Developing digital forensic governance

Marthie Grobler

Council for Scientific and Industrial Research (CSIR)

CSIR
our future through science

Introduction

- Many modern-day businesses evolve around data, information and technology
- This surge in the use of technology and electronic media necessitates the use of Information Technology (IT) governance, as well as Digital Forensic (DF) governance

This paper presents a DF governance framework and its mapping on the SANS ISO/IEC 38500:2009 Corporate governance of Information Technology structure

DF governance definition

- *"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"*

Introduction

- 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 adoption of this framework by organisations will serve as internal guidance document when addressing digital incidents and attacks

Background

- Governance - Greek word *kubernáo*, meaning 'to steer'
  - process of administration and management of a specific organisational entity, involving the enforcement and control of policies and standards
- A set of procedures and responsibilities exercised by the executive management of an organisation
- Focus on providing strategic direction
  - achievement of objectives
  - managing risks
  - appropriate utilisation of resources

Background

- The importance of information forms the foundation for the need for DF governance
- The move from paper to digital leaves sensitive business information more exposed and vulnerable to misuse by technology adept individuals

Need for DF and governance

- DF involves the
  - preservation,
  - identification,
  - extraction, and
  - documentation

  of digital evidence stored as data or magnetically encoded information
- This includes the
  - recovery,
  - analysis, and
  - presentation

  of digital evidence in a way that is admissible and appropriate in a court of law

Necessitates accuracy in following forensic procedures, rules of evidence and legal processes

Framework for DF governance

- The implementation ensures that an organisation effectively covers all relevant aspects that can holistically affect the organisation
  - corporate mechanism to implement proper management and administration in a top-down approach

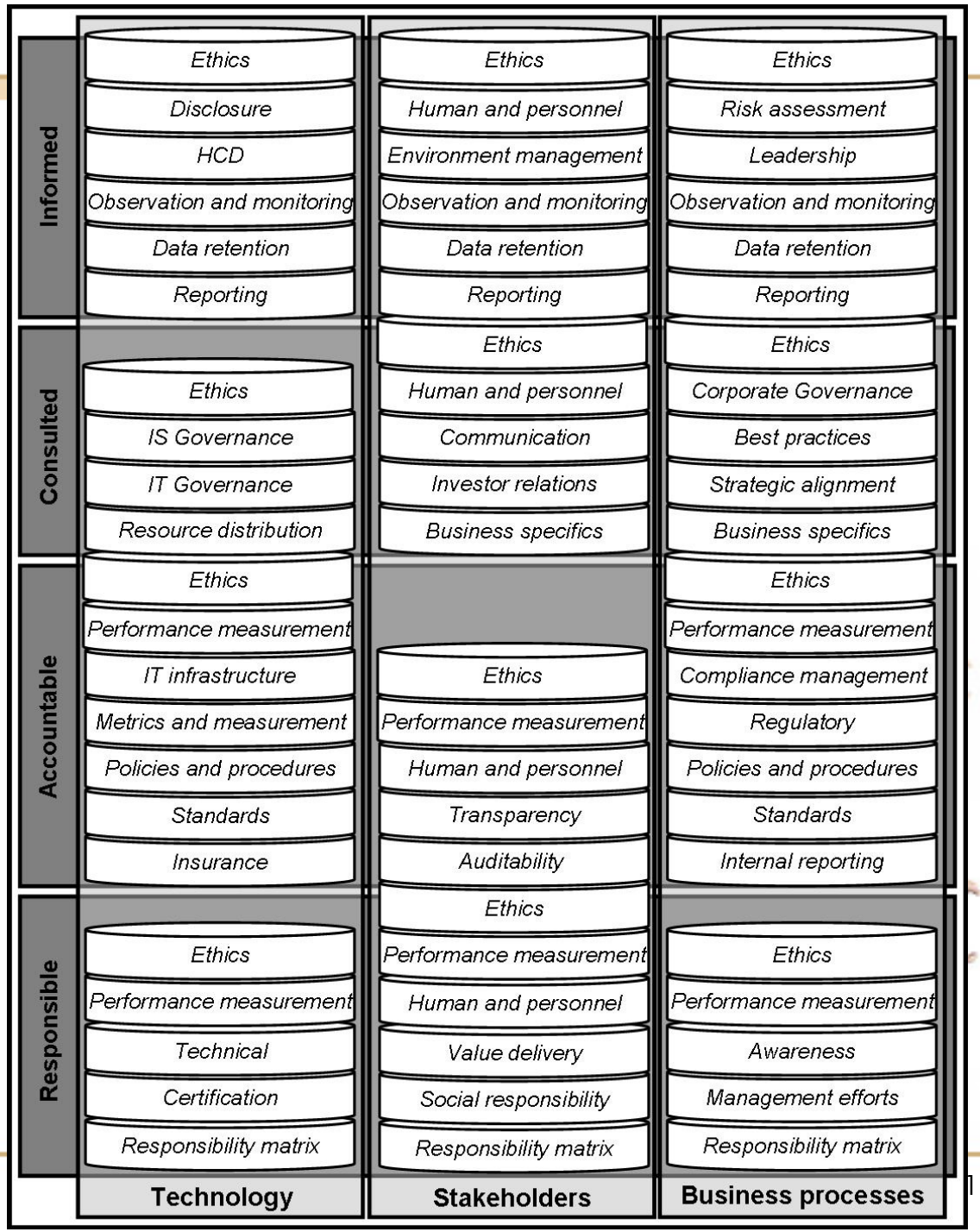
Framework for DF governance

- **Main aim:**
  alignment of the DF approach
  with the organisational strategy
  in an attempt
  to support
  the development of the organisation
  in delivering consistent business value

Framework for DF governance

- Preliminary framework for DF governance
  - The framework is built on a matrix with x-axis ***Technology, Stakeholders*** and ***Business processes***
  - The y-axis is presented by RACI matrix: ***Responsible, Accountable, Consulted*** and ***Informed***

Framework for DF governance



Framework for DF governance

- *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* refer to any commercial processes where digital crime can be involved, such as procurement

Framework for DF governance

- *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
- *Informed* indicates the person that needs to know of the decision or action

Framework for DF governance

- Forensic investigators should have a balanced knowledge of most aspects of the preliminary DF governance framework
  - wide knowledge of relevant legislation and policies,
    procedures,
    codes of practice and
    guidelines for investigating digital evidence
  - understanding of business processes and stakeholders involved with the DF processes

Mapping IT governance and DF governance

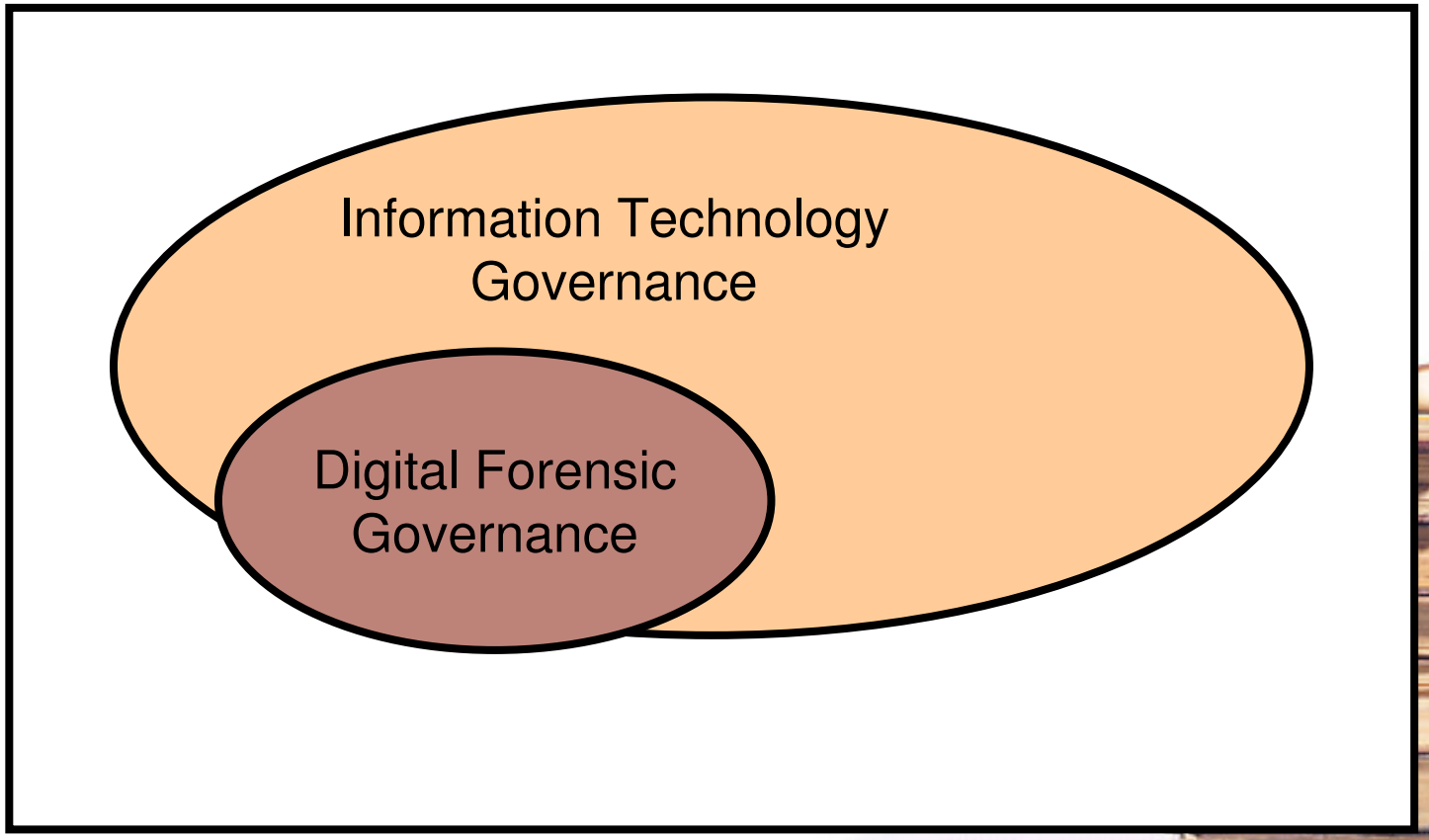
- IT governance is a multi-faceted discipline focusing on the relationship between IT management and the business functions of an organisation
- IT governance focuses on specific policies and procedures that determine how an organisation directs and controls

  the use of its technology resources

  to realise

  the organisation's business goals

Mapping IT governance and DF governance



Mapping IT governance and DF governance

- SANS ISO/IEC 38500 provides guidance on the effective and efficient corporate governance of IT
  - to provide a framework of principles for Directors to use when

    evaluating,

    directing and

    monitoring

    the use of IT within organisations
  - enable effective IT governance to assist management to understand and fulfil their legal, regulatory and ethical objections in respect of their organisations' IT use

Mapping IT governance and DF governance

- ISO/IEC 38500 sets out six principles for good IT governance
  - **Principle 1: Responsibility**
  - **Principle 2: Strategy**
  - **Principle 3: Acquisition**
  - **Principle 4: Performance**
  - **Principle 5: Conformance**
  - **Principle 6: Human behaviour**

Mapping IT governance and DF governance

DF governance \ ISO/IEC 38500	1	2	3	4	5	6
auditability	x				x	
awareness	x	x			x	x
best practices					x	
business specifics		x				
certification				x	x	x
communication		x				
compliance management					x	
….						

Benefits of DF governance

- Specific management responsibility should become the responsibility of the DF experts
  - these individuals have more experience with regard to DF tools and techniques
  - understand the relevant best practices, standards, policies and procedures better
  - better understanding of the discipline by executive management
  - better utilisation of the organisation's digital resources to support the business goals

Benefits of DF governance

- Discipline experts manage a rather technical discipline
- The suitability of DF products, processes and services are improved for use according to their intended purposes
- DF governance removes many barriers to international trade and cooperation
- Proper management ensures 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

Conclusion

- The DF discipline developed rather rapidly, but up to date has very little international standardisation with regard to processes, procedures or management
- In the same sense, little international standardisation has been done with regard to setting the technical foundation of DF, in terms of ISO/IEC 24774
- The intention is that the implementation of this framework will result in better DF governance within any organisation

mgrobler1@csir.co.za
marthiegrobler@gmail.com