A CONTEXTUAL MODEL TOWARDS UNDERSTANDING INFORMATION TECHNOLOGY GOVERNANCE PRINCIPLES, STRUCTURES AND MECHANISMS

WINFRED YAOKUMAH

Abstract

Although top executives depend on IT (information technology) to achieve strategic and operational goals and to meet legal and regulatory compliance, IT governance is often not well understood by the board of directors and executive management. The intent of this paper is to provide guidelines and understanding of the context of IT governance to organizational leaders. The study employs a qualitative examination of peer-reviewed journals, published documents, and IT practitioner sources containing IT standards and frameworks to (1) classify and discuss the high-level view of the inter-related components of IT governance, and (2) develop a contextual model of IT governance. The contextual model integrates corporate governance theories, IT governance mechanisms, and IT governance domains. The strength of this model is its simplicity, which is devoid of complexities that normally confound the boards of directors and top executives when implementing IT governance. Therefore, the model will provide guidance to the top executives and IT leaders the choices to initiate IT governance according to governance principles, IT governance mechanisms, statutory and regulatory compliance, and standard IT governance practices.

1 Introduction

Corporate executives depend on information to effectively perform corporate governance functions (von Solms, 2006). The board of directors and executive management can only make the right decisions for the enterprise when the financial and audit reports, which are generated from IT (information technology) systems, are accurate and reliable. Information technology involves the selection, creation, application, integration, and administration of computing technologies to meet the needs of organizations (Association of Computing Machinery and Institute of Electrical and Electronics Engineers [ACM-IEEE], 2008). Therefore, critical to corporate governance effectiveness is the information and the systems that process, store, and transmit such information. Thus, corporate governance relies on computing systems to obtain information for effective internal controls, ensure compliance, and for the generation of reliable information for strategic decision making.

According to von Solms (2006), information is the lifeblood of all organizations and core to all business processes; therefore, the information assets and systems (software, hardware, networks) upon which organizational leaders depend must be properly protected from risks, misuse, compromise, harm, or destruction. Consequently, the top executives must be responsible for governing IT resources within the organization. This view point is captured in the well-accepted definition of corporate governance as:

A set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly (ISACA, 2006, p. 1).

According to Weill, IT governance "is about systematically determining who makes each type of decision (a decision right), who has input to a decision (an input right) and how these people (or groups) are held accountable for their role" (2004:3). Comparing the definitions of corporate governance and IT governance, it can be observed that IT governance principles closely resemble corporate governance functions as both are carried out through some fundament key elements: oversight responsibility, enacting policy, account-ability, strategic planning, and resource allocation (Allen, 2006; Bergsma, 2011). Accordingly, good IT governance draws on corporate governance principles in determining roles and responsibilities within the organizational structure that govern IT assets, manages, and uses IT resources to realize corporate goals.

Therefore, for successful implementation of IT governance, the board of directors should establish ownership for IT within the organization. The boards must take board level action by setting direction, drive policy and strategy, provide resources, assign responsibilities, and set priorities. Also, senior level management should provide oversight for the development of a IT framework, policy development, assign roles and responsibilities, implement, monitor, ensure awareness and training (ISACA, 2006).

However, top executives can only effectively govern IT when they understand the context of IT governance. Wilkin and Chenhall (2010) remarked that IT risk is often not well understood by boards of directors and executive management although they depend on IT to achieve the strategic and operational goals of the organization. In a study cited by Beasley et al. (2007), 73% of top executives believe that organizations are faced with high risks emanating from IT and 27% of top executives do not understand enterprise risks.

The intent of this paper is to provide guidelines and understanding of the context of IT governance to organizations that want to adopt IT governance practices.

The study employed qualitative examination of peer-reviewed journals, published documents, and IT practitioner sources containing IT standards and frameworks to (1) identify, classify and discuss the high-level view of the inter-related components of IT governance, and (2) develop a contextual model of IT governance. The strength of this model is its simplicity, devoid of complexities that could confuse top executives when adopting IT governance, thus, providing guidance to executives on choices to initiate IT governance according to governance principles, IT governance mechanisms, statutory and regulatory compliance, and standard IT governance practices.

2 Proposed Information Technology Governance Contextual Model

The Contextual Model of IT Governance is classified into four layers (see Figure 2). At the highest level is Corporate Governance Theories (Layer 1) that present the overall strategic direction and control of information technology governance. This layer aligns IT governance with corporate governance (von Solms, 2006). The figure also consists of IT Governance (Layer 2), which are made up of models (centralized, decentralized, federal), processes (COBIT, ISO 27002, ITIL), relational mechanisms (strategic dialog, training, knowledge sharing, effective communication), and structures (consisting of boards of directors, chief executive officers, top management, IT executives, IT committees). The IT Governance Motivation (Layer 3) describes the motivation for IT governance practices, leading to IT Governance Domains (Layer 4), which are IT governance domains (focus) areas such as strategic alignment, resource management, risk management, performance measurement, and value delivery. Finally, the core of the model represents the benefits. Each layer of the model is presented and discussed in the following sections

2.1 Layer 1: Corporate Governance Theories

The Corporate Governance Theories layer describes the underlying corporate governance theories of IT Governance and provides mapping to IT governance domain areas (Layer 4) (see Figure 2). Though there are others, three governance theories are presented here, namely agency theory, stakeholder theory, and organizational theory.

2.1.1 Agency Theory

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. The theory has important application in governance of organizations and significant implications for IT governance. Firstly, the agency theory assumes that the basis of the organization is efficiency (Eisenhardt, 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 (i.e., performance measurement of IT governance domain).

Secondly, Yu and Mylopoulos (1994) proposed three different levels of agency relationship: general, committed, and critical. The three levels of agency theory is 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). These levels guide organizations to make conscious efforts to minimize risks (i.e., risk management domain of IT governance) associated with organizational information assets (see Figure 2).

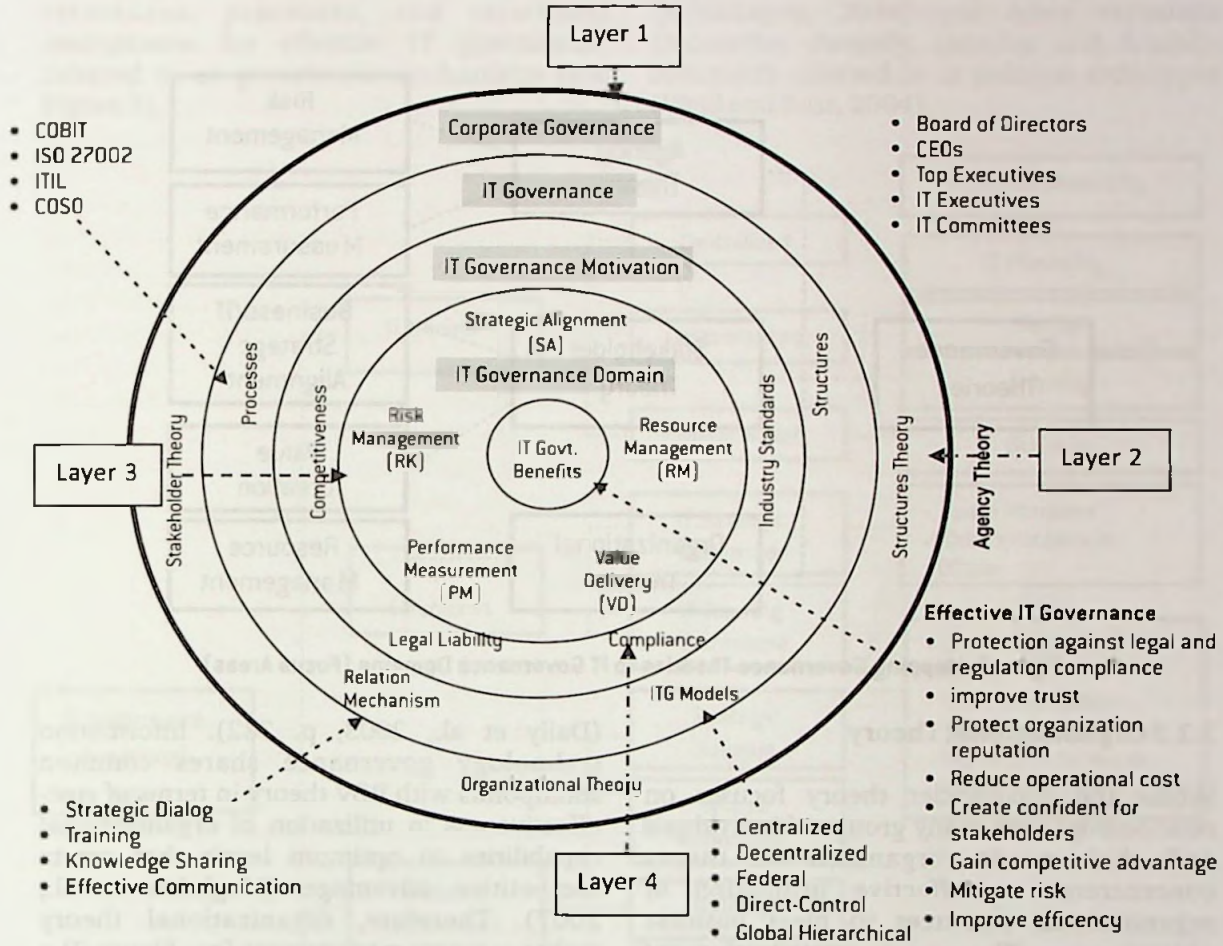

Figure 2. Contextual Model of IT Governance

2.1.2 Stakeholder Theory

With respect to good corporate governance, the stakeholder theory attempts to address various groups of stakeholders (suppliers, investors, customers, political groups, employees, communities, government, and trade associations) deserving and requiring management's attention (Sundaram and Inkpen, 2004) and looking forward to obtain benefits (Donaldson and Preston, 1995). According to Clarkson (1995), the stakeholder theory is considered as a system where there are stakeholders and the purpose of the organization is to create wealth (value) for its stakeholders. Therefore, value creation is a focus area of corporate governance practices, but the firm can maximize value if it considers

the interests of its stakeholders. Moreover, the stakeholder theory improves alignment of stakeholders' interest with organizational goals. Moghdeb et al. (2007) noted that aligning key stakeholders' concerns with business objectives can have a positive impact on the results of the organizational performance. Thus, the stakeholder theory also involves alignment creation with the stakeholders to influence the achievement of the organ-ization's objectives (see Figure 2).

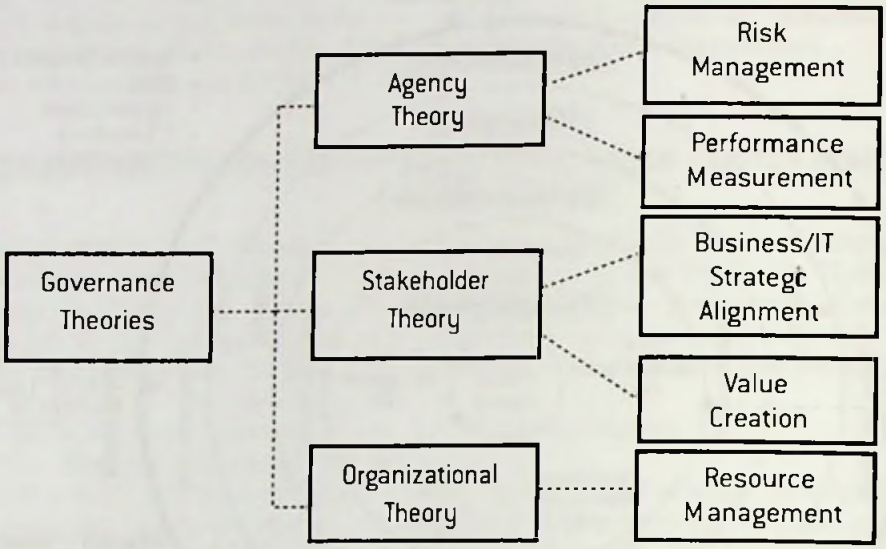

Figure 2. **Mapping Governance Theories to IT Governance Domains (Focus Areas)**

2.1.3 Organizational Theory

Whilst the stakeholder theory focuses on relationships with many groups of individuals and their needs, organizational theory concentrates on effective utilization of organizational resources to meet business objectives. The most contribution of organizational theory relevant to IT 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 et al., 2000). Organizations are viewed as a pool of human resources, capabilities, and competencies. In this respect, governance is considered as the "determination of the broad uses to which organizational resources would be deployed" (Daily et al., 2003, p. 382). Information technology governance shares common standpoints with RBV theory in terms of cost-effectiveness in utilization of organizational capabilities to optimum levels that create competitive advantage (Moghdeb et al., 2007). Therefore, organizational theory makes resource management (see Figure 2) a core corporate governance practice in organizations.

2.2 Layer 2: IT Governance Models and Mechanisms

Managing information technology functions is a challenging and complex task as a result of constant changes in business needs, rapid technological changes (Sandrino-Arndt, 2008). This requires top management to

utilize IT models and governance mechanism to facilitate governance of IT related functions. Weill and Ross (2004) put forward IT governance models and De Haes and van Grembergen (2004) proposed a mixture of structures, processes, and relational mechanisms for effective IT governance, referred to as governance mechanisms (see Figure 3).

2.2.1 IT Governance Models

Information technology literature identifies three IT governance models: centralized, decentralized, federal governance models (Hvalshagen, 2004) and other variations (monarchy, duopoly, anarchy, and feudal), commonly referred to as political archetypes (Weill and Ross, 2004).

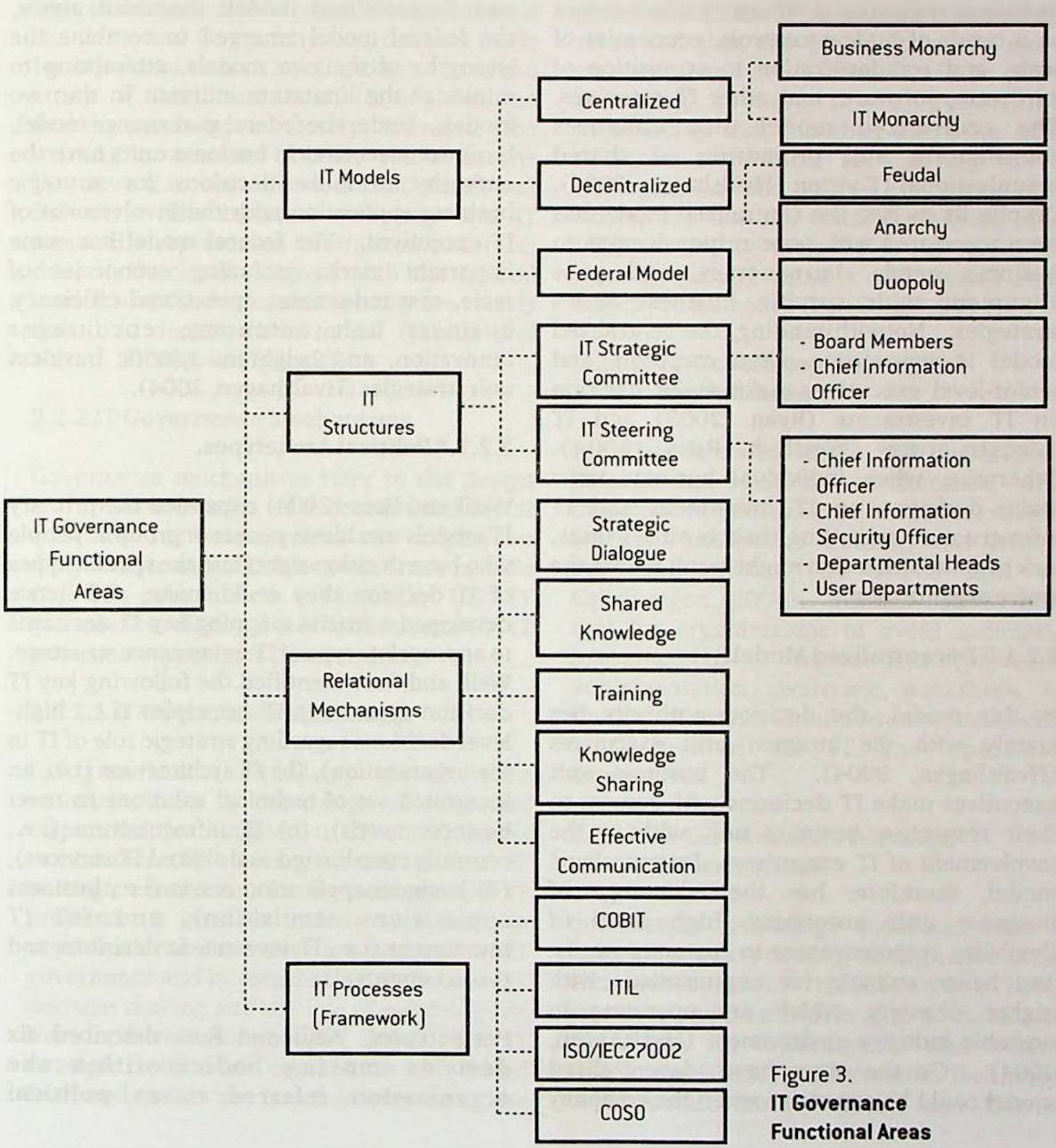

Figure 3.
IT Governance Functional Areas

2.2.1.1 **Centralized Model.**

Under the centralized model, decision authority rests on the corporate IT executives or central IT organizational body (Brown and Nasuti, 2005). The model suggests that all IT decisions, which affect the entire organization, should be made by a centralized body. The benefits of the centralized model include organizational efficiency which comes as a result of budget controls, economies of scale, and standardization in acquisition of hardware, software, and other IT resources. The centralized model also enhances coordination and promotion of shared organizational IT vision (Hvalshagen, 2004). Despite its merits, the centralized model has been associated with poor responsiveness to business needs, bureaucracy, and poor alignment with specific business unit's strategies. Notwithstanding, the centralized model is appropriate when corporate and senior-level executives make major decision on IT investments (Ryan, 2005) and IT infrastructure (Weill & Ross, 2004). Otherwise, when individual business units make decisions on IT investment and IT infrastructure regarding their business units, lack of standardization might result within the entire organization.

2.2.1.2 **Decentralized Model.**

In this model, the decision authority lies mainly with the business unit executives (Hvalshagen, 2004). The business unit executives make IT decisions with respect to their respective business unit without the involvement of IT executives. Decentralized model, therefore, has the advantage of business unit autonomy, high level of flexibility, responsiveness to customer needs, and hence suitable for organizations with higher diversity, which are operating in unstable industry environment (Hvalshagen, 2004). On the other hand, decentralized model could be expensive when the company introduces new technology supposed to permeate the entire organization. Thus, lack of standardization could hinder deployment of integrated systems such as enterprise resource planning (ERP).

2.2.1.3 **Federal Model.**

Considering the limitations of both centralized and decentralized models discussed above, the federal model emerged to combine the strengths of the two models, attempting to minimize the limitation inherent in the two models. Under the federal governance model, business executives in business units have the authority to make decisions for strategic business application with the involvement of IT executives. The federal model has some important merits including economies of scale, cost reductions, operational efficiency, business unit autonomy, encourages innovation, and heightens specific business unit strategies (Hvalshagen, 2004).

2.2.1.4 **Political Archetypes.**

Weill and Ross (2004) expanded the primary IT models to address people or group of people who have decision rights and the specific types of IT decision they could make, and hence developed a matrix mapping key IT decisions to appropriate type of IT governance structure. Weill and Ross identified the following key IT decision types: (a) IT principles (i.e., high-level decisions regarding strategic role of IT in the organization), (b) IT architecture (i.e., an integrated set of technical solutions to meet business needs), (c) IT infrastructure (i.e., centrally coordinated and shared IT services), (d) business application needs (i.e., business applications acquisition), and (e) IT investment (i.e., IT investment decisions and project approval).

Furthermore, Weill and Ross described six decision making bodies within the organization referred to as political

archetypes: (a) business monarchy (i.e., mainly senior business executives and may include chief information officer), (b) IT monarchy (i.e., individual or group of IT executives), (c) federal (i.e., business executives and representatives, with IT involvement), (d) IT duopoly (i.e., decision making involves IT executives and a group of business leaders), (e) feudal (i.e., business unit making decisions based on the needs of the unit), and (f) anarchy (i.e., decision made by individual user or small group). A careful study of Weill and Ross' (2004) decision making archetypes closely mirrored the existing governance models found in the literature (i.e., centralized, decentralized, and federal). The business monarchy and IT monarchy represented centralized structure; duopoly is closely aligned with the federal model; and the feudal and anarchy are closely linked to decentralized model (Brown and Nasuti, 2005) (see Figure 3).

2.2.2 IT Governance Mechanisms

Governance mechanisms refer to the design and implementation of a coordinated set of activities that management can employ on daily basis to meet IT objectives. These include (1) IT governance structures, (2) IT governance relational mechanisms, and (3) IT governance processes (frameworks).

2.2.2.1 IT Governance Structures.

Information technology governance structures refer to the design of roles and responsibilities assigned to IT and business committees (IT steering committee and IT strategic committee) for overseeing major IT projects. It involves making sure that the organizational executives are engaged in IT governance and by establishing the locus of IT decision making and the line of reporting (de Haes and van Grembergen, 2004). The IT strategic committee operates at the board level and assists the board in overseeing the organization's IT-related matters. The IT steering committee operates at executive level and has specific responsibility for overseeing various major IT projects; manage IT priorities, costs, resource allocation, and making sure that IT policies are understood throughout the organization (de Haes and van Grembergen, 2004). An important issue, therefore, is the executive participation in IT governance. De Haes and van Grembergen remarked that the board, business and IT management have a crucial role to play in ensuring success of IT governance, maintaining that the chief executive officer (CEO) is responsible for carrying out the strategic plans and policies established by the board, and that the chief information officer (CIO) should be included in the senior-level decision-making process and should report directly to the board (von Solms, 2004).

2.2.2.2 IT Governance Relational Mechanisms.

A critical factor in aligning IT to business is through the relational mechanisms, which include strategic dialogue, shared knowledge, training, knowledge sharing, and effective communication (de Haes and van Grembergen, 2004). Anthes (2005) noted that for organizations to avoid anticipated resistance to IT frameworks (processes) implementation, awareness, workshops, and training programs should be instituted, which must involve the IT and operations departments.

2.2.2.3 IT Governance Processes (Frameworks).

Information technology processes refer to strategic decision making through monitoring and performance measurement tools, processes and frameworks such as the Control Objectives for Information and related Technology (COBIT), Information Technology Infrastructure Library (ITIL), and ISO/IEC

27002 (de Haes and van Grembergen, 2009). Information Technology Governance Institute (ITGI, 2008) observed that, in an environment of increasing regulatory controls, adopting IT frameworks, standards and best practices helps organizations to adhere to regulatory compliance, realize value from IT investments and IT services, and benefit from increased efficiency; thereby reduce costs and limit risks.

2.2.2.3.1 **ISO/IEC 27002 Framework.**

ISO/IEC 27002 is an international security standard that provides guideline for implementing information security within an organization (ITGI, 2008). The focus of ISO/IEC 27002 is to improve information security practices in an organization and can be used to create information security policies, procedures, assignment of roles and responsibilities, documentation of operational procedures, and risk manage-ment (Myler and Broadbent, 2006). ISO/ IEC 27002 ensures business continuity, compliance with legal, and audit control. ISO/IEC 27002 contains implementation guidelines consisting of the following: risk assessments, security policy, asset inventory, accountability, physical security, operating procedures, access controls, business continuity, and compliance (Myler and Broadbent, 2006). Each domain is built around topics regarding administration, technical, and physical measures and are driven from top to down (strategic to operational level) on the organization levels.

2.2.2.3.2 **COBIT Framework.**

COBIT framework is a set of best practices for IT governance and management. COBIT is an internationally accepted IT governance framework and management guideline based on industry best practices and standard (Lachapelle, 2007; Sahibudin et al., 2008). COBIT ensures alignment between IT and business goals, manages IT-related risks, and ensures compliance, business continuity and security (ITGI, 2008). COBIT framework supports IT governance and ensures that IT and business objectives are aligned, maximizing return on IT investment, and managing IT-related risks and opportunities (ITGI, 2008; ITGI, 2010).

2.2.2.3.3 **ITIL Framework.**

Information Technology Infrastructure Library (ITIL) was purposely developed to serve as a standard for IT service management (ITGI, 2010). It is the most "widely accepted approach to IT service management in the world and provides a cohesive set of best practice, drawn from the public and private sectors internationally" (ITGI, 2010). ITIL framework consists of service support, service delivery, security management, ICT infrastructure manage-ment, applications management, and the business perspective. The main goal of ITIL is to provide a vendor-independent approach for service management and the philosophy behind the "development was the recognition of increased dependence on IT, which has to be managed by high quality IT services" (ITGI, 2010, p. 14).

2.2.2.3.4 **Assessing IT Governance Frameworks.**

The information technology related frameworks developed to enhance IT governance cover IT governance, information security, and IT operations and services (Schlarman, 2007). ISO/IEC 27002 focuses on organizational, administrative, security implementation and certification aspects of IT security and COBIT concen-trates on IT governance (Saint-Germain, 2005). ISO/IEC 27002 is much more detailed and provides direct guidelines on 'how' things should be done while COBIT focuses on IT governance and addresses 'what' must be done, and ITIL is strong in IT-service management.

2.3 Layer 3 IT Governance Motivation

The factors that motivated the adoption of IT governance efforts in organizations were noted in the IT governance literature (Bowen et al., 2007; Herath et al., 2010; Pironti, 2006). Studies found regulatory compliance, legal liability, and protection of the organization's reputation (CSI, 2010; von Solms, 2006), business objectives, and prevalence of security threats (Jirasek, 2011). Legal and regulatory compliance include Sarbanes-Oxley (SOX), Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Billey Act(GLBA) all of USA; Basel II of EU; Data Protection Act of 1998 of UK, and Electronic Transaction Act 772 of Ghana. Table 1 summarizes some key legislation that impacted IT governance practices in organizations.

Table 1: **Some Regulations Influencing IT Governance Adoption**

Legislations	Target Area	Country
Sarbanes-Oxley (SOX) Act of 2002	Financial Reporting & Governance (impacting IT security systems, practices and controls)	USA
Health Insurance Portability and Accountability Act (HIPAA)	Privacy and Security	USA
Federal Information Security Management Act (FISMA)	Protecting information and systems	USA
FACTA; Gramm-Leach-Bliley Act (GLBA)	Privacy	USA
Combines Code on Corporate Governance; Financial Services and Markets Acts	Financial Reporting & Governance	UK
Data Protection Act of 1998	Privacy	UK
Basel II	Financial Reporting & Governance	EU
Data Privacy Laws	Privacy	EU
Electronic Transaction Act 772 of 2008	Security of Electronic records	Ghana
PROATIA (Promotion of Access to Information Act) Act of 2000	Access to Electronic records	South Africa
ECT (Electronic Communications and Transactions) Act of 2002	Prevent abuse of information systems	South Africa
KING III Code of Governance for SA 2009	Information Governance	South Africa

2.4 Layer 4: IT Governance Domain

For information IT governance to be effectively practiced in organizations, ITGI (2006) observed that it has to be evident in its five critical domain areas: (a) strategic alignment (i.e., aligning information technology with the business), (b) value delivery (i.e., cost optimization and proving the value of information technology), (c) risk management (i.e., safeguarding of information technology assets, disaster recovering, and business continuity), (d) resource management (i.e., optimizing knowledge and information technology infrastructure), and (e) performance measurement (i.e., tracking project delivery and monitoring information technology services) (see Figure 4).

2.4.1 Business/IT Strategic Alignment.

Strategic alignment is generally regarded as a critical success factor for organizations' IT effectiveness and assumes one of the most important issues for IT executives (Luftman and Kampaiah, 2008). Strategic business and information technology alignment ensure that IT investments support business needs, integrate with existing architectures, and facilitate business processes (Law and Ngai, 2007) in order to create business value (O'Donnell, 2005). Wilkin and Chenhall (2010) remarked that when IT strategy and plans are aligned with strategic business goals IT would provide capabilities that deliver business value.

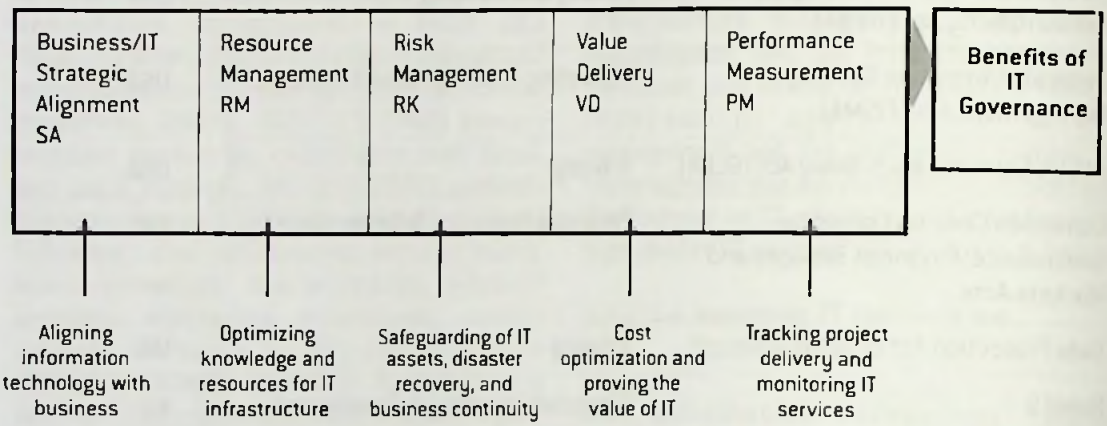

Figure 4: **IT Governance Domain Areas**

2.4.2 Resource Management.

An important factor in successful IT programs is the organization's ability to effectively develop and manage IT capabilities (Peppard and Ward, 2004). IT resource management includes managing people, skills, processes, and technologies for the purpose of enhancing efficiency and effectiveness of business solutions. IT resource management can be achieved through formulation, enactment, and adherence to processes, budgets, and tactical plans for applying IT strategies to support, enhance, and complement business strategies (Wilkin and Chenhall, 2010).

2.4.3 Risk Management Domain.

Enterprise risk management as a process, effected by the entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise,

designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives (Beasley et al., 2007). IT risk could create formidable challenges to meeting strategic goals and objectives or the organization (Risk IT, 2009). Therefore, IT risks must be managed appropriately.

2.4.4 **Value Delivery Domain.**

Val IT (2008) defined value as the "total life-cycle benefits net of related costs, adjusted for risk and (in the case of financial value) for the time value of money" (p. 10). Value delivery pertains to optimization of IT investments in support of organizational goals (ITGI, 2008). The goals of IT governance value delivery is to ensure that IT services are available as required, there is minimal interruption to IT services, automated business transaction and exchanges can be trusted, and cost-effective plans for critical IT risk can be maintained (ITGI, 2006).

2.4.5 **Performance Measurement.**

Performance measurement involves quantifying, monitoring, and reporting on the performance of IT processes and related activities to ensure that organizational objectives are achieved (ITGI, 2008). Performance measurement is very important in evaluating IT operational performance and value (Schwarz and Hirschheim, 2003). It relates to IT project success (Bowen et al., 2007) with increased recognition of the need to measure not just tangible assets but also intangible assets that often defy financial measurement (Sveiby, 1997).

3 Discussion

Being motivated mainly by legal and regulatory compliance (Layer 3 of Figure 1), organizations are giving serious thoughts to governing IT from the board level. Von Solms (2006) and ITGI (2010) note that organizations can derive maximum benefits from IT resources, if IT is governed from the board to the operational level (top-down). IT governance offers organizations many benefits, including gaining competitive advantage, reduction of operational cost, protection against legal and regulatory compliance, improved customer trust, creating stakeholder confidence, protection of organizational reputation, mitigation of IT risks, and improved efficiency (see Layer 5 of Figure 1). Therefore, IT functions are no more merely a technical operational and management issue, but governance concern. Layer 1 of Figure 1 showed how corporate governance spans IT governance.

The theories that underpin corporate governance directly reflect IT governance domain (focus) areas. The agency theory maps to IT risk management and performance measurement, stakeholder theory maps to business/IT strategic alignment and IT value delivery, and organizational theory maps to IT resource management. Unlike other functional units on the organization, IT cuts across every organizational unit and functions, involving the boards of directors, the top executive management, all heads of departments, and user operational staff. Indeed, governing IT across an entire organization would require putting specific governance mechanisms in place. Layer 2 of Figure 1 showed the governance structures - IT strategic committees (operate at board level), IT steering committee (operate at top management level) (Huang et al. (2010), and the reporting lines of the chief information officer (IT leader). Von Solms (2005) suggested that the IT leader should report to the chief executive officer.

In addition, organizations must select governance models based on the nature of their operations. In many cases, a mixture of

models is recommended. The centralized model comprises business monarchy and IT monarchy; federal model consists of duopoly, and decentralized model contains the feudal and anarchy. Organizations should permit various decision making structures within the models to make appropriate decisions on IT. Decisions about IT principles and IT investments should be made by business monarchy; decision regarding IT architecture and IT infrastructure should be taken by IT monarchy; and decision on business applications should be taken by federal archetype.

Moreover, for management of day-to-day IT operations and processes, the top executive management must choose tested IT frameworks and standards: COBIT for IT governance; ITIL for IT-service manage-ment; and ISO/IEC 27002 for information security. To bind all the components together is the relational mechanisms (e.g., effective communication, strategic dialog, training and workshops, knowledge sharing). IT governance would then be evident within its domain (focus) area to reap the desired results (see Figure 4).

4 Conclusions

Based on the corporate governance theories, the conceptual model of IT governance offers a high-level integrated view of IT governance. Existing works discussed IT governance principles, models, and mechanisms in isolation, creating the need to provide an integral model that offers the top executives, who are generally non IT experts, understanding of how IT governance components relate together. This paper identified, classified and discussed the high-level view of the inter-related components of IT governance, and developed a contextual model of IT governance. The model provided a simplistic view, devoid of complexities that could confuse the board of directors and executive management when adopting IT governance; offering them guidance on choices to initiate IT governance according to governance principles, IT governance mechanisms, statutory and regulatory compliance, and standard IT governance practices. The model, however, did not provide details on how to implement IT governance; further work would focus on how organizations should implement IT governance.

References

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

Ali, S. and Green, P. (2007), "IT governance mechanisms in public sector organizations: An Australian context", *Journal of Global Information Management*, Vol. 15 No. 4, pp. 41-63.

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.

Anthes, G. H. (2005), "Catches on". *Computerworld, Vol.39 No.* 44, pp.39–41.

Association for Computing Machinery (ACM) and IEEE Computer Society (2008), "Curriculum Guidelines for Undergraduate Degree Programs in Information Technology", available at: http://www.acm.org [accessed 8 January 2013].

Beasley, M. S., Frigo, M. L. and Litman, J. (2007), "Strategic risk management: Creating and protecting value", *Strategic Finance*, Vol. *88 No.* 11, pp. 24-32.

Bergsma, K. (2011), "Information security governance", **available at:** http://www.educause.edu **[accessed 8 January 2013].**

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.

Brown, W. C. and Nasuti, F. (2005), "Sarbanes-Oxley and enterprise security: IT governance - what it takes to get the job done". *Information Systems Security, Vol. 14 No.* 5, pp. 15–28.

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.

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 van Grembergen, W. (2004), "IT Governance and its mechanisms", *Information Systems Control Journal,* Vol. 1.

De Haes, S. and van 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.

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.

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

Herath, T., Herath, H. and Bremser, W. G. (2010). "Balanced scorecard implementation of security Strategies: A framework for IT security performance management", *Information Systems Management*, Vol. 27 No. 1, pp. 72-81.

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.

Huang, R., Zmud, R. W. and Price, R. L. (2010), "Influencing the effectiveness of IT governance practices through steering committees and communication policies", *European Journal of Information Systems,* Vol. 19 No. 3, pp. 288-302.

Hvalshagen, M. (2004), "Transforming the IT organization for the state of Virginia", *Information Systems Management*, Vol. 21 No. 4, pp. 52-61.

ISACA (2006), "Information security governance: Guidance for boards of directors and executive management", available at: https://www.isaca.org [accessed 20 January 2013].

ITGI (2006), *Information security governance: Guidance for boards of directors and executive management* (2nd ed.), *available at:* www.itgi.org [accessed 20 January 2013].

ITGI (2008), "Aligning COBIT 4.1, ITIL v3 and ISO/IEC 27002 for business benefit", available at: www.itgi.org [accessed 20 January 2013].

ITGI (2010), "COBIT 4.1 Executive summary and framework", available at: www.isaca.org [accessed 20 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.

Jirasek, V. (2011), "Practical application of information security models", *Information Security Technical Report,* Vol. 17 No. 2, pp. 1-8.

Lachapelle, E. (2007), *Control Objectives for Information and related Technology*, Veridion Inc., Montreal, Canada.

Law, C. C. H. and Ngai, E. W. T. (2007), "ERP systems adoption: An exploratory study of the organizational factors and impacts of

ERP success", *Information & Management,* Vol. 44 No. 4, pp. 418–432.

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

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.

Myler, E. and Broadbent, G. (2006), "ISO 17799: Standard for security", *Information Management Journal, Vol. 40 No.* 6, pp. 43-52.

O'Donnell, E. (2005), "Enterprise risk management: A systems-thinking framework for the event identification phase", *International Journal of Accounting Information Systems,* Vol. 6 No 3, pp. 177–195.

Peppard, J. and Ward, J. (2004), "Beyond strategic information systems: Towards an IS capability", *The Journal of Strategic Information Systems,* Vol. 2, pp. 167–194.

Pironti, J. P. (2006), "Information security governance: Motivation, benefits and outcomes", available at: www. isaca.org [accessed 10 January 2013]..

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

Ryan, L. V. (2005), "Corporate governance and business ethics in North America: The state of the art", *Business and Society*, Vol. 44 No. 1, pp. 40–73.

Sahibudin, S., Sharifi, M. and Ayat, M. (2008), "Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations", *IEEE Computer Society.*

Saint-Germain, R. (2005), "Information security management best practice based on ISO/IEC 17799", *Information Management Journal, Vol. 39 No.* 4, pp. 60–65.

Sandrino-Arndt, B. (2008), "People, portfolios and processes: The 3P model of IT governance", *Information System Control Journal,* Vol. 2, pp. 36-39.

Schlarman, S. (2007), "Selecting an IT control framework", *Information Systems Security*, Vol. 16 No. 3, pp. 147–151.

Schwarz, A. and Hirschheim, R. (2003), "An extended platform logic perspective of IT governance: Managing perceptions and activities of IT", *The Journal of Strategic Information Systems,* Vol. 12 No. 2, pp. 129–166.

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

Sveiby, K.E. (1997), *The new organizational wealth: Managing & measuring knowledge-based assets,* Berret-Koehler Publishers, San Francisco, CA.

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].

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

Von Solms S.H.B. (2005), "**Information security governance - compliance management vs operational management",** *Computers & Security*, Vol. *24 No. 6, pp. 443-447.*

Von Solms, B. (2005). "Information security governance: COBIT or ISO 17799 or both?", *Computers & Security,* Vol. 24 No. 2, pp. 99-104.

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

Weill, P. (2004), "Don't just lead govern: How top-performing firms govern IT", *MIS Quarterly,* Vol. 3 No. 1, pp. 1-17.

Weill, P. and Ross, J. W. (2004), "A matrix approach to designing IT governance", *Sloan Management Review,* Vol. 46 No. 2, pp. 26-34.

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.

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.

ABOUT THE AUTHOR

Dr. Winfred Yaokumah

He is currently the Dean of the Faculty of Engineering, Science and Computing(FESAC) at the Pentecost University College (PUC). He is also an Adjunct Lecturer at the PUC Graduate School. He could be reached on: wyaokumah@pentvars.edu.gh and 024 428 3488.