Taylor & Francis
Taylor & Francis Group

Technological and Economic Development of Economy

ISSN: 2029-4913 (Print) 2029-4921 (Online) Journal homepage: http://www.tandfonline.com/loi/tted21

Controls-based approach for evaluation of information security standards implementation costs

Dmitrij Olifer, Nikolaj Goranin, Arnas Kaceniauskas & Antanas Cenys

To cite this article: Dmitrij Olifer, Nikolaj Goranin, Arnas Kaceniauskas & Antanas Cenys (2017) Controls-based approach for evaluation of information security standards implementation costs, Technological and Economic Development of Economy, 23:1, 196-219, DOI: 10.3846/20294913.2017.1280558

To link to this article: http://dx.doi.org/10.3846/20294913.2017.1280558

TECHNOLOGICAL AND ECONOMIC DEVELOPMENT OF ECONOMY
ISSN 2029-4913 / eISSN 2029-4921

2017 Volume 23(1): 196–219
doi:10.3846/20294913.2017.1280558

CONTROLS-BASED APPROACH FOR EVALUATION OF INFORMATION SECURITY STANDARDS IMPLEMENTATION COSTS

Dmitrij OLIFER[a], Nikolaj GORANIN[b], Arnas KACENIAUSKAS[a], Antanas CENYS[b]

[a] *Department of Graphical Systems, Faculty of Fundamental Sciences, Vilnius Gediminas Technical University, Saulėtekio al. 11, LT-10223, Vilnius, Lithuania*
[b] *Department of Information Systems, Faculty of Fundamental Sciences, Vilnius Gediminas Technical University, Saulėtekio al. 11, LT-10223, Vilnius, Lithuania*

Received 22 December 2016; accepted 06 January 2017

Abstract. According to the PricewaterhouseCoopers analysis, the average cost of a single information security and data protections breaches has increased twice during 2015 (Pricewaterhouse Coopers 2015). Amount of organizations who reported serious breach has also risen (from 9% in 2015 to 17% in 2016) (PricewaterhouseCoopers 2016). To achieve their goals criminals are using different techniques starting from Social engineering (phishing, whaling) and finishing with malware execution (such as ransomware) on target machines. Recent attacks (attack on Central Bank of Bangladesh, fraud attack on Mattel CEO and attack on Thailand state-run Government bank ATM) show, that criminals are very well organized, equipped and spend a lot of money and time to prepare their attacks. To protect themselves organizations are required to ensure security in depth principles and implement complex Security solutions, which are able to ensure the needed level of information security in appropriate costs.
However, information security cost-benefits assessment is complicated, because of lack of structured cost-benefit methods and issues with comparing IT security solutions in light of prevailing uncertainties. Existing methods are oriented on processes, environment lifecycles or specific standard implementations. Because of that, existing methods do not cover all needed security areas and methods reusability is a complicated task. Trying to solve this issue, we have proposed a new method for information standards implementation costs evaluation, based on information security controls.

Keywords: security standards, cost-benefit methods, risk analysis, vulnerability analysis, gap analysis, impact, security controls.

JEL Classification: C052.

Introduction

Security management and organization assets protection became one of the key points of organization success. According to Dhillon and Backhouse (2000) security becomes fundamental in our society and the survival of organizations depends on correct management of

Corresponding author Dmitrij Olifer
E-mail: *dmitrij.olifer@vgtu.lt*

up-to-date security elements. According to the technical report (PricewaterhouseCoopers 2015) developed by PricewaterhouseCoopers company, average costs of single information security and data protections breaches have increased twice during the last year. From 600 000 £ in 2014 to 1 460 000 £ in 2015. Such analysis results explain why information security requirements implementation is so important in nowadays.

From information security point of view, it is impossible to ensure absolute protection of organization assets or information. Because of that, each organization must define needed level of information and assets protection, which would satisfy their risk appetite and implement security management controls, which would ensure such level of protection. Existing security standards and requirements defined in such standards helps to achieve such goal and ensure that organization is implementing due diligence principles.

Nowadays there exist a set of widely recognized and approved security standards. Some of them are developed by governments (Sarbane-Oxley Act 2002), Health Insurance Portability and Accountability Act (HIPAA:2002) and are mandatory for organizations working in specific areas (like example financial sector or health assurance area). Other security standards were developed by commercial organizations, however some of them standards also become mandatory for organizations working in specific areas (e.g. Payment Card Industry Data Security Standard 2016).

It is need to be mentioned, that information security requirements could be implemented in different ways, starting from implementation of additional organizational controls (procedures, policies implementation) and finishing with complex technical solutions deployments. Li and Tang (2013) proposed to four main contents of Information security engineering, Security management, Communication security, Access of information systems and Secure IS development. Wangwe *et al.* (2012) proposed to concentrate on other three areas (Governance, Operational, Technical) to ensure effective information security management. Some authors were concentrated on specific information security areas, starting from network security and finishing cloud security. To protect data during client/server operation on network Kuo (2007) proposed an intelligent agent-based collaborative information security framework. Tsalis *et al.* (2013) proposed way how could be calculated return of Security investments for Cloud platforms.

From business perspective it is important to ensure that cost-business-justification for information security investments is in focus. Such approach, allows organizations to ensure effective and efficient IT Security budget management. It is very important to ensure, that incident losses together with countermeasures/controls deployment costs are lower, than incident loses without countermeasures/controls in place. Deployed controls and countermeasures should reduce organizations incident/risk probability to an acceptable level and appropriate cost.

However, information security cost-benefits assessment is complicated, because of lack of structured cost-benefit methods and issues with comparing IT security solutions in light of prevailing uncertainties. This problem became even greater for organizations, which try to implement the requirements of more than one information security standard. Such situation is common for bank sector organization, when they are trying to implement Sarbanes-Oxley act requirements, ISO27001 (International information security standard 2013) and PCI DSS security standards (2016) requirements.

Organization which are trying to implement more than two security standards requirements are challenged to solve such issues as duplication of requirements in different security standards and inefficient usage of organization resources, when similar security requirements are implemented in separate way for each security standard. Because of that, Security cost-benefit evaluation, used for such organizations, must have these additional restrictions in mind.

Use of cost-benefits evaluation and information security cost evaluation methods would let organization to identify how effective countermeasure/controls deployment would be and how it would help organization to reduce potential losses in case of incident or breach. Unfortunately, the amount of cost-benefits evaluation and information security evaluation methods is limited and majority of methods concentrate on processes, lifecycles steps and specific requirements of separate IT security standards. Because of that, existing methods do not cover all information security areas and could not be easily re-used for new standard re-evaluation. Our goal is to identify information security implementation cost-benefits evaluation method, which would let us calculate information security implementation costs/benefits, for organizations, which use two or more different security standards. Method approach and calculation results must be understandable for Senior management. Method must be easily re-usable for new security standards implementation costs calculations and should cover all Security areas and controls types (Administrative, Technical, Physical).

1. Existing Information security implementations cost-benefit evaluation methods

As it was mentioned, the main purpose of cost-benefit evaluation is to ensure that costs spent on information security are lower than benefits provided by them. In our case that means, that information security requirements implementation costs, are lower than damage caused by lack of protection. Unfortunately, information security do not generate direct profits for business and to evaluate the benefits organizations calculate potential losses, that could happen, if existing controls would not be in place. Cost-benefit calculation is a complicated process, however calculations the results could be presented as a difference between the expected losses before countermeasures/controls deployment and after.

Currently there exist different proposals on how the information security cost-benefits could be calculated. Lubich (2006) and Mercuri (2003) propose to use the Return on Security Investments (further – ROSI) metric. Similar metric, Return on Investments, is used in business to evaluate benefits of the taken business solution:

$$ROI = \frac{B - C}{C}, \tag{1}$$

where B denotes the "Gain of investment" and C denotes the "Cost of Investment". Information security solution returns on investments are distributed over time and because of that do not provide objective value. To solve this issue another metric is used – Net Present Value, which allows comparing benefits and costs over different time periods:

$$NPV = \sum_{i=0}^{n} \frac{B_t - C_t}{(1+i)^t}, \tag{2}$$

where B_t denotes present value of net benefits of period t, C_t denotes all costs, I denotes the discount rate and n denotes the time period.

As it was mentioned previously, information security does not generate direct benefits, because of that, this formula for information security was modified by adding additional criteria:

$$NPV = -I_0 + \sum_{t=1}^{T} \frac{\Delta E(L_t) + \Delta OCC_t - C_t}{(1+i_{calc})^t}, \quad (3)$$

where I_0 denotes the initial investment for security measure, $\Delta E(L_t)$ denotes the reduction in expected loss in t, ΔOCC_t denotes the reduction in opportunity costs in t, C_t denotes the cost of security measure in t and i_{calc} denotes the discount rate. Presented model returns a positive or negative value. Investments are economically effective when *NPV* is positive and do not equal 0.

From the information security point of view some of information security solutions still have to be implemented even if their NPV is negative, it mostly related to implementation controls which are mandatory for accreditations according to the information security requirements. Another disadvantage of such calculation methods is metric scope. Unfortunately, this metric is applied to separate solution, requirement implementation or control implementation. For overall security cost of benefits presentation NPV calculated for different solution could be assemble.

Arora *et al.* (2004) and Arora and Hall (2005) have proposed another framework for cost-benefits evaluation. Their framework is more related to the organization risk management evaluation and costs related to it. To evaluate the cost-benefits from the information security implementation they propose calculating the Risk-based Return on Investments (RROI):

$$RROI(security\ solution) = \frac{R_B - R_R - I_C}{I_C}, \quad (4)$$

where R_B denotes the Baseline Risk, R_R denotes the residual risk and I_C denotes the Implementation cost. Such calculation is closely related to the evaluation of security incidents and possibility of their occurrence. Advantage of such methods, that it lets calculating metrics for the overall information security area. Main disadvantage is that it concentrates on incidents and because of that could not take into account some controls which are mandatory from the regulatory point of view, but are not closely related to root cause of incidents (e.g. lack of documentation).

As we can see, both proposed cost-benefits methods still required organization clearly define information security costs.

2. Information security costs evaluation

As it could be seen from Return on Security Investments, NPV and Risk-based Return on Investments methods, key points in all calculation are Investment costs and Implementation costs, in other words budgets related to countermeasures/controls deployment. Cost-benefit methods use this component, however do not explain how they should calculated.

The major problem with Investment costs and Implementation costs calculation methods is related to the complexity of countermeasures/controls deployment. Countermeasures/Controls deployment is a complex process, which involves different organization sub-processes and their implementations, that are controlled by different organization teams. Security countermeasures/controls deployment is even more complicated, since identified risk, could be reduced in different ways, from applying organizational procedures till deploying complex technical solutions.

Before starting to analyze existing information security costs evaluation methods let identify major cost factors, which are involved in information security requirements implementation. De Bruijin *et al.* (2010) separate information security costs to 2 categories: One-off costs and Recurring costs. Table 1 presents subgroups of One-off and Recurring costs.

One-off costs generated in planning, design and implementation stage and recurring costs generated yearly during maintenance and support phases. Separate costs factor calculation could be different, and some of them could be calculated in a quantitative way, other

Table 1. Information security implementation costs

Description			
One-off costs		Recurring costs	
License	Licensing cost of tool or product. Only applied to vendor-based solutions.	Support	Support cost from the vendor. With some licensing schemes, a yearly fee has to be paid as well.
Policies	Policies and plans developed by to ensure organization information security requirements implementation and maintenance.	Administration	Costs for updaiting and configuring the solution. Reflecting changes in the business in the policies. User support (help desk).
Hardware	Hardware procurement, installation and configuration.	Monitoring	Monitoring the system.
Implementation	The full process of implementing the security measure. Usually this has impact on the infrastructure and the organization. The implementation of the security measure often is phased and can require a long term.	Auditing	Audits and tests performed to ensure the correct implementation and workings of the system.
Embedding	The embedding of the implementation in the organization. Employees are needed to be hired or get training. Other employes might also need training or at least be notified og the changes.		

would require to apply qualitative techniques. However, all below provided information security costs evaluation methods embed these costs factors during evaluation.

Brecht and Nowey (2012) proposed information security cost categorization approaches from different information security perspective. Authors categorize information security costs for such approaches:

– ***The Balance Sheet Oriented approach;***

This approach is understandable for management, because provides information security implementation costs in the way of IT-related budget planning. Gartner (2011) proposed to use 4 categories: Personnel Costs; Hardware; Software and Outsourcing/managed security Services. Such approach even it is understandable to organization management has some disadvantages. Classification of security costs into hardware and software is problematic, because often they are part of the same solution. Approach more oriented to IT security, than on information security.

– ***The Security measure life-cycle approach;***

Information security solutions evaluated according to the Information technology lifecycle. Such approach separate information security costs between Lifecycle phases: costs of purchase, costs of setup, costs of operation and costs of change. Advantages of such view on costs, is that each single control could be easily evaluated according to costs related to it. However, such approach do not involve organizational part of information security, such as policies, procedures and guidelines.

– ***IT-security process oriented approach;***

Humpert-Vrielink and Vrielink (2012) proposed to view on the information security costs from IT and Security points of view. Author categorize costs into 4 groups such as: costs for tool, consulting costs, costs for operation and costs of risk. Method concentrates on a single information security requirement or control evaluation. However, it could be easily applied to cover requirements or controls in all needed information security areas. The Security measure life-cycle approach, described above, could be embedded into this method and will provide income for tool costs evaluation.

The proposed model is not compatible with standard cost account models, used by business, and because of that information gathering could be complicated.

– ***The ISO/IEC 27001 oriented approach;***

The international standard ISO 27001 is widely used around the world. Brecht and Nowey (2012) proposed to look on information security implementation through ISO 27001 controls point of view. Authors separated costs into 12 controls areas defined in standard. If needed each of area could be divided into sub-costs. Authors proposed 2 additional metrics: determinability which describes how difficult the determination of the related costs is in practice and the information security cost ratio which describes the real percentage of the costs that may be accounted to information security.

Standard is covering wider range of controls and is not only related to information security that why it is difficult to evaluate what part of implementation cost is related to information security and which is not.

– ***The Information Security Management System – Layers approach.***

For accreditations according to one of the existing information security standards, organization has to prove that it ensures effective Organization Security management. It could be done by implementing Information Security Management system in the organization. Approach is evaluating information security implementation through such categories as: Management System, People and processes, Architecture and concepts, Operational Measures and Prerequisites (e.g. Inventory of assets or introduction of information ownership). Advantages of such approach, that area with High information security costs ratio separated from area with low costs. Disadvantages that for each area must be used separately.

As it was mentioned above, main goal of our evaluation is to choose method, which would be most effective for information security implementation costs evaluation, when organization is implementing two or more information security standards and their requirements. As it was defined by Jacobson *et al.* (1997) and Griss (2001) the main obstacles for effective component reuse are coming from the following areas: Business, Process, Organization, Engineering and Infrastructure. According to Zavadskas and Vilutienė (2006) the analysis of the purpose is to be achieved by using attributes of effectiveness, which have different dimensions, different weight as well as different directions of optimization. In our case for methods evaluation we have chosen five criteria, which cover 4 out of 5 Jacobson defined areas (Intelligibility for Senior management, Links with existing information security standards and Information security aspect coverage for Process area, Calculation complexity for Engineering, Reusability for Organization).

Information security costs methods mentioned above were evaluated by seven information security experts working in information security area. All specialist are working Educational sectors. Amount of information security specialist was chosen relating to analysis performed by Clemen and Winkler (1999) and Hora (2009). Both authors highlighted that differences among experts can be very important in determining the total uncertainty expressed about a question. Clemen and Winkler examine the impact of dependence among experts using a normal model and conclude that three to five experts are adequate. Hora created synthetic groups from the responses of real experts, and found that three to six or seven experts are sufficient, with little benefit from additional experts beyond that point. Because of that, for methods evaluation we invited seven experts, however evaluation itself was performed according to 5 expert opinion. Trying to make evaluation less subjective, best and worst evaluation results were eliminated. Each factor was evaluated in scale from 1 to 10, where 1 shows that method does not satisfy the requirement and 10 shows that it fully satisfies it. Averages of experts evaluations were used as qualitative values for each criteria. Table 2 presents evaluations results:

Graphical presentation for comparison results are presented in Figure 1.

As we can see from provided results, each method has his weak points. Best result was achieved by IT-security process oriented approach, however this method difficult to understand for senior management and method reusing for another IT security standard implementation could be an issue. However, this approach allows covering all information security areas. Starting from operational controls and finishing with technical risk mitigation controls implementation.

Table 2. Information security costs implementation methods evaluation

Cost evaluation method	Intelligibility for Senior management	Links with existing information security standards	Calculation complexity	Information security aspects coverage	Reusability	Overall results
The Balance Sheet Oriented approach	10	3	6	4	7	30
The Security measure life-cycle approach	7	6	7	6	9	35
IT-security process oriented approach	5	8	8	9	8	38
The ISO/IEC 27001 oriented approach	6	9	4	10	8	37
The Information Security Management System – Layers approach	4	9	4	10	7	34

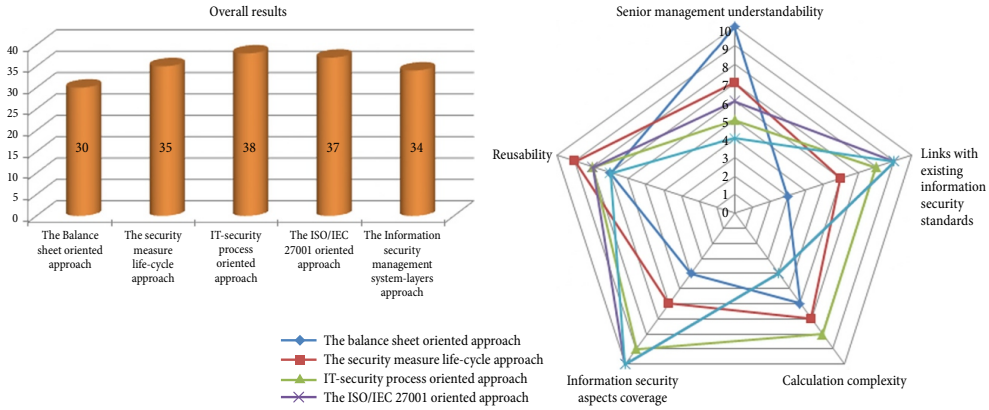

Fig. 1. Information security costs implementation methods comparison results

Other methods had some disadvantages, which do not let them to be effectively used for new information security standard requirements implementation purpose. Main disadvantages are: issues with covering organizational controls related to information security, too narrow or too wide view on security control cost evaluation, problems to separate controls between different categories of costs.

3. Information security costs for information standard control implementation

Because of the disadvantages of existing methods identified above, we are proposing the new cost evaluation method. As foundation for information security standard evaluation costs the IT security process oriented approach was taken. However, this approach was

amended by adding components related to Risk evaluation, which is mandatory in the security assurance process. The information security standard costs evaluation involve 2 main processes:

– Risk assessment process;

– Security control implementation process.

Risk assessment process is a mandatory process in any Information security activities, starting from information security management and finishing with information security audits. This process allows evaluation of the current situation and identification of missing gaps and probability of their exposure. Agrawal (2017) performed comparative study on information security Risk analysis methods and evaluated 4 different risk analysis methods (CIRA, CORAS, ISRAM and IS method).

As it was stated above, the proposed information security costs evaluation method should be applicable for organizations of different size. Because of that it was proposed to involve in information security costs evaluation formula additional coefficient φ. This coefficient allows to evaluate the organization's complexity, maturity and correlating information security costs. The proposed information security costs evaluation equation (Eq. 5) is the following:

$$C_{Security} = \varphi(C_{Risk\_assessment} + \sum_{i=1}^{n} C_{Security_{control_{implementation}\,i}}(standard)), \quad (5)$$

where φ – the complexity and maturity coefficient; $C_{Risk\_assessment}$ – Risk assessment costs, which explanation will be defined and described below (Eq. 7); $C_{Security\_control\_implementation_i}(standard)$ – Security control implementation (Eq. 15).

Complexity and maturity coefficient depends on 2 coefficients: *Complexity level* and *Maturity level*:

$$\varphi = \frac{Complexity\_level}{Maturity\_level}. \quad (6)$$

Complexity level defines Overall Organization systems complexity, and varies in the range from 1 to 5, where: 1 is Simple systems; 2 is Somewhat Complex systems; 3 is Complex systems; 4 is Very Complex systems; 5 is Highly Complex systems. Complexity level is evaluated and defined by the organization and is directly related to the amount of existing systems, systems interconnections, amount of processes maintained by these systems, amount of authorized users, amount of different roles and privileges, etc. Complexity level is evaluated in a Qualitative way by experts.

Maturity level defines the Overall organizations' maturity. For maturity level evaluation is used Capability Maturity Model (CMM). Harmer (2014) represented this model in his book related to Governance of Enterprise IT. Maturity levels are distributed in the range from 1 to 5, where: Level 1 – Initial (Chaotic); Level 2 – Repeatable; Level 3 – Defined; Level 4 – Managed; Level 5 – Optimizing.

Interdependency of complexity level and maturity levels dependency ensure, that costs of information security assurance in organizations with low maturity level and high systems complexity level will be higher than in organizations with high maturity level. I.e. maturity is decreasing the information security implementation and Assurance costs, while use of complex systems will increase them.

Risk assessment is a well-known and explained process, where all components could be evaluated from the costs point of view. According to the common practice, defined in different standards (NIST SP 800-30 2012), Risk assessment process must involve such steps as:

- Critical asset analysis. Such analysis involves assets identification, evaluation of their importance and impact to organization functionality;
- Vulnerabilities analysis (Identify vulnerabilities within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation);
- Threat analysis (Identify threat sources that are relevant to organizations; Identify threat events that could be produced by those sources; Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful);
- Impact evaluation (Determine the adverse impacts to organizational operations and assets, individuals, other organizations, and the overall resulting from the exploitation of vulnerabilities by threat sources (through specific threat events));
- Penetration testing (Attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities);
- Gap analysis (Existing situation comparing with information security standards requirements and identifying controls or implementations which are not aligned with mandatory standard requirements).

3.1. Risk assessment costs evaluation formula

The Risk assessment costs are calculated according to the following equation:

$$C_{Risk\_assessment} = C_{Asset\_analysis} + C_{Vulnerabilities\_analysis} + C_{Threat\_analysis} + C_{Impact} + C_{Penetration\_testing}(N) + C_{Gap\_analysis}, \quad (7)$$

where $C_{Asset\_analysis}$ – costs related to Critical asset analysis, $C_{Vulnerabilities\_analysis}$ – costs related to Vulnerabilities analysis, $C_{Threat\_analysis}$ – costs related to Threat analysis, $C_{Gap\_analysis}$ – costs related to gap analysis and $C_{Penetration\_testing}(N)$ – costs related to Penetration testing needed for Risk assessment, where N is amount of different organization systems, which have to be tested, C_{Impact} – costs related to Impact evaluation.

3.1.1. Critical asset analysis

Two sides are involved in Critical asset analysis process: consultant, performing Risk assessment and Organization's employees). These two sides are working together to gather the needed information. Because of that critical asset analysis overall costs will be the sum of Consultant and organization employees, who are involved in this process, costs.

These costs depend on time needed for consultant and employee conversations, discussions, information sharing. Additional time spent on the analysis process will increase the overall Critical asset analysis costs.

According to the provided statement, the Critical asset cost calculation is performed according to the Eq. 8:

$$C_{Asset\_analysis} = C_{consultant}(t) + \sum_{i=1}^{n} C_{Personal_i}(t), \quad (8)$$

where $C_{consultant}(t)$ is Security consultant costs, $C_{Personal_i}(t)$ – Organization's employee costs and ***t*** is time spent to perform the analysis.

Although more than one consultant can participate in risk assessment, we are simplifying the model and combine if the consultants into one by increasing the hour price.

Information security consultant and organization employee costs can be calculated by multiplying time ***t*** on hour costs, defined by their contracts:

$$C_{Consultant}(t) = Hour\_price * t; \quad (9)$$

$$C_{Personal}(t) = Hour\_price * t, \quad (10)$$

where $Hour\_price_{consultant}$ is consultant price per hour and $Hour\_price_{personal}$ average employee time price.

3.1.2. Vulnerability analysis

Vulnerability analysis process implementation is similar to Critical Asset analysis process. It means that vulnerability assessment is performed by information security consultant. Who has to identify and review list of vulnerabilities which are the most common for such type of organization, environments, etc. Information security consultant has to evaluate which vulnerabilities are relevant in this particular case.

Because of that, it could be stated that Vulnerability analysis process also involve 2 main parts: 1st is conversation and discussion with organization employees to gather information related to such analysis; 2nd part is gathering information for evaluation.

According to this vulnerability analysis costs could be calculated according to the Equation 11:

$$C_{Vulnerabilities\_analysis} = \alpha C_{consultant}(t) + \left(\beta C_{consultant}(t) + \sum_{i=1}^{n} C_{Personal_i}(t) \right), \quad (11)$$

where $C_{consultant}(t)$ is Security consultant costs and $C_{Personal_i}(t)$ is Organization employee costs. α and β are coefficients which define percentage of time spent for discussion with organization employees and information evaluation. Consultant and employee costs calculation is defined in Equation 9.

3.1.3. Threats analysis

During the Risk assessment the existing threats have to be evaluated. This part of risk assessment process is fully implemented by information security consultant and because of that cost calculation for this process directly depends on time needed for information security consultant to evaluate the existing threats and is calculated according to equation X:

$$C_{Threat\_analysis} = C_{Consultant}(t), \quad (12)$$

where $C_{consultant}(t)$ is Security consultant costs, calculated by Equation (9).

3.1.4. Impact analysis

One of the key principles in information security is to ensure, that information security costs are not higher than potential impact to the organization. Because of that an important step in Information Risk evaluation process is related to Impact analysis. This process involves two main participants: Information security consultant, who is responsible for explaining to organizations employees, what can happen with organization critical assets if identified threats will be exploit and organization employees who are responsible for evaluating the potential impact and defining it in financial way.

Impact analysis is to be calculated according to equation X:

$$C_{Impact} = C_{consultant}(t) + \sum_{i=1}^{n} C_{Personal_i}(t), \quad (13)$$

where $C_{consultant}(t)$ is Security consultant costs and $C_{Personal_i}(t)$ is Organization employee costs. Consultant and employee costs calculation are defined in Equation (9).

Impact costs require inputs from organization management, because of that cost of such evaluation is higher than other calculation steps.

3.1.5. Penetration testing

In some cases information security consultant and organization employee are not able to identify all existing vulnerabilities, that can be exploited. In such case organization is recommended to perform Penetration testing. Before performing penetration testing information security consultant has to define penetration testing scope, identify technical teams which will be involved in it. Penetration testing is performed by a specialist who has the appropriate knowledge level and experience in ethical hacking. Such experts cost are usually defined in contracts.

Because of that Penetration testing costs could be calculated, according to the equation:

$$C_{Penetration_{testing}}(N) = C_{consultant}(t) + \sum_{i=1}^{n} C_{Personal_i}(t) + Fix\,cost,\ defined\,by\,contract, \quad (14)$$

where $C_{consultant}(t)$ are Security consultant costs and $C_{Personal_i}(t)$ are Organization employee costs. Consultant and employee costs calculation is defined in equation (9), $\boldsymbol{N}$ is amount of different organization systems, that have to be tested.

3.1.6. Gap analysis

After collecting the required information, information security consultant has to analyze it and verify from the information security standard point of view. Any requirements, which are mandatory according to the information security standard, and not implemented in the organization have to be identified and listed. This process involves results from all previous steps, however it is performed only by the information security consultant. Because of that such process costs calculations could be done in the same way as Threats analysis costs calculations (Eq. 12).

3.2. Security control implementation costs

The next step in information security standards requirements implementation is identification of security controls, which have to be implemented by organization. To identify the list of needed controls information security consultant has to identify critical assets, evaluate the related risk and to choose the appropriate mitigation strategy.

The overall security controls implementations costs will be the aggregated sum of separate control implementation costs. To highlight the security controls, that are related to critical assets, we are proposing to add Control criticality coefficient $m_{i(Risk_i)}$, which depends on Risk identified for Critical asset and varies from 0 to 1, i.e. if risk, that critical asset will be exploited is higher, then cost of such control will increase.

Security control implementation is directly linked with the chosen Mitigation strategy and action needed to implement it. According to such statement, security control implementation costs could be calculated in such way (Eq. 16):

$$C_{Security\_control\_implementation} = \sum_{i=1}^{n} (m_i(Risk_i) * (C_{Mitigation\_strategy_i} + C_{Action_i})), \quad (15)$$

where $m_i(Risk_i)$ is Control criticality coefficient and $Risk_i$ is calculated according to (Eq. 16):

$$Risk_i = Vulnerability_i * Threat_i * Impact_i, \quad (16)$$

where $Vulnerability_i$ are the vulnerabilities identified for asset *i*, $Threat_i$ are the threats identified for asset ***i***, $Impact_i$ is impact identified for asset *i*.

3.2.1. Mitigation strategy costs

Mitigation strategy depends on management risk appetite and information about historical issues, that have happened to specific critical asses in the past. Historical data could be gathered by organization individually or it could be statistical data common for specific area (financial, infrastructure or government organization).

Usually 4 main mitigation strategies are defined:

Risk accepted – when organization management understand existing risk, but because of low probability of negative events or because of high price of mitigation controls decide do not implement any actions to reduce it.

Risk avoided – when organization management understand existing risk and decide to remove risk source.

Risk remediated – when organization management understand existing risk and are taken action to reduce it till acceptable level.

Risk transferred – when organization management understand existing risk and pass it to 3rd party, which is responsible for it management or compensation in worst cases.

According to that the Mitigation strategy could be defined as:

$$C_{Mitigation\_strategy} = \begin{cases} -C_{Action}, \ where \dfrac{\Delta T(t_{in})}{T(l_j)} * \bar{W} \le Risk\_apetite \ and \ C_{Action} \ is \ HIGH & (Risk \ ACCEPTED) \\ 0, \ where \dfrac{\Delta T(t_{in})}{T(l_j)} * \bar{W} \le Risk\_apetite \ and \ C_{Action} \ is \ ACCEPTABLE & (Risk \ AVOIDED) \\ C_{Metrics\_control}, \ where \dfrac{\Delta T(t_{in})}{T(l_j)} * \bar{W} > Risk\_apetite \ and \ C_{Action} \ is \ ACCEPTABLE & (Risk \ REMEDIATED) \\ C_{insurance} + C_{Metrics\_control} - C_{Action}, \ where \dfrac{\Delta T(tt_{in})}{T(l_j)} * \bar{W} > Risk\_apetite \ and \ C_{Action} \ is \ HIGH & (Risk \ TRANSFERRED) \end{cases},$$

where *Risk_apetite* is organization willing to handle the existing risk, $\Delta T(t)$ – amount of security incidents during defined time t_{in}, $T(l_j)$ – amount of impacted systems, l_j – asset impacted by security incident, j – asset number, $\bar{W}$ - impact average, $C_{Metric\_control}$ – cost of metrics control operations, which could involve $C_{personal}$ and C_{Action} for additional specific tools, $C_{insurance}$ – cost of insurance, according to the signed off contract with the 3rd party (insurance company?).

3.2.2. Action costs

After confirmation of the risk mitigation strategy, chosen control has to be implemented. This process is directly linked to Security measure life cycle approach. In our calculation we identify 2 main tasks, which are Action implementation costs and Control operation costs. Implementation costs are related to time, needed to implement chosen actions. For calculation simplicity, time could not be longer than one year, otherwise it would be problematic to calculate Return on investments values.

$$C_{Action} = C_{Implementation}(t) + C_{Operation}, \quad (18)$$

where $C_{Implementation}(t)$ is action implementation costs and $C_{Operation}$ is Control operation costs.

3.2.3. Action implementation costs

This part of our equation (Eq. 19) depends on additional sub steps related to hardware and software procurements and their deployment costs. Environment purchase could be evaluated as one time cost freezed in time and deployment costs are related to the deployment project. Environment definition include hardware, software and any other technical components required for system or solution business as usual activities. According to this Action implementation costs could be calculated in the following way (Eq. 19):

$$C_{Implementation}(t) = C_{Environment\_purchase} + C_{deployment}(t), \quad (19)$$

where $C_{Environment\_purchase}$ – are hardware and software procurement costs and $C_{deployment}(t)$ – are project deployment costs.

It is needed to be mentioned that the same hardware and software could be used to ensure more than one information security control. In that case Control implementation costs must be calculated only one time. Any other controls should not be involved into

calculation, except situation, when existing control was amended and such amendment costs were not calculated previously.

Deployment project costs could be divided into 3 main groups:

- Personal, who is performing such deployment actions. Technically it could be the team or even whole department who will be deploying it.
- Configuration costs, which could be implemented by 3rd party as a one-time contact cost.
- Costs related to personal training and awareness, before letting them use a new system. Training/Learning or Awareness sessions could be implemented internally or performed by external systems.

Such approach allows us calculating the Deployment costs as following (Eq. 20):

$$C_{deployment}(t) = \sum_{i=1}^{n} C_{Personali} + C_{configuration} + C_{Training/Awareness}, \quad (20)$$

where $C_{Personali}$ is Organization employee costs, which are defined by Equation (9), $C_{configuration}$ – configuration costs, $C_{Training/Awareness}$ – training/awareness costs.

3.2.4. Operation costs

Operation costs are continuous costs, that are applicable to the control during the whole life cycle. These costs also include Environment support costs. Very often organizations are signing the Support agreements with hardware and software vendors trying to ensure the security and functionality of hardware and software in use. However, use of hardware and software also requires from organization to ensure its internal maintenance, for that purpose often used internal resources. And the last part is related to the amendments implemented on existing solutions (hardware or software) and is defined as Other services. Such amendments could involve implementation of new functionality, changes in process workflow and others.

Operation costs could be calculated according to the equation (Eq. 21):

$$C_{Operation} = C_{Environment\_support} + \sum_{i=1}^{n} C_{Personali} + C_{Other\_services}, \quad (21)$$

where $C_{Environment\_support}$ is Environment support costs, $C_{Personali}$ – Organization employee costs, which are defined by Eq. (9), $C_{Other\_services}$ – cost of additional services needed for effective control functioning.

4. Results and discussion

To verify the applicability and effectiveness of the proposed information security costs evaluation method, the modeling experiment was performed. Due to the advantage of the proposed approach (control based) we can simulate calculations for one specific IT security requirement. During the experiment, information security costs were evaluated for two abstract companies ACME and EMCA, that are generally used for such modeling tasks. Both of the companies being modeled were implementing Logging and Monitoring control, required by ISO 27001 and PCI DSS standards. The starting modeling conditions are presented in Table 3.

Table 3. Experiment background

ACME	EMCA
– ACME implementation is not aligned\certified by any IT security standard, however some security areas (e.g., Logical Access management) are effectively covered by the organization. – ACME Complexity level = 3, has ACME has complex information systems, which are used for data management and interchange with 3rd parties. – ACME maturity level = 2 "Repeatable". Some processes in the organization are implemented, however they are weakly documented. – Risk assessment and penetration testing for both systems in scope were performed by the same 3rd party. – ACME has 342 employees and 5 main departments (Management board; HR; Finance; IT support; Developers). – Consultant hour rate – 30 €. – Employee hour rate – 11 €.	– EMCA organization is already certified and is aligned with ISO 27001 standard, however wants to be aligned with PCI DSS standard. – EMCA Complexity level = 3, EMCA has complex information systems, which are used for data management and interchange with 3rd parties. – EMCA maturity level = 4 "Managed". Main processes are fully managed, that means they are documented, monitored and are fully under the day by day control. – Risk assessment and penetration testing for both systems in scope were performed by the same 3rd party. – EMCA has 245 employees and 5 main departments (Management board; HR; Finance; IT support; Developers). – Consultant hour rate – 30 €. – Employee hour rate – 11 €.

Information security implementation costs for both organizations were calculated according to the proposed methodology. Calculation results are presented in Table 4, where the calculation equation is provided as well as related comments on each step.

Information security costs for Logging and monitoring control implementation was also calculated by five existing methods provided above. Calculation according to The Balance sheet oriented approach took approximately the same amount of time as calculation according to new method (~ 1 hour to gather information and calculate control implementation cost). Cost calculations for ACME organization was easy and effective, because we didn't have any controls in place and tried to implement new control from scratch. For EMCA cost calculations was complicated, because we need to identify cost of existing controls and also cost of additional actions. Need to be mentioned, that from Security point of view standard mapping we need perform manually. It means, that each new standard would require from us such additional standard and requirements mapping actions, which are growing exponentially with amount of mapped standards.

The Security measure life-cycle approach required 40 minutes to perform calculations, however risk analysis costs and procedural controls implementation costs identification was complicated. Need to be mentioned, that this method let easily re-use result from previous calculations, so calculation for EMCA organization, which tried to be aligned with second IT security standard was done quicker than for ACME organization.

IT security process oriented approach take 1.5 hour to perform calculations. Most complicated part was risk calculation, because it required to have historical data about incidents related to this control. Another spotted issue, that calculated risk do not have any correlation with mitigation controls. From security point of view, it means, that is not clear why one or another decision was made.

Table 4. Calculation results

Formula	ACME	EMCA	Comments
Complexity and maturity coefficient $\varphi = \frac{Complexity\_level}{Maturity\_level}$	$\frac{3}{2} = 1.5$	$\frac{3}{4} = 0.75$	Higher organization maturity level let decrease the information security implementation and Assurance costs for EMCA.
Critical asset analysis $C_{Asset\_analysis} = C_{consultant}(t) + \sum_{i=1}^{n} C_{Personal_i}(t)$ $C_{Consultant}(t) = Hour\_price * t$ $C_{Personal}(t) = Hour\_price * t$	$C_{Asset\_analysis} = (30*5) + (11*5) + (11*5) = 206$ €	$C_{Asset\_analysis} = (30*2) + (11*2) + (11*2) = 104$ €	Critical asset analysis took: 5 hours in ACME and 2 hours in EMCA 2 organization employees have participated in asset analysis.
Vulnerability analysis $C_{Vulnerabilities\_analysis} = \alpha C_{consultant}(t) + \left(\beta C_{consultant}(t) + \sum_{i=1}^{n} C_{Personal_i}(t)\right)$ α and β are coefficients which define percentage of time spent for discussion with organization employees and information evaluation.	$\alpha = \frac{2}{5} = 0.4$ $\beta = \frac{3}{5} = 0.6$ $C_{Vulnerabilities\_analysis} = (0.4*30*2) + (0.6*30*3 + 11*3 + 11*3) = 144$ €	$\alpha = \frac{1}{3} = 0.33$ $\beta = \frac{2}{3} = 0.66$ $C_{Vulnerabilities\_analysis} = (0.66*30*2) + (0.33*30*1 + 11*1 + 11*1) = 84.56$ €	Vulnerability analysis took: 3 hours in ACME and 1 hours in EMCA 2 hours consultant spent to identify summarize vulnerabilities 2 organization employees participated in asset analysis.
Threats analysis $C_{Threat\_analysis} = C_{Consultant}(t)$	$C_{Threat\_analysis} = 30*4 = 120$ €	$C_{Threat\_analysis} = 30*4 = 120$ €	Threat analysis took 4 hours for both organizations.
Impact analysis $C_{Impact} = C_{consultant}(t) + \sum_{i=1}^{n} C_{Personal_i}(t)$	$C_{Impact} = (3*30) + (3*11 + 3*11) = 156$ €	$C_{Impact} = (3*30) + (3*11 + 3*11) = 156$ €	Critical asset analysis took: 3 hours in ACME and 2 hours in EMCA.

Continue of Table 4

Formula	ACME	EMCA	Comments
Penetration testing $C_{Penetration\_testing}(N) = C_{consultant}(t) + \sum_{i=1}^{n} C_{Personal_i}(t) + Fix\ cost, defined\ by\ contract$	$C_{Penetration\_testing}(1) =$ $30*1+11*1+1250 = 1291$ €	$C_{Penetration\_testing}(1) =$ $30*1+11*1+1250 = 1291$ €	Penetration testing require 1 hour activities from consultant and employee. And cost 1250 € During test was tested 1 system (Logging and Monitoring).
Gap analysis $C_{Gap\_analysis} = C_{Consultant}(t)$	$C_{Gap\_analysis} =$ $2*30 = 60$ €	$C_{Gap\_analysis} =$ $2*30 = 60$ €	Threat analysis took 2 hours for both organizations.
Risk assessment process $C_{Risk\_assessment} = C_{Asset\_analysis} + C_{Vulnerabilities\_analysis} + C_{Threat\_analysis} + C_{Impact} + C_{Penetration\_testing}(N) + C_{Gap\_analysis}$	$C_{Risk\_assessment} =$ $(206+144+120+156+1291+60) = 1977$ €	$C_{Risk\_assessment} =$ $(104+84.56+120+156+1291+60) = 1815{,}56$ €	Sum of calculations done above Risk assessment cost depends from organization configuration and assessment scope.
$m_i(Risk_i)$ is Control criticality coefficient $Risk_i = Vulnerability_i * Threat_i * Impact_i$	$m_i - 0.7$	$m_i - 0.3$	This coefficient will be identified during risk assessment process. Because of that for ACME: $m_i - 0.7$ and for EMCA: $m_i - 0.3$.
$C_{Mitigation\_strategy} =$ $-C_{Action}$, $where \frac{\Delta T(t_{in})}{T(l_j)} * \overline{W} \le Risk\_apetite$ and C_{Action} is HIGH		$(Risk\ ACCEPTED)$	
0, $where \frac{\Delta T(t_{in})}{T(l_j)} * \overline{W} \le Risk\_apetite$ and C_{Action} is ACCEPTABLE		$(Risk\ AVOIDED)$	
$C_{Metrics\_control}$, $where \frac{\Delta T(t_{in})}{T(l_j)} * \overline{W} > Risk\_apetite$ and C_{Action} is ACCEPTABLE		$(Risk\ REMEDIATED)$	
$C_{insurance} + C_{Metrics\_control} - C_{Action}$, $where \frac{\Delta T(tt_{in})}{T(l_j)} * \overline{W} > Risk\_apetite$ and C_{Action} is HIGH		$(Risk\ TRANSFERRED)$	

Continue of Table 4

Formula	ACME	EMCA	Comments
$\Delta T(t)$ – amount of security incidents during defined time t, $T(l_j)$ – amount of impacted systems lj – asset impacted by security incident, j – asset number, $\overline{W}$ – Impact average amount.	$\frac{\Delta T(t)}{T(l_j)} * \overline{W} =$ $\frac{136}{17} * 137 = 1096$ For ACME risk is below Risk appetite, so depending from cost of mitigation controls ACME could ACCEPT risk or AVOID it Let predict, that ACME will Avoid risk.	$\frac{\Delta T(t)}{T(l_j)} * \overline{W} =$ $\frac{136}{17} * 137 = 1096$ For EMCA risk is above Risk appetite, so depending from cost of mitigation controls EMCA could REMEDIATE risk or TRANSFER it Let predict, that EMCA will Remediate their risk	This information is taken from statistic data for market area or from organization historical data. For ACME and EMCA we are taken market statistics: ΔT – 136 incidents for Finance insurance and credit sector T – 17 assets for both organizations $\overline{W}$ – 137 € Risk appetites: for ACME is 1500 for EMCA is 1000
Security control implementation costs $C_{Security\_control\_implementation} =$ $\sum_{i=1}^{n}(m_i(Risk_i) * (C_{Mitigation\_strategy_i} + C_{Action_i}))$ $C_{Metrics\_control}$ – Cost of metrics control operations, which could involve $C_{personal}$ and C_{Action} for additional specific tools, $C_{insurance}$ – Cost of insurance, according to signed off contract with 3rd party.	$C_{Security\_control\_implementation} =$ $0.7 * C_{Action_i} =$ 0.7 * 352 = 246.4 €	$C_{Security\_control\_implementation} =$ $0.3 * (C_{Metrics\_control} + C_{Action_i}) =$ 0.3* (500 + 878 + 10860) = 3671.4 €	Security implementation costs for ACME and EMCA will be calculated differently, because they chose different mitigation strategy.
Action costs $C_{Action} =$ $C_{Implementation}(t) + C_{Operation}$	$C_{Action} = C_{Operation}$	$C_{Action} = C_{Implementation}(t) + C_{Operation}$	ACME to avoid risk, will decommissioned legacy systems from their environment. In that case Actions cost are equal to Operation costs, needed to remove legacy environment. EMCA will deploy logs gathering tool (Splunk), create monitoring team.

End of Table 4

Formula	ACME	EMCA	Comments
Action implementation costs $C_{Implementation}(t) = C_{Environment\_purchase} + C_{deployment}(t)$ $C_{Environment\_purchase}$ – are hardware and software procurement costs.	–	$C_{Implementation}(t) = 500\ € + C_{deployment}(t)$	Splunk tools for EMCA with all needed environment will cost 500 €.
Deployment project costs $C_{deployment}(t) = \sum_{i=1}^{n} C_{Personali} + C_{configuration} + C_{Training/Awareness}$ $C_{configuration}$ – is configuration costs, $C_{Training/Awareness}$ – is training/awareness costs.	–	$C_{deployment}(t) = (3*11*16) + 250 + 100 = 878\ €$	In Splunk deployment will participate 3 EMCA employees. And they will need 16 hours to fully deploy it. Configuration costs are defined in contract with Splunk organization and will cost 250 €. Training will cost EMCA 100 €.
Operation costs $C_{Operation} = C_{Environment\_support} + \sum_{i=1}^{n} C_{Personali} + C_{Other\_services}$ $C_{Environment\_support}$ is Environment support costs, $C_{Other\_services}$ – is cost of additional services needed for effective control functionality.	$C_{Operation} = \sum_{i=1}^{n} C_{Personali} = 4*11*8 = 352\ €$	$C_{Operation} = 150 + (2*2*11*20*12) = 10860\ €$ annually	ACME will need to decommission legacy environment. It will be done by 4 employees during 8 hours. Splunk environment support cost organization 300 € annually. Splunk maintained by 2 employees ~2 hours during the day. EMCA do not have other services.
Information security implementation costs $C_{Security} = \varphi(C_{Risk\_assessment} + \sum_{i=1}^{n} C_{Security\_control\_implementation_i}(standard))$	$C_{Security} = 1.5*(1977 + 246.4) = 3355.1\ €$	$C_{Security} = 0.75*(1815.56 + 3671.4) = 4115.22\ €$	As we can see additional controls implementation costs depends from Risk mitigation decision and from environment configuration.

The ISO/IEC 27001 method let calculate information security costs during 35 minutes. During calculation was difficult to identify control implementation costs related to such areas as organization and people. Need to be mentioned, that method, show itself as very effective during calculation for EMCA organization. Method closely aligned to ISO/IEC 27001 standard, which cover practically all information security areas and because of that was could be easily mapped with PCI DSS standard requirements.

The Information Security Management System – Layer approach was low effective for single control calculation. It took 1.75 hour to calculate Logging and Monitoring control costs according to this method. And need to be mentioned, that some important areas such as Architecture and concepts during single control calculation was ignored, because their calculation required involvement of other system costs, which was out of scope for our experiment.

New proposed method in comparison with existing methods has one weak point – it is complicated calculation. However even such complicated calculation took only 2 time more time than quickest cost calculation method. And it is need to be mentioned, that calculation is complicated only for the first time, during the second cost evaluation huge part of performed calculations results could be reused, because of their control orientation. It means, that previous calculation results could be easily reused if it is needed.

As advantages of this method, could be mentioned, that he is control oriented, and as such is fully aligned with existing security standards and procedures and could cover all needed information security aspects.

According to Yolles (1999) viability systems are complex actor systems which are able to survive under change through adoption. The same viability criteria could be applied to proposed method. Our experiment, with implementation of single security requirement/control in 2 different organizations proved, that method could be effectively applied in different organizations with different level of complexity and maturity. According to demands it could be used to verify any existing information security standard implementation costs, as soon as list of security requirements/controls related to this standard are defined.

The proposed method could be most effectively used, with specific tools or solutions, which would let to map two or more information security standard. In that case, after first evaluation, organization would be able clearly identify which controls or areas in their organization are not secured or aligned with standard, and according to calculation results from previous evaluation predict, how much it will cost them. And such effectiveness could be achieved by using IT security standard automatisation tools.

For new method comparison with already existing method we were using the same five criteria. Table 5 presents information security consultant evaluation results for new proposed method:

Table 5. Proposed method evaluation

Cost evaluation method	Intelligibility for Senior management	Links with existing information security standards	Calculation complexity	Information security aspects coverage	Reusability	Overall results
Proposed method	8	10	2	10	9	39

In comparison with existing information security costs implementation methods proposed method is most effective in Links with existing information security standards and Information security aspects coverage areas.

Conclusions

The existing methods analysis has shown, that existing methods are not effective to solve above described problem of information security implementation cost-benefits identification for organizations, which use two or more different security standards. The following disadvantages of the existing methods were identified: Complicated calculation process (IT security process oriented approach), Fair security aspects coverage (The Balance sheet oriented and The Security measure life-cycle approaches), complicated way to reuse calculations for implementation of new standard in the same organization.

To eliminate the identified disadvantages the new information security implementation costs evaluation method was proposed. The proposed method is based on the control-based approach, orientation on planned risk management strategy and organization maturity and system complexity integration in implementation cost calculations. Such approach ensures, that calculation method is aligned with different security standards and requirements.

New method applicability and effectiveness were verified during the modeling experiment. For the experiment virtual companies with different maturity and implemented systems complexity levels were used. For calculation simplicity, calculations were performed only for single Logging and Monitoring control.

The new method is not very effective during the first iteration from calculation duration and complexity point of view. At that phase the proposed method shows lower results, compared to the existing methods, however, time difference was not significant. Advantages of the new method were approved during the further calculation iterations, when previous calculations were reused. Because of the control-based approach, this method is agnostic and could be easily linked with any IT security standard and allows covering almost any IT security aspect.

The proposed method was evaluated by the same evaluation scheme as the existing methods and got higher results, except time consumption. However, this negative aspect is significantly reduced during further iterations.

Further experimental tests and integration with IT security standards automation tools would allow increasing the method effectiveness.

References

Agrawal, V. 2017. A comparative study on Information Security Risk analysis methods, *Journal of computers* 1(12): 57–67. https://doi.org/10.17706/jcp.12.1.57-67

Arora, A.; Hall, D.; Pinto, A.; Ramsey, D.; Telang, R. 2004. *An ounce of prevention vs. a pound of cure: how can we measure the value of IT security solutions?* [online], [cited 1 December 2016]. Available from Internet: http://www.courant.nyu.edu/ComplexSystems/literature/Arora,etal.pdf

Arora, A.; Hall, D. 2005. Measuring the risk-based value of IT security solutions, *IT Professionals* 6(6): 35–42. https://doi.org/10.1109/MITP.2004.89

Brecht, M.; Nowey, T. 2012. A closer look at Information Security costs, in *11th Annual workshop on the Economics of Information Security WEIS 2012*, 25–26 June 2012, Berlin, Germany.

Clemen, R. T.; Winkler, R. L. 1999. Combining probability distributions from experts in risk analysis, *Risk Analysis* 19(2): 187–20. https://doi.org/10.1111/j.1539-6924.1999.tb00399.x

Dhillon, G.; Backhouse, J. 2000. Information system security management in the new millennium, *Communications of the ACM* 43(7): 125–128. https://doi.org/10.1145/341852.341877

de Bruijn, W.; Spruit, M. R.; van den Heuvel, M. 2010. Identifying the cost of security, *Journal of Information Assurance and Security* 5(2010): 074–083.

Gartner. 2011. *IT Budget: Information Security & Risk Management Spend Metrics* [online], [cited 27 December 2011]. Available from Internet: http://www.gartner.com/technology/metrics/it-security-risk-spending.jsp

Griss, M. 2001. CBSE success factors: integrating architecture, process and organization, Chapter 9 in G. T. Heineman, W. T. Councill (Eds.). *Component-based software engineering: putting the pieces together.* Addison-Wesley.

Harmer, G. 2014. *Governance of enterprise IT based on COBIT®5. A management guide.* IT Governance Publishing.

HIPAA:2002. Health Insurance Portability and Accountability Act. US mandatory regulatory requirements for Health Insurance sector.

Hora, S. C. 2009. *Expert judgment in risk analysis.* Non-published Research Reports [online], [cited 1 December 2016]. Available from Internet: http://create.usc.edu/research/publications/2420

Humpert-Vrielink, F., Vrielink, N. 2012. A modern approach on Information Security measurement, *ISSE 2012 Securing Electronic Business Processes,* 48–53. https://doi.org/10.1007/978-3-658-00333-3_5

Jacobson, I.; Griss, M.; Jonsson, P. 1997. *Software reuse: architecture, process and organization for business success*. Addison-Wesley-Longman.

Kuo, M. H. 2007. An intelligent agent-based collaborative information security framework, *Expert systems with applications* 32(2): 585–598. https://doi.org/10.1016/j.eswa.2006.01.053

Li, M.; Tang, M. 2013. Information Security engineering: a framework for research and practices, *International Journal of Computers Communications & Control* 8(4): 578–587. https://doi.org/10.15837/ijccc.2013.4.579

LST ISO/IEC 27001:2013. *Information technology – Security techniques – Information security management systems – Requirements*. International Information Security standard.

Lubich, H. P. 2006. IT-Sicherheit: Systematik, aktuelle Probleme und Kosten-Nutzen-Betrachtung. HMD, *Wirtschaftsinformatik* (248): 6–15. (in German)

Mercuri, R. T. 2003. Analyzing security costs, *Communications of the ACM* 46(6): 15–18. https://doi.org/10.1145/777313.777327

NIST SP 800-30. 2012. *Guide for Conducting Risk Assessments*. US standard. https://doi.org/10.6028/NIST.SP.800-30r1

PCI DSS:2016. *Payment Card Industry Data Security Standard*. International Information Security standard.

PricewaterhouseCoopers. 2015. *Information Security Breaches survey conducted by PwC in association with InfoSecurity Europe* [online], [cited 1 December 2016]. Available from Internet: http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

PricewaterhouseCoopers. 2016. *Information Security Breaches survey conducted by PwC* [online], [cited 1 December 2016]. Available from Internet: http://www.pwc.be/en/news-publications/publications/2016/information-security-breaches-survey.html

Sarbane-Oxley act of 2002. US mandatory regulatory requirements.

Tsalis, N.; Theoharidou, M.; Gritzalis, D. 2013. Return on security investment for Cloud platforms, in *Fifth international conference on cloud computing technology and science (cloudcom),* 2013 IEEE, 2–5 December 2013, Bristol, England. https://doi.org/10.1109/CloudCom.2013.115

Wangwe, C. K.; Eloff, M. M.; Venter, L. 2012. A sustainable information security framework for e-government – case of Tanzania, *Technological and Economic Development of Economy* 18(1): 117–131. https://doi.org/10.3846/20294913.2012.661196

Yolles, M. 1999. *Management systems: a viable systems approach.* Financial Times Management.

Zavadskas, E. K.; Vilutienė, T. 2006. A multiple criteria evaluation of multi-family apartment block's maintenance contractors: I-Model for maintenance contractor evaluation and the determination of its selection criteria, *Building and Environment* 41(5): 621–632. https://doi.org/10.1016/j.buildenv.2005.02.019

Dmitrij OLIFER. He received Bachelor's and Master's degree in Informatics Engineering from Fundamental Sciences Faculty at Vilnius Gediminas Technical University. His research results was published in journal *International Journal of Computers, Communications & Control (IJCCC)*. Member of ISACA organization. Keeps the CISM and CISA certificates. As Lithuanian police department Information security specialist participated in Europol Security Board meetings. Keeps the position of Information Security consultant in Barclays Group Operation Lithuania. Research interests: information security management, information security process modelling, risk analysis and management.

Nikolaj GORANIN. Doctor, Associated Professor at the Department of Information Systems, Vice-Dean for Research and International Relations at Faculty of Fundamental Sciences at Vilnius Gediminas Technical University. Has job experience as a system administrator, FP6 and EU structural funds project coordinator. Member of ISACA Lithuania Board. Keeps the position of Chief Information Security Officer at Level 1 (VISA classification) service provider (responsible for PCI DSS compliance and certification). Keeps the CISM and CISA certificates. Has published over 30 papers. Research interests: information security technologies, information security management, artificial intelligence in information security, information security process modelling.

Arnas KACENIAUSKAS. Doctor, Associated Professor at the Department of Graphical Systems. Graduated in applied mathematics from the Vilnius University, Lithuania, in 1995. The MS degree in computer science received from the VGTU in 1996. Doctor thesis "Modelling of viscous incompressible flows and free surfaces by the finite element method" defended and PhD degree received from VGTU in 2000. Research interests: comprise parallel and distributed computing, computational fluid dynamics, computational electromagnetics, the finite element method, the discrete element method, free surfaces and moving interfaces.

Antanas CENYS. He received his PhD in Vilnius University. He is the Dean of Science in Vilnius Gediminas Technical University. In 1999, he received the Lithuanian National Award of Science. He has more than 70 publications in journals such as *Electronics and Electrical Engineering, International Journal of Computers, Communications & Control (IJCCC), Information Technology* and *Control, Chaos, Solitons & Fractals* and more. His research interests include cryptography and network security, nonlinear dynamics in information technologies and electronic systems, nonlinear time series analysis in physics and biology, advanced mathematical methods and their applications, theory of chaotic systems and semiconductor theory.