MANAGING DIGITAL EVIDENCE – THE GOVERNANCE OF DIGITAL FORENSICS

MM Grobler (Council for Scientific and Industrial Research, Pretoria, South Africa)
IZ Dlamini (Council for Scientific and Industrial Research, Pretoria, South Africa)

Governance in general is becoming increasingly important in contemporary management, but specifically the governance of Digital Forensics. In order to manage governance disciplines effectively, closer attention needs to be paid to the technical aspects of specialised fields covered within an organisation. This paper presents a novel, scientific definition of Digital Forensic (DF) governance and a preliminary best practice framework.

Similar to other existing organisational governance disciplines, DF governance assists organisations in guiding the management team and stakeholders in setting up mandates and expected actions from the organisation's incident response team. The DF governance framework is designed with a strong input from related governance disciplines, as well as a sound knowledge of the DF discipline. It can support and supplement the role technology and information plays within the business environment. The adoption of this framework by organisations will serve as internal guidance document when addressing digital incidents and attacks.

Key phrases: Information Technology (IT), Information Security (IS), Digital Forensics (DF), governance, framework

1 INTRODUCTION

"There is a deep connection between security, development and respect for human rights, democratic values and good governance in everything we are attempting …"

Traian Basescu

With the boom of Information Technology (IT) and enhanced technological developments, the IT environment evolved to the specialised discipline of Information Security (IS). This has again made provision for the rapid development of Digital Forensics (DF), focusing on digital evidence dispersed through business systems. Regardless of the specific entity, all disciplines involve some form of policies and standards, necessitating the proper facilitation of governance, as indicated by Basescu's quote above.

DF involves the preservation, identification, extraction and documentation of digital evidence stored as data or magnetically encoded information (Vacca 2002:731). This extends to include the recovery, analysis and presentation of digital evidence in a way that is admissible and appropriate in a court of law. This necessitates a crucial accuracy in following forensic procedures, the rules of evidence and the legal processes. In short, DF pertains to any digital artefacts found in computers or other digital resources that may have legal value in the business environment.

The DF governance discipline developed rather rapidly, but up to date has very little international standardisation with regard to processes, procedures or management. To enhance this discipline and to properly utilise the benefits it has proven so far, DF need to be governed just as related information disciplines (such as IS governance and IT governance) need to be governed.

The importance of DF governance in the business environment relates directly to executive management's understanding of the discipline, and their ability to utilise the organisation's digital resources to support the business goals. This article, accordingly, emphasises the importance of DF governance in the business environment by addressing the overlap between DF and corporate governance, as presented in Figure 1. This relationship is formalised by providing a layout for the DF governance framework.

The purpose of this article is to present a scientific definition for the DF governance discipline, as well as a preliminary best practice framework. At the time of writing, no formal definition or framework could be found, supporting the notion to develop this discipline. To enable this purpose, the article will conduct a brief literature overview on existing governance literature, explore current research on DF governance and present a definition and framework for DF governance.

2 GOVERNANCE DISCIPLINE

A proper understanding of DF governance within the business environment is necessary to support the important role that technology and information plays in organisations. DF governance is not only aimed at incident response *(ex ante* - remedial*),* but can contribute to better technology management and integration in supporting organisational strategies (*ex post* – preventative).

Governance refers to the process of administration and management of a specific organisational entity, involving the enforcement and control of policies and standards (Mueller & Phillipson 2007: Internet). The importance of information in the business environment has been proven repeatedly. Due to this business value, it is crucial for organisations to protect their information and to do this under the auspice of confidentiality. The amount of risks that face information in the business environment does not allow anything less than the properly facilitated governance thereof.

Businesses unfortunately often regard computer and information security related issues as a purely technical concern, and it rarely gains the attention of executive management (including top management and the Board of Directors). Computer and

information security rarely gets the necessary strategic attention it should. The associated problems have transgressed into bigger problems. Documentation, such as the newly published King III Report on Governance for South Africa (IODSA 2009:103), requires that organisations share private business information resources openly with stakeholders, often without the boundaries of a secured Virtual Private Network environment. As a result, sensitive business information has become more exposed and vulnerable to misuse by technology adept individuals (Posthumus & Von Solms 2004:638,639). These advances in technology called for the development of a new discipline: *DF governance* (see Section 3).

2.1 Defining governance

Governance is a set of procedures and responsibilities exercised by the executive management of an organisation. The focus of governance is generally aimed at providing strategic direction, ensuring the achievement of objectives and managing risks (Moulton & Coles 2003:580). The focus is on managing the respective organisation and utilising its resources appropriately. Governance involves *"… monitoring and overseeing strategic direction, socio-economic and cultural context, externalities, and constituencies of the institution …"* (Bihari 2008:6). This generic governance definition provides a basic direction for all governance disciplines.

Governance can be seen as the leadership of a specific discipline to ensure the successful completion of discipline specific goals and objectives, within the specified resources (Mueller & Phillipson 2007: Internet). The governance framework is a corporate mechanism to implement proper management and administration in a top-down approach.

2.2 Governance background

The word governance derives from the Greek word *kubernáo,* meaning 'to steer' (European Commission 2002:2). The formal implementation of governance became a standard part of many organisations following a number of major corporate failures and scandals that helped to focus attention on the need of proper governance (previously seen as a burdensome administrative task). Organisations realised that governance is a crucial part of management responsibility. The discipline evolved to include a number of specialised sub-disciplines (Anderson 2001:60).

In general, executive management is responsible and accountable to the organisation's shareholders concerning all governance functions. They should ensure that the organisation produces business value and a fair amount of return on investment (King Report 2001: Internet). Executive management should further

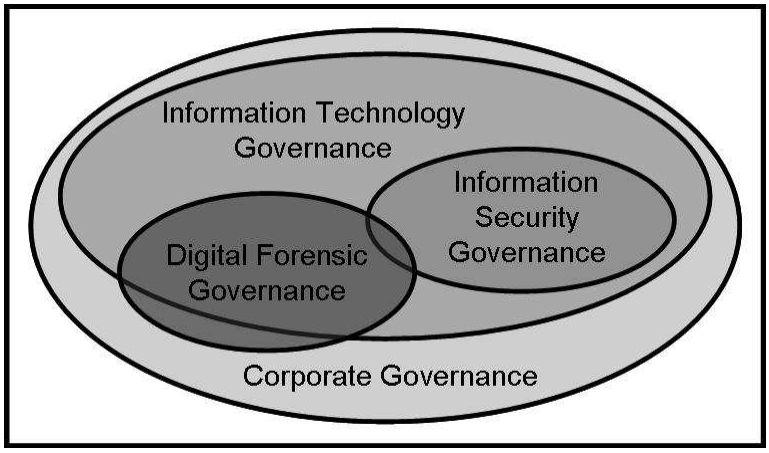
ensure that organisations comply with all applicable laws, regulations and codes of practice (Posthumus & Von Solms 2004:643). Governance laws and regulations hold the executive management accountable for the way their organisations operate, introducing severe criminal penalties for negligent supervision.

2.3 Governance sub-disciplines

The governance concept includes a number of specialised sub-disciplines. The first specialisation relevant to DF governance is corporate governance. From this discipline, the IT governance and IS governance disciplines evolved. Figure 1 shows the relation between these disciplines and positions DF governance within the bigger structure. Since all three governance types have some impact on DF governance, all three governance types are crucial to a successfully implemented DF governance structure.

Corporate governance is the all-inclusive governance discipline, relating primarily to the responsibilities of the executive management. It defines the relationship between an organisation and its shareholders (Hinde 2004:4), including all processes, policies, customs and laws. Corporate governance ensures the strategic guidance of an organisation, as well as executive management's accountability to the organisation and its shareholders (Von Solms 2001:217). When implemented properly, corporate governance ensures the well-being of the organisation (Lessing & Von Solms 2008:2). Figure 1 shows that corporate governance is a very broad discipline, and that all subsequent governance disciplines evolved as sub-disciplines of corporate governance.

Figure 1: Relationships between different governance disciplines



Adapted from: Von Solms & Louwrens 2006:243

IT governance is a multi-faceted discipline focusing on the relationship between IT management and the business functions of an organisation (Lessing & Von Solms 2008:2). IT governance focuses on specific policies and procedures that determine how an organisation directs and controls the use of its technology resources to realise the organisation's business goals. This is a continuous process, requiring ongoing review and adjustment (Posthumus & Von Solms 2005:12). Although the ultimate responsibility for the organisation's functioning lies with executive management, IT managers are responsible for the administration of IT governance within an organisation. Figure 1 shows that IT governance is a specialised sub-discipline of corporate governance.

IS governance is the process of addressing IS at an executive level (Posthumus & Von Solms 2004:639). It can be considered as the establishment and maintenance of the control environment to manage risks relating to information and its supporting processes and systems (Moulton & Coles 2003:581). IS governance ensures that IS strategies are aligned with the organisation's objectives and consistent with applicable laws and regulations (ISACA 2006: Internet). Figure 1 shows that IS governance is a specialised sub-discipline of IT governance.

The fourth governance discipline depicted in Figure 1 is **DF governance**. DF governance is a specialised sub-discipline of IT governance, with some overlap with corporate governance and IS governance. Section 5 will address this discipline in detail.

2.4 Governance framework

Corporate governance indicates that the executive management of an organisation is ultimately responsible for implementing governance. However, governance sub-disciplines are often too specialised - this responsibility need to be disseminated to specific roles of authority and expertise in the relevant departments and knowledge domains (Mueller & Phillipson 2007: Internet). This ensures that the responsibility is still at an adequate authority level, but with sufficient technical and business expertise to manage the discipline appropriately.

The governance framework should focus on establishing a chain of responsibility, authority and communication channels within the organisation. It should put in place mechanisms to measure policies, procedures and standards, implementation progress and enforcement. The governance framework should look holistically at the entire business process (e.g. corporate entity, IT, IS and DF), including the relationship with the organisation's employees, suppliers and customers. The framework should ensure a balance between coordinating regulations and standards,

satisfying the customer (Mueller & Phillipson 2007: Internet), and aligning with the suppliers.

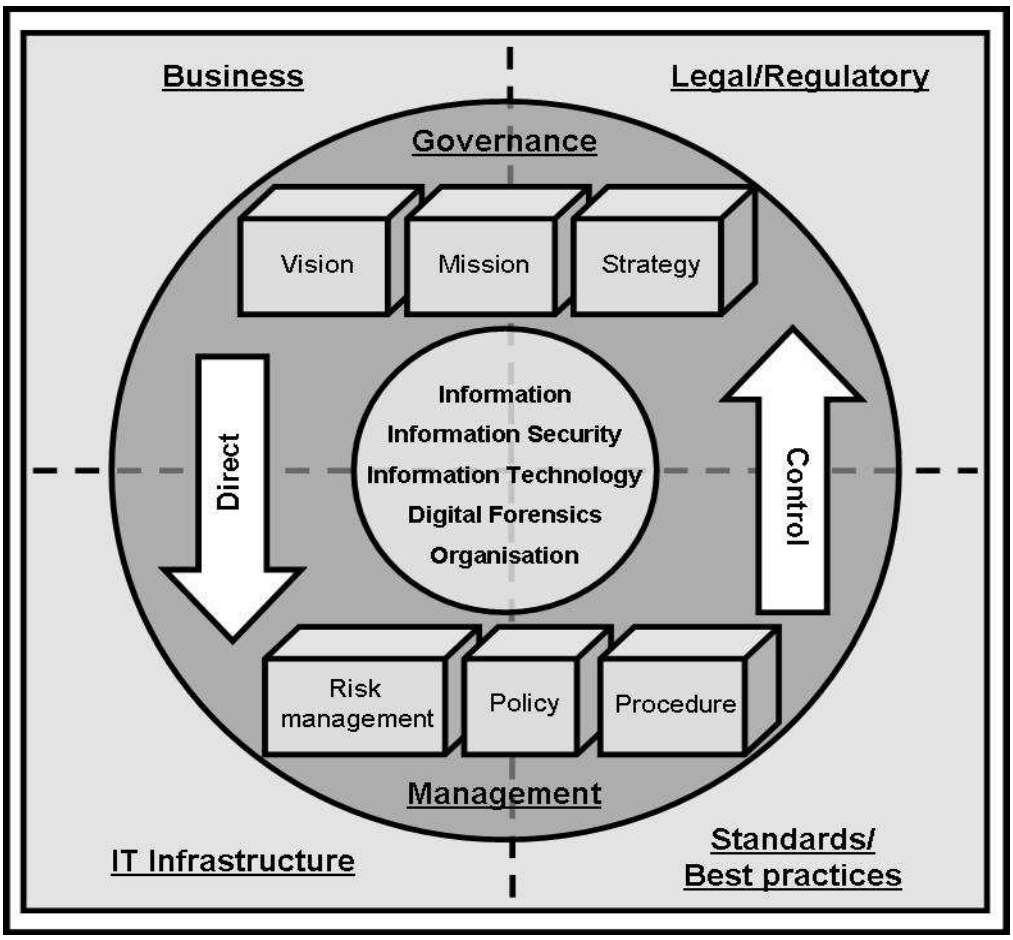
In general, all governance frameworks adhere to the confidentiality, integrity and availability (CIA) principles. *Confidentiality* relates to the protection of sensitive information from unauthorised disclosure and interception. Maintaining *integrity* involves maintaining the accuracy and completeness of information. *Availability* refers to the accessibility of information by the relevant parties, at the right time. If any of these characteristics of information has been compromised, management can make ill-advised decisions, potentially affecting the larger organisation negatively. If the governance framework addresses the CIA principle appropriately, it can assist the discipline in mitigating risks to the information through the application of a suitable range of security controls. These controls should be an appropriate mix of physical, technical or operational security controls (Posthumus & Von Solms 2004:639,640,642).

A governance framework consists of two distinct sides: governance and management (see Figure 2). The *governance side* directly involves the executive management's function, as well as the direction of the organisation. The main responsibilities of the governance side are business and legal/regulatory aspects, involving the vision, mission and strategy of the organisation. The governance side strongly involves all strategy decisions, and regulates the overall direction of the organisation (Bihari 2008:6; Pemble 2004:18). The governance side directs the management aspects.

The *management side* is more concerned with the implementation and execution of the organisational strategy, as well as the functional and operational management levels. The main responsibilities of the management side are IT infrastructure, standards and best practices. This involves risk management, policy and procedure development and implementation. Successful management requires the commitment from various managers within the organisation. This side can also be referred to as the tactical or operational role of the executive management. The management side controls the governance aspects.

Generally, the management side is more hands-on activities than the governance side, involving supervision and goal accomplishment (Bihari 2008:6; Pemble 2004:18), opposed to the vision, mission and strategy of the governance side.

Figure 2: The governance and management sides of a governance framework



Adapted from: Posthumus & Von Solms 2004:645

2.5 Benefits of a properly implemented governance framework

A governance framework should answer three fundamental questions: (1) what decisions must be made for effective management, (2) who should make those decisions and who has input rights, and (3) how will the decisions be agreed on and implemented. Some benefits of a properly implemented governance framework (Afshar, Cincinatus, Hynes, Clugage & Patwardhan 2007:3,4,9,10; People First 2009:2,4; Turle 2009:51) include:

- clearly defined responsibility matrix;
- defined strategic direction and scope;
- diminished scope creep within specific projects and discipline boundary;
- pre-defined structure for future business cases;
- defined service delivery and/or operating models;

- defined risk and compliance management plans;
- easy administration of project reports;
- appropriate data protection and governance policies in place;
- achieving business agility and innovation;
- improved communication between top and bottom levels;
- increasing customer satisfaction and retention;
- customised processes specific to the discipline;
- defining and enforcing policies specific to the discipline; and
- improved data quality across the organisation.

DF and DF governance are crucial for organisations working with digital devices. Not only will it improve the trust of stakeholders regarding the organisation's management, but it may also improve the organisation's status among competitors and other organisations. DF governance may decrease incidents, as well as cost, time and effort related to forensic investigations. Proper DF governance may also decrease the occurrence of inadmissible evidence from the organisation's forensic investigations, since procedures, regulations and policies pertaining the handling of digital evidence will be in place (Vacca 2002:731). DF governance also directs an organisation to proper:

- strategic alignment;
- risk management;
- resource management;
- performance measurement; and
- value delivery (ISACA 2006: Internet).

3 GOVERNANCE OF DF

Many governance models exist that applies specifically to corporate governance, IT governance and IS governance. At the time of writing, there was no model developed solely for DF governance or any model based on acknowledged best practice and related documents. Considering the potential benefits of a properly implemented DF governance framework, this research is long overdue. The overlap between the highly technical DF discipline and the business approach of governance, makes DF governance a highly specialised discipline. Few individuals have sufficient interdisciplinary knowledge on computer, legal and business aspects.

3.1 The need for DF governance

DF governance is a relatively new discipline, with very little current research or formal structure. It relates the process of governing and administration of evidence that are admissible in court. The International Standard Organisation's Joint Technical Committee 1 (ISO/IEC JTC1) commissioned a study group in 2008 to investigate the feasibility of an international standard on DF governance. At the time of writing, there are no ISO/IEC JTC1 standards that specifically address DF governance. However, there is an international awareness of problems associated with the variation in the inter-jurisdictional transfer of information relating to legal proceedings (ISO 2009:4).

The intention of this paper is to identify a close relationship between the corporate governance and DF governance disciplines. Technically, this new discipline should be the corporate governance of DF, aiming to address concerns of the Corporate Board (see Figure 1). This includes a harmonisation strategy for integrating the different parts of related standards and best practices (ISO 2009:6) into a single DF governance guide.

The impact of this study on the existing governance disciplines should be complementary. Not only does this study provide a formal comprehensive definition for DF governance, but it also provides a wide-ranging framework for DF governance. Implementing organisations can use this framework as a guideline when addressing rising numbers of computer incidents within their boundaries, especially when these incidents are addressed internally.

3.2 Who should be concerned with DF governance?

It is quite important that an organisation’s management be involved in all the different facets of governance. It is critical that executive management understands that their accountability and responsibility in terms of corporate governance extends into the IT governance discipline (Posthumus & Von Solms 2005:13), and likewise extends to the IS and DF governance disciplines (this interdependent relationship was illustrated in Figure 1).

In general, senior management should be accountable for the protection and execution of all forensic cases that may jeopardise the reputation of the organisation. It is therefore significant for them to ensure that the management of digital data within the organisation runs smoothly at all times for later analysis in case of incidents. This also includes the partnership among the employees, executive management, steering committee, network administrator and chief IS officer. All these employees have different responsibilities, working towards the protection of the organisation’s interest and developing the organisational strategies. The executive management

can be responsible for DF governance, but the chief IS officer and network administrator should be responsible for discipline specific accountabilities that require specific expertise. Preferably, the chief IS officer should be responsible for the appointment of qualified DF investigators to handle specific incidents. The executive management, the discipline's management and the investigators should work hand in hand. DF is a very technically specialised discipline, but the governance thereof overlaps with other governance disciplines (ISACA 2006:19).

DF governance should not be a standalone framework within the organisational governance structure. All parties involved should work cooperatively with other parties within the specific field to ensure successful governance (ISACA 2006:20). This will ensure quick and efficient handling of IS breaches with in-house forensic expertise. Proper training in this regard will limit the potential negative impact security breaches may have on an organisation's public reputation. In accordance with this forensic training, investigators can be measured with regard to their compliance with the international standard, ISO 27037 *Guidelines for identification, collection and/or acquisition and preservation of digital evidence*. At the time of writing, this standard was only available in draft version.

3.3 Why are DF and DF governance important?

Different types of cyber incidents are reported daily, across the world. However, organisations tend to not report a large percentage of crimes to prevent a bad reputation in the business world and a potential loss of clients (Nucci 2009: Internet). These incidents can be handled in-house, when an organisation have an implemented DF governance framework.

With the recent flux of identity theft and identity fraud, organisations need to take care in sharing, accessing and handling their data (Sophos 2009:6). This is even more important in the event of a cyber incident. No matter how small the discovered incident is, it needs proper investigation to discover its source, purpose, impact and responsible suspect. Proper handling can also aid in establishing trends and characteristics to use in future. Accordingly, DF and DF governance are crucially important.

3.4 Defining DF governance

DF governance is a subset of the other organisational governance types (see Figure 1) and has to fulfil the main objective of the overarching organisational governance structure. To ensure success and a proper impact, DF governance must have a formal definition to set the boundaries of the discipline and identify the relationship with interrelated governance disciplines.

Based on the research done on other governance disciplines, *DF governance can be defined as:*

- the administration and management of a set of procedures and responsibilities pertaining to any evidence found in computers and other organisational digital resources that may have legal value,
- aimed at ensuring forensic admissibility in a court of law, the successful prosecution of perpetrators in the cyber dimension, the assessment of digital outputs and the achievement of objectives set out in the organisational strategy with regard to DF,
- within the limits of specified organisational resources,
- as facilitated by the Board of Directors, executive management and any DF knowledgeable authorities indicated by the Board of Directors and/or executive management.

The successful implementation of DF governance depends on the scope and richness of the DF governance definition and framework employed by an organisation. The definition is supplemented by the preliminary framework.

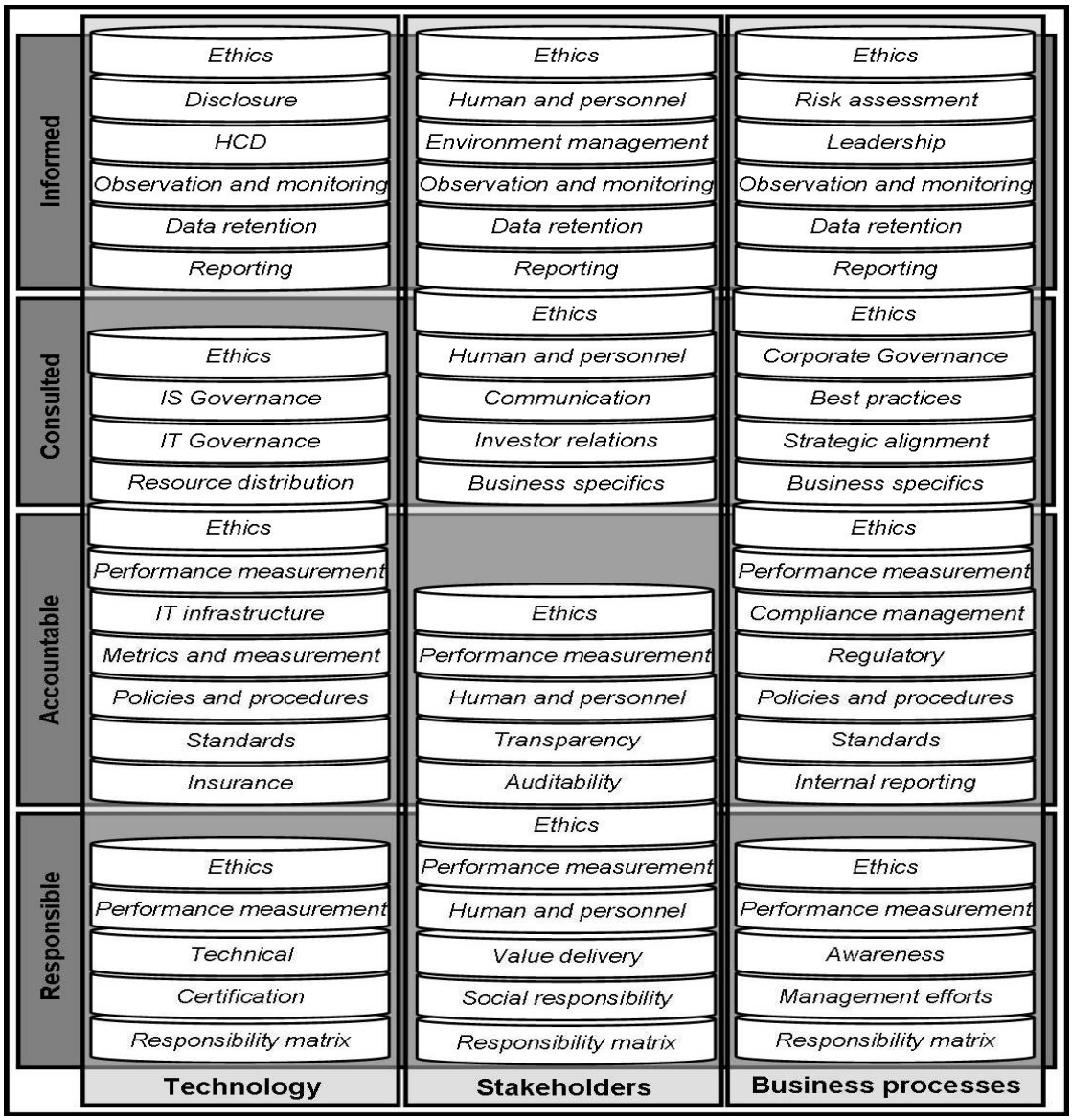
4 A PRELIMINARY FRAMEWORK FOR DF GOVERNANCE

The implementation of a framework document ensures that an organisation effectively covers all relevant aspects that can holistically affect the organisation (Lessing & Von Solms 2008:2). To enable this, the DF governance framework can be assessed based on its compliance with the DF governance definition, in particular the DF evidence's admissibility to a court of law. The DF governance framework should support the DF discipline by employing organisational policies. The main aim of DF governance should be the alignment of the DF approach with the organisational strategy in an attempt to support the development of the organisation in delivering consistent business value.

This research paper builds the DF governance framework on the RACI matrix, addressing **R**esponsibility, **A**ccountability, **C**onsultation and **I**nformation (Mueller & Phillipson 2007: Internet). A RACI matrix is a chart of all the activities or decision making authorities undertaken in an organisation set against all the people or roles. At each intersection of activity and role it is possible to assign somebody responsible, accountable, consulted or informed for that activity or decision. *Responsible* indicates the person who performs an activity or does the work; *Accountable* indicates the person who is ultimately accountable and has Yes/No/Veto; *Consulted* indicates the person that needs to feedback and contribute to the activity; and *Informed* indicates the person that needs to know of the decision or action (Morgan 2008: Internet).

According to Posthumus and Von Solms (2004:639), a properly designed governance framework should ultimately address three fundamental elements: technology, stakeholders and business processes. These elements are incorporated into the RACI matrix. With regard to DF, *technology* can be considered as any new developments in hardware and software, forensic specific software and hardware, data mining and data extraction. *Stakeholders* refer to staff, customers and clients, suppliers and vendors, the disciplinary and judicial system. *Business processes* are at the heart of business success. It may refer to any commercial processes where digital crime can be involved, such as procurement. Figure 3 shows the preliminary DF governance framework.

Figure 3: Preliminary DF governance framework



Source: Own compilation

In general, forensic investigators should have a balanced knowledge of most aspects of the preliminary DF governance framework. They should have a wide knowledge of relevant legislation and policies, procedures, codes of practice and guidelines for investigating digital evidence. The next sections briefly introduce all the elements included in the DF governance framework.

4.1 Technology elements

The *Responsible* component of the RACI matrix refers to all technology elements requiring a level of trust, or answerability for an act or its consequences. With regard to technology elements, this component is directed to IT or DF authorities. Table 1 presents the technology elements that falls under the *Responsible* component of the RACI matrix.

Table 1: Technology elements – Responsible component

DF governance framework: Technology elements – Responsible component	
responsibility matrix	determines and documents who is responsible for each individual task and activity, mapped onto the work breakdown structure
certification	formally validating specific facts and competency regarding DF in an organisation, such as software certification to confirm forensic soundness, or investigator certification to confirm that the investigator are competent to handle DF cases
technical	as a sub part of IT, DF is a highly technical discipline that needs both complex technology as well as advanced technical expertise
performance measurement	ongoing assessment and tracking of technology performance against set goals and objectives
ethics	principles and morals concerning right and wrong and may refer to the organisation's legitimate purchase of software licences

The *Accountable* component of the RACI matrix refers to all technology elements requiring liability for one's actions. With regard to technology elements, this component is directed to IT or DF management. Table 2 presents the technology elements that falls under *Accountable* component of the RACI matrix.

Table 2: Technology elements – Accountable component

DF governance framework: Technology elements – Accountable component	
insurance	security precaution measures that needs to be taken for all the technological resources to prepare for the worse before it happens
standards	internationally established norms or requirements for a specific field of specialisation, for example ISO 27037 are relevant to the DF technical field
policies and procedures	rules and guidelines on how to handle all hardware and software resources within the organisation, including the technological equipment and assets
metrics and measurements	a structure to measure whether DF and digital evidence meet specific criteria to address the need, applicability and admissibility of DF in a given situation, e.g. the Frye and Daubert metrics
IT infrastructure	the sum of facilities, structures and capabilities needed to ensure the efficient functioning of the IT environment within organisational boundaries, hardware, software, policies and procedures

Performance measurement and ethics (already introduced under the *Responsible* component) also falls under RACI's *Accountable* component.

The *Consulted* component of the RACI matrix refers to all technology elements requiring the action of getting advice or input from another entity. With regard to technology elements, this component is directed to IT or DF management. Table 3 presents the technology elements that falls under *Consulted* component of the RACI matrix.

Table 3: Technology elements – Consulted component

DF governance framework: Technology elements – Consulted component	
resource distribution	ensuring that the relevant resources (e.g. time, money, expertise, hardware, software) are available when required
IT governance	Figure 1 shows an overlap between DF governance and IT governance: both disciplines are heavily dependant on technology
IS governance	Figure 1 shows an overlap between DF governance and IS governance: both disciplines are heavily concerned with the security and justice related to information

Ethics (already introduced under the *Responsible* component) also falls under RACI's *Consulted* component.

The *Informed* component of the RACI matrix refers to all technology elements requiring the action of imparting knowledge of some facts to another entity. With regard to technology elements, this component is directed to IT or DF management. Table 4 presents the technology elements that falls under *Informed* component of the RACI matrix.

Table 4: Technology elements – Informed component

DF governance framework: Technology elements – Informed component	
reporting	the presentation of results based on analysed evidence gathered from the digital storages
data retention	the preservation of data generated by IT resources as either hard or soft copy, including the retrieval of the stored data from the digital storage media using different IT tools
observation and monitoring	the pre-securing of digital resources, combined with an intrusion detection system to observe data passing through
human capacity development (HCD)	effort to advance the skills and knowledge of individuals through training, workshops and further education to promote synergy within an organisation
disclosure	process of public revelation of internal information by an entity to individuals or organisations outside that entity

Ethics (already introduced under the *Responsible* component) also falls under RACI's *Informed* component.

4.2 Stakeholder elements

The *Responsible* component of the RACI matrix refers to all stakeholder elements requiring a level of trust, or answerability for an act or its consequences. With regard to stakeholder elements, this component is directed to stakeholder communication. Table 5 presents the stakeholder elements that falls under the *Responsible* component of the RACI matrix.

Table 5: Stakeholder elements – Responsible component

DF governance framework: Stakeholder elements – Responsible component	
responsibility matrix	the list of tasks and the activities that are required from the organisational stakeholders' side
social responsibility	the responsibility of the stakeholder to manage the public reputation of the organisati**on within the community whilst ensuring that the organisation-community** needs awareness remains intact
value delivery	the standard and quality of the services delivered by stakeholders in ensuring that the person responsible for malicious activity is caught
human and personnel	ensuring that employees and customers know their rights and the organisational rules when it come to digital storages and their operation
performance measurement	ongoing assessment and tracking of technology performance against set goals and objectives
ethics	principles and morals concerning right and wrong and may refer to the organisation's legitimate purchase of software licences

The *Accountable* component of the RACI matrix refers to all stakeholder elements requiring liability for one's actions. With regard to stakeholder elements, this component is directed to both executive management, and IT or DF management. Table 6 presents the stakeholder elements that falls under *Accountable* component of the RACI matrix.

Table 6: Stakeholder elements – Accountable component

DF governance framework: Stakeholder elements – Accountable component	
auditability	transparency of stakeholders' activities regarding digital resource tasks
transparency	easily presentable and understandable presentation of all digital incidents, balancing auditability and potential information leaks

Human and personnel, performance measurement and ethics (already introduced under the Responsible component) also falls under RACI's Accountable component.

The Consulted component of the RACI matrix refers to all stakeholder elements requiring the action of getting advice or input from another entity. With regard to stakeholder elements, this component is directed to IT or DF management consulting stakeholders.

Table 7 presents the stakeholder elements that falls under Consulted component of the RACI matrix.

Table 7: Stakeholder elements – Consulted component

DF governance framework: Stakeholder elements – Consulted component	
business specifics	shareholders have a right to business specific information that may impact their future with the organisation
investor relations	sound relations between investors, shareholders and the organisation itself should exist
communication	means used by stakeholders to pass specific information to employees and customers, including general organisational rules, news or incident reports

Human and personnel (already introduced under the *Responsible* component) also falls under RACI's *Consulted* component.

The *Informed* component of the RACI matrix refers to all stakeholder elements requiring the action of imparting knowledge of some facts to another entity. With regard to technology elements, this component is directed to all management informing the stakeholders. Table 8 presents the stakeholder elements that falls under *Informed* component of the RACI matrix.

Table 8: Stakeholder elements – Informed component

DF governance framework: Stakeholder elements – Informed component	
reporting	the presentation of the results found from evidence gathered from the digital storages by the stakeholders; this evidence is analysed, and from that analysis the report is generated and possibly presented at court of law
data retention	the preservation of data generated by IT resources as either hard or soft copy, including the retrieval of the stored data from the digital storage media using different IT tools
observation and monitoring	the pre-securing of digital resources, combined with an intrusion detection system to observe data passing through
environment management	the administration of organisational impacts on the external business environment

Human and personnel, and ethics (already introduced under the *Responsible* component) also falls under RACI's *Informed* component.

4.3 Business process elements

The *Responsible* component of the RACI matrix refers to all business process elements requiring a level of trust, or answerability for an act or its consequences. With regard to business process elements, this component is directed to executive management.

Table 9 presents the business process elements that falls under the *Responsible* component of the RACI matrix.

Table 9: Business process elements – Responsible component

DF governance framework: Business process elements – Responsible component	
responsibility matrix	determines and documents who is responsible for each individual task and activity, mapped onto the work breakdown structure
management efforts	business strategies and tasks that are expected from stakeholders and the executive management in managing the DF in the organisation
awareness	formally informing customers and employees about their responsibilities regarding digital information and communication, and consequences when breaching rules related to digital resources
performance measurement	ongoing assessment and tracking of organisational performance against set goals and objectives
ethics	principles and morals concerning right and wrong and may refer to the organisation's legitimate purchase of software licences

The *Accountable* component of the RACI matrix refers to all business process elements requiring liability for one's actions. With regard to business process elements, this component is directed to executive management. Table 10 presents the business process elements that falls under *Accountable* component of the RACI matrix.

Table 10: Business process elements – Accountable component

DF governance framework: Business process elements – Accountable component	
internal reporting	the regular presentation of internally conducted DF cases to the organisational management, executive management and stakeholders
standards	internationally established norms or requirements for a specific field of specialisation, for example the ISO 27001 are relevant to Information Security Management System Requirements
policies and procedures	rules and guidelines on how to handle all hardware and software resources within the organisation, including the technological equipment and assets
regulatory	principles or conditions enforced by an authoritative body, controlling DF related operations
compliance management	evaluation of whether the digital data rules and regulations are followed as expected and whether they do comply with national regulations as such

Performance measurement and ethics (already introduced under the *Responsible* component) also falls under RACI's *Accountable* component.

The *Consulted* component of the RACI matrix refers to all business process elements requiring the action of getting advice or input from another entity. With regard to business process elements, this component is directed to executive management.

Table 11 presents the business process elements that falls under *Consulted* component of the RACI matrix.

Table 11: Business process elements – Consulted component

DF governance framework: Business process elements – Consulted component	
business specifics	shareholders have a right to business specific information that may impact their future with the organisation
strategic alignment	coordination of organisational plan of action to work towards a common DF oriented goal
best practices	recommended actions and performances when handling digital data or when one encounters a digital incident
corporate governance	Figure 1 shows an overlap between DF governance and corporate governance, both disciplines are heavily dependant on management responsibilities

Ethics (already introduced under the *Responsible* component) also falls under RACI's *Consulted* component.

The *Informed* component of the RACI matrix refers to all business process elements requiring the action of imparting knowledge of some facts to another entity. With regard to business process elements, this component is directed to executive management. Table 12 presents the business process elements that falls under *Informed* component of the RACI matrix.

Table 12: Business process elements – Informed component

DF governance framework: Business process elements – Informed component	
reporting	the presentation of results based on analysed evidence gathered from the digital storages
data retention	the preservation of data generated by IT resources as either hard or soft copy, including the retrieval of the stored data from the digital storage media using different IT tools
observation and monitoring	the pre-securing of digital resources, combined with an intrusion detection system to observe data passing through
leadership	ruling and guiding employees towards excellence in DF
risk assessment	the evaluation of organisational digital data mandates with regard to its ability to overcome the existing and future threats

Ethics (already introduced under the *Responsible* component) also falls under RACI's *Informed* component.

4.4 Discussion

The success of the DF governance framework are based on its ability to enable an organisation to identify a DF risk, assign responsibility for managing that risk, and implement and manage controls (Moulton & Coles 2003:582). Although these are not the only critical aspects of the DF governance framework, it is the main points that fit the DF governance definition. The implementation of the DF governance framework will assist an organisation in:

- developing the DF strategy in support of business strategy and direction;

- establishing communication channels that support DF governance activities;
- identifying legal and regulatory issues affecting the organisation;
- developing business cases to support DF investments; and
- obtaining executive management's commitment and support for DF throughout the organisation (ISACA 2006: Internet).

Governance has proven to accommodate organisational mandates (Bihari 2008:5). When comparing the framework of existing governance disciplines with the preliminary DF governance framework, it overlaps largely with regard to management responsibility, guiding employees and customers, and protecting the organisation's reputation. The main difference is the strong focus on DF and forensic procedures.

The executive management are still accountable for formulating rules and regulations to be followed in all forensic investigations, including internal investigations. However, they should utilise the expertise of forensic knowledgeable employees and consultants to provide technical guidance. These rules and regulations in turn serve as guidance to the organisational computer response team on responding to computer incidents. In this way, the organisation does not need to hire external cyber experts, reducing the potential for information leakage.

The DF governance framework proposed by this work is the first attempt in solving some of the organisational digital management problems. The framework is currently in first draft, and future rework may be needed as further research is done on the DF governance discipline.

5 CONCLUSION AND RECOMMENDATIONS

The main aim of this research project was to formally define DF governance and to develop a basic inter-disciplinary framework that organisations should consider to ensure DF governance within their structures. DF governance is a complex discipline requiring commitment and administration in order to protect an organisation's business information-assets and reputation. If an organisation is governed appropriately, all the governance disciplines can support the day to day functioning of the organisation. In particular, DF governance can support and supplement the prominent role that technology and information plays in organisations today.

The DF governance framework is presented together with its components (see Figure 3). The intention is that the implementation of this framework will result in better DF governance within any organisation. The preliminary framework is a

preliminary outline that can be further refined with future research, and can be modified to suit specific needs of individual organisations.

BIBLIOGRAPHY

AFSHAR M., CINCINATUS M., HYNES D., CLUGAGE K. & PATWARDHAN V. 2007. *SOA governance: framework and best practices. An Oracle White Paper.* California: Oracle Corporation.

ANDERSON P.W. 2001. Information Security Governance. *Information Security Technical Report,* 6(3):60-70.

BIHARI E. 2008. *Information security governance and Boards of directors: Are they compatible?* In: Proceedings of the 6th Australian Information Security Management Conference, edited by C. Valli & A. Woodward:4-18.

EUROPEAN COMMISSION. 2002. *Étymologie du terme "gouvernance"* [online]. URL: http://ec.europa.eu/governance/docs/doc5_fr.pdf (Accessed 27 November 2009).

HINDE S. 2004. Crime and punishment: corporate governance. *Computer Fraud & Security,* 6:4-7.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. 2006. *Information Security Governance.* URL: http://www.isaca.org/Content/NavigationMenu/Security/CISM_Certification/Exam_Information1/Content_Areas1/Information_Security_Governance.htm (Accessed 26 August 2009).

INSTITUTE OF DIRECTORS IN SOUTHERN AFRICA. 2009. *Draft code of governance principles for South Africa – 2009.* Parklands, South Africa: IODSA.

INTERNATIONAL STANDARDS ORGANISATION. 2009. *Report of the SG on Digital Forensics to the – SC7 AG Meeting, Hyderabad, India, May 24 2009.* SG Presentation. ISO/IEC JTC1/SC7 Software and Systems Engineering document N4313.

IODSA see *Institute of Directors in Southern Africa.*

ISACA see *Information Systems Audit and Control Association.*

ISO see *International Standards Organisation.*

KING REPORT. 2001. *The King Report on Corporate Governance.* URL: http://www.iodsa.co.za/IoD%20Draft%20King%20Report.pdf (Accessed 13 June 2009).

LESSING M.M. & VON SOLMS S.H. 2008. *Building a world class information security governance model. In*: IST-Africa 2008 Conference Proceedings, edited by P. Cunningham & M. Cunningham.

MORGAN R. 2008. *How to do RACI charting and analysis: a practical guide.* URL: http://www.projectsmart.co.uk/how-to-do-raci-charting-and-analysis.html (Accessed 1 December 2009).

MOULTON R. & COLES R.S. 2003. Applying information security governance. *Computers & Security,* 22(7): 580-584.

MUELLER L.M. & PHILLIPSON A. 2007. *The emerging role of IT governance.* URL: http://www.ibm.com/developerworks/rational/library/dec07/mueller_phillipson/ index.html (Accessed 26 August 2009).

NUCCI A. 2009. *Shedding light on the dark cyber world.* URL: http://telephonyonline.com/commentary/contributed/cyber-crime-terrorism-0804/ (Accessed 27 August 2009).

PEMBLE M. 2004. What do we mean by "information security?" *Computer Fraud & Security,* 5:17-19.

PEOPLE FIRST. 2009. *People First Governance Framework.* URL: http://www.gcio. nsw.gov.au/people-first-the-nsw-government-ict-strategy/PF%20Governance%20 Framework-6May09-%20Public%20Version.pdf (Accessed 26 August 2009).

POSTHUMUS S. & VON SOLMS R. 2004. A framework for the governance of information security. *Computer & Security,* 23:638-646.

POSTHUMUS S. & VON SOLMS R. 2005. IT oversight: an important function of corporate governance. *Computer Fraud & Security,* 6:11-17.

SOPHOS. 2009. *Security threat report: July 2009 update.* Sophos: Boston.

TURLE M. 2009. Data security: past, present and future. *Computer Law & Security Review,* 25(1):51-58.

VACCA R. 2002. Computer forensics – computer crime scene investigation, Hingham: Charles River Media, Inc:731.

VON SOLMS B. 2001. Corporate Governance and Information Security. *Computers & Security,* 20:215-218.

VON SOLMS S.H. & LOUWRENS C.P. 2006. The relationship between digital forensics, corporate governance, IT governance & IS governance. In: *Digital crime and forensic science in cyber space*, edited by P. Kanellis. Washington: Idea Group:242-265.