson, J. M. (2009). An integrated framework for information security management. 30, pp. 58-69. Review of business : a quarterly publication of the Business Research Institute.

Maynard, S. B., Ruighaver, A. B., Ahmad, A. (2011). Stakeholders in security policy development. 9th Australian Information Security Management Conference, pp. 182-188. Perth Western Australia.

Parker, D. B. (1976). Crime by computer. Charles Scribner's Sons.

Rutkowski, A., Kadobayashi, Y., Furey, I. (2010). CYBEX – The Cybersecurity Information Exchange Framework (X.1500). ACM SIGCOMM Computer Communication Review , 40 (5), 59-64.

Sherwood, J., Clark, A., Lynas, D. (2005). Enterprise Security Architecture: A Business-Driven Approach.

Solms, R. v. (1998a). Information security management: guidelines to the management of information technology security (GMITS). Information Management & Computer Security , 6 (5), 221-223.

Solms, R. v. (1998b). Information security management: the Code of Practice for Information Security Management (BS 7799). Information Management & Computer Security , 6 (5), 224 - 225.

Solms, R. v. (1996). Information security management: The second generation. Computers & Security , 15 (4), 281–288.

Solms, R. v. (1999). Information security management: why standards are important. Information Management & Computer Security , 7 (1), 50-58.

Suter, M. (2007). A Generic National Framework For Critical Information Infrastructure Protection (CIIP). Retrieved 11.15.2015 from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

Trček, D. (2003). An integral framework for information systems security management. Computers & Security , 22 (4), 337-360.

Van Kessel, P., Allan, K. (2014). Get ahead of cybercrime. EY's Global Information Security Survey 2014.

Vassiliou, M. S., Alberts, D. S., Agre, J. R. (2014). *C2 Re-envisioned: The Future of the Enterprise*. CRC Press.

Vázquez, D. F., Acosta, O. P., Brown, S., Reid, E., Spirito, C. (2012). Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships. In R. O. C. Czosseck (Ed.), 4th International Conference on Cyber Confl ict (pp. 429-445). Tallinn: NATO CCD COE Publications.

Vries, J. P. (2010). The Resilience Principles: A Framework for New ICT Governance. Journal on Telecommunications and Hight Technology Law.

Yin, S., Li, X., Gao, H., Kaynak, O. (2015). Data-based techniques focused on modern industry: An overview. *IEEE Transactions on Industrial Electronics*, *62*(1), 657-667.

WEB (a). (2014). Belden Research Reveals Dragonfly Malware Likely Targets Pharmaceutical Companies. Retrieved 11.15.2015 from http://www.businesswire.com/news/home/20140915005170/en/Belden-Research-Reveals-Dragonfly-Malware-Targets-Pharmaceutical#.VZbJ__mqqko

WEB (b). Center for Strategic and International Studies. (2015). The Economic Impact of Cybercrime and Cyber Estionage. http://www.mcafee.cmo/

WEB (c). SABSA Institute. (2014). Welcome to the official SABSA website. Retrieved 11.15.2015 from http://www.sabsa.org/

WEB (d). Government of South Australia. (2014, September). ISMF Information Security Management Framework. Retrieved 11.15.2015 from http://dpc.sa.gov.au/sites/default/files/pubimages/documents/ocio/ISMF_v3.pdf

WEB (e). European security trends and threats in society. (2012, March). D.7.2 Stakeholder identification and analysis. Retrieved 11.15.2015 from http://ettis-project.eu/wp-content/uploads/2012/03/D7_2.pdf

WEB (f). Codenomicon. (2014, April). The Heartbleed Bug. Retrieved 11.15.2015 from http://heartbleed.com/

WEB (g). ENISA (2015, January 27). ENISA Threat Landscape 2014. Retrieved 11.15.2015 from https://www.enisa.europa.eu/activities/risk- management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

WEB (h). McAfee® Foundstone® Professional Services and McAfee Labs™. (2011, February 11). Global Energy Cyberattacks: "Night Dragon". Retrieved 11.15.2015 from http://www.mcafee.com/in/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

WEB (i). European Union Agency for Network and Innovation Security. An evaluation framework for Cyber Security Strategies. (2014). https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies

WEB (j). PwC. (2015). Turnaround and transformation in cybersecurity. Retrieved 11.15.2015 from http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

WEB (k). Committee on Foreign Affairs, U.S. (2013). Cyber attacks: an unprecedented threat to U.S. national security. Retrieved 11.15.2015 from http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg80123/pdf/

Received July 18, 2016, revised December 30, 2016, accepted January 19, 2017