Assessing Future Value of Investments in Security-Related IT Governance Control Objectives – Surveying IT Professionals

Waldo Rocha Flores, Teodor Sommestad, Hannes Holm and Mathias Ekstedt
Royal Institute of Technology, Stockholm, Sweden
waldorf@ics.kth.se
teodors@ics.kth.se
hannes.holm@ics.kth.se
mathiase@ics.kth.se

Abstract: Optimizing investments in IT governance towards a better information security is an understudied topic in the academic literature. Further, collecting empirical evidence by surveying IT professionals on their relative opinion in this matter has not yet been explored to its full potential. This paper has tried to somewhat overcome this gap by surveying IT professionals on the expected future value from investments in security-related IT governance control objectives. The paper has further investigated if there are any control objectives that provide more value than others and are therefore more beneficial to invest in. The Net Present Value (NPV) technique has been used to assess the IT professional's relative opinion on the generated future value of investments in 19 control objectives. The empirical data was collected through a survey distributed to professionals from the IT security, governance and/or assurance domain and analyzed using standard statistical tools. The results indicate that the vast majority of investments in control objectives is expected to yield a positive NPV, and are beneficial to an organization. This result implies that investments in control objectives are expected to generate future value for a firm, which is an important finding since many of the benefits from an investment are indirectly related and may occur well into the future. The paper moreover contributes in strengthening the link between IT governance and information security.

Keywords: IT governance, control objectives, information security, net present value

1. Introduction

Contemporary enterprises are largely dependent on Information Technology (IT) as it supports many critical business and administrative functions. This dependency has unfortunately led to an increase in potential threats to the enterprise and its information assets. Enterprises are therefore compelled to invest in information security to mitigate threats, manage incidents and avoid negative consequences on business objectives. Information security is however dependent on many factors that concern both technical and organizational aspects. Assessing the value of a security investment before the investment decision is taken is therefore challenging, and makes it difficult for a decision-maker to prioritize different investment alternatives.

Information security is closely linked to IT governance as a core objective for IT governance is to ensure the protection of critical information assets (Calder and Watkins 2008). Investments in IT governance control objectives pay off by providing value by harmonizing decisions about the management and use of IT with desired business objectives (Van Grembergen and De Haes 2008) (Weill and Ross 2004) (Simonsson, Johnson and Ekstedt 2010). As the close link between IT governance and information security exists, it is reasonable to believe that investments in IT governance also are beneficial for an organizations information security. A problem is, however, that benefits to the organization are often indirectly related to the investment and may occur well into the future. It may therefore be difficult for managers in an organization to demonstrate the expected future value of investing in IT governance control objectives. And to effectively direct investments endeavours, a crucial question is if there exist any differences in how effective these investments are in generating value. The need for decision support regarding investment opportunities in security is therefore needed.

In this article we have investigated the value in terms of reduced negative consequences from security incidents generated from investments in IT governance control objectives (time, people or money etc.).

To answer this question we have surveyed IT professionals in the security, governance and/or assurance domain and asked them on their opinion regarding the value of investments in IT

Reference this paper as: Flores, W, R, Sommestad, T, Holm, H and Ekstedt, M. "Assessing Future Value of Investments in Security-Related IT Governance Control Objectives – Surveying IT Professionals" *The Electronic Journal Information Systems Evaluation* Volume 14 Issue 2 2011, (pp216-227), available online at www.ejise.com

governance control objectives. The Net Present Value (NPV) technique was used in order to assess the IT professional's relative opinion on the value these investments is expected to provide.

The structure of the paper is outlined as follows. Section 2 presents some related work to motivate our contribution in respect to previous research. In section 3 the control objectives from COBIT Security Baseline. The same section introduces the Net Present Value technique and discuses why it was the appropriate choice of evaluation technique in regards to the purpose of the study. Section 4 presents the methodology used in the study. Section 5 presents and analyses the results. Section 6 discusses the results and finally, section 7 concludes the paper.

2. Related works

In the IT governance field there exists several studies concerning the impact of different governance components functioning as enablers or inhibitors on IT success and external quality experienced by the business. In the following these are outlined.

(Simonson, Johnson and Ekstedt 2010) have performed a study regarding the correlation between internal ITG process maturity defined by COBIT, and external quality of delivered IT services experienced by the business. By collecting data from case studies in 35 European organizations and analysing statistical correlations of the dataset, internal processes such as: definition of the organization and quality management were identified to have the strongest correlation to external quality. Furthermore, processes, such as problem management, showed no correlation. In addition, (Debreceny and Gray 2009) assessed the IT governance maturity of organizations with respect to predefined IT governance maturity attributes.

Five hypotheses, regarding the potential relationship between different ITG inhibitors (Lack of communication, Inadequate stakeholder involvement, Lack of clear ITG principles and policies, Lack of clear ITG processes and Inadequate support of financial resources) and the negative effect on ITG success of Korean firms were empirically investigated in (Lee, et al. 2008). By using multiple regression analysis, it was shown that all five inhibitors negatively affected IT success of the firms.

The purpose in (Syaful and Green 2009) was to examine what ITG mechanisms (e.g. IT steering committee and IT organizational structure) generate more effective overall ITG, in the most cost-efficient way. In addition, a sub question was to empirically examine the relationship between effective ITG and the level of IT outsourcing decisions. To answer these questions, 176 members of the Information Systems Audit and Control Association (ISACA) in Australia were surveyed. By analysing the proposed hypotheses, the authors concluded that mechanisms such as the existence of ethic or culture compliance in IT, corporate communication systems and involvement of senior management in IT correlates with effective ITG.

(Prasad, Heales and Green 2010) used a capabilities-based approach to obtain a deeper understanding of ITG effectiveness. An integrative model was developed to investigate if IT steering committee affect the internal process performance, trough IT-related capabilities, which in turns affect customer service process performance and firm-level performance. The model was tested empirically by a field survey. The results revealed that executive management driven IT governance initiatives exhibit higher levels of IT-related capabilities. Further, the authors also found that higher levels of IT-related capabilities demonstrate improvement in internal process-level performance. This improvement in internal process-level performance influenced improvement in customer service, and overall improvement in firm-level performance.

The link between IT governance and information security has been elevated in (Calder and Watkins 2008). The use of the information security management standard ISO 27000, as an IT governance framework was proposed by the authors, and the authors further discussed the relevance of the standard as a framework for fulfilling general objectives with IT governance. In COBIT (ISACA 2007a) the same line of reasoning can be found. COBIT describes the processes that are primarily and secondarily related to information security in its appendices.

This study examines how control objectives associated with IT governance support information security and generate future value in terms of reducing negative consequences from security incidents. There are several studies that assess the importance of different security goals, for instance (Bartolini and Sallé 2004) (Su, Bolzoni and Eck 2007) (Neubauer, Klemen and Biffl 2005). These

authors have assessed the priority or impact of security objectives on information security. This article, however, assess the impact of investment in IT governance objectives on security.

The impact of objectives related to security can be assessed in a number of ways. Economic methods are often used to evaluate different security strategies. For example, (Gordon and Loes 2002) (Mercuri 2003) (Sonnenreich, Albanese and Stout 2006) have described methods where economic variables were used to evaluate security alternatives regarding the cost of investments and the value they provide. Security per se does not provide business value. The benefit of security investments are instead assessed in terms of the reduced cost from security incidents. Therefore, economic techniques such as the NPV or return on investment (relabeled as return on security investment) have been suggested by (Gordon and Loes 2002) (Sonnenreich, Albanese and Stout 2006).

In the present paper, NPV technique is used to empirically assess the relative value investments in 19 IT governance control objectives are expected to provide. To the authors knowledge this has not yet been presented in the academic literature.

3. Theoretical foundation

This section describes the best-practice guideline that served as a basis for the survey and Net Present Value that served as the evaluation technique used to evaluate generated future value of investment in control objectives.

3.1 COBIT security baseline

Control Objectives for Information and related Technology Standards (COBIT) is currently the most well-established best-practice IT governance guideline and covers all relevant parts of corporate governance and management of information technology. It outlines 34 IT processes, their purpose and the controls that should be used to govern them (ISACA 2007a)(Debreceny and Gray 2009) (Simonsson, Johnson and Ekstedt 2010). A core part of COBIT concerns information security and the 19 most essential IT governance control objectives toward better information security has therefore been extracted from COBIT and presented in COBIT Security Baseline (ISACA 2007b). In this paper COBIT security baseline (ISACA 2007b) was used as the basis for developing the survey used for collecting data.

COBIT security baseline describes 19 security-related control objectives that are cross-referenced to related COBIT processes and related control sections in ISO/IEC 27002:2005 (ISO/IEC 2005). The control objectives are grouped into four domains: Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME) (c.f. Figure 1). The domains map to IT´s traditional responsibility areas of plan, build, run and monitor. Within the COBIT framework, these domains, as shown in Figure 1, cover the following:

- *Plan and Organize* (PO): This domain provides direction to solution delivery and service delivery. It covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives.
- *Acquire and Implement* (AI): This domain provides the solutions and passes them to be turned into services. To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives.
- *Deliver and Support* (DS): This domain receives the solutions and makes them usable for end users. It is also concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and operational facilities. All IT processes need to be regularly assessed over time for their quality and compliance with control requirements.
- *Monitor and Evaluate* (ME): This domain serves the purpose of monitoring all processes to ensure that the direction provided is followed. Further, the domain addresses performance management, monitoring of internal control, regulatory compliance and governance.

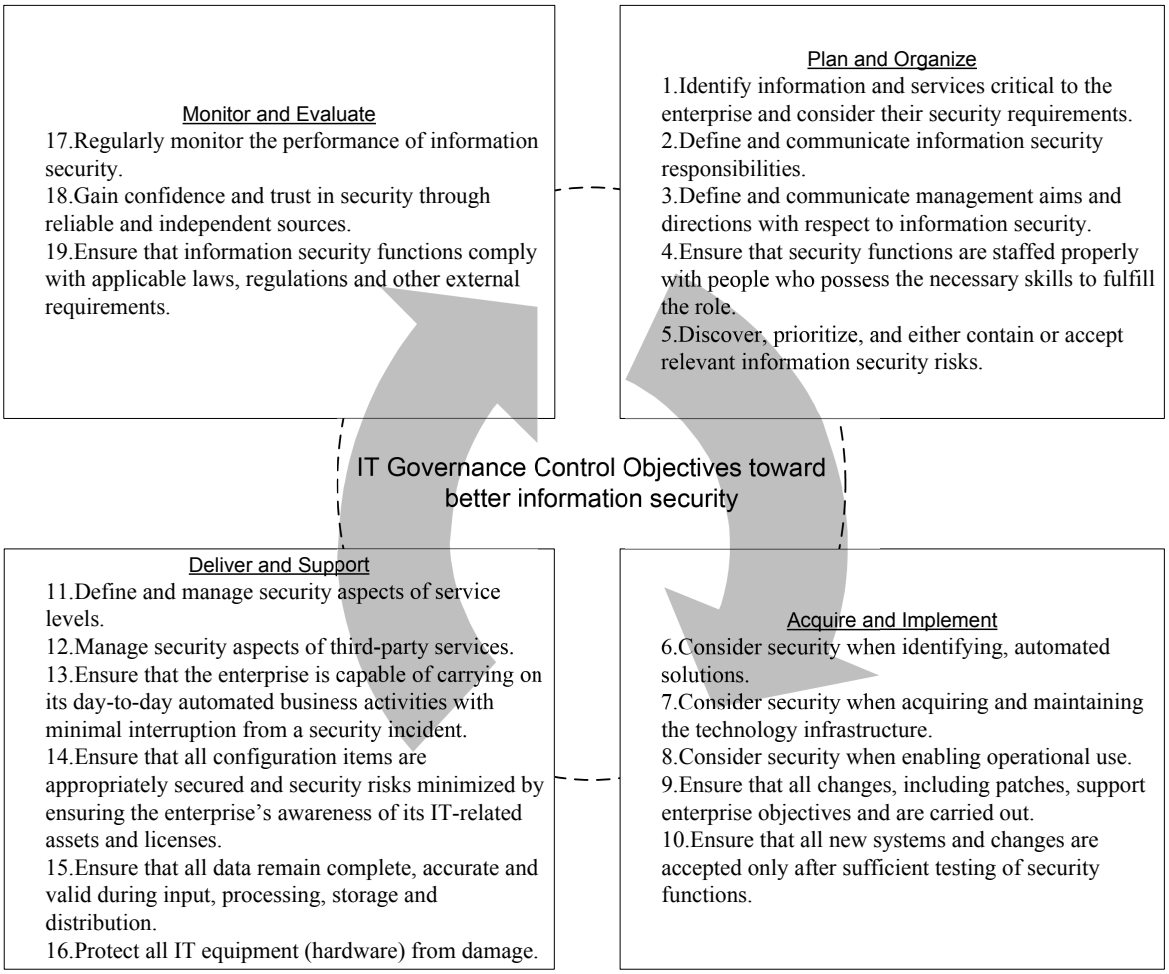

Figure 1: IT governance control objectives drawn from COBIT security baseline

3.2 Net Present Value

The Net Present Value method was used to assess the generated future value of the 19 control objectives. In this section this evaluation method will be described, and the reason for why it was an appropriate choice of method in regards to the purpose of the study will also be argued.

The ultimate goal for an enterprise with an investment is to create value for their shareholders. Value for an enterprise's shareholders is created by making beneficial *real* investment decisions. The meaning of *real* investments is expenditures that generate cash in the future and, as opposed to financial investments, like stocks and bonds, are not financial instruments that are traded in the financial markets (Grinblatt and Titman 1998). Applied to our case a good real investment opportunity is an investment (in time and resources etc.) in a control objective that generates future value in terms of reduced impacts from security incidents. The shareholder in our case is the business, which is the recipient of the information services

To aid a decision maker (in general on an executive level) in determining whether an investment creates value for the shareholder, a manager responsible for information security need to argue and communicate the rational with the choice of the investment alternative in a an effective and understandable way for the decision maker (Johnson 2006). By focusing on communicating security issues concerning business issues and providing related business benefits, risks and benchmarks the importance of a security investment can be heightened. The financial metric Net Present Value (NPV) has shown to improve the effectiveness of the communication and can therefore be used to evaluate different security investment alternatives so that the most beneficial investment alternative can be identified and communicated in an understandable way for the decision maker (Theo, Renkemaa and Berghoutb 1997). The use of NPV as an evaluation tool for security investments at the proposal stage has also been suggested by (Gordon and Loes 2002).

The starting point in the NPV method is the cost of capital for an investment, otherwise known as the required return. The cost of capital is the amount that an investor requires to compensate her for the time value of money tied up in the investment and for taking on risk in the investment. Thus, it represents the costs for her to take on the investment alternative and it is the minimum return that investors expect for providing capital to an investment, thus setting a benchmark that an investment has to meet. For an investment to add future value, it must earn more than the cost of capital. When calculating the NPV for an investment the following formula is used:

$$NPV = \sum_{t=0}^{\infty} \frac{R_t}{(1+i)^t} \quad (1)$$

The cost of capital rate (i) is used as the discount rate. This is the rate of return that could be earned on an alternative investment with similar risk. R_t is the net cash flow, i.e. the amount of cash, inflow minus outflow, at time t. To calculate the NPV for an investment each cash inflow/outflow associated with it is discounted back to its present value. The NPV is the sum of all present values from the time series of cash flows. If the NPV is larger than zero it is beneficial to make the investment and the investment is therefore a good *real* investment opportunity. If NPV is less than zero it will not add value and thus be a less attractive investment opportunity. Applied to our case a an attractive investment opportunity is an investment in security that generates future value in terms of reduced impacts from security incidents and provides value to the shareholder. To estimate the value of investments in control objectives the NPV of all 19 control objectives was assessed by surveying IT professionals.

4. Method

This study utilizes a survey as a measurement tool, this due to the obvious strengths in terms of statistical analysis and cost efficiency. The aim of the study is not to reach in-depth information regarding each of the 19 control objectives; it is simply to gain an understanding of the relative impact of control objectives on information security and can thus be categorized as an exploratory study.

4.1 Population and sample

When constructing a survey it is important to specify a population with favorable attributes and choose a representative sample from that population (Saunders, Lewis and Thornhill 2009). A natural prerequisite for respondents is that they can relate to the questions of the survey (Blair 2005). In this case it meant a population of experienced professionals in the IT security, governance and/or assurance domain.

A strategic sample consisting of a conference with approximately 100 participants satisfying the population constraints was used. Of this population 22 answered the survey. 15 respondents were professionals in IT Security, 9 were professionals in IT Assurance and 11 were professionals in IT governance. The most common combination was IT Security and IT governance. Four respondents came from the banking industry, six from the energy industry, three from the public administration sector, two from the telecommunication sector, two from transport logistics and one consultant. One respondent did not specify his or her sector.

The majority of the respondents were CISA (Certified Information System Auditor) and/or CISM (Certified Information Security Manager); twelve respondents were CISA, six CISM and three CGEIT (Certified in the Governance of Enterprise IT). Only four respondents did not hold any certification. Thus, the respondents originate from many different branches and a diverse number of roles. Although slightly diminutive this sample is considered representative of the population.

4.2 The survey

A face-to-face survey was carried out since all respondents were at the same geographical location (Blair 2005). The survey consisted of two pages of which the first according to recommendation by (Blair 2005) introduces the concepts of COBIT Security baseline, NPV, and a description of how to answer the questions. Furthermore, the first page also includes three questions used to assess background information of respondents. The first question concerned the domain the IT professional work in, the second if the respondent holds any certification and the third in which industry the IT

professionals are active in. The second page of the survey consisted of 19 questions utilized in order to gain information regarding the significance of the IT governance control objectives in the COBIT security baseline. All of the 19 questions included in the survey were taken directly from COBIT security baseline without any manipulation.

For each of the 19 control objectives the respondents were asked to indicate the size of the corresponding NPV on a scale. In figure 2, the 5 questions belonging to the *Plan and Organize* domain are presented to provide information of the question format. The questions were answered using ratio scale, with 0 NPV in the middle, positive NPV to the right and negative NPV to the left. The results were interpreted using a ruler with a millimeter scale, rounded to the nearest complete mm. The outcome was then rescaled to the interval [-5,+5] in order to generate more pedagogical results.

Please estimate how investments in each of the areas below would add additional value (NPV) to an organization in the industry you work in.

4. **Control objectives (investment opportunities)**	**Yields the following NPV** (Negative | Positive)
4.1. Identify information and services critical to the enterprise and consider their security requirements.	NPV=0
4.2. Define and communicate information security responsibilities.	NPV=0
4.3. Define and communicate management aims and directions with respect to information security.	NPV=0
4.4. Ensure that security functions are staffed properly with people who possess the necessary skills to fulfill the role.	NPV=0
4.5. Discover, prioritize, and either contain or accept relevant information security risks.	NPV=0

Figure 2: Question format

4.3 Analysis methods

Three tools were utilized to analyze the results of the survey: box plots, tests for normality and statistical measurements. *Box plots* (sometimes referred to as "box and whisker plots") were first used to evaluate the results. Box plots were chosen to be used due to the favorable non-parametric distribution requirement by the tool. The box plot provides a graphical representation of a dataset according to percentiles. The bottom of a box (the lower quartile, Q1) is the 25th percentile and the top of the box (the upper quartile, Q3) is the 75th percentile. The band in the box represents the median (50th percentile). Data in the 1st-24th percentile and the 76th-100th percentile are represented by whiskers and/or dots (outliers). More information regarding box plots can be found in (McGill, Tukey och Larsen 1978).

Tests for normality were performed using QQ-plots (Warner 2008). Outliers who did not meet the normality assumption were removed according to the recommendation by (Montgomery 2005) in order to improve the overall data quality. The evaluation of the data set with box plots gave an understanding of the data before manipulation; therefore test for normality was performed after analyzing the box plots. *Standard statistical measurements* such as mean, standard deviation and confidence intervals were finally used to present the survey results. Descriptions of these measures can be found in (Montgomery 2005).

5. Results and analysis

A control objective with a positive NPV should be interpreted as a control objective that adds value and is beneficial to invest in. If the NPV is less than zero it will not add value and is therefore not an attractive investment opportunity. Further, the control objective with highest NPV will be the most attractive investment opportunity when compared to other investments in control objectives with similar risk. Figure 3 shows a box plot over the 19 control objectives and table 1 describes their mean, standard deviation and confidence intervals. The results from the survey indicate that the vast majority of security investments have a positive net present value, and are thus beneficial for an organization

to invest in. The mean of all NPVs but one is positive. A 95 percent confidence interval over the mean values of respondent assessments indicate that the true mean (the mean of the population) lies between the upper (UB) and lower (LB) in the 95 % of the cases. In the remaining part of this section, the results will be discussed on a domain-level and thereafter each domain will be discussed.

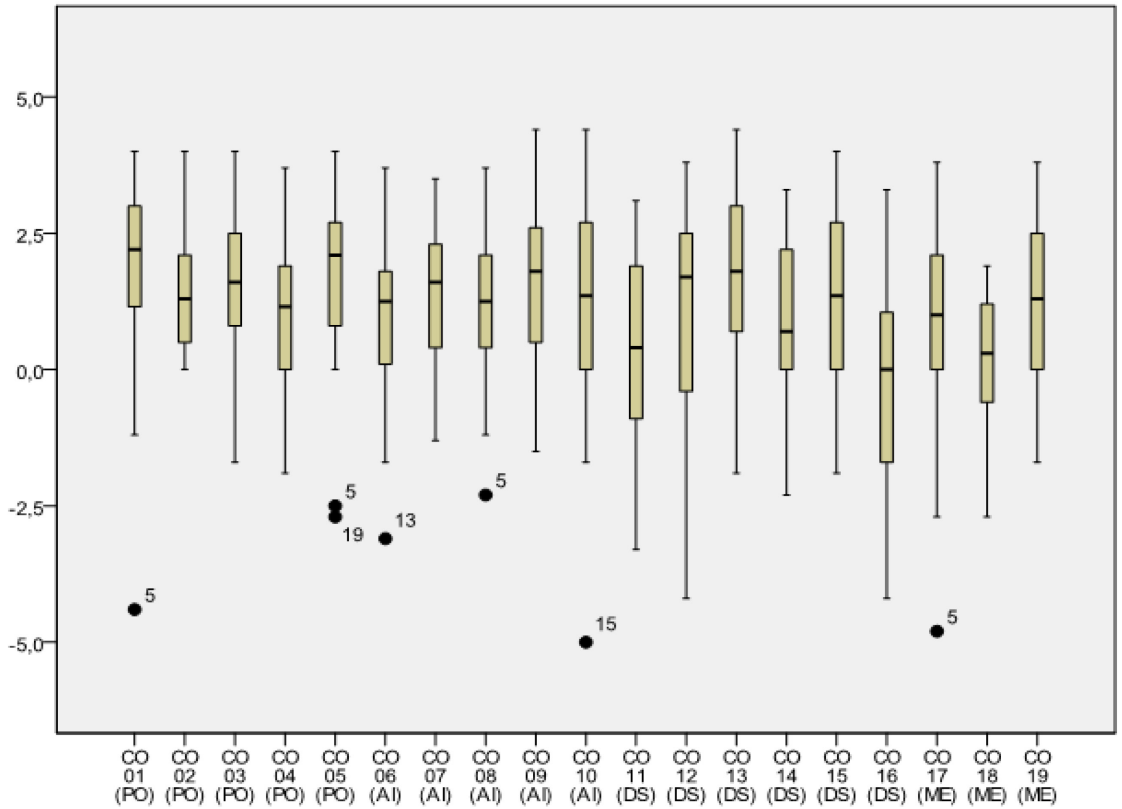

Figure 3: Assessments of control objectives investment potential

Table 1: Control objectives ranking

Objective	Mean	Std dev	LB (95%)	UB (95%)
CO1	2.0	1.4	1.4	2.6
CO2	1.5	1.3	1.0	2.1
CO3	1.7	1.5	1.1	2.3
CO4	1.1	1.5	0.5	1.7
CO5	2.0	1.1	1.5	2.5
CO6	1.2	1.3	0.6	1.7
CO7	1.3	1.3	0.8	1.9
CO8	1.3	1.2	0.8	1.9
CO9	1.6	1.5	1.0	2.3
CO10	1.5	1.6	0.8	2.2
CO11	0.5	1.8	-0.3	1.2
CO12	1.0	2.2	0.0	1.9
CO13	1.6	1.8	0.8	2.4
CO14	0.8	1.6	0.1	1.5
CO15	1.3	1.7	0.5	2.0
CO16	-0.2	1.9	-1.0	0.7
CO17	0.9	1.7	0.1	1.6
CO18	0.1	1.2	-0.4	0.6
CO19	1.3	1.5	0.6	1.9
Mean	1.2	1.5	0.5	1.9

5.1 Domains

A box plot of the results aggregated to the domain level can be seen in Figure 4. Plan and organize (PO, CO1-CO5) have the highest median, followed by acquire and implement (AI, CO6-CO10). Deliver and support (DS, CO11-CO16) and monitor and evaluate (ME, CO17-CO19) have relatively similar medians and ranges, although DS have a higher degree of spread of data. Table 2 shows the mean of the domain experts' assessments of NPV for control objectives within each domain. As can be seen here the highest mean is associated to the domain *Plan and organize* and the lowest is associated with *Deliver and Support* and *Monitor and evaluate*. Also, the mean of the NPV is positive for all four domains.

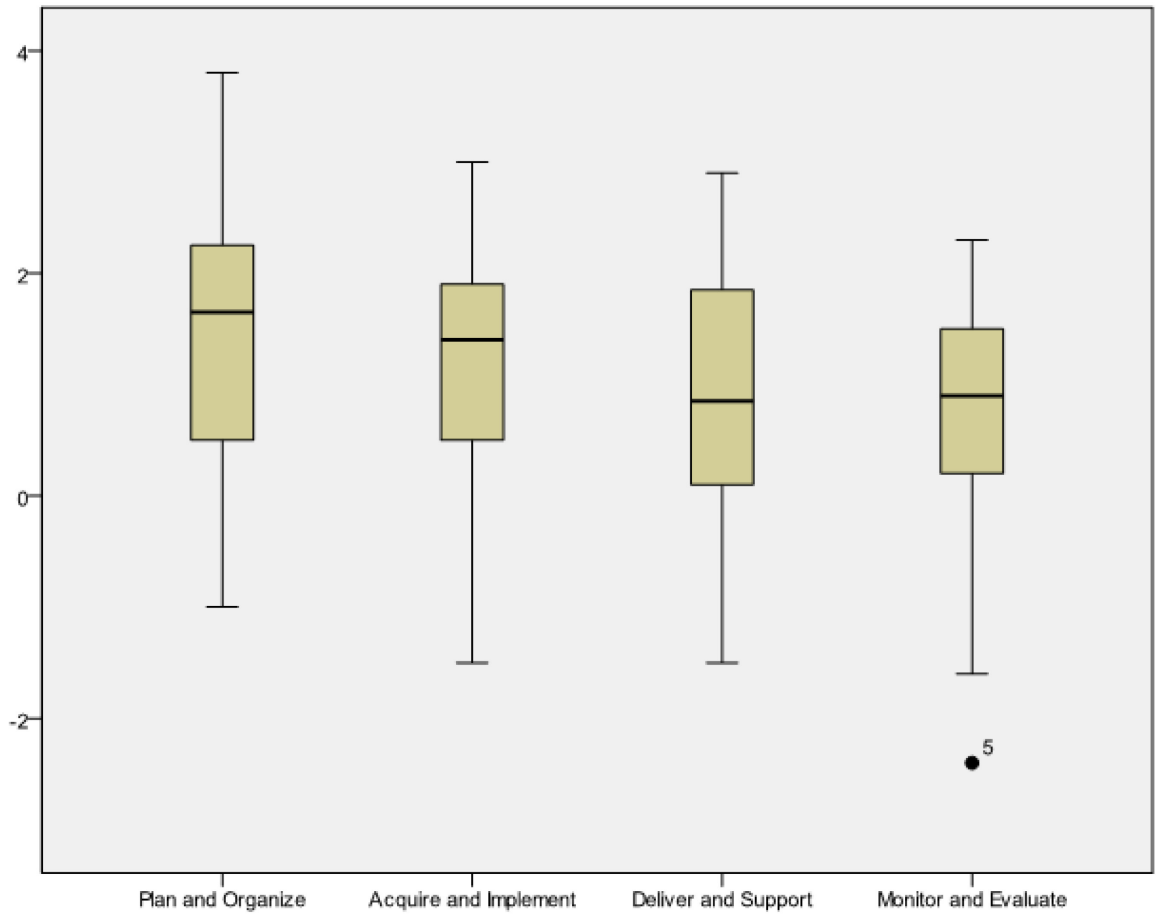

Figure 4: Box plots per domain

Table 2: Control domains mean and spread

Domain	Mean	Std dev	LB (95%)	UB (95%)
PO	1.6	1.1	1.2	2.1
AI	1.3	1.1	0.8	1.8
DS	0.8	1.3	0.3	1.4
ME	0.8	1.0	0.3	1.2

5.1.1 Plan and organize

As can be seen in the box plot in Figure 3, investments in all control objectives in this domain are presumed to yield relatively high NPVs. QQ-plots indicate that the outliers need to be removed in order to satisfy the assumption of normality. The variables with the highest median, smallest box and lowest range is CO1 ("Identify information and services critical to the enterprise and consider their security requirements") and CO5 ("Discover, prioritize, and either contain or accept relevant information security risks").

5.1.2 Acquire and implement

Investments in control objectives within this domain are generally believed to render a positive NPV. The two control objectives with highest means are CO9 (“Ensure that all changes, including patches, support enterprise objectives and are carried out”) and CO10 (“Ensure that all new systems and changes are accepted only after sufficient testing of security functions”) .The boxes in this domain are approximately the same size, with the exception of which is slightly larger than the rest. CO10 does however have a strong outlier on the negative side which increases its standard deviation (cf. figure 3 and table 1).

5.1.3 Deliver and support

There is some variation between the expected NPV of investments in this domain. For instance, the mean NPV associated with CO16 (“Protect all IT equipment from damage”) is negative, but CO13 (“Ensure that the enterprise is capable of carrying on its day-to-day automated business activities with minimal interruption from a security incident”) has the fourth largest mean NPV. Compared to the other domain there seems to be a higher disagreement among respondents on the NPV associated with investments in this domain. The assessments of NPV associated with CO12 (“Manage security aspects of third-party services”) is for example spread between highest return assessed to well below zero.

5.1.4 Monitor and evaluate

The monitor and evaluate domain consist of three control objectives. Their mean values are associated with a comparably low NPV. For instance is CO18 (“Gain confidence and trust in security through reliable and independent sources“) assessed to yield a NPV close to zero. Also within this domain is the spread of assessments comparably high. A 95 percent confidence interval over the respondents’ assessments does for example stretch between 0.1 and 1.6 for CO17 (“Regularly monitor the performance of information security”).

6. Discussion

The result from this survey is intended to reflect the opinion from a number of professionals within the IT security, governance and/or assurance domain. The reliability and validity of the instrument used to measure their opinion is described in section 6.2. The section below will discuss the results of this measurement.

6.1 Value of investments in control objectives

This paper has provided empirical data from a panel of IT professionals regarding the value in terms of reduced negative consequences from security incidents generated from investments in IT governance control objectives (time, people or money etc.). 16 out of 19 control objectives are associated with a 95 percent confidence interval that only span over the positive side of the scale. This indicates that the panel agrees that investments in IT governance control objectives strengthen security objectives and are therefore beneficial. This is a finding that can be useful for a practitioner as it may be difficult to demonstrate the expected NPV of investing in control objectives since the benefits to the firm are often indirectly related to the investment and may occur well into the future.

When it comes to individual control objectives the results gives some indications that C05 (“Discover, prioritize, and either contain or accept relevant information security risks”) and CO1 (“Identify information and services critical to the enterprise and consider their security requirements”) are beneficial to engage in. The less beneficial control objectives are CO16 (“Protect all IT equipment from damage.”) and CO18 (“Gain confidence and trust in security through reliable and independent sources”). The respondents’ answers regarding individual control objectives vary, the box plot in Figure 3 and the 95 percent confidence interval in Table 1 indicate this. However, the variations are small. Four explanations for these small variations are possible:

- Positive lopsidedness
- Respondent experience
- Existence of internal correlation
- The domain is understudied

These are now further discussed.

Positive lopsidedness: The mean of the respondents assessments result in a positive NPV for all control objectives but one. This reflects a general belief among respondents in the benefit associated with investments on control objectives associated with security. As earlier described the respondents are individuals which have a vested interest in IT /security governance and practice such activities on a daily basis. With this as a basis the positive lopsidedness in NPVs could be attributed to an expected bias in the respondent's judgment. While the positive lopsidedness could be an effect of the IT professionals biased opinions it could also reflect the situation in enterprises today. The software security market has grown in recent years (Gartner 2009) (Gartner 2010) and forecasts of the security market such as (DefenseNews 2010) predict an increase in coming years. Such data indicate that many organizations do see a benefit in investments that strengthen security objectives.

Respondent experience: The IT professionals responding to the survey have different backgrounds and experiences. Some variation among their opinions can therefore be expected. The assessments made of NPV potentials were also made for organizations in the industry where the respondent is a professional. Some variation can thus be explained by differences among industries. For example, the regulations that apply to organizations vary with industry. A regulation might require certain investments to be made and in that way influence the NPV that can be obtained from future investments associated with a control objective.

Existence of internal correlation: It is reasonable to believe that there exists internal correlation between the control objectives. Therefore, an investment in a single control objective cannot yield significantly higher NPV than investments of combination of control objectives. The respondents have not taken this fact into account as the survey didn't ask for investments in combinations of control objectives explicitly.

The domain is understudied: The results can also be explained by the fact that the domain is understudied and therefore a lack of understanding among professionals of the structure and the dependencies between different security components (e.g. control objectives) exists. From a decision-makers point of view it is difficult to prioritize different security alternatives and identify the cause and effect of a investment decision before the decision is taken and implemented. In order to increase the understanding of the dependencies between different security components, but also to perform various kinds of analysis, before a decision is taken, architectural models can be employed. In (Rocha Flores and Ekstedt 2011) a method for analyzing information security components and also enabling inference between these security components is proposed. Such decision support tools can improve the understanding of the dependencies between control objectives and might be useful for future research in the domain.

Regardless of the reason for why there is a deviation among respondents the variation in their answers indicates how much agreement that exist among them on the general case. The variation in respondents answers vary over questions. The box plot in Figure 3 and the 95 percent confidence interval in Table 1 indicate this. As can be seen from these there is a substantial spread in the respondents assessments. On the other hand most control objectives (16 out of 19) are associated with a 95 percent confidence interval that only span over the positive side of the scale. This indicates that the IT professionals agree that investments in IT governance control objectives are beneficial. Based on the spread in this data it appears as the accuracy of domain experts assessments of investment opportunities in the IT governance domain is associated with a significant uncertainty. Future work could investigate the reasons for the spread among the domain experts' rankings of such investment opportunities.

6.2 Instrument validity

This section first address the instrument's validity in terms of: *content-, construct-, external-* and *internal validity* (Boudreau, Gefen and Straub 2001) (Brewer 2000).

Content validity is the degree to which items in an instrument reflect the content universe to which the instrument will be generalized (Boudreau, Gefen and Straub 2001). E.g., if this study aimed to draw conclusions on profitability of the COBIT security baseline using only results from control objectives 1-4 the content validity would be low. Normal methods of measuring content validity are through literature review and expert panels/judges (Boudreau, Gefen and Straub 2001). All control objectives

of the COBIT security baseline are included in the survey. Furthermore, all survey questions are taken directly from the framework without any manipulation. However, while the baseline concepts are thoroughly covered there might be slight problems with the prioritization technique employed (NPV). The NPV of a potential investment is a commonly used indicator on how lucrative investments are for an organization, but when making investment decisions other factors could also be considered. In particular, the risk of the investment and the opportunity costs associated with it could be of essence. These factors are only implicitly measured in this survey and one should therefore be somewhat careful when interpreting the relative ranking associated with different investments. Finally, the survey was studied by two academic experts in the area who assessed the tools content validity as high.

Construct validity is the extent to which an operationalization measures the concepts that it purports to measure (Boudreau, Gefen and Straub 2001), i.e. whether the survey measures the benefit of investing in different control objectives and domains. First of all, neither the COBIT security baseline nor prioritizations of its elements are abstract in such a manner that could cause significant problems with the construct validity. Second, the baseline and prioritization potency of NPV are generally thought of as highly valid theory. Finally, the tool was tested (and discussed) by two academic experts and one respondent which were thought to be representative of the specified population. These pilot studies both hinted toward high construct validity.

Another important validation concept is *external validity*; the degree to which the results of a study can be generalized [30]. This study is on one hand built upon a sanctioned theoretical framework and a to some extent representative sample. However, it is to the authors' knowledge also the first study performed relating to the COBIT security baseline and NPV; therefore it is not possible to compare the results of this study to the results of previous research. Also, the sample is too small to draw any certain general conclusions.

An additional well regarded attribute of validity is *internal validity* (Brewer 2000). However, since no evaluation of causal relationships was made in this study, internal validity is not applicable here.

7. Conclusion

Optimizing investments in information security is a complex task. The study presented in this article has tried to somewhat make the investment decision more rational by investigating the value in terms of reduced negative consequences from security incidents generated from investments in IT governance control objectives (time, people or money etc.). The paper uses the NPV method as the evaluation technique to assess the future value of these investments. By surveying IT professionals in the security, governance and/or assurance domain regarding the NPV that could be obtained from these investments study found that investments in control objectives are beneficial for a firm to engage in.

The paper has therefore provided data that supports the theory that investments in IT governance also are beneficial for the information security in an organization. The paper has further shown that the NPV method can be used to assess value of investments in the security and governance domain.

The mean NPV vary between the control objectives, and there are some indications of control objectives that provide more value than others. However, as it is reasonable to believe that there exists internal correlation between the control objectives, interesting future work includes therefore more research into the internal correlation between the control objectives and also the impact of prioritization between control objectives. Research could investigate if the provided benefit for a firm depends on proper prioritization and/or investment of a combination of control objectives, and if so, identify which control objective/objectives that should be prioritized or combined for achieving as much value as possible from an security investment decision.

References

Bartolini, C, and M Sallé. "Business Driven Prioritization of Service Incidents." *DSOM, LNCS 3248.* 2004. 64-75.

Blair, Czaja R. *Designing surveys.* Sage Publications Inc, 2005.

Boudreau, Marie-Claude, David Gefen, and Detmar W Straub. "Validation in Information Systems Research: A State-of-the-Art Assessment." *MIS Quarterly* 25, no. 1 (2001): 1-16.

Brewer, Marilynn B. "Research Design and Issues of Validity." In *Handbook of research methods in social and personality psychology*, by Harry T Reis and Charles M Judd, 3-17. Cambridge: Cambridge University Press, 2000.

Calder, A, and S Watkins. *IT governance A manager´s guide to Data Security and ISO 27001/ISO 27002.* Kogan Page, 2008.
Cronobach, L J. "Coefficient alpha and the internal structure of tests." *Psychometrika,* ([14] L.J. Cronbach, "Coefficient alpha and the internal structure of tests," Psychometrika, vol. 16, 1951, pp. 297-334.) 16 (1951): 297-334.
Debreceny, R, and G.L Gray. "IT Governance and Process Maturity: a Field Study." *In Proceedings of the 42nd Hawaii International Conference on System Sciences.* 2009.
DefenseNews. *IT Security Market Heats Up - Demand Growing for Guidance on Cyber Protection.* DefenseNews, 2010.
Gartner. *Gartner says worldwide security software market on pace to grow 8 per cent in 2009.* Gartner, 2010.
Gartner. *Gartner says worldwide security software revenue grew 18.6 per cent in 2008.* Gartner, 2009.
Gordon, L.A, and M.P Loes. "The Economics of Information Security Investment." *ACM Transactions on Information and System Security Vol. 5, No. 4*, 2002: 438–457.
Grinblatt, M, and S Titman. *Financial Markets and Corporate Strategy.* McGraw-Hill International Edition, 1998.
Hardy, G. "Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges." *information security technical report*, 2006: 55-61.
ISACA. *COBIT Security Baseline: An Information Security Survival Kit 2nd edition.* ISACA, 2007b.
ISACA. *Control Objective for Information and Related Technology Standards.* ISACA, 2007a.
ISO/IEC. "Code of Practice for Information Security management, ISO/IEC 27002:2005." Switzerland, 2005.
Johnson, E.C. "Security awareness: switch to a better program." *Network Security*, 2006: 15-18 .
Lee, Chi-Hoon, Jung-Hoon Lee, Jong-Sung Park, and Kap-Young Jeong. "A Study of the Casual Relationship between IT Governance Inhibitors and Its Success in Korea Enterprises*" In Proceedings of the 41st Hawaii International Conference on System Science*. 2008.
McGill, Robert, John W Tukey, and Wayne A Larsen. "Variations of Box Plots." *The American Statistician* 32, no. 1 (1978): 12-16.
Mercuri, R.T. "Analyzing Security Costs." *Communications of the ACM Vol. 46, No. 6*, 2003: 15-18.
Montgomery, Douglas C. *Introduction to Statistical Quality Control.* Vol. 5. New Jersey: John Wiley & Sons, Inc., 2005.
Neubauer, T, M Klemen, and S Biffl. "Business Process-based Valuation of IT security." *EDSER.* St. Louis, Missouri, USA, 2005.
Prasad, Acklesh, Heales, John, and Green, Peter. "A capabilities-based approach to obtaining a deeper understanding of information technology governance effectiveness: Evidence from IT steering committees." *International Journal of Accounting Information Systems* 11, 2010: 214-232.
Rocha Flores, and Ekstedt, Mathias. "Information Security Governance Analysis Using Probabilistic Relational Models". *In Proceedings of 8th International Workshop on Security in Information Systems*. 2011
Saunders, Mark, Philip Lewis, and Adrian Thornhill. *Research Methods for Business Students.* Edinburgh: Pearson Education Limited, 2009.
Simonsson, M, P Johnson, and M Ekstedt. "The effect of IT Governance Maturity on IT Governance Performance." *Information Systems Management*, December 2010: 10-24.
Sonnenreich, W, J Albanese, and B Stout. "Return On Security Investment (ROSI) - A practical Quantitative Model." *Journal of Research and practice in Information Technology, Vol. 38, No. 1*, 2006.
Su, X, D Bolzoni, and P.V Eck. "Understanding and Specifying Information Security Needs to support the Delivery of High Quality Security Services." *In Proceedings of the international Conference on Emerging Security Information, Systems and Technologies.* 2007.
Syaful, Ali, and Green, Peter. "Effective information technology (IT) governance mechanisms: An IT outsourcing perspective." *Information Systems Frontiers*, 2009.
Theo, J.W, E.W Renkemaa, and Berghoutb. "Methodologies for information systems investments evaluation at the proposals stage: a comparative review." *Information and Software Technology Vol. 39 No. 1*, 1997: 1-13.
Van Grembergen, W, and S De Haes. *Implementing information technology governance: Models, practices, and cases.* IGI Pub., 2008.
Warner, R. M. *Applied Statistics.* SAGE Publications, 2008.
Weill, P, and J.W Ross. *IT governance: How top performers manage IT decision rights for superior results.* Harvard Business School Press, 2004.
Whitman, M.E. "In defense of the realm: understanding the threats to information security." *International Journal of Information Management*, February 2004: 43-57.
Yin, R K. *Case study research: Design and Methods.* Washington D.C: SAGE Publications, 2003.

