An Empirical Examination of the Relationship Between Information Security/Business Strategic Alignment and Information Security Governance Domain Areas

Winfred Yaokumah
Pentecost University, Ghana

Steven Brown
Capella University, United States

Abstract

The purpose of this study was to examine empirically the extent of the relationships between information security governance (ISG) strategic alignment and other individual information security domain areas consisting of risk management, value delivery, performance measurement, and resource management in order to ascertain whether the domain areas were integrated for ISG success in Ghanaian organizations. Corporate governance theories, including agency theory, stakeholder theory, and organizational theory, were employed to explore the literature. These theories were mapped to strategic alignment, risk management, resource management, performance measurement, and value delivery domains of information security governance. Random sampling strategy was used and data were collected via web survey. The data analysis employed a linear regression analysis to determine the degree of correlation among the domain areas. The study found that relationships between information security governance strategic alignment and other ISG domains were positively statistically significant. Strategic alignment was related to risk management (R^2 = .836); to value delivery (R^2 = .718), to performance measurement (R^2 = .722), and to resource management (R^2 = .747). The results highlighted consistent importance of strategic alignment practices as a predictor of organizational information security risk management, performance measurement, resource management, and value delivery. This implies that effective information security governance strategic alignment greatly improves organizations' risk management, resource management, performance measurement, and delivers business value. Therefore, organizations should improve strategic alignment attributes in order to attain effective information security governance.

Introduction

An important aspect of corporate governance is to ensure that organizational information assets are secured. Information asset can be understood as an item of value that contains information which can be human, technological, software, or other. Keeping information safe and secure is a key necessity for every modern organization and the board of directors and executive management are ultimately accountable for the organization's success (von Solms, 2006). It is therefore imperative that the top

executives take responsibility for the protection of their company's information asset. Research discussed information security extensively but rather few studies addressed information security as corporate governance concern particularly in the developing nations (El-Meligy, 2011).

Corporate governance is a set of processes and structures for controlling and directing an organization (Abdullah and Valentine, 2009). Accordingly, corporate governance constitutes a set of rules which govern the relationships between management, shareholders, and other stakeholders (Ching et al., 2006). Information security governance is regarded as a part of corporate governance function. Information Technology Governance Institute (ITGI, 2006) defined information security governance as "a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security programme" (p. 18), all in an attempt to protect sensitive information from unauthorized access, accidental loss, destruction, disclosure, modification, or misuse (Tassabehji, 2005). Information security governance, thus, involves oversight, policy formulation, accountability, strategic planning, and resource allocation to mitigate risk to critical organization data (Allen, 2006). Therefore, a study on information security governance must be based on the fundamental theories of corporate governance.

Corporate governance theories can have effect on information security governance practices as they address "people (agents), their accountability, their roles, their interactions, their activities, and their use of resources" (Valiris and Glykas, 2004, p. 73). Among these theories are the agency theory, resource-based view (RBV) of the organization theory, and the stakeholder theory. Abdullah and Valentine (2009) suggested that a combination of various theories should be considered when describing good governance rather than theorizing corporate governance based on a single theory. These three theories are relevant in defining the constructs that form information security governance domain areas. Deriving constructs from previously established and proven theories offered a well grounded and comprehensive understanding of the phenomenon and aided the choice of established measures (Moghdeb et al., 2007). Five constructs have been derived from corporate governance theories. These constructs correspond with information security governance domain areas consisting of strategic alignment (SA), value creation (VD), risk management (RK), resource management (RM), and performance measurement (PM) and which were identified by IT governance Institute (ISACA, 2006).

Previous studies suggest that for successful information security governance in organizations, with the aim of mitigating information security risks from the corporate governance level, there should to be positive relationships among SA, VD, RK, RM, and PM (ITGI, 2008; Oppliger, 2007; Wilkin and Chenhall, 2010). According to ITGI (2008), information security value delivery to the organization depends on strategic alignment between information security and business objectives, indicating that organizations can obtain value from security investment when there is an alignment between information security and business goals. Wilkin and Chenhall (2010) explained that business value can be realized with strategic business and IT alignment even without the use of other governance structures and processes. Similarly, Johnston and Hale (2009) and Oppliger (2007) found SA as the cornerstone for RK. Moreover, Prybutok et al. (2008) and Neirotti and Paolucci (2007) identified SA as positively linked to PM. Again, SA is imperative for RM (Wilkin and Chenhall, 2010). However, these studies were based on qualitative examination of the constructs, lacking empirical proof of the relationships between SA and other domain areas.

This study empirically examines the extent of the relationship between information security/business strategic alignment and individual information security domain areas, which are risk management, value delivery, performance measurement, and resource management (De Haes and Van Grembergen, 2009) in organizations. Collecting data from Ghanaian organizations, this study aims at establish the degree of the relationships among the variables with the intent of ascertaining whether the domain areas are appropriately integrated for ISG success. In order to investigate these areas effectively, it is important, first of all, to discuss the different underlying governance theories and to map ISG domain areas to their intellectual origins. In order for organizations to minimize security risks, the study

posits that it is critical to align the security/business strategic objectives with the information security domains.

Literature Review

Corporate governance theories are an appropriate theoretical foundation for studies on information technology and security governance (Bihari, 2008; Posthumus, von Solms, and King, 2010; Wouldson and Pollard, 2009). In conducting organizational research, Eisenhardt (1989) suggested that theory should be used as an initial guide to design and data collection. Also, Walsham (1995) emphasized the importance of creating an initial theoretical framework that takes account of previous knowledge and forms a sensible theoretical basis for an empirical work. Corporate governance theorists analyzed governance structures, processes, practices, and effectiveness from different theoretical perspectives, including agency theory (Fama and Jensen 1983), organization theory (Habbershon and Wouldiams 1999; Carney 2005, Le Breton-Miller and Miller 2006, and stakeholder theory (Freeman, 1984). Notwithstanding, there are other theories (such as stewardship theory) that could be applicable in deriving the constructs for this study, but the three selected theories have significant potential impact on achieving information security governance practices as discussed in the following section.

Figure 1 summarizes how corporate governance theories define the domains of information security governance. In the context of information security governance practices, the three governance theories map to information security governance domain areas. Thus, the agency theory maps to risk management and performance measurement and monitoring, stakeholder theory maps to strategic alignment and value creation, and organizational theory maps to resource management.

Agency Theory: Risk Management and Performance Measurement

The agency theory is based on a fundamental premise that owners (principals) establish a relationship with managers (agents) and delegate work to them (Alchian and Demsetz, 1972). In this theory, the owners or principals, who are the shareholders of the organization, hire the agents to perform tasks, and expect them to act and make decisions in the principal's best interest. It has been observed that the agents do not always make decisions in the best interest of the principal (Padilla, 2002) but rather decisions are made based on self-interest (Jensen and Meckling, 1976).

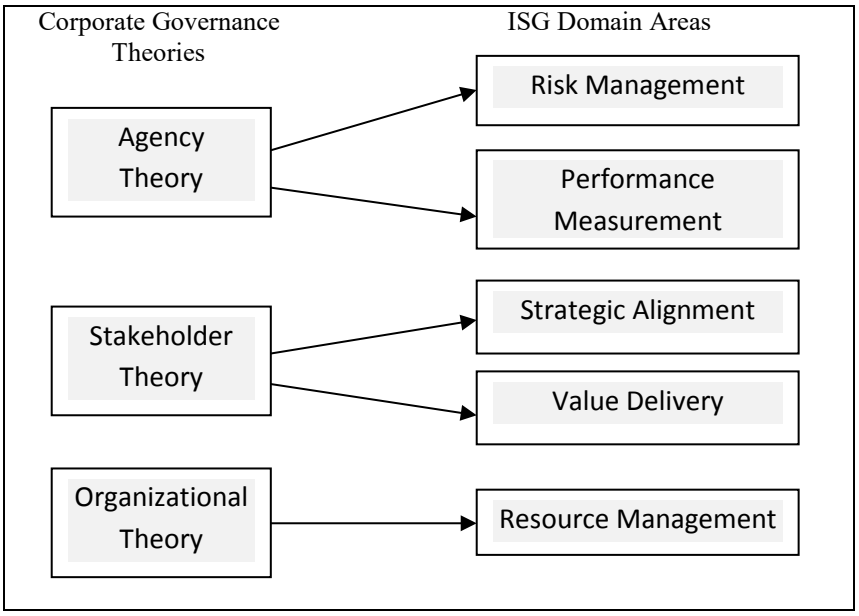

Figure 1: Mapping Corporate Governance Theories to ISG Domain Areas

Note: ISG: information Security Governance

Agency theory has important application in the governance of organizations. Eisenhardt (1989) identified two different uses of agency theory: the positivist and the general approaches. The positivist approach focused mainly on the principal-agent relationship in terms of owners and managers in respect with large and public corporations (Berle, 1932). In this arrangement, the agents are controlled by principal-made rules with the intent to maximize shareholder values (Abdullah and Valentine, 2009). The more general approach is the principal-agent relationship that can be applied to employer-employee, buyer-supplier, and other agency relationships (Harris and Raviv, 1979). The positivist approach applies to organizations where the agents must follow the principal-made rules and guidelines to govern the organizations' information security.

Agency theory has significant implications for information security governance practices. Firstly, the agency theory assumes that the basis of the organization is efficiency (Eisenhardt, 1988, 1989), which is one of the fundamental drivers of good governance. Managers are, therefore, expected to make sure performance through monitoring and measurement within their organizations is efficient (Valiris and Glykas, 2004) and effectively monitored. Performance measurement is said to be in place when the board of directors and executive management ensure that the organization quantifies, monitors, and reports on the performance of security processes in order to ensure that organizational objectives are achieved (ITGI, 2008; Thatcher and Pingry, 2007; Wang and Alam, 2007).

Secondly, Yu and Mylopoulos (1994) proposed three different levels of agency relationship: general, committed, and critical. These levels relate to the degree to which the agents are affected if the job fails. The three levels of agency theory translated into different levels of commitment and responsibilities that establish accountability and control (Valiris and Glykas, 2004), as well as punishments and rewards (Jensen and Meckling, 1976), leading organizations to make conscious efforts to minimize risks (managing risks) associated with organizational information assets. Risk management will be achieved when the boards of directors ensure that risk assessment and mitigation strategies are embedded into the organization's operations to guarantee quick reporting and response to the ever-changing risk challenges (Hardy, 2006). The intent of risk management is to mitigate risks and reduce adverse impacts on information assets to a satisfactory level (Bonabeau, 2007; Hu and Cooke, 2007; ITGI, 2006). Consequently, the ultimate goal of all organizational information security and assurance effort is to manage risk (Ask, Bjornsson, Johansson, Magnusson, and Nilsson, 2007; Gellings, 2007). Therefore, risk management is attained when it is efficiently, effectively, and consistently meeting an organization's security expectations and defined objectives (ITGI, 2008).

Stakeholder Theory: Strategic Alignment and Value Delivery

In relation to the agency theory, Freeman (1984) extended corporate accountability to cover a broad range of stakeholders. Abdullah and Valentine (2009) defined stakeholder theory as "any group or individual who can affect or is affected by the achievement of the organization's objectives" (p. 91). The theory suggested that managers in organizations have a network of relationships to serve (Abdullah and Valentine, 2009), which are the suppliers, investors, customers, political groups, employees, communities, government, and trade associations.

With respect to good corporate governance, the stakeholder theory attempts to address various groups of stakeholders deserving and requiring management's attention (Sundaram and Inkpen, 2004) and all the stakeholders in the business look forward to obtain benefits (Donaldson and Preston, 1995). Clarkson (1995) added that in the stakeholder theory the organization is considered as a system where there are stakeholders and the purpose of the organization is to create wealth (value) for its stakeholders. Therefore, the firm can maximize value if it considers the interests of its stakeholders. Hence, value creation is a focus area of corporate governance practices. On the contrary, Freeman (1984) contended that this complex network of relationships with many stakeholders can affect decision making processes because the stakeholder theory involves not only creating values for the organization and its stakeholders but also involves complex structures and processes.

Notwithstanding, the basic focus of the stakeholder theory is on managerial decision making that advocates that organizations are accountable to all its stakeholders and strive to create value for the stakeholders.

The value information security investments delivers to enterprises is realized when the strategic management ensures that the organization increases the chance of selecting information security investments (a) with the highest potential of creating business value, (b) by increasing the likelihood of successful execution of selected investments, and (c) by reducing the risk of failure, particularly those risks that have high impact on the organization (Val IT, 2009). The board of directors must ensure that information security investments increase business value, reduce unnecessary costs; improve the quantity and quality of services, and enhance the overall level of confidence among the stakeholders (Gregor et al., 2006; Kobelsky et al., 2008). According to Hardy (2006) effective value delivery is achieved when the actual costs and return on security investment are properly managed.

Moreover, the stakeholder theory improves alignment of stakeholders' interest with organizational goals. Moghdeb, Indulska, and Green (2007) noted that aligning key stakeholders' concerns with business objectives can have a positive impact on the results of organizational performance. Governance in this case involves alignment creation through the stakeholders that constitute the structures involved in processes to affect the achievement of the organization's objectives.

Strategic alignment between information security and business strategy is established in an organization when the strategic management ensures that information security strategies are in harmony with business strategies (Hardy, 2006). For strategic alignment to be effective, the business strategy should encompass key information security capabilities, future security requirements, people, and information assets that can be deployed to meet business needs (Bernroider, 2008; Neirotti and Paolucci, 2007; Prybutok et al., 2008; Thomas et al., 2009). Effective strategic alignment, therefore, must be dynamic, shared, and reshaped to meet changing business and security landscapes (Coutaz et al. 2005; Grover and Segars 2005) in order to avoid business failure.

Organizational Theory: Resource Management

Whilst the stakeholder theory focuses on relationships with many groups for individuals and their needs, organizational theory concentrates on effective utilization of organizational resources to meet business objectives. There are other aspects of organizational theory, but the most contribution of organizational theory relevant to information security governance is the resource-based view (RBV). The RBV of the organizational theory concentrates on the role of the board of directors in providing access to essential resources needed by the organization (Hillman, Canella, and Paetzold, 2000). According to Hillman, Canella, and Paetzold (2000), the directors bring resources to the organization in the form of information, skills, and competencies. Organizations are viewed as a pool of human resources, capabilities, and competencies. Hence, the objective of governance is to generate, combine, and activate such resources to attain a competitive advantage. In this respect, governance is considered as the "determination of the broad uses to which organizational resources would be deployed" (Daily, Dalton, and Canella, 2003).

Beside resources, RBV theory focuses on capabilities. Capabilities are accumulated knowledge in organizations resulting from using its existing resources in an efficient and effective way to achieve its ultimate objectives (Idris, Abdullah, Idris, and Hussain, 2003). In this regard, information security governance practices share common standpoints with RBV theory in terms of cost-effectiveness in utilizing organizational capabilities to optimum levels that create competitive advantage (Moghdeb, Indulska, and Green, 2007). The point of reference of organization theory, therefore, is strategic management of resources and competencies to achieve organizational goals. Thus, organizational theory makes resource management, which includes information security resources, a core corporate governance practice in organizations.

Information security resources management can be viewed as the degree to which the board of directors ensures that appropriate resources and adequate skills exist in the organization to manage information security projects and activities (Hardy, 2006). Effective board governance of security resource can result in significant cost saving and, hence, place the organization in the strong position of taking on new and beneficial initiatives (Hardy, 2006) whereas ineffective resource management toward IS implementation can result in substantial business loss (Allen et al., 2008; Silva and Hirschhein, 2007).

Conceptual Model and Research Questions

Prior studies established relationships among information security governance domain areas (Abu-Musa, 2010; ITGI, 2006; Wilkin and Chenhall, 2010). Figure 2 shows conceptual model of the relationships between the individual information security governance domain areas and information security/ business strategic alignment. The relationship between individual ISG domain areas of (a) resource management and strategic alignment, (b) value delivery and strategic alignment, (c) performance measurement and strategic alignment, and (d) risk management and strategic alignment are presented in the model.

The following four research questions were derived from the conceptual model (Figure 2).

RQ1.
What is the extent of the relationship between strategic alignment and risk management?

RQ2.
What is the extent of the relationship between strategic alignment and value delivery?

RQ3.
What is the extent of the relationship between strategic alignment and performance measurement?

RQ4.
What is the extent of the relationship between strategic alignment and resource management?

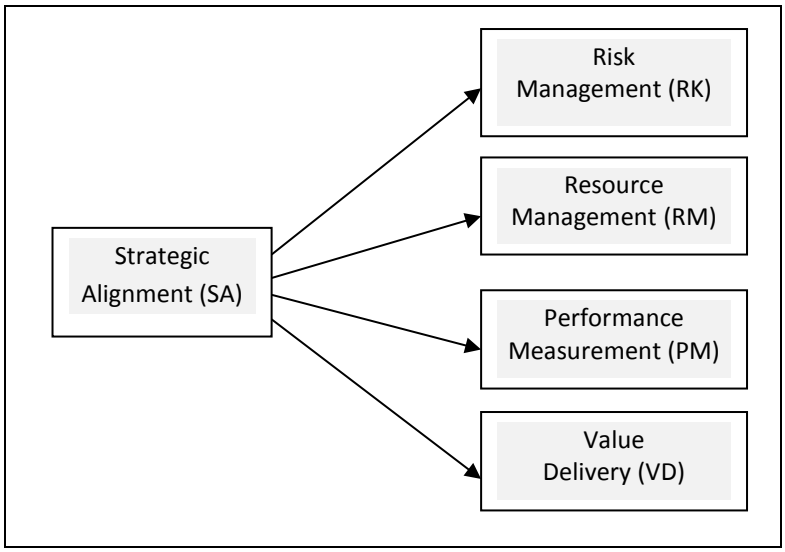

Figure 2. Relationship between SA and other ISG Domain Areas

Methodology

The accessible population of this study was the organizations located within Greater Accra municipal area of Ghana that employed information technology to store, process, or transmit customers' personal identifiable data. One hundred and twelve organizations were identified and grouped according to their respective industry sectors. Specifically, the industry sectors include (a) public services, (b) public utilities, (c) financial institutions, (d) education institutions (both private and public), and (e) healthcare institutions. Other industry sectors that met the criteria for selection were grouped under others (Oil and Gas, IT companies, Manufacturing, etc), making six sectors.

A total of 120 organizations were identified from within the industry sectors and 360 respondents were randomly selected (three from each organization) were invited to take part in the study. Details of the samples include (a) forty-seven (6 public and 41 private) universities (141 participants), (b) thirty licensed banks registered in Ghana (90 participants), (c) three public utility companies (water, electricity, telecommunication) (9 participants), (d) twenty-two government public service institutions (66 participants), (e) five healthcare institutions (15 participants), and (f) thirteen others (IT, Manufacturing, Oil and Gas, etc.) (39 participants).

A Web-based survey was employed to collect the data. The survey enabled the participants to complete the survey questionnaire via the Internet. To improve response rate, the researcher adopted the Maronick's (2009) three strategies of data collection; namely pre-notification, personalized appeals, and promises of reward (access to the study's findings) for completing the survey. The data collected were analyzed using SPSS (Statistical Package for Social Scientists) version 17.0.

The survey instrument, Information Security Governance Assessment tool developed by Educause (2006) was adapted to collect data regarding RK, PM, RM; items on SA and VD were formulated from ISG literature (ITGI, 2006; 2008; Neirotti and Paolucci, 2007; Thomas et al., 2009; Bonabeau, 2007; Johnson and Hale, 2009; Allen et al., 2008; Gregor et al., 2006; Korbelsky et al., 2008; Wang and Alam, 2007; Thatcher and Pingry, 2007). Field and pilot tests were conducted on the instrument to establish its validity and reliability. Validity was established by conducting a field test using a panel of experts; two security practitioners and three senior academic faculty members, who have significant experience with information security governance issues. Participants in the field test submitted their responses via email to the researcher. The feedback from the experts resulted in making some minor revisions to the instrument.

The five variables consist of 50 items and are measured on a 5-point Likert-like scales (*1 - not implemented, 2 - planning stages, 3 - partially implemented, 4 - close to completion, and 5 - fully implemented*) to measure participants' responses concerning the degree of ISG practices. For the instrument reliability using pilot testing, data were collected from 15 respondents drawn from within the sample frame (but who were not included in the study's actual data for measurement) and analyzed to determine the reliability coefficient (Cronbach's alpha). The reliability coefficients of the measures are: Strategic Alignment (SA) .972; Value Delivery (VD) .920; Resource Management (RM) .975; Risk Management (RK) .951; and Performance Management (PM) .979. The measures were all far above the threshold of 0.7 (or higher) and were considered acceptable according to Nunnally's (1978) guidelines.

Data Analysis and Results

The research question evaluates the extent of the relationship between information security domain practices and information security governance strategic alignment in Ghanaian organizations. The research questions correspond to the four hypotheses which would be used to assess the extent of the relationship between strategic alignment and the other information security governance domain areas. The research hypotheses argued that information security governance domain practices, namely risk management (RK), resource management (RM), performance measurement (PM), and value delivery

(VD) are not positively related to information security governance strategic alignment (SA). In testing for all the four hypotheses, the construct SA was assigned the dependent variable, and the constructs RM, PM, VD, and RK the independent variables.

Simple regression analysis was employed to test the four null hypotheses (H_o1 to H_o4) in turn. The regression models tested were stated as:

H_o1: The information security governance strategic alignment with business objectives (SA) is not positively related to information security governance risk management (RK) practices.

$$RK = \beta_0 SA + \beta_1$$

H_o2: The information security governance strategic alignment with business objectives (SA) is not positively related to information security governance value delivery (VD).

$$VD = \beta_0 SA + \beta_1$$

H_o3: The information security governance strategic alignment with business objectives (SA) is not positively related to information security governance performance (PM) measurement practices.

$$PM = \beta_0 SA + \beta_1$$

H_o4: The information security governance strategic alignment with business objectives (SA) is not positively related to resource management (RM) practices.

$$RM = \beta_0 SA + \beta_1$$

where RK, VD, PM, and RM are the dependent variables; SA is the independent variable; β_1 is a constant; and β_0 is the slope (regression coefficient).

The data analysis was in two-fold: to summarize the data so that it would be easily understood and to provide the answers to the research questions (Kelly, Clark, Brown, and Sitzia, 2003) by using linear regression analysis. A total of 81 valid responses were received and out of this number, 28.4% respondents (corresponding to 23 participants) were from educational institutions (colleges, universities), 22.2% respondents (corresponding to 18 participants) were from financial institutions, 7.4% (corresponding to 6 participants) were from Public Utility companies (Water, Electricity, Telecom), 13.6% (corresponding to 11 participants) were from Public services, 8.6% (corresponding to 7 participants) were from Health Care institutions and 19.8% (corresponding to 16 participants) were from other sectors.

The large majority of respondents (40 in total or 48.4%) who participated in the study were IT Specialists (Managers) with the responsibility of managing and performing IT functions in their various organizations. Eleven respondents (representing 13.6%) were Business or Line Managers. Only one Board of Director and one Chief Executive Officer participated in the study. Five Chief Information Officers (representing 6.2%) and 5 Financial Controllers or Accountants (also representing 6.2%) took part in the study. Six (representing 7.4%) respondents were Internal Auditors, seven (representing 8.6%) were Human Resource Managers, and five (representing 6.2%) were others (i.e., IT consultants) also participated in the study.

For the number of years respondents had worked on the current job position, over a quarter of the participants (25.9%) had 1-5 years of experience. Well over one third of the participants (37%) had 6-10 years of experience. Twenty-one percent had 11-15 years of experience, 9.9% and 5% had 16-20 years and over 20 years of experience respectively.

Strategic Alignment and Risk Management - Testing of Hypothesis 1

In order to determine the proportion of the variance in the risk management practices that is explained by information security governance strategic alignment, a simple linear regression analysis was conducted. The mean score on the information security risk management practices was 2.93 (N = 81; SD = 1.18) and the mean score on the information security governance strategic alignment was 3.14 (N = 81; SD = 1.14)**.** The summary of the simple linear regression results were presented in Table 1, 2, and 3. The results indicated that as high as 83.6% (R^2 = .836) of the variance in risk management (RK) was explained by the strategic alignment (SA) practices (see Table 1).

The test statistic was significant ($F_{(1, 79)}$ = 403.926; p < 0.001), showing that strategic alignment significantly and positively relates to information security governance risk management (see Table 2). Hence, the null hypothesis was not supported and should be rejected. As could be observed from Table 3, the higher the level of information security strategic alignment with business objectives, the higher the information security risk management ($t(79)$ = 20.098; p < .001), suggesting that SA makes significant contribution to information security risk management.

Table 1: ***Model Summary for Regression of ISG Risk Management on Strategic Alignment***

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
	.915[a]	.836	.834	.48140

a. Predictors: (Constant), SA (Strategic Alignment)

b. Dependent Variable: RK (Risk Management)

Table 2: ***ANOVA (RK) for Regression of ISG Risk Management on Strategic Alignment.***

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	93.610	1	93.610	403.926	.000[a]
	Residual	18.308	79	.232		
	Total	111.918	80			

a. Predictors: (Constant), SA

b. Dependent Variable: RK

Table 3: ***Coefficients for Regression Model of ISG Risk Management on Strategic Alignment.***

Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	(Constant)	-.061	.158		-.385	.701
	SA	.953	.047	.915	20.098	.000

a. Dependent Variable: RK (Risk Management)

Strategic Alignment and Value Delivery - Testing of Hypothesis 2

To determine the proportion of the variance in the value information security delivers to Ghanaian organizations explained by the strategic alignment practices, a simple linear regression analysis was performed**.** The mean score on the information security value delivery was 3.15 (N = 81; SD = 1.13) and the mean score on the information security strategic alignment was 3.14 (N = 81; SD = 1.14)**.** The results indicated that 71.8% (R^2 = .718) of the variance in ISG value delivery (VD) was explained by the strategic alignment (SA) practices (see Table 4).

Table 5 shows the test statistics ($F_{(1, 79)}$ = 200.998; $p < 0.001$), indicating that strategic alignment significantly and positively relates to information security governance value delivery. Hence, the null hypothesis was not supported and should be rejected. Table 6 reveals that the higher the level of strategic alignment practices, the higher business value information security delivers to the organization (t (79) = 14.177; $p < .001$), indicating that SA makes significant contribution to the model (information security value delivery).

Table 4: Model Summary for Regression of ISG Value Delivery on Strategic Alignment.

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.847[a]	.718	.714	.60505

a. Predictors: (Constant), SA (Strategic Alignment)

b. Dependent Variable: VD (Value Delivery)

Table 5: ANOVA for Regression of ISG Value Delivery on Strategic Alignment.

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	73.581	1	73.581	200.998	.000[a]
	Residual	28.920	79	.366		
	Total	102.502	80			

a. Predictors: (Constant), SA (Strategic Alignment)

b. Dependent Variable: VD (Value Delivery)

Table 6: Coefficients for Regression Model of ISG Value Delivery on Strategic Alignment.

Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	(Constant)	.499	.199		2.508	.014
	SA	.845	.060	.847	14.177	.000

a. Dependent Variable: VD (Value Delivery)

Strategic Alignment and Performance Measurement - Testing of Hypothesis 3

A simple linear regression analysis was conducted to determine the proportion of the variance in the performance measurement that is explained by the strategic alignment practices. The mean score on the information security performance measurement practices was 2.85 (N = 81; SD = 1.32) and the mean score on the information security governance strategic alignment was 3.14 (N = 81; SD = 1.14)**.** The results indicated that 72.2% of the variance in PM was explained by the SA (see Table 7).

The test statistic was significant ($F_{(1, 79)} = 204.771$; $p < 0.001$), showing that strategic alignment significantly and positively relates to information security governance performance measurement (see Table 8). Consequently, the null hypothesis was not supported and would be rejected. Table 9 shows that the higher the level of strategic alignment, the higher the effectiveness of information security governance performance measurement (t (79) = 14.310; p < .001), revealing that SA has made significant contribution to the model (information security performance measurement).

Table 7: Model Summary for Regression of ISG Performance Measurement on Strategic Alignment.

Model Summary[b]				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.849[a]	.722	.718	.70172
a. Predictors: (Constant), SA (Strategic Alignment)				
b. Dependent Variable: PM (Performance Management)				

Table 8: ANOVA for Regression of ISG Performance Measurement on Strategic Alignment.

ANOVA[b]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	100.832	1	100.832	204.771	.000[a]
	Residual	38.901	79	.492		
	Total	139.733	80			

a. Predictors: (Constant), SA (Strategic Alignment)
b. Dependent Variable: PM (performance Measurement

Table 9: Coefficients for Regression Model of ISG Performance Measurement on Strategic Alignment.

Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	(Constant)	-.252	.231		-1.093	.278
	SA	.989	.069	.849	14.310	.000

a. Dependent Variable: PM (Performance Measurement)

Strategic Alignment and Resource Management - Testing of Hypothesis 4

In order to determine the proportion of the variance in the resource management that is explained by the strategic alignment practices, a simple linear regression analysis was conducted. The mean score on the information security resource management practices was 2.92 (N = 81; SD = 1.20) and the mean score on the information security governance strategic alignment was 3.14 (N = 81; SD = 1.14). The results found that 74.7% (R^2 = .747) of the variance in RM was explained by the SA practices (see Table 10).

The test statistic was significant ($F_{(1, 79)}$ = 233.433; p < 0.001), showing that strategic alignment significantly and positively correlates with information security governance resource management (see Table 11). Therefore, the null hypothesis was not supported and was rejected. Table 12 reveals that the higher the level of strategic alignment practices, the higher the information security governance resource management (t (79) = 15.279; p < .001), suggesting that SA has made significant contribution to the model (information security resource management).

Table 10: Model Summary for Regression of ISG Resource Management on Strategic Alignment.

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.864[a]	.747	.744	.60719

a. Predictors: (Constant), SA (Strategic Alignment)

b. Dependent Variable: RM (Risk Management)

Table 11: ANOVA for Regression of ISG Resource Management on Strategic Alignment.

ANOVA[b]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	86.061	1	86.061	233.433	.000[a]
	Residual	29.125	79	.369		
	Total	115.186	80			

a. Predictors: (Constant), SA(Strategic Alignment)
b. Dependent Variable: RM (Risk Management)

Table 12: Coefficients for Regression Model of ISG Resource Management on Strategic Alignment.

Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	(Constant)	.050	.200		.252	.802
	SA	.914	.060	.864	15.279	.000

a. Dependent Variable: RM(Risk Management)

Summary and Discussion

The research questions and the associated research hypotheses empirically established the degree of relationship between strategic alignment and other information security governance domains: risk management, resource management, performance measurement, and value delivery. The null hypotheses stated that information security governance strategic alignment with business objectives was not positively related to information security governance domain areas. All the hypotheses were not supported and therefore rejected. The following discusses the extent of the relationship between the constructs, its implications and consistency with the earlier studies.

The relationships between information security governance strategic alignment and other domains were found to be positively statistically significant: strategic alignment to risk management (R^2 = .836); strategic alignment to value delivery (R^2 = .718), strategic alignment to performance measurement (R^2 = .722), and strategic alignment to resource management (R^2 = .747). The results highlighted consistent importance of information security/business strategic alignment as crucial for organizational information security risk management, performance measurement, resource management, and value delivery. This implies that effective information security governance strategic alignment greatly improves organizations' risk management, resource management, performance measurement, and delivers business value.

Confirming the relationships, Wilkin and Chenhall (2010) noted that strategic alignment determines the direction for other ISG domain areas. As such, with organization having SA in place, business value would be delivered. Value delivery comes as a result of effective investment and planning, including tactical plans for risk management and resource management. Again, the realization of ISG value to the organization is informed by coordinated performance measurement. Therefore, value delivery and risk management are regarded as outcomes depending upon sound practices in strategic alignment, performance measurement, and resource management (Wilkin and Chenhall, 2010).

This study is also consistent with previous studies that shown direct (positive) relationship between strategic alignment and risk management (Abu-Musa, 2010); strategic alignment and resource management (Hardy, 2006; Luftman and Kempaiah, 2008); strategic alignment and performance measurement (Tugas, 2010); and strategic alignment and value delivery (Johnston, 2009). Specifically, effective security governance involves strong support from executive management (Hu and Cooke, 2007; Risk IT, 2009) which should involve strategic planning (Oppliger, 2007), management practices and strategic implementation (Johnson and Hade, 2009). Effective security governance should be championed by CEO (chief executive officer) (Hu and Cooke, 2007) with clear and established CIO (chief information officer), CISO (chief information security officer), CEO responsibilities and reporting line.

Conclusion

This study strongly supports the understanding that information security governance effectiveness could be realized through sound corporate governance theories (Carney 2005; Le Breton-Miller and Miller 2006) which are based on the (1) commitment of the organization's stakeholders with the purpose of aligning key stakeholders' interest with business objectives (stakeholder theory); (2) availability of resources with the aim of strategically manage resources and competencies to achieve organizational goals (resource-based view of organizational theory), and (3) the responsibility and accountability of the agents to ensure that performance through monitoring and measurement is efficient (agency theory) and effectively monitored in order to minimize risks.

It is important the boards of directors at the strategic level establish strong alignment between the business and information security with the aim of ensuring that security delivers business value through appropriate policies of risk management, resource management, and performance measurement. Therefore, organizations should improve strategic alignment attributes in order to attain

effective information security governance. Hence, more research is required as to how organizational leaders can improve strategic alignment between the business and information security

References

Abdullah, H. and Valentine, B. (2009), "Fundamental and ethics theories of corporate governance", *Middle Eastern Finance and Economics,* Vol. 4, pp. 88-96.

Abu-Musa, A.A. (2010), "Information security governance in Saudi organizations: An empirical study", *Information Management and Computer Security,* Vol. 18 No. 4*,* pp. 226-276.

Alchian, A. and Demsetz, H. (1972), "Production, information costs, and economic organization", *American Economic Review*, Vol. 62 No. 5, pp. 777-795.

Allen, M. W., Armstrong, D. J., Reid, M. F. and Riemenschneider, C. K. (2008), "Factors impacting the perceived organizational support of IT employees", *Information & Management,* Vol. 45 No. 8, pp. 556-563.

Allen, E. B. (2006), "Framing the framework: A review of IT governance research", *Communications of the Association for Information Systems*, Vol. 15, pp. 696-712.

Ask, U., Bjornsson, H., Johansson, M., Magnusson, J., and Nilsson, A. (2007). IT Governance in the light of paradox - A social systems theory perspective. In Proceedings of the 40th Hawaii International Conference on System Sciences, IEEE. Big Island, Hawaii, pp. 3-6.

Bernroider, E. W. N. (2008), "IT governance for enterprise resource planning supported by the DeLone-McLean model of information systems success", *Information & Management*, Vol. 45 No. 5, pp. 257–269.

Berle, A. (1932), *The modern corporation and private property*. New York: Macmillan.

Bihari, E. (2008), *Information security governance and boards of directors: Are they compatible?* Proceedings of the 6th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia.

Bonabeau, E. (2007), "Understanding and managing complexity risk", *MIT Sloan Management Review,* Vol. 48 No. 4, pp. 62–68.

Carney, M. (2005), "Corporate governance and competitive advantage in family controlled firms", *Entrepreneurship Theory and Practice,* Vol. 29 No. 3, pp. 249-265.

Ching, K. W., Tan, J.S. and Ching, C. R. G. (2006), "*Corporate governance in East Asia: The road ahead*", Prentice Hall Publication.

Clarkson, M. B. E. (1995), "A stakeholder framework for analyzing and evaluating corporate social performance", *Academy of Management Review*, Vol. 20 No. 1, pp. 92-117.

Coutaz, J., Crowley, J. L., Dobson, S. and Garlan, D. (2005), "Content is key", *Communications of the ACM,* Vol. 48 No. 3, pp. 49–53.

Daily, C.M., Dalton, D.R. and Canella, A.A. (2003), "Corporate governance: Decades of dialogue and data", *Academy of Management Review,* Vol. 28 No. 3, pp. 371-382.

De Haes, S. and A. H. an Grembergen, W. (2009), "An Exploratory Study into IT governance implementations and its impact on business/IT alignment", *Information Systems Management,* Vol. 26 No. 2, pp. 123-137.

De Haes, S., and Van Grembergen, W. (2009), "Exploring the relationship between IT governance practices and business/IT alignment through extreme case analysis in Belgian mid-to-large size financial enterprises", *Journal of Enterprise Information Management*, Vol. 22 No. 5, pp. 615-637.

Donaldson, T. and Preston, L.E. (1995), "The stakeholder theory of the corporation: Concepts, evidence and implications", *Academy of Management Review*, Vol. *20 No.* 1, pp. 65-91.

Educause (2006), "Information security governance assessment tool", available at http://www.educause.org (accessed 12 October, 2012).

El-Meligy, H. (2011), "*IT governance, security and safety in developing countries"*, available at: http://www.isaca.org (accessed 5 November 2012).

Eisenhardt, K. M. (1989), "Agency theory: An assessment and review", *Academy of Management Review*, Vol. 14 No. 1, pp. 57-74.

Fama, E. F. and Jensen, M. C. (1983), "Separation of ownership and control", *Journal of Law and Economics,* Vol. 26, pp. 301-326.

Gellings, C. (2007), "Outsourcings relationships: The contract as IT governance tool". *Proceedings of the 40th Hawaii International Conference on System Sciences, IEEE*. Big Island, Hawaii, pp. 3-6.

Gregor, S., Martin, M., Fernandez, W., Stern, S. and Vitale, M. (2006), "The transformational dimension in the realization of business value from information technology", *The Journal of Strategic Information Systems,* Vol. 15 No. 3, pp. 249-270.

Grover, V., R. M. and Segars, A. H. (2005), "An empirical evaluation of stages of strategic information systems planning: Patterns of process design and effectiveness", *Information & Management,* Vol. 42 No. 5, pp. 761-779.

Habbershon, T. G. and Wouldiams, M. L. (1999), "A resource-based framework for assessing the strategic advantages of family firms", *Family Business Review, Vol. 12 No.* 1, pp. 1-25.

Hardy, G. (2006), "Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges", *Information Security Technical Report,* Vol. 11 No. 1, pp. 55-61

Harris, M. and Raviv, A. (1979), "Some results on incentive contracts with application to education and employment, health insurance, and law enforcement", *American Economic Review*, *Vol. 68*, pp. 20-30.

Hillman, A.J., Canella, A.A. and Paetzold, R.L. (2000), "The resource dependency role of corporate directors: Strategic adaptation of board composition in response to environmental change", *Journal of Management Studies, Vol. 37 No.* 2, pp. 235-255.

Hu, Q. P. H. and Cooke, D. (2007), "The role of external and internal influences on information systems security - A neo-institutional perspective", *The Journal of Strategic Information Systems,* Vol. 16 No. 2, pp. 153-172.

Idris, F., Abdullah, M., Idris, M. A. and Hussain, N. (2003), "Interacting resource-based view and the stakeholder theory in developing the Malaysian excellence model: A conceptual model", *Singapore Management Review*, Vol. 25 No. 2, pp.91-109.

ITGI (2006). *Information security governance: Guidance for boards of directors and executive management* (2nd ed.}, available at www.itgi.org (accessed 7 January 2013).

ITGI (2008), *Information security governance: Guidance for information security managers, available at* www.itgi.org (accessed 7 January 2013).

Jensen, M.C. and Meckling, W. (1976), "Theory of the firm: Managerial behavior, agency costs and ownership structure", *Journal of Financial Economics*, Vol. 3, pp. 305-360.

Johnston, A. C., and Hale, R. (2009), "Improved security through information security governance", *Communications of the ACM,* Vol. 52 No. 1, pp. 126-129.

Kelly, K., Clark, B., Brown, V. and Sitzia, J. (2003), "Good practices in the conduct and reporting of survey research", *International Journal of Quality in Health Care,* Vol. 15 No. 3, pp. 261-266.

Kobelsky, K., Hunter, S. and Richardson, V. J. (2008), "Information technology, contextual factors and the volatility of firm performance", *International Journal of Accounting Information Systems,* Vol. 9 No. 3, pp. 154-174.

Le Breton-Miller, I. and Miller, D. (2006), "Why do some businesses out-compete? Governance, long-term orientations, and sustainable capability?", *Entrepreneurship: Theory and Practice,* pp. 731-746.

Luftman, J. N. and Kempaiah, R. (2008), "Key Issues for IT executives 2007", *MIS Quarterly Executive,* Vol. 7 No. 2, pp. 99-112.

Maronick, T. (2009). "The role of the internet in survey research: Guidelines for researchers and experts", *Journal of Global Business and Technology, Vol. 5 No.* 1, pp. 22.

Moghdeb, F. B., Indulska, M. and Green, P. (2007), "Business process improvement and organizational theory - the missing link", *Managing Worldwide Operations & Communications with Information Technology,* pp. 253-256.

Neirotti, P. and Paolucci, E. (2007), "Assessing the strategic value of information technology: An analysis on the insurance sector", *Information & Management,* Vol. 44 No. 6, pp. 568-582.

Nunnally, J. C. (1978), *Psychometric theory (2nd ed.).* New York: McGraw-Hill.

Oppliger, R. (2007), "IT security: In search of the holy grail", *Communications of the ACM,* Vol. 50 No. 2, pp. 96–98.

Padilla, A. (2002), "Can agency theory justify the regulation of insider trading", *The Quarterly Journal of Austrian Economics*, Vol.5 No.1, pp. 3-38.

Pinsonneault, A., and Kraemer, K. L. (1992). *Survey research methodology in management information systems: An assessment*. Unpublished manuscript, Graduate School of Management, University of Califonia, Irvine, Califonia.

Posthumus, S., von Solms, R. and King, M. (2010), "The board and IT governance: The what, who, and how", *South African Journal of Business Management,* Vol. 41 Vol. 3.

Prybutok, V. R., Zhang, X. and Ryan, S. D. (2008), "Evaluating leadership, IT quality, and net benefits in an e-government environment", *Information & Management,* Vol. 45 No. 3, pp. 143-152.

Risk IT. (2009), "Enterprise risk: Identify, govern and manage IT risk", available at http://www.isaca.org (accessed 10 January 2013).

Rungtusanathan, M. J., Choi, T. Y., Hollingworth, D. G., Wu, Z. and Forza, C. (2003), "Survey research in operations management: Historical analysis", *Journal of Operations Management,* Vol. 21, pp. 475-488.

Silva, L. and Hirschheim, R. (2007), "Fighting against windmills: Strategic information systems and organizational deep structures", *Management Information Systems Quarterly,* Vol. 31 No. 2, pp.327-354.

Sundaram, A.K. and Inkpen, A.C. (2004), "The corporate objective revisited", *Organization Science*, Vol. 15 No. 3, pp. 350-363.

Tassabehji, R. (2005), *Information security threats: From evolution to prominence.* In Evcyclopedia of Multimedia Technology and Networking (Margherita Pagani), Idea Group Inc., ISBN: 1-59140-496-6, pp. 404-410

Thomas, R. J., Schrage, M., Bellin, J. B. and Marcotte, G. (2009), "How boards can be better - A manifesto" *MIT Sloan Management Review,* Vol. 50 No. 2, pp. 69–74.

Tugas, F.C. (2009), "Assessing the level of information technology (IT) processes performance and capability maturity in the Philippine food, beverage, and tobacco (FBT) industry using the COBIT framework", *Information and Management Sciences,* Vol. 13 No. 2, pp. 68-73.

Valiris, G. and Glykas, M. (2004), "Business analysis metrics for business process redesign", *Business Process Management*, Vol. 10 No. 4, pp. 445-480.

Val IT. (2008), "Enterprise value: Governance of IT investments- the Val IT framework 2.0", available at http://www.isaca.org/valit/ (accessed 10 January 2013).

Von Solms, B. (2006), "Information security – The fourth wave", *Computers & Security,* Vol. 25, pp. 165- 168.

Walsham, G. (1995). *Interpreting Information Systems*. Chichester, John Wiley & Sons.

Wang, L. and Alam, P. (2007), "Information technology capability: Firm valuation, earnings uncertainty, and forecast accuracy", *Journal of Information Systems,* Vol. 21 No. 2, pp. 27-48.

Wilkin, C. L. and Chenhall, R. H. (2010), "A review of IT governance: A taxonomy to inform accounting information systems", *Journal of Information Systems*, Vol. 24 No. 2, pp. 107-146.

Wouldson , P. P. and Pollard, C. E. (2009), "Exploring IT governance in theory and practice in a large multi-national organizations in Australia", *Information Systems Management,* Vol. 26, pp. 98-109.

Yu, E. and Mylopoulos, J. (1994), "Using goals, rules, and method to support reasoning in business process reengineering", *Paper presented at the 14th Hawaii International Conference on Systems Science*, San Diego, CA.