JICLT
Journal of International Commercial Law and Technology
Vol. 8, No.4 (2013)

VoIP: A Corporate Governance Approach to Avoid the Risk of Civil Liability

Tian Gerber♣, Kerry-Lynn Thomson, Mariana Gerber

Abstract: Since the deregulation of Voice over Internet Protocol (VoIP) in 2005, many South African organizations are now attempting to leverage its cost saving and competitive values. However it has been recently cited that VoIP is one of the greatest new risks to business. This risk is cited to increase Information Security insurance premiums in the near future. Due to the dynamic nature of the technology, regulatory and legislative concerns such as lawful interception of communications and privacy may also contribute to business risk. VoIP consists of both direct communications (voice conversation) and indirect communications (voice mails, emails and instant messaging). Due to this dual nature, complying with regulations such as the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) should be considered. In order to leverage value from the VoIP implementation, an executive or SME owner should look to implement the technology with knowledge of the potential risk of civil liability. This is further highlighted by the King III Report which makes the Directors and CEO of an organisation ultimately responsible for IT Governance and Information Security Governance. The report goes further to say, any new technology, such as VoIP, should comply with all South African legislation and regulations. This responsibility encourages the practice of both due care and due diligence. However, recent trends exercised by Information Security professionals, responsible for drafting Information Security policies, often neglect the regulatory requirements and choose to only implement international best practices with no considerations to the risk of civil liability. Although these best practice frameworks may inadvertently comply with existing local legislation, a chance of an oversight is a possibility. Oversights may not only result in criminal sanctions but also civil action due to losses or damages suffered by a third party. Using both the identified regulations and relevant international best practices one may attempt to ensure good Governance with regards to VoIP's dual nature. The aim is to aid executives and SME owners in mitigating the risk of civil liability to better leverage VoIP's value by utilizing the proposed VoIP: Civil Liability Risk Table. This should aid in the exercise of due care and due diligence when implementing VoIP as a means of conducting business communication.

1. Introduction

The adoption of VoIP has increased both locally and internationally in recent years. This increased rate of adoption is largely due to the value a VoIP implementation may provide an organization. The VoIP implementation provides this value in two primary ways. Firstly a VoIP implementation is more cost effective than other communication implementations and secondly enables employees to work more efficiently dues to its dual natures of both direct and indirect communications. This dual nature allows employees to communicate utilizing multiple communication platforms from a single VoIP device. However this value is at risk from potential security threats from both external and internal sources. It has been noted that VoIP alters the existing risk portfolios, enabling risks such as identity theft, intellectual property theft and interruption of service, which may result in damage to a third party which may lead to civil liability. The risk introduced by implementing VoIP has warranted increased payments on security and privacy insurance premiums by international organizations (Trautman & Altenbaumer-Price, 2011). These risks, should value be maintained, could possibly be mitigated by adhering to applicable best

♣ Corresponding author: Tian Gerber , NMMU email: s207013987@live.nmmu.ac.za

practices and exercising proper governance. An exploration of laws applicable to a VoIP implementation and appropriate best practices and guidelines should be explored.

2. Guidelines and Legislation

When implementing a new technology, such as VoIP, as a means of communication, an organization should first investigate all implementation requirements IoDSA, 2009, pp. 71-72). For the purposes of this dissertation the term Director(s) will represent members of the board and all applicable directors serving the board such as the CIO or CEO. Besides managing the change to a new communication implementation or the training that needs to be conducted, Directors responsible for governing the organization and therefore Information Technology (IT) matters should look at applicable legislation, guidelines and best practices (IoDSA, 2009, p. 73; Nthoiwa & Francis, 2010; Kotze, 2012). This is done as part of organization's legal obligation to provide information security with regards to both external and internal threats (Etsebeth, 2011; Trautman & Altenbaumer-Price, 2011). This should aid in ensuring that the VoIP implementations and its utilization are in adherence to all civil law requirements and implemented with sound Corporate Governance principles. The King III Report provides Principles for the proper Corporate Governance of an organization. These Principles provide the high level controls that should be considered when addressing governance. The King III report makes specific provision for IT Governance and an entire chapter is devoted to providing Principles for the proper governance of IT. One such principle, 5.5 statement 33 or 5.5 (33), states the following with regards to compliance with applicable laws and codes: "When considering the company's compliance with applicable laws, rules, codes and standards, the Directors should ensure that IT related laws, rules, codes and standards are considered. Companies must comply with applicable IT laws and consider adherence to applicable IT rules, codes and standards, guidelines and leading practices" (IoDSA, 2009, p. 73). This makes the responsibility of the governing Board of Directors two-fold. The Directors should ensure compliance to all applicable laws within South Africa and, further, all applicable laws, codes, standards, guidelines and leading practices with regards to any technological implementation, such as VoIP. This is further compounded by an international IT best practice framework, COBIT 5, which makes provision for the monitoring and assessment of compliance with external requirements (ISACA, 2011, pp. 207-210). This requires Directors to take the necessary steps to avoid the most prevalent civil liability risks as part of their legal obligation to provide adequate information security for voice communication (Etsebeth, 2011). The organization may be held civilly liable should all of the following constitutes of a delict be found to be true: "A delict is the act of a person that in a wrongful and culpable way causes harm to another" (Neethling, Potgieter, & Visser, 2006, p. 3). Therefore, to avoid a delict, an organization may need to prove that it has in fact adhered to all applicable IT rules, codes and standards, guidelines and leading practices to prevent harm to another. This is done as the organization should be aware, or be made aware, of the potential risk to clients and employees utilizing the VoIP implementation. If the organization is unable to motivate the lack of applicable IT controls and Processes, it may be held civilly liable for losses and damages (Etsebeth, 2011). An organization would need to demonstrate that it is implementing the best security practices and exercising good governance with regards to VoIP. In the section to follow, as a possible means to avoid liability, the implementation of appropriate King III guidelines and COBIT 5 controls with regards to a VoIP implementation will be discussed.

3. VoIP Best Practices

The Principles and Processes to follow were identified through a process of qualitative content analysis (Krippendorff, 2003, p. 18). Applicable Principles were identified from the King III Report as it is the primary good governance code for South African organizations wishing to list themselves on the JSE and makes specific notation of the importance of governing IT within an organization. Furthermore, the latest iteration of the COBIT framework, COBIT 5, was analyzed as it is considered an international best practice with regards to IT governance practices. The Principles and Processes were identified for the purposes of aiding with the governance and securing of a VoIP implementation. The identified Principles and Processes will be proposed as possible answers to questions that may be asked of an organization in the case of potential civil liability. In order to implement VoIP correctly, in accordance with governance best practices, securely and within the scope of South African law, international best practices could be

followed. This would provide for practical Processes to ensure IT Governance and Information Security Governance is both correctly and practically implemented. To follow are the King III Principles and COBIT 5 Processes identified by the researcher as the most applicable to avoiding civil liability with regards to a VoIP implementation:

3.1 King III

The King III Report serves as a means of guiding organizations in proper corporate governance practices. The report contains principles that an organization should adhere to if they wish to implement good corporate governance. The report goes further to state that good governance is not something that exists separate from the law. Therefore, it is paramount to extrapolate principles from the King III Report with regards to the VoIP implementation to ensure good governance in order to avoid civil liability risk. This section contains suggested principles for the proper implementation of VoIP. The Principles were chosen based on their influence on the securing or governing of a VoIP implementation or in some cases both as shown in Table 1. Each Principle discussed below is from the fifth chapter of the King III Report entitled, "The Governance of Information Technology (IT)". Each principle, therefore, is numbered 5, followed by the section number and the line number within the chapter in brackets.

Table 1: Principles, Governance and Security Alignment

Process	VoIP Governance	VoIP Security
5.1 (1)	*	*
5.1 (4)	*	
5.1 (5)	*	
5.1 (9)	*	*
5.3 (16)	*	*
5.5	*	*
5.6 (38)	*	*
5.6 (39)	*	
5.6 (40)		*
5.6 (42.1)		*
5.6 (42.2)		*
5.6 (42.3)		*

- **Principle 5.1 (1)**

  This principle states that an organization should understand and manage the risks, benefits and constraints of IT and by association IT implementations. Therefore, the Directors should understand the strategic importance of IT, assume responsibility for the governance of IT and place IT Governance on the Directors' agenda.

- **Principle 5.1 (4)**

  The Directors, in accordance with this principle, should ensure that IT Governance charters and policies are established and implemented within the organization. This should provide decision making rights and an accountability framework for IT Governance.

- **Principle 5.1 (5)**

  An organization, having established IT Governance charters and policies, should ensure that all employees are aware of them. Therefore, the Directors should oversee the cultivation and promotion of IT Governance and manage a culture of awareness.

- **Principle 5.1 (9)**

  Crucial systems to organization operations, such as IT implementations, should be regularly monitored and reported on. The Directors should take necessary steps to ensure that there are Processes in place to ensure complete, timely, relevant, accurate and accessible reporting from management to the Directors.

- **Principle 5.3 (16)**

  Effective IT policies, Processes, procedures and standards should be implemented with the view to minimize IT risk, enabling the delivery of value and ensuring organization continuity.

- **Principle 5.5**

  IT should form an integral part of the company's risk management. A risk portfolio should be established to identify potential risks with regards to the IT implementations and the utilization thereof.

- **Principle 5.6 (38)**

  The Board should ensure the necessary systems are in place for personal information to be treated by the company as an important business asset and that all personal information is processed by the company is identified.

- **Principle 5.6 (39)**

  All applicable legislation pertaining to the handling of personal information should be noted and adhered to.

- **Principle 5.6 (40)**

  The Directors should ensure that an Information Security Management System (ISMS) is developed, implemented and recorded in an appropriate and applicable Information Security framework. The ISMS should ensure the confidentiality, integrity and availability of information. Furthermore, the ISMS should address technological security measures, security processes and securing people's interactions with the organization's IT implementations (Heyink, 2011).

- **Principle 5.6 (42.1)**

  Confidentiality of information communicated via any IT implementation should be maintained.

- **Principle 5.6 (42.2)**

  The integrity of information traversing the IP network between IT devices should be maintained to prevent possible spoofing threats.

- **Principle 5.6 (42.3)**

  The organization should also make certain that information is only available to those who have the right to access it.

These high level Principles may aid Directors in IT Governance and, consequently, Information Security Governance responsibilities. However, the King III Report that provides these Principles also recommends the exploration of applicable IT best practices. International governance frameworks such as COBIT 5 should be taken into consideration by Directors as part of their duty to proper corporate governance and to avoid civil liability risk (Trautman & Altenbaumer-Price, The Boards Responisbility for Information Technology Governance, 2011).

3.2 COBIT 5

COBIT 5 is a governance and management framework for information and IT. This exposure draft of the new version 5 of the framework will allow organizations to prepare to achieve their governance and management objectives relating to IT and its implementations. Various COBIT 5 Processes such as "Evaluate, Direct & Monitor" (EDM), "Direct, Service & Support" (DSS), "Monitor, Evaluate & Assess" (MEA) and "Align, Plan & Organize" (APO) have been identified by the researcher as important for the securing and or proper governance of a VoIP implementation as shown in Table 2. Each Process is listed using its acronym and number representing it within the COBIT 5 document Listed below is each identified Process, as well as the associated sub-processes required to achieve the Process's overall goal.

Table 2: Processes, Governance and Security Alignment

Process	VoIP Governance	VoIP Security
EDM01	*	
DSS07		*
MEA01	*	*
APO12	*	*

- **EDM01 Set and Maintain Governance Framework**

  A governance framework should be established with the approval of the Directors with regards to the governing of IT. The IT implementations should be monitored to ensure adequate governance oversight. The appropriate policies and procedures should be developed with regards to governance practices and implemented in the organization. Organizational employees should be made aware of these policies and their compliance and effectiveness monitored (ISACA, 2011, pp. 24-28). This core process of COBIT 5 comprises the following sub-Processes:

  - EDM01.01 Evaluate the design of enterprise governance of IT
    Continually identify and engage with the organization's stakeholders, document an understanding of the requirements and make judgment on the current and future design of Governance of the organization's IT implementations.

  - EDM01.02 Direct the governance system
    Inform leadership, the Directors, and obtain their support, buy-in and commitment to the governing of IT. Guide structures, Processes and practices for governance of IT implementations in line with agreed governance design principals.

  - EDM01.03 Monitor the governance system
    Monitor the effectiveness and performance of an organization's governance of IT implementations, as well as assess existing structures.

- **DSS07 Manage Information Security**

  This process makes provision for the protection of organization information in order to maintain a level of Information Security risk that is in line with the organization's risk appetite. In order to maintain this level of risk the appropriate Information Security roles and responsibilities, policies, standards and procedures should be put into place. An ISMS could possibly enable the maintenance of this level of risk should it provide security for the aspects reflected in this COBIT 5 process's sub-Processes listed below (ISACA, 2011, pp. 179-184):

- DSS07.01 Protect against malware
  Implement and maintain preventative and corrective measures across an organization to protect information systems.

- DSS07.02 Manage network and connectivity security
  Use security measures and related management procedures to protect information over all methods of connectivity.

- DSS07.03 Manage endpoint security
  Ensure that endpoints are secured at a level that is equal to or greater than defined security requirements of information that is processed, stored or distributed.

- DSS07.04 Manage user identity and access
  Ensure users have access to information and communication functionality in accordance with organization requirements.

- DSS07.05 Manage physical security
  All access to premises, buildings and areas should be justified, authorized, logged and monitored.

- DSS07.06 Manage sensitive documents and output devices
  Establish appropriate safeguards over sensitive IT assets.

- DSS07.07 Manage information security incidents
  Clearly define and communicate the characteristics of potential IT security incidents and provide guidance to the incident management process.

- DSS07.08 Manage information handling
  Manage information assets securely throughout their lifecycle.

- **MEA01 Monitor & Evaluate Performance and Conformance**

  The organization's organization and IT goals along with relevant metrics should be collected, validated and evaluated. The implementation of conformance goals and metrics should enable systematic and timely reporting (ISACA, 2011, pp. 190-195):

  - MEA01.01 Establish a monitoring approach
    Engage stakeholders to establish and maintain a monitoring approach to define the objects, scope and method for measuring the IT implementation's service delivery and contribution to the organizations objectives.

  - MEA01.02 Set performance and conformance targets
    Work with stakeholders to define, periodically review, update and approve the performance and conformance targets within the performance measurement system for the IT implementations.

  - MEA01.03 Collect and process performance and conformance data
    Collect and process IT implementation data both accurately and timely.

  - MEA01.04 Analyze and report performance
    Periodically review IT implementation performance against targets. A method should be used that provides an all-round view of the IT implementations performance and fits within the enterprise monitoring system.

  - MEA01.05 Ensure the implementation of corrective actions

Assist the stakeholders in identifying, initiating and tracking corrective actions in order to address anomalies within an IT implementation.

- **APO12 Manage Risk**

  This COBIT 5 Process highlights the continual identification, assessment and reduction of IT-related risks within the risk appetite of the organization established by the Directors (ISACA, 2011, pp. 99-104). The following COBIT 5 Processes could be followed to ensure adequate risk management.

  - APO12.01 Collect data
    Identify and collect IT implementation information relevant to enabling of effective IT related risk identification, analysis and reporting.

  - APO12.02 Analyze risk
    Develop useful information on IT implementations to support risk decisions that take into account the organization relevance and risk factors, such as risk appetite.

  - APO12.03 Maintain risk profile
    Maintain an inventory of known IT implementation risks and risk attributes. These attributes should include the expected frequency, potential impact, response, related resources, capabilities and current control activities.

  - APO12.04 Articulate risk
    Provide information on the current state of the IT implementation exposures and opportunities in a timely manner.

  - APO12.05 Define a risk management action portfolio
    Ensure that measures for seizing strategic opportunities and reducing risk to an acceptable level are managed as a portfolio.

  - APO12.06 Respond to risk
    Respond in a timely manner with effective measures to limit the magnitude of loss from IT implementation risk events.

The King III Principles and COBIT 5 Processes relate to IT implementations in an organization. Therefore, as VoIP is an IT implementation of a new communication medium, it follows that these Principles and Processes are applicable to VoIP implementations. The Principles and Processes should be implemented to augment existing Corporate Governance practices or establish new governance practices with regards to VoIP. This should be done in order to protect an organization from being negligent with regards to VoIP Information Security, avoid vicarious liability and possible civil action due to privacy infringement. As stated before, it can be argued that, when implementing a VoIP solution, new risks are not introduced, rather existing Information Security risk portfolios are altered (James & Woodward, 2007). In the sections to follow, questions that would be posed to the Directors or delegated Management to test whether the organization should be held liable for damages suffered, as a result of the exploitation of these VoIP risks, will be proposed. As answers to these questions, the applicable King III principles and COBIT 5 Processes will be proposed through a process of further qualitative content analysis (Krippendorff, 2003). Therefore, an in-depth discussion of each of the most prevalent civil liability risks should be explored after implementing VoIP. The questions refer to both the internal and, where applicable, external threats that create a risk of civil liability with regards to a VoIP implementation. If an organization implements these Principles and Processes they may be able to avoid the most prevalent risks of civil liability both internally and externally. In the sections to follow the most prevalent civil liability risks namely Negligent Information Security, Vicarious Liability and Privacy Infringement will be discussed along with all before mentioned questions, Principles and Processes associated with each.

4. Negligent Information Security

Should a security breach occur, internally or externally, the organization should establish that they were not negligent with their own Information Security. Information is considered to be one of the most important assets of an organization (von Solms B. , 2006). This information takes on many forms, such as the communications conducted over the VoIP implementation. If a security breach were to occur, the organization should be able show that it has taken adequate steps in securing this important asset. The organization needs to show that it acted as any other reasonable person would have when implementing VoIP and securing it. In South Africa, to test whether a person has acted reasonably, the following definition is provided: "The defendant is negligent if the reasonable person in his position would have acted differently; and according to the courts the reasonable person would have acted differently if the unlawful causing of damages was reasonably foreseeable and preventable" (Neethling, Potgieter, & Visser, 2006). The organization should be able to prove that it prevented any foreseeable damages and/or losses. According to Etsebeth, there are a number of questions an organization may ask itself in order to test its negligence with regards to securing the VoIP implementation (2011).

In the section to follow, each question shall be stated followed by an excerpt from a table. These table excerpts contain the Principles and Processes identified by the researcher to be applicable to a VoIP implementation. These recommendations are split into internal threats and external threats, where applicable. Internal threats may stem from improper utilization of the VoIP implementation or the malicious actions of an employee that has internal access to the VoIP implementation. Whereas the external threats stem from individuals attempting to utilize the VoIP implementation from an external location and would not necessarily have internal access to the VoIP implementation as he or she is not an employee. These table excerpts will be correlated to form a holistic table for the mitigation or avoidance of the most prevalent civil liability risks with regards to a new communication implementation, such as VoIP.

4.1 Did the organization act like a reasonable person would have acted in the same circumstances?

Table 3: Negligent Information Security

Internal		**External**	
King III Principle	**COBIT Process**	**King III Principle**	**COBIT Process**
5.1 (4) (5)	**EDM01; MEA01**	**5.1(1) (9); 5.6 (40)**	**EDM01; DSS07; MEA01**

Should a breach in the VoIP implementation security be exploited, can the organization show that it did in fact act like a reasonable person would have acted in the same circumstance with regards to the VOIP implementation and its security, both internally and externally? An organization may begin to show its intent to act as a reasonable person by implementing the identified Principles and Processes in Table 3.

(i) Internal

An organization should ensure that employees receive the necessary Information Security awareness and training. This is highlighted by statements in principle 5.1 of King III, whereby the Directors, having established adequate Governance policy, should also make all employees aware of what is required of them when utilizing the VoIP implementation. This is further compounded by COBIT 5 Processes EDM01 and MEA01. Firstly, EDM01 requires that a Governance framework, or adequate corporate Governance approach, is adopted and monitored. The Directors should agree to the implementation of a corporate Governance approach to the VoIP implementation and establish a relevant Governance policy. Secondly, MEA01 deals with the monitoring of the Corporate Governance approach. It is made apparent that employee compliance to the policy should be monitored.

(ii) External

To safeguard against the external risk of not acting as a reasonable person given certain circumstances there are a number of Principles and Processes to consider. Looking to King III Principles 5.1 (1) and Principle 5.1 (9) it is made apparent that corporate Information Security is the responsibility of the Directors. The Directors should take reasonable steps to protect and monitor systems crucial to organization operations, such as the VoIP implementation, on a continuous basis. The Directors should ensure that a balanced approach exists between all components of Information Security, namely physical, technological and procedural security (Etsebeth, 2011). This may be accomplished by adhering to Principle 5.6 (40) regarding the implementation of an ISMS to oversee the overall security of the VoIP implementation. The Directors may choose to delegate the task of implementing policies, procedures and practices in conjunction with the ISMS to IT management as stated in principle 5.3 (16). In order to adhere to these Principles the following COBIT 5 process could be implemented. EDM01 establishes that the Directors recognize its corporate Information Security responsibility. Furthermore, implementation of MEA01 will ensure that the adequate reporting is established with regards to VoIP and that the Directors are continuously kept up to date with the organization critical implementation. Finally, DSS07 would address the requirement for a secure approach to implementing an ISMS with regards to VoIP. Having established what a reasonable person should do given the same circumstances, one must still determine whether the organization was aware of the foreseeable consequences.

4.2 Were the consequences foreseeable?

Table 4: Negligent Information Security

Internal		**External**	
King III Principle	**COBIT Process**	**King III Principle**	**COBIT Process**
5.1; 5.3(16);5.5	**APO12;MEA01**	**5.1(9);5.5**	**DSS07; APO12**

The proper implementation of Principles and Processes, in this case, will not help identify all foreseeable consequences and will not answer this question to its fullest extent, as this question can, arguably, only be asked once a risk has been exploited. However, the potential consequences as result of a security breach should be explored during proper risk management and Information Security Practices. Therefore, it may be shown that an organization was aware of the foreseeable consequences if the organization adheres to the Principles and Processes, both internally and externally listed in Table 4:

(i) Internal

The Directors should establish VoIP governance policies and charters. The Directors should, in adherence to King III principle 5.1 (5), ensure that all employees are made aware of the policies and consequences for not adhering to established policies. The Directors could delegate the task of implementing VoIP specific policies in adherence with principle 5.3 (16) of King III to appropriate management. These VoIP implementation specific policies should be drafted in light of potential consequences possibly identified by proper risk management as stated in Principle 5.5. By implementing processes APO12 and MEA01 the Directors may monitor compliance to established corporate Information Security policies, procedures and practices with regards to VoIP. This would aid in fostering security awareness and culture for the VoIP implementation.

(ii) External

The King III principle 5.5 should be adhered to. IT should form an integral part of the organization's risk management. This requires the identification of possible threats and vulnerabilities existing in the VoIP implementation that may result in possible risk to the organization. Furthermore, King III principle 5.1

(9), states that the Directors should be required to regularly check on crucial organization systems operations. This should aid in ensuring no external threats compromise the value of the VoIP implementation. The Directors should be aware of the necessary Processes that should be implemented to ensure complete, timely, relevant, accurate and accessible reporting with regards to the VoIP implementation and its security. By implementing COBIT 5 Processes DSS07 and APO01, the organization should be able to identify all applicable threats that VoIP may present, enabling the organization to identify, mitigate, avoid and monitor the applicable risks.

It must be noted that simply being aware of the possible consequences will not ensure that an organization is not negligent with regards to Information Security. The organization must still show that it took adequate steps in preventing the foreseen threats from materializing.

4.3 Would a reasonable person (organization) have taken steps to prevent the threat from materializing?

Table 5: Negligent Information Security

Internal		**External**	
King III Principle	**COBIT Process**	**King III Principle**	**COBIT Process**
5.1; 5.3(16);5.6 (40)	**DSS07; APO12; MEA01**	**5.3 (16) ;5.6 (40) (42.1)(42.2) (42.3) 5.1(9);5.5**	**DSS07; APO12; MEA01**

An organization could show that it had taken reasonable steps to prevent the threat from materializing by implementing the Principles and Processes in Table5 with regards to the IT and VoIP implementation:

(i) Internal

Employees should have been made aware of the applicable corporate security policies. An organization still needs to be adequately prepared to address risks posed by employees. These risks should be identified, mitigated and monitored. King III Principle 5.3 (16) highlights the task of minimizing risks introduced by IT implementations such as VoIP. Furthermore Principle 5.6 (40) should be taken into consideration for internal controls, by means of an ISMS, with regards to the utilization of the VoIP implementation. The process APO12 provides further sub-Processes for the management of risks, DSS07 should be considered for internal security controls and MEA01 deals with the monitoring of compliance to policies so that the organization may take disciplinary steps to ensure that risks do not materialize.

(ii) External

The employees delegated the task of IT governance, according to principle 5.3 (16), should ensure that all the applicable policies and procedures are implemented in order to protect the VoIP implementation from external threats. Therefore, the Directors, through management, should ensure the establishment of an ISMS that would seek to prevent the materialization of potential risks to the VoIP implementation. An ISMS should be implemented with DSS07 and principle 5.6 (40) in mind. Furthermore, the ISMS should ensure that threats that pose risks to confidentiality, integrity and availability should be mitigated as stated in statements 42.1, 42.2 and 42.3. The organization should identify, mitigate and monitor risks posed by threats to the VoIP implementation according to APO12. The Directors should also receive accurate and timely reporting with regards to the implementation in line with process MEA01. Having established what reasonable Directors should consider with regards to the VoIP implementation, the Directors should also be aware of their possible liability due to the actions of those employed by the organization.

5. Vicarious Liability

Should a security breach, caused by the actions of an employee internal to the organization, with regards to the VoIP implementation, the organization may be held strictly liable for the delict. The organization would be indirectly (vicariously) liable for damages caused. This form of liability applies where there is a relationship between the two parties such as that between the employer (organization) and the employee (Neethling, Potgieter, & Visser, 2006, p. 338). Furthermore, the Director representing the organization in subsequent legal action may hold the appointed management personally liable or may be personally held liable as a result of his or her failure to aid the organization in avoiding the risk of civil liability due to vicarious liability (Nthoiwa & Francis, 2010). There are a number of questions that may be used to test whether an organization should be held vicariously liable for damages and/or losses (Etsebeth, 2011).

5.1 Did an employer-employee relationship exist between the parties?

Table 6: Vicarious Liability

Internal	
King III Principle	**COBIT Process**
5.1 (4) (5) 5.3 (16)	**EDM01 ; MEA01**

Was there a relationship between the organization and employee who breached information? Did the organization relay to the employees how he or she should interact with the VoIP implementation and were they informed of required security practices? Applying the Principles and Processes shown in Table 6 may not establish a relationship but would serve to show an existing dialogue between employee and employer regarding the VoIP implementation.

(i) Internal

According to King III (5.1) statement 4, the Directors should have established an applicable IT Governance policy, establish accountability and outline the organizations approach to IT implementations such as VoIP. This should provide all employees with an internal set of rules, as part of their contract of employment. Furthermore, Principle 5.3 (16) notes that all applicable policies and procedures regarding IT implementations utilization should be established, enabling employees to interact with the VoIP implementations in an acceptable manner during the course of their duties. It is required of the Directors, according to principle 5.1 (5), to make employees aware of the policy, be it by means of the employment contract or further training. This would result in a relationship between the employer and employee with regards to the proper use of a VoIP implementation in the course of their duties. In accordance with COBIT processes, EDM01 and MEA01 should be implemented. EDM01 states that a governance framework should be established and communicated to employees. Furthermore, employees should be required to, as a stakeholder in the organization, assist in the monitoring, reporting and corrective actions with regards to the VoIP implementations where ever possible. This shows a further link between the employee and employer.

Once an adequate relationship has been established, it must still be determined whether a wrongful human act was in fact committed by the employee.

5.2 Was a wrongful human act committed?

Table 7 Vicarious Liability

Internal	
King III Principle	**COBIT Process**
5.3 (16) ; 5.5	**APO12 ; MEA01**

As seen in section 4.5.1, the organization should provide employees with the required policy and procedures. These policies and procedures should be made available to employees. These policies and procedures should contain all rules and regulations that should dictate the actions of an employee when utilizing the VoIP implementation which should reflect the identified Principles and Processes in Table 7. The policies and procedures should reflect all acts deemed as a wrongful act. Contravening these policies and procedures may be seen as a risk to the organization and should be monitored and mitigated. Should an employee violate these, a wrongful act could have been committed.

(1) Internal

According to King III principle 5.5, a risk portfolio should be established to identify potential risks with regards to utilizing the VoIP implementations. These potential risks, in line with principle 5.3 (16), should form part of the effective IT policies, Processes, procedures and standards and should be implemented with the view to minimize IT risk with regards to the VoIP implementation. These policies should detail what a wrongful act is with regards to the VoIP implementation. Therefore, in accordance with APO12, all actions that would constitute a wrongful act should be seen as a potential risk as the organization may be held vicariously liable and should be treated accordingly. Having identified these risks, adequate monitoring should be implemented to aid in their mitigation by means of process MEA01.

Having established that the actions of the employee are wrongful and therefore should be against the organization's policy, was the wrongful action committed within the scope of that employee's employment?

5.3 Was the act committed in the scope of employment?

Table 8: Vicarious Liability

Internal	
King III Principle	**COBIT Process**
5.1 (4) ; 5.3 (16)	**APO12 ; MEA01**

In order for an organization to be able to escape vicarious liability it must show that the act was done completely outside the scope of employment and done for purely personal means of the employee: "If the employee, viewed subjectively, has not only exclusively promoted his own interests, but, viewed objectively, has also completely disengaged himself from the duties of his contract of employment", then the employee can be seen as acting outside of the scope of employment (Neethling, Potgieter, & Visser, 2006, p. 338). Therefore, the duties of the employee and the scope of the employment should be clearly defined by the organization as shown by the principles in Table8.

(i) Internal

First of all Principle 5.1 (4) notes that the accountability of Directors should be established with regard to IT and its implementations such as VoIP. Furthermore, the King III Principle 5.3 (16) advocates that effective IT policies, processes, procedures and standards should be implemented with the view to

minimize IT risk. These policies should detail the exact scope of employment and duties that may be carried out over the VoIP implementation. Adequate monitoring, according to MEA01 and in accordance with RICA, should be exercised to ensure that the VoIP implementation is in fact being used for its intended purpose. Furthermore, the possible risks of employees utilizing the implementation outside the scope of employment should be managed by means detailed in APO12.

Finally, besides negligent Information Security and possible vicarious liability, which may both result in damages to a third party, there is still the possibility of causing damages to a third party or even employees utilizing the VoIP implementation by means of privacy infringement.

6. Privacy Infringement

Many organizations that have recognized that information is an important asset to the organization have moved to improve their means of communications. These improvements seek to aid in better productivity of employees and better management of information. Many organizations implement VoIP with other consolidated mediums for this reason. However, since it is apparent that information is valuable, it is paramount that particular private information with regards to stakeholders and organization transactions be kept private.

The following questions, which may be asked of an organization to determine civil liability, are summarized into one main question as each subsequent question serves as a sub-question in answering the main question regarding whether privacy has indeed been infringed upon (Etsebeth, 2011).

6.1 Is the information properly collected, stored and distributed?

Table 9: Privacy Infringement

Internal		**External**	
King III Principle	**COBIT Process**	**King III Principle**	**COBIT Process**
5.1 (4)(5) 5.6(38)(39)	**EDM01; MEA01**	**5.3 (16)**	**APO12; MEA01**

An organization should ensure the lawful acquisition, distribution and storage of private information. An organization may implement the following Principles and Processes, as shown in Table 9, with regards to its VoIP implementation.

(i) Internal

The Directors are required, when referring to principle 5.1 (4), to establish governance policies to reflect how the organization wants personal information to be handled within the organization. The Directors should oversee the employee awareness of information handling policies regarding the VoIP implementation in accordance with King III principle 5.1 (5). In addition, King III principle 5.6 (38) specifies that it is the responsibility of the board to ensure that personal information is identified and treated accordingly. Furthermore, Principle 5.6 (39) stipulates that all legislation pertaining to the handling of personal information must be adhered to. The Directors, when implementing process EDM01, should establish how private information is governed and subsequently ensure that the Governance is monitored. Therefore, utilizing MEA01, the handling of private information should be monitored and corrective action taken if necessary.

(ii) External

Effective IT policies, processes, procedures and standards should be implemented with the view to minimize IT risk. The King III principle 5.3 (16) should aim to mitigate the risk of privacy infringement through proper policy, Processes and procedures. In accordance with APO12, risks to private information during collection, distribution and storage should be identified and appropriate steps taken to mitigate

them. The handling of private information should be monitored and corrective action taken if necessary according to COBIT 5 process MEA01.

In addition to this, when obtaining data, its accuracy should be determined and maintained during its storage at the organization.

6.2 Is the information accurate?

Table 10: Privacy Infringement Table Excerpt 2

Internal		External	
King III Principle	**COBIT Process**	**King III Principle**	**COBIT Process**
5.3(16)	**APO12; MEA01**	**5.6(42.2) (42.3)**	**DSS07**

Appropriate procedures should be in place, shown in Table 10 , to ensure the integrity and availability of the information to aid in the avoidance of the risk of privacy infringement.

(i) Internal

Effective IT policies, Processes, procedures and standards should be implemented with the view to minimize the potential risk presented by the VoIP implementation. This should be done in accordance with King III principle 5.3 (16). These policies should ensure that information is correct and only accessible to the information owner. The risk of information being accessed and altered by parties, potentially employees, who have no right to the information should be identified, mitigated and monitored in accordance with APO12. Furthermore, compliance to policy with regards to information integrity should be monitored for compliance following the steps of process MEA01.

(ii) External

The integrity of information traversing the VoIP implementation that is processed by employees over the VoIP implementation should be maintained in line with principle 5.6 (42.2). The organization should also make certain that information is only available to those who have the right to access it in accordance with principle 5.6 (42.3). In order to ensure the integrity and availability of the information, adequate security measures should be taken as discussed in COBIT 5 process DSS07.

Accurate data reception and keeping it up to date may not be enough to prevent persistent threats from intercepting or altering information. Technical, procedural and physical Information Security precautions should be implemented with regards to the VoIP implementation.

6.3 Were appropriate technical, procedural and physical security measures taken to safeguard the individual/group against the risk of loss, damage, destruction of or unauthorized access to personal information?

Table 11: Privacy Infringement

Internal		External	
King III Principle	**COBIT Process**	**King III Principle**	**COBIT Process**
5.3(16); 5.6 (38)(40)	**APO12; MEA01; DSS07**	**5.6 (40) (42.1) (42.3)**	**DSS07**

An overall governance shift towards Information Security should be exercised. All possible security measures to ensure the confidentiality, integrity and availability of information to those with permission on the enterprise VoIP should be implemented as shown in Table11.

(i) Internal

According to Principle 5.3 (16), the delegated employees such as management, should ensure that all the required policies, procedures and standards should be implemented in order to protect information on a communication technology implementation. These policies and procedures should stipulate what is considered personal information and should determine how such information should be treated with regards to its security in accordance with Principle 5.6 (38). This should be done in conjunction with Principle 5.6 (40), ensuring an adequate ISMS is implemented for the VoIP implementation. When reviewing MEA01, it is apparent that applicable internal privacy policies and adherence to them should be monitored and corrective action should be taken if they are found to be inadequate. All necessary internal security measures should be taken to prevent infringement of privacy by means of process DSS07 and in light of proper risk management as detailed in APO12.

(ii) External

The Directors should ensure that an ISMS is developed and implemented. This would aid in preventing threats from materializing and therefore mitigating the risk posed to private information by the VoIP implementation. The confidentiality of personal information communicated via the VoIP implementation, should be assured by all available security means. In addition, the integrity of personal information traversing the IP network between VoIP devices should be maintained and that personal information is only available to those who have the right to access it. All appropriate security precautions, in accordance with process DSS07, should be taken when implementing VoIP as the primary means of communication to ensure that all possible methods have been used to secure private information.

An organization that has implemented the previously mentioned Principles and Processes may begin to protect personal information from risk.

There are many risks that an organization will face during the course of operations. The organization may be held civilly liable for damages caused by any of the actions mentioned in previous sections. Organizations should be sure to practice proper IT Governance with regards to its communications assets such as VoIP. Should an organization exercise proper Governance and adhere to best practices, it may avoid civil liability.

7. An Approach to Avoiding the most Prevalent Risks of Civil Liability to Organizations in South Africa

Having listed the most prevalent civil liability risks to organizations in South Africa and the subsequent questions the organization would be required to answer, an approach to avoiding these risks will be established in this section. Each risk and subsequent answer may be answered or addressed by appropriate Principles and Processes found in the King III Report and the COBIT 5 Framework respectively. The table excerpts discussed with the risks, questions, Principles and Processes all come together to form the "VoIP: Civil Liability Risk Table".

Table 12: VoIP Civil Liability Risk Table

		Internal		External	
		King III Principle	COBIT Process	King III Principle	COBIT Process
Negligent Information Security	Did the company act like a reasonable person (organization) would have acted in the same circumstances?	5.1 (4)(5)	EDM01; MEA01	5.1 (1)(9); 5.6 (40)	EDM01; APO13; MEA01
	Were the consequences foreseeable?	5.1 (5); 5.3 (16); 5.5	APO12; MEA01	5.1 (9); 5.5	APO12; APO13
	Would a reasonable person (organization) have taken steps to prevent the threat from materializing?	5.3 (16); 5.6 (40)	APO12; APO13; MEA01	5.3 (16); 5.6 (40) (42.1) (42.2) (42.3)	APO12; APO13; MEA01
Vicarious Liability	Did an employer-employee relationship exist between the parties?	5.1 (4)(5); 5.3 (16)	EDM01; MEA01		
	Was a delict committed?	5.3 (16); 5.5	APO12; MEA01		
	Was the act committed within scope of employment?	5.1 (4); 5.3 (16)	APO12; MEA01		
Privacy Infringement	Is the information properly collected, stored and distributed?	5.1 (4)(5); 5.6 (38)(39)	EDM01; MEA01	5.3 (16)	APO12; MEA01
	Is the information accurate?	5.3 (16)	APO12; MEA01	5.6 (42.2) (42.3)	APO13
	Were appropriate technical, procedural and physical security measures taken to safeguard the individual/group against risk of loss, damage, destruction of or unauthorized access to personal information?	5.3 (16); 5.6 (38)(40)	APO12; APO13; MEA01	5.6 (40) (42.1) (42.2) (42.3)	APO13

Should an organization wish to implement VoIP, the organization could refer to this table to ensure that its existing Governance practices, policies and procedures are in line with the recommended Principles and Processes to aid in the prevention of the most prevalent civil liability risks that organizations in South Africa could face. To demonstrate how the table may be used, an analogy is outlined in the following paragraphs. Organization A wishes to change its primary means of communication from PABX to VoIP. As VoIP is a more cost effective and dual-natured communication medium the value to the organization is apparent. However, since information in multiple formats will be traversing the VoIP implementation, the implementation should be properly secured. Organization A could check the "VoIP: Civil Liability Risk Table" and note that it would be at risk of being negligent with regards to its Information Security if it does not make the securing of the VoIP implementation a Governance concern. It is also noted that all appropriate controls should be put in place with adequate policies and procedures. Next, Organization A realizes that a clear policy on how and for what purposes the VoIP implementation is to be used is needed. This clear policy and organizational awareness of it may aid Organization A in avoiding the risk of vicarious liability. Finally, it is noted that personal and private information should be treated with the utmost care. By following the table's questions and related Principles and Processes the organization may make informed decisions on how to treat private information when utilizing the VoIP implementation. This should aid in ensuring that the risk of private information of employees or clients is never revealed without permission. As shown in the scenario, by answering each question and following the appropriate Principles and Processes, good Governance should be apparent in organization. Due diligence and due care are being adhered to as foresight with regards to civil liability is displayed by the Directors. This

shows the foresight of the organization to identify and mitigate the risks, before implementing the VoIP implementation as the primary means of communication.

8. Verification

The "VoIP: Civil Liability Risk Table" underwent a process of elite interview in order test its validity as a means of avoiding the most prevalent civil liability risks. Three experts were chosen from the fields of corporate governance and the South African legal system. Two experts were long standing members in the legal system and both have over 10 years' experience with cases relating civil liability. The final expert is a noted expert in the field of corporate governance, especially the subsequent field of information security governance. These experts, due to the process of elite interviewing, have purposefully been kept anonymous. Each expert individually reviewed the table and answered prepared questions relating to the tables effectiveness as a tool to avoid the most prevalent civil liability risks when implementing a new technology. All three of the experts unanimously agreed that utilizing the "VoIP: Civil Liability Risk Table" would aid an organization in avoiding the most prevalent civil liability risks when implementing new communication technologies such as VoIP. Minor changes were recommended for the table, however, all recommended changes were made to the "VoIP: Civil Liability Risk Table" before the submission of this paper. One key change was that the acronym of COBIT Process DSS07 was changed to APO13, to better align the Processes in the final released version of COBIT 5.

9. Conclusion

VoIP has the potential to provide an organization with a more feature rich communication medium at a reduced cost. However, all this value will be diminished if an organization does not take the time to ensure that the adequate Governance and Information Security steps regarding the VoIP implementation are taken by the Directors. Adequate steps should be taken with regards to policies and procedures that should be implemented in parallel with the VoIP implementation to prevent the known and potential risks. A VoIP implementation has much value to offer any organization that takes the time to implement it correctly and even more to an organization that considers the implications of civil liability risk.

References:

Etsebeth, V. (2011). Defining the Current Corporate IT Risk Landscape. *Journal of International Commercial Law and Technology , 6* (2), 62-73.

Heyink, M. (2011). *Information Security Guidelines for Law Firms.* Retrieved September 11, 2012, from ISSA: http://www.lssa.org.za/upload/Information%20Security%20Guideline%202011.pdf

IoDSA. (2009, September 1). *Law Documents: King III Report.* Retrieved from University of Preoria Library: http://www.library.up.ac.za/law/docs/king111report.pdf

ISACA. (2011). *COBIT 5: Process Reference Guide (Exposure Draft).* ISACA.

James, P., & Woodward, A. (2007). Securing VoIP: A Framework to Mitigate or Manage Risks. *Australian Information Security Mnagement Confernece* (pp. 103-116). Perth: Edith Cowan University.

Kotze, B. (2012, January 30). *King III consolidaters role of IT in corporate governance.* Retrieved September 11, 2012, from ITWeb: http://www.itweb.co.za/index.php?option=com_content&view=article&id=52014

Krippendorff, K. (2003). *Content Analysis: An Introduction to Its Methodology.* SAGE.

Neethling, J., Potgieter, J. M., & Visser, P. J. (2006). *Law of Delict.* Pretoria: LexisNexis.

Nthoiwa, J., & Francis, L.-A. (2010, February 24th). *Better governance with King III.* Retrieved September 11, 2012, from iWeek: http://www.iweek.co.za/special-report/better-governance-with-king-iii

Trautman, L. J., & Altenbaumer-Price, K. (2011). The Boards Responisbility for Information Technology Governance. *The John Marshall Journal of Computer and Information Law* (29), 313-345.

von Solms, B. (2006). Information Security - The Fourth Wave. *Computers and Security* , 165-168.

.* * * * *

Cite as: Gerber, Tian, Thomson, Kerry-Lynn and Gerber,Mariana. VoIP: A Corporate Governance Approach to Avoid the Risk of Civil Liability.*Journal of International Commercial Law and Technology*, Vol.8 No.4 (October, 2013)