The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0968-5227.htm

Information security governance implementation within Ghanaian industry sectors

An empirical study

Winfred Yaokumah
Department of Information Technology, Pentecost University College, Accra, Ghana

Received 9 June 2013
Revised 16 August 2013
25 August 2013
Accepted 25 August 2013

Abstract

Purpose – The purpose of this study is to assess the levels of information security governance (ISG) implementation among major Ghanaian industry sectors. The intent is to benchmark inter-industry sector ISG implementation and to identify areas that may require improvement.

Design/methodology/approach – Random sampling strategy was used, and data were collected via Web survey. The data analysis utilized a one-way analysis of variance to determine the differences in means of the levels of implementation of ISG focus areas among five main industry sectors.

Findings – The results showed that, as a whole, all the industry sectors have only partially implemented ISG. In particular, there existed statistical significant differences in ISG implementation among the industry sectors. Ranking ISG implementation, Financial Institutions were close to completion, Utility Companies, Others (Information Technology, Oil and Gas, Manufacturing) and Public Services had PI ISG and health care and educational institutions were at the planning stages. The result also revealed that all the industry sectors made marginal effort trying to align information security to business strategy, and performance measurement remained the least implemented focus area.

Originality/value – Organizational leaders could use these findings to benchmark industry sectors' ISG implementation, which could lead to competitiveness. Again, international enterprises that do businesses with these industry sectors would better understand the level of involvement of the top executives in governing information security toward the protection of valuable information assets.

Keywords Risk management, Benchmarking, Information security, Business alignment

Paper type Research paper

1. Introduction

Studies conducted in few developing nations suggested that information security programs have not been effectively implemented or governed by the top organizational leaders (Abu-Musa, 2010; El-Meligy, 2011; Wolfpack, 2011). An empirical study, South African Information Security Thermometer Survey, found that only 26 per cent of the 80 organizations surveyed have established information security steering committee (Wolfpack, 2011). The study further found that 42 per cent of organizations studied had their boards assumed responsibility for the governance of information security, while 58 per cent had plans or no plan to implement information security governance (ISG) board responsibility.

According to El-Meligy (2011), information and communication technology governance and security were left unaddressed in the developing nations, and he

Information Management & Computer Security
Vol. 22 No. 3, 2014
pp. 235-250

0968-5227
DOI 10.1108/IMCS-06-2013-0044

cautioned that if developing countries failed to address information security as governance concern, it could "compromise worldwide transactions, increase the time needed to complete deals, expose confidential information, and hinder important data from being used effectively" (p. 1). Thus, if the developing nations fail to deal with information security as governance concern, the problem is that the international enterprises that do business with organizations in developing countries may have valuable data compromised and hence incur losses.

Developing nations, for example, Ghana and Nigeria, were noted for credit card misuse. As a result, major credit card merchants and financial institutions no longer issue or accept credit card transactions from Ghana. In 2008, about 58 per cent of US and Canadian merchants shut off international online orders by credit cards from Ghana (Modern Ghana, 2009). With the current relatively stable political environment in some developing nations, coupled with the inflow of foreign investments in these countries, it has become imperative information security is given prominent attention.

To ensure security issues are addressed across geographical boundaries, Anasimov (2006) proposed global hierarchical model of ISG, and El-Meligy (2011) advised supporting organizations such as Information Technology Governance Institute (ITGI) and Information Systems Audit and Control Association to take proactive approach to increase security awareness and encourage security governance in developing countries and their governments' agencies. Therefore, a critical appraisal of the extent of ISG (Johnston *et al.*, 2009) implementation in different environments (countries) and inter-organizational settings (Wilkin and Chenhall, 2010) in the developing countries is essential.

The purpose of this quantitative cross-sectional survey research is to assess the levels of ISG implementation among major Ghanaian industry sectors. The intent is to benchmark inter-industry sector ISG implementation and to identify areas that require improvement. The level of ISG implementation can be measured by the factors defined within ISG focus areas (ITGI, 2006, 2008). These factors can map to levels defined in the ISG maturity model, which were specified in the Control OBjectives for Information and related Technology (COBIT) standard (ITGI, 2010).

Based on these high levels of ISG documents and the global hierarchical model of ISG (Anasimov, 2006), this study proposes two related research questions.

RQ1. What is the level of ISG implementation in Ghanaian industry sectors?

RQ2. Are there any differences among industry sectors relating to the level of implementation of ISG focus areas?

2. Literature review

2.1 Motivation for ISG implementation

Developments in the field of corporate governance and the related legal and regulatory compliance (von Solms, 2006) have led many organizations to implement ISG (Khoo *et al.*, 2010). ISG forms:

> 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 (ITGI, 2006, p. 18).

One of the major regulations that impacted organizations with respect to implementing ISG was Sarbanes – Oxley Act (SOX). SOX Act was enacted to protect stakeholders by

tasking the top management to improve organization's internal controls. SOX made top executives and boards of directors personally accountable for security of information and the information technology (IT) systems that process, transmit and store information upon which the top executives make strategic decisions. However, SOX applies only to those businesses that are quoted on the New York Stock Exchange, yet has a wider effect throughout the global supply chain.

The developed nations have taken the lead in developing legal frameworks and regulatory compliance to protect information. Some developing nations have seen the need to protect critical information assets (Abu-Musa, 2010; von Solms, 2006) by mandating and strengthening existing institutions. Among developing nations, South Africa enacted Electronic Communications and Transactions Act of 2002. Ghana made significant effort to put in place legal and regulatory frameworks and enforcement agencies to protect information assets. The Electronic Transactions Act 772 (2008) of Ghana has the primary aim of developing:

> A safe, secure and effective environment for the consumer, business and the government to conduct and use electronic transactions; and to ensure compliance with accepted international technical standards in the provision and development of electronic communications and transactions (p. 6).

Apart from protection against legal and regulatory compliance, other factors that have led organizations to implement ISG include improvement of trust and confidence among the stakeholders, protection of organization's reputation, reduction in operational cost due to protection against legal liabilities, gaining competitive advantage, mitigating risk and improved efficiency (Risk, 2009; Pironti, 2007; Val, 2008; von Solms, 2006).

2.2 ISG models

The US Corporate Governance Task force (2004) remarked that "the best way to strengthen USA information security is to treat it as a corporate issue that requires the attention of Boards and CEOs" (p. 1). Information security must be handled by concerted effects of all organizational leaders across the globe. Addressing this challenge, Anasimov (2006) proposed a global hierarchical model of ISG. The ITGI developed authoritative documents to guide boards of directors, chief executive officers and chief information officers. These documents are the *Information Security Governance: Guidance for Boards of Directors* and the COBIT standard, which aim at providing guidance for organizational leaders to minimize IT-related risks and metrics to assess maturity levels of ISG implementation. The global hierarchical model of ISG and the ISG maturity models are discussed in the next section.

The global hierarchical model of ISG takes a global view of governing IT-related risks (Anasimov, 2006). The model uses the top – down approach to governance. From the top to bottom, Anasimov listed four major types of institutions that govern global information security; these are:

(1) international organizations (such as International Organization for Standardization and Institute of Electrical and Electronics Engineering);

(2) global IT companies (such as Microsoft and Oracle);

(3) states (such as governmental and non-governmental bodies); and

(4) the business community.

Each of these bodies performs some specific tasks or functions that influence others.

According to Anasimov (2006), in the sphere of ISG, the international organizations develop rules and establish agreements for overall IT community, provide support for professional conference and research activities and create opportunities for standardization of IT products in terms of software, hardware and services; the global IT companies develop new solutions and support organizational methodologies, products and services; the governmental organizations regulate the activities of different entities and protect and maintain integrity of the information infrastructure; and the business community (organizations) protects their own information assets and develops enhanced internal policies, practices and culture.

While the global hierarchical model of ISG has a global view of information security, the ISG maturity model provides metric for benchmarking the level of ISG (ITGI, 2010). The ISG maturity model has six levels, namely, non-existence, initial/*ad hoc*, repeatable but intuitive, defined process, managed and measurable and optimized.

As specified in the model, the *non-existence* represents the stage where an organization does not consider business impacts associated with security vulnerabilities and threat to IT operations, does not perform risk assessment for processes and does not consider the need for information security. It is also a stage where no responsibilities and accountabilities are assigned to personnel. This phase can be mapped to a stage where ISG is not implemented in the organization. But with the initial/*ad hoc* stage, organizations recognize the need for information security and consider IT risks but in an *ad hoc* manner (ITGI, 2010). Under this phase, informal risk assessment is performed but not measured, and responsibilities for IT security are unclear. This stage can be considered as a planning stage (PS) of ISG implementation.

Moreover, at the *repeatable but intuitive* stage, the organization understands that IT risks are important, and has risk assessment that is immature and under development. Responsibilities and accountabilities are assigned to security coordinator with no management authority while security policies are being developed (ITGI, 2010). This stage can also be considered as a PS of ISG implementation. However, with the defined *process stage*, risk assessment follows a defined process, documented and made available to staff; security awareness programs are promoted by management; and responsibilities and accountabilities are assigned, though not enforced (ITGI, 2010). This stage can be considered as partial implementation of information security information.

Further, at the *managed and measurable* stage, risk assessment follows standard procedure, and IT risk management (RK) is senior-level responsibility, clearly assigned, managed and enforced (ITGI, 2010). Security policies and practices are completely developed and put in place. This is the stage where security risk and impact assessment are constantly performed. This phase can be mapped to close to completion (CC) of ISG implementation. Finally, at the *optimized* stage, RK has been fully developed and structured and processes are enforced; information security is a joint responsibility of business and IT management, which are aligned with the organization's security/business objectives (ITGI, 2010). In addition, information on new security threats and vulnerabilities is gathered and constantly analyzed. Security is integrated into applications at design time, and users are accountable for managing security. This stage can be described as fully completed ISG implementation.

2.3 ISG focus areas

As maturity model of ISG specified the levels of ISG maturity within an organization, ITGI (2006, 2008) recommended five focus areas within which organizational leaders should function to realize these levels. These are:

(1) *Strategic alignment* (i.e. aligning information security with the business). Strategic alignment (SA) 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 SA to be effectively implemented, the business strategy should encompass key information security capabilities, future security requirements, people and information assets that could be deployed to meet business needs (Neirotti and Paolucci, 2007; Thomas *et al.*, 2009).

(2) *Risk management* (i.e. safeguarding of IT assets, disaster recovering and business continuity). RK is 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 RK is to mitigate risks and reduce adverse impacts on information assets to a satisfactory level (ITGI, 2006).

(3) *Resource management* (i.e. optimizing knowledge and information security infrastructure). The board of directors should ensure that appropriate resources and adequate skills exist in information security project implementation (Allen *et al.*, 2008).

(4) *Performance measurement* (i.e. tracking project delivery and monitoring information security services). The board of directors and executive management ensure that the organization quantifies, monitors and reports on the performance of security processes so as to make sure that the organizational objectives are achieved (ITGI, 2008).

(5) *Value delivery* (i.e. cost optimization and proving the value of information security). 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; Val, 2009).

3. Research methodology

3.1 Population and sampling strategy

The accessible population of this study comprised the organizations located within Greater Accra municipal area of Ghana that employed IT to store, process or transmit customers' personal identifiable data. A total of 112 organizations were identified and grouped according to their respective industry sectors. Random sampling was conducted to select 360 participants from within the strategic and tactical level management (see Table II). A Web-based survey was used to collect the data. The Web-based 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.

3.2 Constructs validity, reliability and measure

The survey instrument was adapted from Educause (2006) and slightly modified to include variables defined by ITGI (2008) and the COBIT framework. The survey consisted of items that constituted constructs corresponding to the five ISG focus areas, namely, SA, Value Delivery (VD), Resource Management (RM), RK and Performance Management (PM). The survey items were represented by a score on a 5-point Likert-type scale, where:

- 5 (fully implemented, FI) represents the maximum score of the scale;
- 4 (close to completion, CC);
- 3 (partially implemented, PI);
- 2 (planning stages, PS); and
- 1 (not implemented, NI) represents the minimum score.

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. Participants in the field test submitted their responses via email to the researcher. The feedback from the experts resulted in making minor revisions to the instrument. For pilot testing, data were collected from 15 respondents drawn from within the sample frame to determine the reliability coefficient (Cronbach's alpha). Table I shows the reliability coefficients of the measures, which were all found to be far above the threshold of 0.7 (or higher) and were considered acceptable according to Nunnally's (1978) guidelines.

The data collected for the actual study were analyzed using Statistical Package for Social Scientists version 16. The data analysis was twofold: to summarize the data so that it would be easily understood, and to provide the answers to the research questions (Kelly *et al.*, 2003) by employing descriptive statistics and analysis of variance (ANOVA).

4. Results

4.1 Characteristics of respondents

A total of 120 organizations were selected from within the industry sectors, and 360 respondents (three from each organization) were invited to take part in the study. Details of the samples include:

- forty-seven (six public and 41 private) universities (141 participants);
- thirty licensed banks registered in Ghana (90 participants);

Variables	Reliability*
Strategic alignment (SA)	0.972
Value delivery (VD)	0.920
Resource management (RM)	0.975
Risk management (RK)	0.951
Performance management (PM)	0.979

Note: *Reliability measure is Cronbach's alpha

Table I.
Variable reliability

- three public utility companies (water, electricity, telecommunication) (nine participants);
- twenty-two government public service institutions (66 participants);
- five healthcare institutions (15 participants); and
- thirteen others (IT, Manufacturing, Oil and Gas, etc.) (39 participants).

In all, 83 participants completed the survey, representing 23 per cent response rate. There were two incomplete responses and therefore were removed from the analysis. Table II summarizes the characteristics of the respondents.

RQ1. *What is the level of ISG implementation in Ghanaian industry sectors?*
Table III summarizes the ratings of the levels of ISG implementation within the industry sectors. The scale is represented by:

- *NI* (20 per cent);
- *PSs* (40 per cent);
- *PI* (60 per cent);
- *CC* (80 per cent); and
- *FI* (100 per cent).

The overall implementation of ISG for all industry sectors in Ghana is approximately 60.0 per cent (thus, 3 – *partially completed*), indicating that Ghanaian industry sectors have merely partially put in place ISG.

In particular, the industry sectors' ratings from the highest to the lowest are: Financial Institutions (79.7 per cent), thus *CC*; Public Utility companies (70.1 per cent), representing *PI*; Others (IT, Oil and Gas, Manufacturing) (66.5 per cent), indicating *PI*; Public Services (50.1 per cent), indicating *PSs*; Health Care (53.0 per cent), representing *PSs*; and Educational Institutions (43.7 per cent), indicating *PS*. The levels of implementation of each focus area and the items assessed are presented in the following paragraph.

The overall level of RM for all the industry sectors was *moderate* with an overall score of 58.4 per cent, indicating that the industry sectors have *PI* RM (see Table III). In general, participants' responses to the PM scale amounted to 57.0 per cent (*PI*) and that of VD was 58.6 per cent (*PI*). The score on the information security RK scale was 58.6 per cent (representing *PI*). Generally, respondents rated their information security SA as *PI* (62.8 per cent).

RQ2. *Are there any differences among industry sectors relating to the level of implementation of ISG focus areas?*
The *RQ2* inquired whether there were any significant differences among industry sectors relating to the levels of ISG implementation.

The five hypotheses under this research question argued that the levels of ISG implementation, namely, RK, RM, SA, PM and VD do not differ among Ghanaian industry sectors. Table IV showed descriptive statistics of the mean, standard deviation and 95 per cent confidence intervals for the independent variables and the industry sectors: Education, Public Utilities, Public Services, Financial Institutions, Health Care and Others (IT, Oil and Gas, Manufacturing, etc).

Respondents	Number of participants invited (360)	Frequency of participants responded (81)	(%)
Industry sector			
Educational institutions (colleges, universities)	141	23	28.4
Financial Institutions	90	18	22.2
Public Utility Companies (Water, Electricity, Telecom)	9	6	7.4
Public Services	66	11	13.6
Health Care Institutions	15	7	8.6
Others (IT Company, Oil and Gas, Manufacturing, etc.)	39	16	19.8
Job title/Function			
Board of directors	16	1	1.2
Chief executive officers	25	1	1.2
Chief information security officer	5	–	–
Chief information officers	27	5	6.2
Business or line managers	99	11	13.6
IT specialists (managers)	78	40	49.4
Internal auditors	30	6	7.4
Financial controllers or accountants	12	5	6.2
Human resource managers	46	7	8.6
Others	22	5	6.2
Number of years on current position			
1-5		21	25.9
6-10		30	37.0
11-15		17	21.0
16-20		8	9.9
Over 20		5	6.2

Table II.
Sample characteristics

Note: $N = 81$ (Respondents)

Beginning, the Levene's test of homogeneity of variance, which tested for similar variances for all industry sectors, was conducted, and the F statistic had significance value of $p < 0.05$. This indicated violation of homogeneity of variances assumption, signifying that the variances in the levels of ISG implementation among the industry sectors were statistically significantly different. The homogeneity of variance assumption was violated and, as such, the robust tests for equality of means (Welch F test) were used for all industry sectors and were found to be $p < 0.001$, confirming the existence of significant differences among the

ISG domain areas	Scale	Levels of ISG implementation among industry sectors: Educational institutions (%)	Financial institutions (%)	Public utilities (%)	Public services (%)	Health care (%)	Others (%)	Overall (%)
RM	Low	78.2	–	16.7	54.5	57.2	31.3	41.9
	Moderate	17.0	16.7	50.0	36.4	28.6	25.0	33.3
	High	4.3	83.3	33.3	9.1	14.3	33.3	24.7
	Total for sectors	37.8 (PS)	81.2 (CC)	72.0 (PI)	50.6 (PS)	50.8 (PS)	65.8 (PI)	58.4 (PI)
PM	Low	65.2	5.6	33.3	54.6	85.7	31.2	43.2
	Moderate	26.1	16.7	16.7	36.5	–	18.8	21.0
	High	6.6	77.8	50.0	9.1	14.3	50.0	35.8
	Total for sectors	40.2 (PS)	78.8 (CC)	69.2 (PI)	48.6 (PS)	47.2 (PS)	63.8 (PI)	57.0 (PI)
VD	Low	34.7	11.1	16.7	27.3	28.6	37.5	28.4
	Moderate	26.1	–	16.7	27.3	42.9	12.5	33.3
	High	39.1	88.9	66.6	45.5	28.6	50.0	38.6
	Total for sectors	40.6 (PS)	78.8 (CC)	69.2 (PI)	48.6 (PS)	47.2 (PS)	63.8 (PI)	58.6 (PI)
RK	Low	78.3	5.6	33.3	54.6	57.1	31.2	44.5
	Moderate	13.0	11.0	33.4	36.4	28.6	18.8	19.8
	High	8.6	83.4	33.3	9.1	14.3	50.5	35.8
	Total for sectors	42.0 (PS)	78.9 (CC)	66.2 (PI)	48.8 (PS)	54.0 (PS)	65.4 (PI)	58.6 (PI)
SA	Low	60.8	–	16.7	27.3	71.4	31.3	34.6
	Moderate	34.8	22.2	16.7	54.5	14.3	12.5	27.2
	High	4.3	77.8	66.6	18.2	14.3	56.3	38.2
	Total for sectors	48.4 (PS)	82.2 (CC)	71.8 (PI)	54.0 (PS)	50.6 (PS)	69.8 (PI)	62.8 (PI)
Overall ISG implementation		43.7 (PS)	79.7 (CC)	70.1 (PI)	50.1 (PS)	53.0 (PS)	66.5 (PI)	60.0 (PI)

Notes: Low = not implemented (NI) + planning stages (PS)l; moderate = partially implemented (PI); high = close to completion (CC) + fully implemented (FI); 1 – not implemented (20 per cent); 2 – planning stages (40 per cent); 3 – partially implemented (60 per cent); 4 – close to completion (80 per cent); and 5 – fully implemented (100 per cent)

Table III.
Levels of ISG implementation among industry sectors

industry sectors. Consequently, a post hoc test of multiple comparisons was conducted. Following this, an ANOVA was used to test the five null hypotheses in turn.

4.3.1 RK and industry sectors.

H01. There are no significant differences in the levels of ISG RK implementation among industry sectors.

Table V depicted the output of the ANOVA analysis, which determined whether there was a statistically significant difference between and within the group means of the six industry sectors. The result showed that there was at least one significant difference between the industry sectors ($N = 81$; $F_{(5, 75)} = 8.637$; $p < 0.05$). The effect size (f) was 0.37, which is small to medium according to Cohen's (1988) conventions. This suggested statistical significant differences in the level of ISG RK implementation among the industry sectors. On the basis of this, the null hypothesis was not supported and rejected. The Games-Howell post hoc test showed that there was a significant difference in the levels of ISG implementation between the Financial Institutions and the Educational Institutions; between the Financial Institutions and Public Sector; and between the Financial Institutions and Health Care Sector.

In particular, the findings revealed that Health Care Sector, Public Service Sector and Education Sector have no documented information security and privacy programs.

Domain areas	Descriptive statistics	Industry sectors: Educational institutions	Financial institutions	Public utilities	Public services	Health care	Others
RK	*N*	23	18	6	11	7	16
	Mean	2.10	3.96	3.31	2.44	2.70	3.27
	SD	0.76	0.62	1.23	0.86	0.81	1.45
RM	*N*	23	18	6	11	7	16
	Mean	1.89	4.06	3.60	2.53	2.54	3.29
	SD	0.71	0.47	1.23	0.75	0.80	1.36
VD	*N*	23	18	6	11	7	16
	Mean	2.48	3.94	3.75	2.75	3.11	3.38
	SD	0.98	0.54	1.36	0.38	0.81	1.56
PM	*N*	23	18	6	11	7	16
	Mean	2.03	3.86	3.86	2.43	2.36	3.19
	SD	1.03	0.89	1.36	0.96	0.94	1.59
SA	*N*	23	18	6	11	7	16
	Mean	2.42	4.11	3.59	2.70	2.53	3.49
	SD	0.79	0.49	1.02	0.77	0.71	1.52

Table IV.
Descriptive statistics of industry sectors on ISG domains

Notes: N – Number of respondents; SD – Standard deviation

	Summation of squares	*df*	Mean square	*F*	Sig
Between groups	40.896	5	8.179	8.637	0.000
Within groups	71.022	75	0.947		
Total	111.918	80			

Table V.
ANOVA test for significant differences among industry sectors on RK

These sectors do not often determine information security threats and vulnerabilities associated with each of the critical assets and functions, and only partly observe (monitor) state regulations. However, Financial Institutions, Public Utility companies and Others (IT, Oil and Gas, etc.) have processes in place to monitor state legislation or regulations applicable in their organizations.

4.3.2 RM and industry sectors.

H02. There are no significant differences in the levels of ISG RM implementation among industry sectors.

Table VI illustrated that there was a significant difference between the industry sectors as determined by one-way ANOVA ($N = 81$; $F_{(5, 75)} = 13.912$; $p < 0.05$). The effect size (f) was 0.48, which according to Cohen's (1988) conventions, is a medium effect. Therefore, the null hypothesis was not supported (reject the null hypothesis). This indicated that there were statistically significant differences in the levels of information security RM among the industry sectors. The multiple comparisons Games-Howell's post hoc test for conducting post hoc tests on a one-way ANOVA showed significant difference in the levels of RM implementation between the Financial Institutions and the Educational Institutions and Public Sector; Financial

Institutions and Health Care Sector; and Others (IT, Oil and Gas, Manufacturing) and Educational institutions.

Specifically, Financial Institutions and Public Utilities have appointed personnel with primary duty and responsibility for information security (security architecture, compliance, processes, audits, disaster recovery); ensured that security staff had the necessary professional qualifications; instituted ongoing security training program; and had official information security architecture, which was reviewed regularly. On the other hand, Health Care Sector, Public Service Sector and Educational Institutions do not have RM put in place or only *PI* ISG.

4.3.3 VD and industry sectors.

H03. There are no significant differences in the levels of ISG VD implementation among industry sectors.

The one-way ANOVA revealed a statistical significant difference between the industry sectors ($F_{(5,\ 75)} = 4.941$; $p < 0.01$) (see Table VII). The effect size (f) was 0.28, which according to Cohen's (1988) conventions is a small to medium effect. Therefore, the null hypothesis was not supported. The multiple comparisons Games-Howell post hoc test for conducting post hoc tests on a one-way ANOVA where equal variances could not be assumed was conducted. The result showed significant differences in the levels of VD between the Financial Institutions, Educational Institutions and the Public Service Sector.

The Public Service Sector, Health Care Sector and Educational Institutions do not or only partially derive value from security investment. This can be attributed to inadequate implementation of RK and RM, as VD is an outcome of effective implementation of both RK and RM.

4.3.4 Performance measurement and industry sectors.

H04. There are no significant differences in the levels of ISG PM implementation among industry sectors.

Table VIII showed that there was a statistically significant difference between the industry sectors' ISG PM as determined by a one-way ANOVA ($N = 81$; $F_{(5,\ 75)} = 6.323$; $p < 0.05$). The effect size (f) was 0.30, which is a small to medium effect according to Cohen's (1988) conventions. As a result, the null hypothesis was rejected. Games-Howell post hoc test showed that there was a significant difference in the levels of PM between

Table VI. ANOVA Test for significant differences between industry sectors on RM

	Summation of squares	*df*	Mean square	*F*	Sig
Between groups	55.425	5	11.085	13.912	0.000
Within groups	59.761	75	0.797		
Total	115.186	80			

Table VII. ANOVA test for significant differences between industry Sectors on VD

	Summation of squares	*df*	Mean square	*F*	Sig
Between groups	25.399	5	5.080	4.941	0.001
Within groups	77.103	75	1.028		
Total	102.502	80			

the Financial Institutions, Educational Sector, Public Service Sector and Health Care Sector.

Again, the Public Service Sector, Health Care Sector and Educational Institutions do not or only partially have effective security performance measurement processes put in place. Unlike the Financial Institutions and Public Utilities, Public Service Sector, Health Care Sector and Educational Institutions do not periodically test and evaluate their information security programs, nor conduct a periodic independent audit of their information security program to ensure they are in compliance with standard information security framework and related information security policies, standards, procedures, guidelines and best practices.

4.3.5 SA and industry sectors.

H05. There are no significant differences in the levels of ISG SA implementation among industry sectors.

Table IX showed that there was a statistically significant difference between the industry sectors as determined by one-way ANOVA ($N = 81$; $F_{(5,\ 75)} = 8.234$; $p < 0.05$). The effect size (f) was 0.35, which according to Cohen's (1988) conventions is a medium to large effect. Therefore, the null hypothesis was not supported. Games-Howell post hoc test showed that there was a significant difference in the levels of SA between the Financial Institutions, Educational Institutions, Public Services and Health Care Institutions.

Notably, Financial Institutions and Public Utilities apparently put in place information security strategy that considered inputs from the stakeholders, provided a clear statement of how security supports enterprise mission and strategy, instituted security awareness and training programs for enhancing information security acceptance and ensured that executive management were responsibility for the state of the enterprise information security.

Among the five focus areas, Financial Institutions and Public Utilities recorded the highest scores on the SA. This may account for their generally higher performance over all the other industry sectors. This finding is consistent with the study that found SA as pivotal in ISG implementation, which is positively related to RK, RM, PM and VD (Bowen *et al.*, 2007).

Table VIII.
ANOVA test for significant differences between industry sectors on PM

	Summation of squares	*df*	Mean square	*F*	Sig
Between groups	41.434	5	8.287	6.323	0.000
Within groups	98.299	75	1.311		
Total	139.733	80			

Table IX.
ANOVA test for significant differences between industry sectors on strategic alignment

	Summation of squares	*df*	Mean square	*F*	Sig
Between groups	36.533	5	7.307	8.234	0.000
Within groups	66.550	75	0.887		
Total	103.082	80			

5. Discussion

In all, the Financial Institutions had the highest level of ISG implementation. This can be attributed to laws and regulations made by the inspection bodies, such as the central bank, that control the operations and activities of the financial sector. Banks and other financial institutions are under strict compliance reporting with specific laws that make them strengthen internal controls. In addition, the alarming spade of cyber crime in the sub-Saharan Africa (Modern Ghana, 2009) may have necessitated the financial institutions to take strict measures to protect their IT systems and sensitive data from possible security breaches.

Likewise, the Public Utility companies (electricity, water and telecommunication services) regularly process personally identifiable data of their customers and generate reports that are mission-critical and crucial for competitiveness that need to be protected. It is, therefore, not surprising that Public Utility companies endeavor to maximize the implementation of ISG to meet privacy requirements. Also, it is evident that Other Sectors (IT, Oil and Gas, Manufacturing) have made some effort to put in place ISG. This may be as a result of attempt by these industries to comply with industry standards, which in most cases are not enforced.

The Public Service and Health Care Sectors provide services on behalf of the government to the citizens. They, therefore, depend on the central government for budget allocations to handle issues relating to information security. The government of Ghana recently established an agency, NITA (National Information Technology Agency), to be responsible for implementing Ghana's IT policies with the mandate to identify, promote and develop innovative technologies, standards, guidelines and practices among government agencies and local governments (National Information Technology Agency, N.I.T.A., 2010). Not surprising, many government establishments are at the PSs of ISG implementation.

Finally, the institutions of higher learning perform rather poorly on their ISG implementation. This may be attributed to the lack of enforcement of privacy and security laws in higher educational institutions. The National Accreditation Board (NAB), a body established to assess the tertiary institutions, has not been strict when it comes to assessing information security aspects of the operations of these institutions. To protect academic records, educational institutions should take immediate steps to put in place ISG in order to avoid security breaches and law suits. The NAB should adopt stricter measures on tertiary institutions to provide strong security to protect stakeholders' information.

6. Conclusions

This study assesses the levels of ISG implementation among major Ghanaian industry sectors with the intent of identifying the focus areas that require improvement. Six industry sectors: Educational Institutions, Public Utilities, Finance Institutions, Public Services, Health Care and Others (IT companies, Oil and Gas, Manufacturing) were rated to ascertain the level of ISG implementation through ISG focus areas, including RM, SA, PM, VD and RM in each industry sector. The ANOVA analyses showed that the null hypotheses were not supported, indicating that the level of ISG implementation differs significantly among the industry sectors.

As a whole, the industry sectors have PI ISG. In particular, ranking ISG implementation, Financial Institutions outperformed all the other sectors in each of the

five main focus areas, which were *CC* of ISG implementation, followed by Utility Companies and Other Sectors (IT, Oil and Gas, Manufacturing), which had *PI* ISG. The Health Care, Public Services and Educational Institutions were at the *PSs* of ISG implementation. Interestingly, institutions of higher learning perform poorly on their ISG implementation.

As with every research, this study was not without limitations. The response rate was low as a result of the sensitive nature of the study. Evidence suggested that when collecting data of sensitive nature, the researcher should expect very low response (Kotulic and Clark, 2004). Despite this limitation, the sample selection in this study cut broadly across the population subsets; as such, the study's findings could be generalized to the population. To provide a richer understanding and more balanced appraisal of the status of ISG in organizations, future work would involve a longitudinal study combining both qualitative and quantitative methods. Additionally, a similar research would be undertaken across different countries to establish a global benchmark for ISG.

References

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.

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

Anasimov, A. (2006), "Hierarchical model of organizational work in the sphere of information security", In Whitman, M.E. and Mattord, H.J. (1st Eds), *Readings and cases in the management of information security*, Course Technology, CENGAGE Learning, Mason, OH, pp. 129-136.

Bowen, P.L., Cheung, M. and Rohde, F.H. (2007), "Enhancing IT governance practices: a model and case study of an organization's efforts", *International Journal of Accounting Information Systems*, Vol. 8 No. 3, pp. 191-221.

Cohen, J. (1988), *Statistical Power Analysis for the Behavioral Sciences*, 2nd ed., Hillsdale, Lawrence Erlbaum, NJ.

Corporate Governance Task Force (2004), "Information security governance-a call to action", available at: www.educause.edu/library/resources/information-security-governance-call-action (accessed 10 January 2013).

Educause (2006), "Information security governance assessment tool", available at: www.educause.edu/library/resources/information-security-governance-assessment-tool (accessed 10 January 2013).

Electronic Transactions Act 772 (2008), "Ghana's electronic transaction Act 772", available at: www.unesco.org/new/fileadmin/multimedia/hq/ci/wpfd2009/pdf/ghana%20electronic-communications%20act%202008.pdf (accessed 12 January 2013).

El-Meligy, H. (2011), "IT governance, security and safety in developing countries", available at: www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?List=ef7cbc6d-9997-4b62-96a4-a36fb7e171af&ID=129 (accessed 12 December 2012).

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.

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.

ITGI (2006), "Information security governance: guidance for boards of directors and executive management", available at: www.isaca.org/Knowledge-Center/Research/Documents/InfoSecGuidanceDirectorsExecMgt.pdf (accessed 10 January 2013).

ITGI (2008), "Information security governance: guidance for information security managers", available at: www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Information-Security-Governance-Guidance-for-Information-Security-Managers.aspx (accessed 12 December 2012).

ITGI (2010), "COBIT 4.1 executive summary and framework", available at: www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf (accessed 10 January 2013).

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.

Khoo, B., Harris, P. and Hartman, S. (2010), "Information security governance of enterprise information systems: an approach to legislative compliant", *International Journal of Management and Information Systems*, Vol. 14 No. 3, pp. 49-55.

Kotulic, A.G. and Clark, J.G. (2004), "Why there aren't more information security research studies", *Information and Management*, Vol. 41 No. 5, pp. 597-607.

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, p. 22.

Modern Ghana (2009), "Ghana banned from use of credit cards", available at: www.modernghana.com/news/233766/1/ghana-banned-from-use-of-credit-cards.html (accessed 5 November 2012).

National Information Technology Agency, N.I.T.A. (2010), "Mandates of national information technology agency", available at: www.nita.gov.gh/section.aspx?id=1 (accessed 5 November 2012).

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

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

Pironti, J.P. (2007), "Developing metrics for effective information security governance", available at: www.isaca.org/Journal/Past-Issues/2007/Volume-2/Pages/Developing-Metrics-for-Effective-Information-Security-Governance1.aspx (accessed 12 December 2012).

Risk, I.T. (2009), "Enterprise risk: identify, govern and manage IT risk", available at: www.isaca.org/Journal/Past-Issues/2009/Volume-4/Pages/Identify-Govern-and-Manage-IT-Risk-Part-1-andnbsp-andnbsp-Risk-IT-Based-on-COBIT-Objectives-and-Pri.aspx (accessed 12 December 2012).

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.

Val, I.T. (2008), "Enterprise value: governance of IT investments-the Val IT framework 2.0", available at: www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Val-IT-Framework-2.0.aspx (accessed 12 December 2012).

Von Solms, B. (2006), "Information security-the fourth wave", *Computers and Security*, Vol. 25 No. 3, pp. 165-168.

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.

Wolfpack (2011), "The 2011 South African information security thermometer report", available at: www.wolfpackrisk.com/research/south-african-cyber-threat-barometer/ (accessed 5 November 2012).

About the author

Winfred Yaokumah is a Lecturer at the Department of Information Technology, Pentecost University College, Accra, Ghana. He obtained his PhD in Information Technology (2013) with specialization in Information Assurance and Security at the Capella University, USA. He earned his Master's degree in Computer Application Technology (2000) from the School of Computer Science and Engineering, Hohai University, China, and a Bachelor of Science degree in Computer Science (1994) from Kwame Nkrumah University of Science and Technology, Kumasi, Ghana. His research interest includes Information Security, Information Technology Governance, Information Security Governance and IT Leadership. Winfred Yaokumah can be contacted at: winfred91@gmail.com