The board and IT governance: The what, who and how

S. Posthumus
Nelson Mandela Metropolitan University, Republic of South Africa
Shaun.Posthumus@za.pwc.com

R. von Solms*
Nelson Mandela Metropolitan University, Republic of South Africa
Rossouw.VonSolms@nmmu.ac.za

M. King
MEK Corporate Consultants, Republic of South Africa
mking@brait.com

Received November 2009

This paper discusses the importance of corporate governance and the need to implement it effectively in any organization. Furthermore, information technology is discussed along with its impact on enabling an organization to achieve its business goals and attain a competitive edge in industry. This makes IT a critical organizational resource with great strategic impact and necessitates that it be governed effectively through sound IT governance efforts. However, currently there seems to be a significant lack of board-level understanding with respect to the impact of IT on the business and therefore IT may not be adequately directed and controlled. To address this problem, a model is proposed in this paper to enable the board of an organization to develop an understanding of how to issue directives and implement effective control over IT so that IT supports organizational business goals and continues to provide value to an organization.

*To whom all correspondence should be addressed.

Introduction

Most organizations today depend on IT to support and enable business processes and attain a competitive edge, it is crucial that they devote the same level of attention to IT issues as they would to matters of finance and general corporate governance (IT Governance Institute, 2005c). Thus, due to the critical nature of IT within many organizations, a board should extend its strategic directing and controlling responsibility (said to be a fundamental principle of corporate governance) into IT through a system of IT governance in order to ensure that it supports its organization's corporate vision and mission.

Even though many organizations understand the necessity of implementing some form of IT governance, a large majority of organizations have not yet achieved adequate control over IT (Hardy, 2006). Even with comprehensive control frameworks such as COBIT in existence IT governance remains a challenge.

Nolan and McFarlan (2005) also states that most boards have not yet achieved adequate control over IT and are quite ignorant when it comes to IT spending and strategy. Even though corporate information assets have the potential to account for more than 50% of corporate capital expenditure, a large proportion of boards are inclined to rely on a collection of tacit or explicit rules based on best practices implemented by other organizations. The fact is that very few boards actually comprehend the degree to which their organizations are operationally reliant on IT systems or the degree to which IT participates in developing their organizations' business strategies. A reason for this may be because that at present there are no standards for IT governance (Nolan & McFarlan, 2005).

Corporate boards often do not have the essential knowledge required to ask intelligent questions about IT risk and expense. Ultimately, such a lack of board-level insight about IT is unsafe because this places organizations at great risk in much the same way as not properly auditing its books would (Nolan & McFarlan, 2005). Hardy (2006) states that "busy executives and board members need more specific guidance on how to achieve the vaunted goal of effective control". Hence Nolan and McFarlan (2005:98) state: "The question is no longer whether the board should be involved in IT decisions; the question is, how?" This is exactly the question addressed in this paper.

The objective of this paper is to provide the board of an organization with some guidelines on how to practice effective governance, i.e. directing and controlling, of information and related IT resources. These guidelines will be presented in the form of; WHAT should be addressed by the board, WHO should be involved in addressing these aspects and HOW should they be addressed.

The layout of this paper will be dictated by the main argument followed. At first, a brief introduction to corporate governance is provided with the Triple Bottom Line explained. It will be highlighted that few organizations can function effectively today without sound governance principles. Secondly, the value and criticality of information and IT resources in most modern organizations is emphasized. Based on this critical role that IT plays today, IT governance is defined and some key focus areas of modern day IT governance are identified and motivated. The next section will identify a number of key aspects critical to the board of an organization, i.e. the key focus areas related to IT that every board should address. How to determine the IT strategic mode of the organization and *what* should be done by *who* and *how* related to IT governance. Next, these key aspects are presented by means of a model, called the WHAT, WHO and HOW of IT Governance Model. A final conclusion will follow as an epilogue to the paper.

Corporate governance

Corporate governance is generally accepted as the responsibility of the board of directors and is the 'system' that determines how an organization is generally directed and controlled.

Corporate governance defined

In the document; *Corporate Governance: A Framework for Implementation*, Sir Adrian Cadbury stated that "corporate governance is concerned with holding the balance between economic and social goals and between individual and communal goals ... the aim is to align as nearly as possible the interests of individuals, corporations and society" (World Bank Group, 1999:6). This statement suggests that corporate governance involves continuously weighing the interests of an organization's stakeholders against the demands of society. Engaging in this task can be challenging since there are many issues that organizations should consider in order to operate effectively in the current dynamic business environment. The Institute of Directors of Southern Africa (2009) recommends that boards of directors consider more than purely the regulatory aspect, but also demonstrate consideration for market and industry standards, industry status, the investigative media, and the viewpoint of employees, investors, customers, suppliers, consumers, and communities (on a local, national, and international scale), ethical pressure groups, public opinion and confidence and political opinion, etc.

With this in mind it stands to reason that corporate governance is really all about strong leadership efforts (Institute of Directors of Southern Africa, 2009). Strong leadership and good corporate governance are embodied by eight fundamental characteristics. These are accountability, responsibility, fairness, transparency, competence, commitment, courage and inclusivity of stakeholders interests (Institute of Directors of Southern Africa, 2009). When an organization demonstrates these characteristics it can be considered that an effective approach to implementing corporate governance is being undertaken.

Thus, the board of directors is ultimately responsible for the general well-being of an organization. This 'well-being' is gauged through an organization's success in addressing the Triple Bottom Line.

The triple bottom line in corporate governance

Despite consideration for the economic aspects, organizations should now also consider and attend to environmental issues and social investment (ECCO, 2007). This forms the basis of the Triple Bottom Line concept which is said to encompass the evaluation of financial performance, environmental sustainability and social responsibility (Morden, 2007).

Economic prosperity relates to an organization's direct and indirect influence on its stakeholders' financial resources as well as the financial systems at local, national, and global levels. An organization's economic responsibility refers to its profit-making ability and should also demonstrate its emergent global financial integration (ECCO, 2007).

Environmental sustainability relates to the effects of the products or services created by an organization on the natural environment (Institute of Directors of Southern Africa, 2009). An organization should be managed in such a way that the goods and services it provides do not escalate pollution levels or any other form of environmental damage (ECCO, 2007). Thus, innovative practices and technologies require development in order to comply with strict environmentally-friendly codes of good practice, or to retain a competitive edge in markets that are becoming progressively more environmentally aware (Morden, 2007).

Social responsibility requires that an organization's mission, strategy and objectives be in agreement with the values, ethics and culture of the greater social environment in which it operates. This means that an organization should act responsibly towards the interests of all of its stakeholders through all of its dealings and collaborations with these parties. Thus, it should avoid all manner of unprincipled or dubious conduct (Morden, 2007).

During the past ten years it has become evident that producing a profit and being a sustainable business involves a lot more than merely concentrating on the financial bottom line thus, leading to the establishment of the Triple Bottom Line concept. Therefore, in order for an organization to continue to survive in a genuinely profitable and sustainable manner it is important that it yields positive and balanced returns on all three bottom lines (ECCO, 2007). This will also serve to reduce the risk of regulatory intervention which can have an immensely negative impact on an organization.

For any organization to effectively fulfil its corporate governance mandates and to report positively on the Triple Bottom Line, a number of very critical aspects also need to be governed carefully. One of these aspects is information technology (IT), as stated in the King III Report (Institute of Directors of Southern Africa, 2009: 83) "effective IT frameworks and policies, as well as the processes, procedures and standards that these involve, should be implemented with the view to minimise IT risk, deliver

value, ensure business continuity, and assist the company to manage its IT resources efficiently and cost effectively."

Information technology

IT is vital for managing the transactions, information and knowledge required to initiate and maintain economic and social activities. In most organizations, IT has become a fundamental constituent of the business and is essential to reinforce, maintain and grow the business (IT Governance Institute, 2003). This makes IT a critically important asset within many organizations.

The opportunities that IT can present are numerous; savings in time and cost due to improved business processes, ease of collaboration with customers, suppliers and other business partners wherever they may be located, greater competitive advantage and increased business value. A study carried out by global financial services group ING demonstrated that IT-enabled business investments have the potential to produce returns more significant than just about any other conventional investment (IT Governance Institute, 2006). However, with increased complexity, speed, interconnectivity and globalization IT also has the potential to incur great costs and significant risks (IT Governance Institute, 2005c). Factors such as cost, risk and opportunity not only make IT strategic to an organization's growth, it also causes it to be fundamental for an organization's continued existence (IT Governance Institute, 2005c). In reality, today IT goes far beyond playing a simple support role in many organizations as it essentially provides the enablement of new business models and additionally, IT strategy may even become the business strategy (IT Governance Institute, 2005b).

IT investment is no longer just about employing IT solutions, moreover, it's about employing IT-enabled change. Organizations create business value from IT through the way in which they apply it and not the technology itself. There exists a general belief that IT will become a key driver for financial prosperity in the 21st century. Undoubtedly, many organizations depend on IT to attain competitive advantage and, therefore, these organizations should not devote less attention to IT matters than they would to matters of corporate finance or general corporate governance (IT Governance Institute, 2005c).

Generally, board and executive responsibilities concentrate on cost efficiency, revenue enhancement, and building capabilities and all of these are integrated with information and IT. Since IT has become such a key driver in many organizations, and its solutions continue to increase in complexity - consider outsourcing, third-party contracts and global networking for example, the effective governance over IT is a critical success factor for overall corporate prosperity (Hardy, 2006). The IT Governance Institute (2003) states that developments in governance have been driven largely by the need for transparency of business risks and the preservation of shareholder value, the pervasive use of technology has created a significant dependence on IT that requires it to be governed effectively at board level. This can only be achieved by implementing a system of sound IT governance.

IT Governance

IT governance is an aspect of the broader corporate governance function, ensuring that IT is aligned with business goals and delivers value through its investments. IT governance should never be divorced from the issue of intellectual property (IP) and the value thereof to an organization. IT enables people in an organization to complete processes and implement systems in the organization more quickly. When the IP involved in all this is locked into the IT system, the IP becomes part of the information system, rather than separate from it. This makes IT governance a very important function in an organization.

There are many definitions for IT governance. Presenting some of these definitions will help to demonstrate more clearly what IT governance precisely entails.

Robert S. Roussey, CPA and professor at the University of Southern California, states in the IT Governance Institute's Board Briefing on IT Governance that "IT governance is the term used to describe how those persons entrusted with governance of an entity will consider IT in their supervision, monitoring, control and direction of the entity. How IT is applied within the entity will have an immense impact on whether the entity will attain its vision, mission or strategic goals" (IT Governance Institute, 2003:1).

The IT Governance Institute (2003:10) also defines IT governance as "the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives."

Additionally, Van Grembergen (2002:1) defines IT governance as "the organizational capacity exercised by the board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT."

These definitions of IT governance may differ slightly but all three definitions agree on the fact that the board needs to be involved in IT governance. The question that naturally follows from this is; *since the board is involved in governing IT, what should they focus on?*

IT governance: The WHAT factor

From the definitions above, it is clear that a first focal point of the board should be to ensure that IT objectives and plans are strategically aligned with that of business. Therefore, IT should assist an organization in attaining its vision, mission and strategic goals. ***Strategic alignment*** *involves making certain that business and IT plans are linked together; defining, maintaining and validating the IT value proposition; and aligning IT operations with overall business operations (COBIT 4.1, 2007).*

Secondly, in the introduction section of this paper it was mentioned that up to 50% of corporate capital expenditure can be accounted to IT. Taking this into consideration, it

should be clear that the board should be responsible for ensuring proper value delivery so that IT delivers its promised benefits (Institute of Directors of Southern Africa, 2009). ***Value delivery*** *deals with executing the value proposition throughout the delivery cycle, making certain that IT delivers its promised benefits against strategy, focusing on optimizing costs and verifying the inherent value of IT (COBIT 4.1, 2007).*

Thirdly, "An organization's information is among its most valuable assets and is critical to its success. The board of directors, which is ultimately accountable for the organization's success, is therefore responsible for the protection of its information." (Information Security Management and Assurance - A Call to Action for Corporate Governance, 2000). To address this responsibility effectively, it is important that the board undertake some risk management on a continuous basis to ensure that all IT related risks are identified and addressed. ***Risk management*** *necessitates risk awareness by senior corporate officers, a clear understanding of the organization's risk appetite, understanding of compliance requirements, transparency regarding significant organizational risks and embedding of risk management responsibilities into an organization (COBIT 4.1, 2007).*

Fourthly, in section 2, Nolan & McFarlan (2005:102) highlighted that: "The board must ensure that management knows what information resources are out there, what condition they are in, and what role they play in generating revenue…". From this it is clear that resource management is another important aspect to be addressed by the board. ***Resource management*** *is concerned with the best possible investment in, and the appropriate management of vital IT resources which would include applications, information, infrastructure and people. Some important points of concern relate to the optimization of knowledge and the infrastructure (COBIT 4.1, 2007).*

Lastly, Standards Australia defines the Corporate Governance of ICT as follows: "The system by which the current and future use of ICT is directed and controlled. It involves evaluating and directing the plans for the use of ICT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organization." (AS8015, 2005). From this definition it can be deduced that performance measurement of IT should be a definite and continuous concern of the board. ***Performance measurement*** *tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using tools such as balanced scorecards that transform strategy into action to achieve goals measurable beyond traditional accounting, for example (COBIT 4.1, 2007).*

Based on the literature presented above, i.e., COBIT 4.1 (2007), the King III Report (Institute of Directors of Southern Africa, 2009), Information Security Management and Assurance - A Call to Action for Corporate Governance (2000), Nolan & McFarlan (2005) and Standards Australia (AS8015, 2005) it is clear that the five key focus areas for IT governance need to be considered and addressed. These are strategic alignment, value delivery, risk management, resource management and performance measurement. It can therefore be accepted that these five focus areas form the basis of any approach to addressing IT governance effectively. Thus, by successfully addressing these five focus areas, the board should, to a large extent, fulfil its mandate towards IT governance.

Figure 1 provides a graphical representation of these five focus areas that the board should address in meeting their IT governance obligation. These five focus areas cover the WHAT factor of IT governance as far as the board is concerned.

Figure 1: The board and IT governance: The WHAT factor

It is worthwhile to take note of some specific principles applied when implementing general corporate governance, particularly looking at the Triple Bottom Line when attempting to devise an effective means of addressing IT governance. The Triple Bottom Line covers core issues to be directed and controlled in the broader sense of organizational governance. To reiterate, these are; economic prosperity, environmental sustainability and social responsibility. Similarly, based on the literature presented above, it has been highlighted that IT governance covers at least five key focus areas relating to the governing of an organization's IT resources. Thus, it can be said that the concept of a bottom line approach towards governance in its generic sense can be deemed as a practical route to follow and can also act as a macro tick-box. Therefore, in terms of IT governance the concept of a Penta Bottom Line can be used to describe the five focus areas of IT governance. Thus, the WHAT factor introduced and discussed above can be presented in the form of a Penta Bottom Line. This should indicate the minimum criteria that should be addressed by the board as part of their IT governance responsibility, similar to the Triple Bottom Line which serves as a macro guideline on what should be addressed in terms of corporate governance.

The Penta Bottom Line provides a definite guideline as to which IT related aspects should be important to the board. The board should ensure that questions regarding at least

these five aspects are asked and satisfactorily answered to ensure that due care has been applied as far as IT is concerned. The question that follows from this is: Who should do the 'work' in this regard?

IT governance: The WHO factor

It is logical to assume that those employees that are in more direct contact with an organization's systems on a daily basis will have a more intimate understanding of how the systems work and what their general purpose would be. This would be true for executives such as the CIO or CTO for example, however, as far as the board is concerned it becomes a "black box" scenario since they may not have such a deep understanding of the systems themselves. However, it is important to remember that the board stays ultimately responsible and accountable for the well-being of an organization, and therefore also for the performance of IT. For this reason, it is necessary that they seek guidance and advice on matters relating to IT. Hence, it is common practice that various board committees are used to assist the board in this regard. Typically such committees include the Audit Committee (and Risk Management Committee) and in some cases a dedicated IT Oversight Committee.

The Audit Committee is usually responsible for conducting performance reviews of an organization's system of internal control. It is also responsible for reviewing legal and regulatory compliance efforts, including compliance with organizational rules and codes of conduct (Institute of Directors of Southern Africa, 2009). In many organizations the responsibility for board-level IT guidance also falls to the Audit Committee (Changepoint Corporation, 2004)

Additionally, the Risk Management Committee can facilitate a board in corporate accountability and the risks associated with management, assurance and reporting. Its terms of reference include disaster recovery risk, technology risk, operational risk, and compliance and control risks (Institute of Directors of Southern Africa, 2009).

Moreover, the IT Oversight Committee is totally geared toward addressing strategic IT issues in detail. In this regard, the IT Oversight Committee certifies that IT is a standard topic on a board's agenda to be addressed through a structured approach. Additionally, the IT Oversight Committee makes certain that a board receives all the information it requires to make insightful decisions vital to the achievement of strategic alignment, value delivery, risk management, resource management and performance measurement (IT Governance Institute, 2004).

To ensure that such a committee is able to advise the board appropriately on such matters, its makeup is of vital importance. It is recommended that the IT oversight committee be comprised of independent directors (Nolan & McFarlan, 2005). Generally, committee members should be chosen based on their knowledge and experience in understanding the impact of information and related technology on the business. Furthermore, member selection should be customised to each organization depending on the context in which it operates (IT Governance Institute, 2004). The chairperson should be "a tough-minded, IT-savvy business executive", either a CEO or top manager with experience in supervising the use of IT in other organizations to gain strategic advantage. It is also important that at least one committee member be an IT expert whose role would be to function as a peer at senior management and board level (Nolan & McFarlan, 2005).

This is important because there is great risk in the use of information systems when they become pervasive and part of the business plan. Most organizations may not find it possible to have their own CIO. Consequently, they have a service provider and the result is that strategic information, including intellectual property (IP), goes outside the organization. Board members are unaware of the operational risks involved, because the processes are not understood by them. Hence, the debate that maybe the time has come for not only the CEO and the CFO to be a member of the board, but the CIO – when an organization has one – should also be a member of the board.

Once the board has gained an understanding of WHAT is expected of them in terms of IT governance and WHO in an organization is responsible, the question that follows next is: HOW should the 'work' be carried out?

IT governance: The HOW factor

Every organization's approach to IT governance may differ depending on its business needs for and reliance on IT to drive and support its main objectives. For example, IT governance could be a regular task addressed by an organization's audit committee or a fundamental asset that necessitates rigorous board-level scrutiny and support (Nolan & McFarlan, 2005). Every organization should determine their strategic stance in terms of IT governance to help them understand the level of detail it necessitates. Nolan and McFarlan (2005) have defined the IT Strategic Impact Grid for this specific purpose. The next few pages describe the IT Strategic Impact Grid as developed by Nolan and McFarlan (2005). On this grid the board's involvement in IT matters can generally be defined according to two strategies namely, a defensive IT strategy or an offensive IT strategy:

- A ***defensive IT strategy*** focuses on operational reliability. Thus, ensuring that IT systems continue to function normally and without interruption. It is not necessary to outperform competitors through the intelligent application of emerging technology.

- An ***offensive IT strategy*** focuses more on strategic issues. Offensive IT projects are usually ambitious, involve considerable risk and frequently require significant organizational change. An offensive strategy is necessary when an organization adjusts its technology strategy for the purpose of enhancing its competitiveness or elevating itself to a position of industry leadership (Nolan & McFarlan, 2005).

In an organization's strategic approach to IT, whether defensive or offensive, it may adopt a particular mode of IT operation. There are generally four modes of IT operation,

namely, support mode, factory mode, turnaround mode and strategic mode:

- Organizations in ***support mode (defensive IT strategy)*** have a fairly low need for reliable systems and a low need for IT to be strategic. The technology is merely there to support the activities of employees and key business systems are usually run on a batch cycle with the majority of error correction and backup work being executed manually. Customers and suppliers of organizations in support mode generally do not have access to any of the internal systems. Furthermore, these organizations are able to bear constant service disruptions of up to 12 hours without experiencing any severe repercussions to their bottom-line, and rapid Internet response times are not essential.

- Organizations in ***factory mode (defensive IT strategy)*** require dependable systems but it is not essential that they implement cutting edge technology. Such organizations can be equated to manufacturing plants where if a conveyor belt malfunctions, production ceases. They are significantly more dependent on the seamless operation of their technology, due to the fact that the majority of their key business systems are online. If their systems cease normal operation for even a minute they will experience instantaneous losses and switching over to manual procedures can prove to be tedious or even impossible. Factory mode organizations usually rely on their extranets to collaborate with their customers and suppliers. Typically, factory mode organizations are unconcerned about being the first to utilize cutting edge technology, however their boards and executive management need to be aware of innovative practice and must examine the competitive environment for any changes that would necessitate a more aggressive IT strategy to be practiced. It is important for the boards of these organizations to ensure that proper disaster recovery and security procedures are in place because business continuity in IT operations is vital to them.

- In ***turnaround mode (offensive IT strategy)*** technology investments usually account for more than 50% of capital expenditures and more than 15% of corporate costs. Investments in new technology assure significant process and service improvements, reductions in costs and increased competitive advantage. However, these organizations have a fairly low necessity for reliable systems. Similar to organizations in support mode they can also bear repeated service disruptions of up to 12 hours without suffering any significant repercussions, and their fundamental business processes remain on a batch cycle. However, once the new systems have been implemented, it is not possible to switch back to the manual systems.

  Organizations typically move into turnaround mode when they undertake significant IT projects that call for a large scale reengineering effort. This frequently comes with a decision to outsource or to move a considerable segment of organizational operations offshore. The majority of organizations do not stay in turnaround mode for very long because once changes are made, they move into either factory mode or strategic mode.

- ***Strategic mode (offensive IT strategy)*** organizations require the same level of reliability as organizations in factory mode. Additionally, they also seek process and service opportunities, cost reductions and competitive advantages quite aggressively. Similar to organizations in turnaround mode, these organizations have very large IT expenditures. Not all organizations wish or have a necessity to be in strategic mode but they are sometimes pressured into it by competitive forces in industry. Just the same as organizations in turnaround mode, organizations in strategic mode require rigorous IT governance efforts (Nolan & McFarlan, 2005).

Figure 2 illustrates an adaptation of the IT Strategic Impact Grid as expressed Nolan and McFarlan (2005).

It is recommended that boards spend sufficient time understanding their organization's business needs for IT and determining which mode of IT operation best describes their organization's dependence on IT. The IT Governance Institute (2005a:4) states that "attaining good IT governance does not happen by accident, or by telling the CIO to 'make it so'. It needs to be prepared, properly implemented and monitored, if value destruction is to be avoided and value creation achieved. The tone has to be set at the top". Once this is achieved it will become a lot clearer as to which type of board-level committee is suitable to address an organization's IT related issues:

- Generally, organizations in ***support mode*** have a low need for operational reliability and low need for new IT. In this case it is acceptable for an Audit Committee to assist the board with IT governance.

- Organizations in ***factory mode*** normally have a high need for reliability but also low need for new IT. Thus, it is also acceptable for an Audit Committee or even the Risk Management Committee to assist the board with IT governance. In addition to these committees advice from an IT expert may also be acquired.

- Normally organizations in ***turnaround mode*** have a low need for operational reliability and high need for new IT. In turnaround mode board-level IT oversight is vital because strategic IT plans must go forward on time and within the allocated budget, especially when competitive advantage is at issue. Thus, the IT Oversight Committee would assist the board in this context.

- Generally organizations in ***strategic mode*** have a high need for operational reliability and high need for new IT. Organizations in strategic mode definitely require a formal board-level IT Oversight Committee with at least one member being an IT expert (Nolan & McFarlan, 2005).

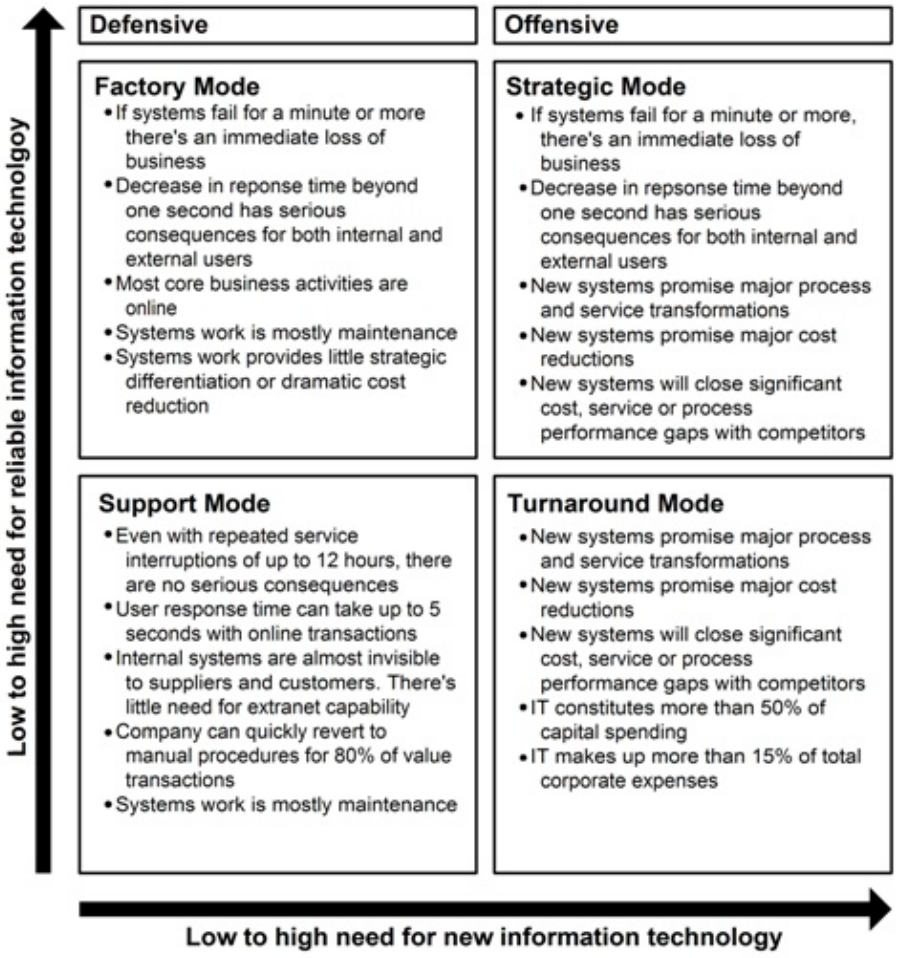

Fig 2: The IT Strategic Impact Grid

If an organization approaches IT governance using a defensive strategy where IT is not required to be of a strategic nature, it is acceptable for a board to use the Audit Committee (or the Risk Management Committee or an Audit and Risk Committee) to direct and control IT operations on their behalf, as was discussed above. The skills of an Audit Committee are normally financially and audit focussed and therefore such a committee does not necessarily have an in depth knowledge of IT to engage in deep and insightful discussions with the board concerning IT strategic issues (Changepoint Corporation, 2004). However, in some cases where it may be necessary, the 'shortcomings' of the Audit Committee might possibly be overcome by appointing a member knowledgeable of IT matters to such a committee. The Audit Committee, or the Risk Management or the Audit and Risk Committee (depending on the specific situation) should report to the board, using the Penta Bottom Line as minimum criteria merely notifying the board of the current state of IT in an organization. Additionally, it should provide enough information to convince the board that due care has been applied as far as IT is concerned.

Organizations implementing an offensive strategy should preferably make use of a dedicated board level committee, such as an IT Oversight Committee for example, to apply due care as far as IT matters are concerned. For an organization this dependant for its well-being on IT, or where such a lot of resources are allocated to IT, it warrants a dedicated board committee to direct and control this operation. In this case the board should not merely be informed or notified of the state of IT, but should actively convince themselves that each of the aspects covered by the Penta Bottom Line have received due care.

Figure 3 graphically represents HOW the various board-level committees should be involved in IT governance depending on the mode the organization is currently operating in.

It is not necessarily "set in stone" how frequently specific board level committees should report to the board. According to the King III Report (Institute of Directors of Southern Africa, 2009) the Audit Committee and Risk Management Committee should report to the board as frequently as they see necessary, with a minimum of at least two to three times a year. Furthermore, the IT Governance Institute (2004) states that an IT Oversight Committee as well should meet as often as required in order to fulfil their responsibilities. Thus, it is ultimately up to the board to determine how often it requires reports on the progress of IT governance based on the criticality of IT in their organization. However, as a general guideline based on the four modes of IT operation presented in this paper, the following recommendations can be made:

Support Mode	Every 12 months (with exceptions)
Factory Mode	Every 6 to 12 months (with exceptions)
Turnaround Mode	Every 3 months
Strategic Mode	Every 3 months

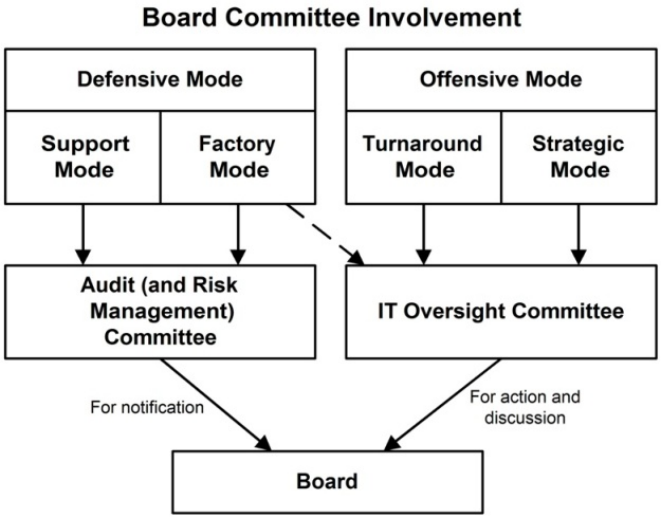

Fig 3: Board committee involvement

- In ***support mode***, the IT system is fairly static and although IT is important to the organization, it is not critical to an extent that the success of the organization is absolutely dependent on it. For this reason, an annual feedback should be satisfactory unless major IT changes have been taken place.

- An organization in ***factory mode*** is very dependent on IT, but the IT system is also fairly static. For this reason, it can be argued that the board should at least get some sort of assurance every six months. If IT plays a critical role in the well-being of the organization, the board can even ask for a report every three months.

- An organization normally does not find itself continuously in the ***turnaround mode***, but once in this mode a three monthly report is absolute imperative. Normally a lot of funds are spent on IT whilst in this mode time and the board should put their minds at ease that progress is satisfactory.

- For an organization in ***strategic mode***, IT is absolutely critical. The board should obtain assurance as regularly as possible that IT is in a 'healthy' state. Thus, an assessment by the board every three months is an absolute minimum.

This section provided guidance on the WHAT, WHO and the HOW as far as the board's involvement in IT governance is concerned. Figure 4 present this information graphically.

Once the successful governance of IT and related information resources is proving effective, thus adding value to an organization and contributing towards its competitive advantage, the implementation of IT governance can be claimed as intellectual property (IP) and should be treated as such.

Conclusion

The WHAT, WHO and HOW of IT Governance Model presented in this paper serves to provide the clarity required to demonstrate to the Board what they should do in order to strategically direct and control IT appropriately. Essentially, it helps to conceptualize the various key issues, i.e., WHAT, WHO and HOW, of IT governance, and the relationships between them, to enable Boards to effectively govern IT. Many authors, standards and reports state that IT must be governed, but few, if any, guidelines exist as to how this should be organized and done. Thus, the model presented in this paper will, in a way that has not been attempted previously, allow any organization attempting to implement IT governance to develop a clearer understanding of what is central to ensuring that IT is able to contribute towards the achievement of strategic business objectives. This also demonstrates that the model is capable of providing any organization, irrespective of size or business orientation, with a sound general approach towards addressing strategic IT-related issues.

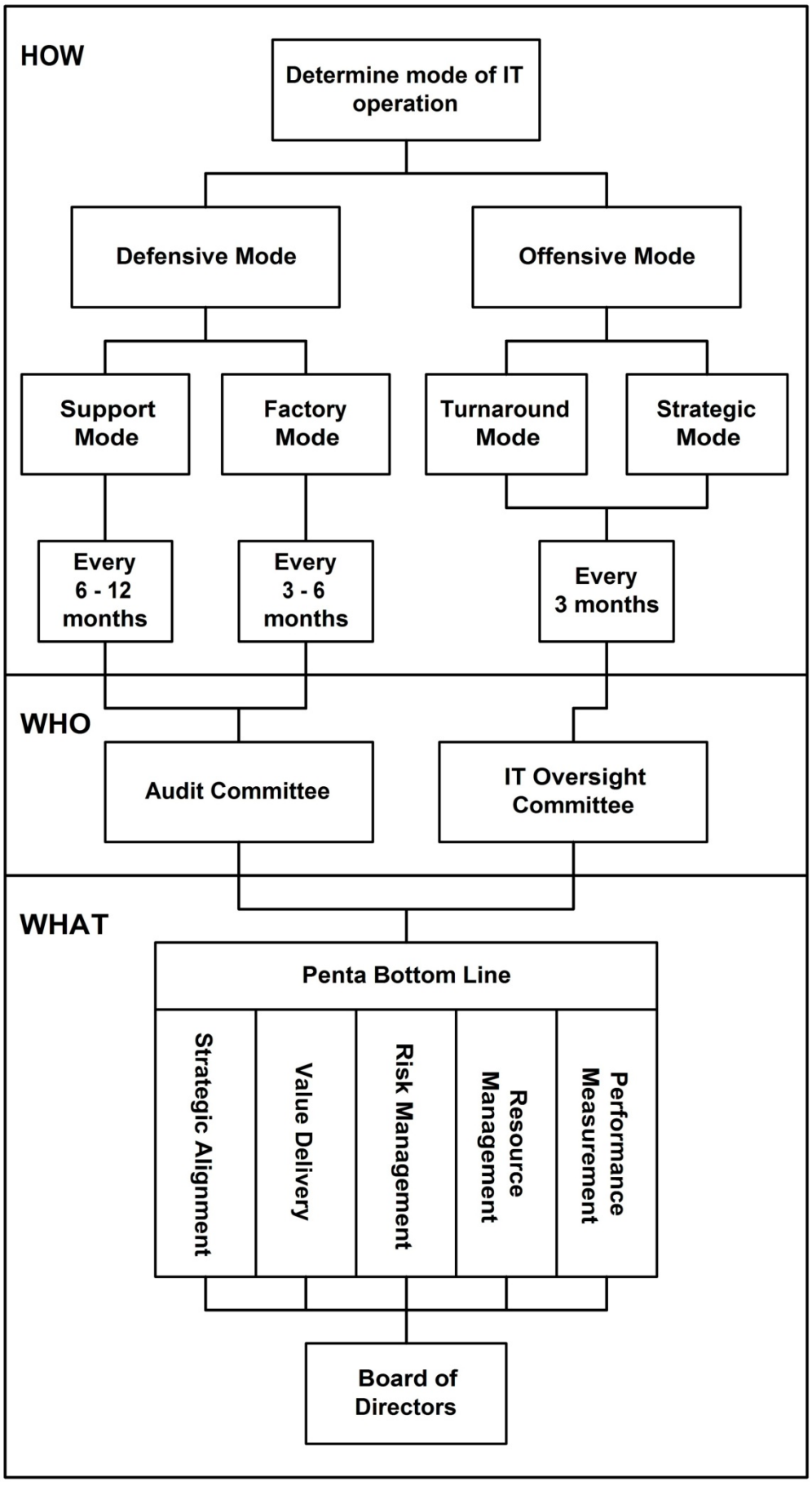

Figure 4: IT governance – The WHAT, the WHO and the HOW

References

Australian Standard AS8015. 2005. Corporate governance of information and communication technology. Standards Australia.

ChangePoint Corporation. 2004. 'Governance: The Board's – and the CIO's – Business'. [online]URL: http://itresearch.forbes.com/detail/RES/1081531053_905.html

COBIT 4.1. 2007. *Control objectives for information and related technology.* IT Governance Institute. [online] URL: http://www.isaca.org/Knowledge-center/cobit/Pages/Downloads.aspx

De Haes, S. & Van Grembergen, W. 2004. 'IT governance and its mechanisms'. [online]URL: http://www.isaca.org/Content/ContentGroups/Member_Content/Journal1/20044/jpdf041-ITGovernanceandIts.pdf.

ECCO. 2007. 'Towards a triple bottom line reporting framework'. [online]URL: http://www.ethics.up.ac.za/publications html.

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: Legal, Regulatory and Compliance Aspects of Information Security*, **11**(1): 55 – 61.

'Information Security Management and Assurance - A Call to Action for Corporate Governance'. 2000. [online]URL: http://www.aicpa.org/assurance/systrust/press/report_b htm

IT Governance Institute. 2003. 'Board briefing on IT governance'. 2nd Edition. [online]URL: http://www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Board_Briefing_on_IT_Governance/26904_Board_Briefing_final.pdf.

IT Governance Institute. 2004. 'IT strategy committee'. [online]URL: http://www.ITgovernance.org/resources htm.

IT Governance Institute. 2005a. 'The CEO's guide to it value @ risk'. [online]URL: http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=20697.

IT Governance Institute. 2005b. 'IT governance domain practices and competencies: IT alignment - Who is in charge?' [online]URL: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Governance-Domains-Practices-and-Competencies-IT-Alignment-Who-Is-in-Charge.aspx

IT Governance Institute. 2005c. 'IT governance executive summary'. [online]URL: http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=19976.

IT Governance Institute. 2006. 'Enterprise value: Governance of IT investments - The val IT framework.' [online]URL: http://www.itgi.org/AMTemplate.cfm?Section=Deliverables&Template=/ContentManagement/ContentDisplay.cfm&ContentID=24259.

IT Governance Institute. 2008. 'IT governance global status report'. [online]URL: http://www.itgi.org/AMTemplate.cfm?Section=ITGI_Research_Publications&Template=/ContentManagement/ContentDisplay.cfm&ContentID=39735.

Institute of Directors of Southern Africa. 2009.' King III Report - The King Report on Corporate Governance for South Africa'.[online]URL: http://african.ipapercms.dk/IOD/KINGIII/kingiiireport/

Morden, T. 2007. *Principles of strategic management.* 3rd Edition. Ashgate.

Nolan, R. & McFarlan, F. W. 2005. 'Information technology and the board of directors', *Harvard Business Review*, **83**(10): 96.

Schwartz, K. D. 2007. 'ABC: An introduction to IT governance'. [online]URL: http://www.cio.com/article/111700.

Van Grembergen, W. 2002. 'Introduction to the minitrack it governance and its mechanisms'. **In** *Proceedings of the 35th Hawaii International Conference on System Sciences (hicss).* January 7-10

Von Solms, R. & Von Solms, S. 2006. 'Information security governance: A model based on the direct-control cycle', *Computers and Security,* **25***:* 408–412.

Whitman, M. E. & Mattord, H. J. 2003. *Principles of information security*. Course Technology.

World Bank Group. 1999. 'Corporate governance: A framework for implementation'. [online]URL: http://www.worldbank.org/html/fpd/privatesector/cg/docs/gcgfbooklet.pdf.