South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

Safeguarding information as an asset: Do we need a redefinition in the knowledge economy and beyond?

Authors:
Adeniji K. Adesemowo[1]
Rossouw von Solms[2]
Reinhardt A. Botha[1]

Affiliations:
[1]School of ICT, Nelson Mandela Metropolitan University, South Africa

[2]Centre for Research in Information and Cyber Security, Nelson Mandela Metropolitan University, South Africa

Corresponding author:
Adeniji Adesemowo,
kayode.adesemowo@nmmu.ac.za

Dates:
Received: 19 Aug. 2015
Accepted: 31 Jan. 2016
Published: 31 May 2016

How to cite this article:
Adesemowo, A.K., Von Solms, R. & Botha, R.A., 2016, 'Safeguarding information as an asset: Do we need a redefinition in the knowledge economy and beyond?', *South African Journal of Information Management* 18(1), a706. http://dx.doi.org/10.4102/sajim.v18i1.706

Background: With the evolution of data, via information into knowledge and beyond, intangible information assets (seen as an integral part of IT assets in this article) increasingly come to fore. A contemporary issue facing organisations in the knowledge economy and beyond is how best to safeguard and derive optimum value from their evolving information assets. A well-known fact is that risk exists because there is the possibility of threats to an asset. Likewise, no assets equals no risk. Although a large body of work is addressing threat models, the nature of the assets of the knowledge economy and beyond has not been well researched.

Objectives: To investigate the definition of information assets across a number of financial, risk and information technology standards, frameworks and regulations, in order to ascertain whether a coherent definition exists across the board. If there is none (or limited), then propose a workable definition that is apt for the knowledge economy and beyond.

Method: Qualitative thematic content analysis and a comparative study based on four main themes (Assets, Types of Asset, Information, and Information Assets). This then serves as a basis for argumentation schemes that lead to a proposed re-definition. The qualitative research approach assists us to address the concern of the incoherent definition of information and information assets across the board.

Results: Contrary to expectations, the research study found the current definition to be incoherent. When the asset to be controlled is not properly defined and understood, it stands the risk of not being identified properly. This implies that the effectiveness, efficiency, reliability of internal control, and compliance with the applicable legislation and regulations would not be appropriate. This article highlights the need for a fundamental shift in how information assets (valuable, but unvalued organisational intangible assets) are being viewed and treated, especially with regard to information risk and internal controls.

Conclusion: This article has identified a major defect in most standards, frameworks, and regulations dealing with regard to the safeguarding and management of information assets (and IT assets). It has established from the review carried out that information assets have not been properly defined across the board. Beyond this significant finding, it was further shown that the principle of risk (assessment) across the board requires the identification of the asset that needs to be controlled. A starting point, then, is a coherent definition (as proposed) for the information asset in itself. Therefore, proper definition across the board might assists in proper identification that could result in appropriate control and graceful handling of the end-of-life disposal.

Introduction

Information has not only permeated the knowledge economy and beyond (Buera & Kaboski 2009:2540; Goede 2011:36), but it has become a critical business asset without which an organisation's competitive advantage would be eroded (Ahmad, Bosua & Scheepers 2014:28; Evans & Price 2014:113; Laney 2014; Laskowski 2014; Naidoo & Van Niekerk 2014:33, 36–37).

This is much in line with Leavitt and Whisler's (1958:41) projection of information having strategic importance (at middle and top management levels), when the technology that processes, transmits, and stores information was rightly termed Information Technology (IT) in their business review paper 'Management in the 1980s'. The permeation of information and its strategic importance resonates well with Moody and Walsh's (1999:2) notion that information is a strategic business asset, which is indeed a 'valuable, but [*largely*] unvalued asset'.

The importance of information can be seen in its strategic relevance across middle- and top-management levels (ISACA 2012; King 2009; Leavitt & Whisler 1958). The use of information

(whether by individuals in an organisation and/or by a group of people at middle, top management and board level, or usage across the whole organisation) has a far-reaching, enterprise-wide impact. Information is a strategic intangible asset, and therefore requires that commensurate internal control(s) be applied to it and the management thereof.

This is much in line with the application of internal controls on any other corporate asset, as stipulated by the Committee of Sponsoring Organisations of the Treadway Commission – COSO (2013), which advises that the safeguarding of assets is of cardinal importance. COSO's internal control requirement mandates a careful balance between effective and efficient safeguarding.

This article posits that information assets, being intangible assets, cannot have internal control(s) applied to them *per se*; but rather control(s) should be applied to the process and/or the container or processor (being the related IT asset). Drawing upon the fundamental issue of internal control, control(s) to be applied to an IT asset must be commensurate with the carrying (information) value of the underlying information asset. However, from an IT/information risk viewpoint, the value can only be determined if the information asset is understood, known, clearly defined (Haider, Koronios & Quirchmayr 2006:288), identified, and appraised appropriately; because any associated risk must be taken into consideration as well (ISO/IEC 2014:14–15).

A challenge arose in this instance when the net value of the information asset (benefit to the organisation) and risk (liability) are not used to determine the level of appropriate control(s) required. The authors are of the view that the inability to apply a commensurate level of control seems to be a factor of not properly understanding 'the information asset' in itself. Knowing 'the information asset' is directly linked to the definition of the 'information asset'. To find answers to these challenges, this article reviews information assets and reputation loss, which then leads into the need to ascertain which definition(s) exists for information assets in the form of standards, frameworks, and regulations.

The ascertaining of information assets' definitions across the board was carried out by using qualitative-content analysis and a comparative review of a number of standards, frameworks, and regulations across financial, asset management, service management, and IT. Next, the findings on the lack of definition, or an inadequate definition thereof, was presented and discussed; and a definition was proposed. The article concludes with the five P-factors of unrelenting reputation loss, as a result of the lack of sufficient internal control over IT assets (container of information asset).

Review: Information asset and reputation loss

Data, information, and knowledge (all integral dimensions of information assets) are terms that are loosely used interchangeably. Yet, they differ from one another. A contextualisation of their meaning could assist us to look at the information component of information assets from a resource angle. As a resource, information gives the strategic competitive advantage (Ahmad *et al*. 2014:28; Moody & Walsh 1999:2); and when it is not safeguarded, as it ought to be, reputation loss, amongst others, can arise.

Data, information and information assets

Taken from the Oxford Dictionary (http://www.oxforddictionaries.com/definition/english/data), data (the plural of datum) is defined as facts and statistics collected together for reference or analysis. Data can also be known as the quantities, characters, or symbols on which operations are performed on by a computer, which may be stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media. Data can even comprise that which is stated in human discourse (Gates & Matthews 2014:107). In Moody and Walsh (1999:2), data are the raw materials for information.

Information, on the other hand, is defined as the facts provided or learned about something or someone. It could otherwise be defined as computing the data that were or are being processed, stored, or transmitted by a computer.

We shall look at the definition of information in King III and COBIT 5 later in this article as part of the finding.

Furthermore, to properly contextualise information and understand its meaning accurately, this article views information in two main lines of personal information and corporate information. Defined in the US Privacy Law, in the EU Directive, in the *Australian Privacy Act*, and in the South African Protection of Personal Information (POPI) Act, personal information is the personally identifiable information (Gates & Matthews 2014:106) that can be used on its own, or with other information to uniquely identify, contact, or locate a single person, or to identify an individual in context (Australian Parliament 1988; California Senate 2002; European Parliament 1995; Parliament of the Republic of South Africa 2013). This is the realm of identity theft (when personal information has been breached, and/or results in a loss of personal reputation).

On the other hand, corporate information is the information that uniquely identifies an organisation (public) or information that is used or processed internally (private), which might not have been made public (concept seen in insider trading, internal control procedures, and intellectual properties). Corporates' 'private' information (business information assets), the focus of this article, are processed and used internally, in order to gain a competitive advantage, to add to, and/or to derive economic values (information management). Furthermore, they are strategically controlled (information governance) to derive optimal investment value (Evans & Price 2014:115). However, when improperly safeguarded or controlled, business information assets could become a liability (e.g. reputation loss).

Information assets and reputation loss

A number of security breaches, some highlighted in Figure 1, arose from improper safeguarding of information assets. These security breaches against business information assets have resulted in reputation issues – and for some, reputation loss to the organisation (Arlitsch & Edelman 2014:49; Jones 2009:3; Silva 2012; Warner 2011:737)

It can be seen that, on the one front, information assets continually remain a target with success; while on the other hand, IT assets that contain the information assets are getting to the 'wild' – with or without control(s) in place. This loss keeps occurring, in spite of the vast array of technologies available, which have been put in place to safeguard IT assets. Additionally, standards, best practices, and guidelines also abound to ensure that (business) information assets are cared for; and that the regulatory laws mandating protection are enforced (Burdon 2010:64–65). Okere, Van Niekerk and Carroll (2012:1) highlighted the human factor, generally dubbed as the 'weakest link', which can possibly be overcome by strengthening the associated information security culture. Hence, it can safely be said that technology, or know-how, or regulations, are not the only key factors in the ongoing security breaches; although they do contribute. There is yet another contributory factor!

Control inefficiency over information assets

Do we then say that these technical and process controls, enabled by hi-tech security technologies, are not effective, or are being misapplied? Or rather, should we say that these multifaceted standards, best-practices, and guidelines are not appropriate enough to ensure a secure environment; or are they just impossible to implement? Perhaps, regulatory deterrents are ineffective in terms of the penalties and enforcement, so that organisations take them with a pinch of salt? This is a point of view taken by Burdon (2010:64), when stating that the general levels of corporate information security practices are inadequate, hence the emergence of data-breach notification laws. All these technical and process controls have their place; and are somewhat effective - to the extent for which they were intended.

Xtra! Xtra! - Read 'bout it!

2015 Jan:	Anthem BlueCross BlueShield Cyber-attack on IT system Target: members' private information Dedicated site Anthemfacts.com dealing with reputation loss
2014 Jan:	Theft of unencrypted laptops behind Coca-Cola breach impacting 74,000# (Identity Protection estimated at US$11m per year)
2014 Jan:	Michaels Store (NYSE:MIK) attack (25th) (Lawsuit already instituted - databreaches.net)
2014 Jan:	Neiman Marcus (NYSE:NMG) attack cautionary (10th) As at Feb. 14, 157-pages analysis, 350,000 customer cards (US$1.1m)
2013 Dec:	Targets Corp (NYSE:TGT) Security Breach 40m cards, 70m Personal Info, forecast > 30m direct/indirect cost
2007:	BlueCross BlueShield Tennessee (BCBST) 57 Hard drives HIPAA/HITECH fine US$1.5m; reputation, legal cost over US$17m
2007:	UK HM Revenue and Customs: Lost two discs, 25m accounts
2007:	TJX (NYSE: TJX) loss of 40 million customer account records
2007:	U.S. Department of Veterans Affairs (VA) loss of information on more than half a million people (initially reported 48000)

Source: Collation of authors' knowledge of the events listed herein and the study of papers listed in the section-(Information Assets and Reputation Loss)

FIGURE 1: Some of the security breaches discussed in this paper sourced from author's collation of breaches in the media and literature.

Research domain: Problem and methodology

Surely, the fundamental of risk remains the possibility of a threat to an asset (ISO/IEC 2014, sec. 2.68); and that of accounting is equity, which is the differential sum of asset and liability (IASB 2010, sec. 4.4). If controls are available, and the means to safeguard assets are advanced and sophisticated nowadays, as seen from the review above, yet security breaches continue to be relatively unabated, then, there is a need to look again at the internal controls and the IT risk chain, with a focus on information risk.

Poller, Türpe and Kinder-Kurlanda (2014) have advocated the strong need to factor stakeholders directly into the risk-analysis equations. The concept of stakeholders used in business impact analysis exercises would then be carried over to risk-analysis exercises as well. Their approach is laudable as it would bring the Responsible, Accountable, Consulted, Informed model to the fore. An interesting space to watch!

Nonetheless, a possible rationale that can be attributed to the risk challenge might be how we value our assets (in this instance, IT assets, which are primary containers for information assets). This shifts us from 'the control' (minimising possibility of threat) to 'what is being controlled' (preservation, maximising, and growing value).

It therefore implies that what is being controlled (IT assets and underlying information assets), requires insightful understanding of its attributes in order to be better understood and identified. Hence, there is a need for a rethink of an IT asset value, especially for risk purposes. In order to do this, there is a need to look deeper into what the real target is in security breaches – which is the underlying information asset. It is the information asset that is not properly defined and understood, as it ought to be.

To the best of the authors' knowledge, as highlighted in the methodology, there has been no literature or white paper that has carried out a comprehensive comparative study on the definition of information assets or IT assets across financial, risk, or IT standards, framework and regulations. Yet, this is critical in gaining insight into what information assets are. The importance of such a comparative study is that it could provide a lens to understudy the missing link that possibly lies in the inherent attribute of an IT asset in itself (its hybrid physical tangible asset and intangible information asset).

Research problem domain

Given that an information asset is the main target in a number of security breaches, because of the value it holds; and noting that the intangible information asset is processed, transmitted and stored in a container (the IT asset), and used

within and/or across a process, then internal control(s) ought to be applied on the information asset via the container and/or the process. These controls are applied on the basis of standards, frameworks, best and good practices, strategic imperatives, regulatory requirements, and stakeholders' expectations. Controls are applied to what is known and/or can be known, and/or to the extent it is known. Therefore, commensurate controls are applied on the basis of the value of what needs to be controlled (information asset) and what is known.

However, is there a coherent definition across the board for an information asset in itself (and its derivatives)?

This is a primary question one needs to ask. Furthermore, one then seeks to find out if the incoherent definition has a bearing on the incommensurate internal controls being applied, and hence on the possible loss of the information asset itself.

This assertion of a lack of coherent definition for an information asset, being a basis for the improper understanding of information assets (which is the inherent underlying carrying value of an IT asset), would hold true by reason of argumentation, if it can be shown that there (truly) exist such incoherent definitions of IT assets, their inherent information assets, and the underlying information. Procedural argumentation (Walton 2013:3, 15), which need not be proved in the absolute, would assist and suffice in this regard.

Thus, procedural argumentation, starting with the underlying information requires a practical reasoning on the lack of, or an incoherent definition of information asset, in order to conclude that it is the basis for the hitherto unknown contributory factor to the lack of commensurate safeguarding of IT assets. If an incoherent definition can be shown to exist, then an improper understanding of information asset would exist. When the assertion holds true, then a redefinition (of information asset) is required to assist with identification of the asset to be safeguarded.

Research methodology

In order to prove the above argumentation schemes (Walton 2013:6), we will now take a qualitative research approach, premised on a thematic content analysis and a comparative study.

The qualitative research approach (Babbie 2012:24) assists us to address the concern of the incoherent definition of information and information assets across the board. This was carried out by a blend of comparative study (Rajasekar, Philominathan & Chinnathambi 2013:10) of standards and frameworks (Susanto, Almunawar & Tuan 2011:24, 25), and content analysis (Krippendorff 2012:1, 4) of the definitions of information and information assets, as well as the context thereof (Krippendorff 2012:24).

The thematic content analysis was based on four main themes (Assets, Types of Asset, Information, and Information Assets). This analysis was done comparatively across a number of financial and information system standards, frameworks, and regulations, as outlined in Figure 2. Logical discussion of the findings would then form a basis for a redefinition.

Although, the standards, frameworks, and regulations were purposively selected, based on their universal adoption or oversight in their fields, others were based on discussion in literatures in this article, notably those in Naidoo and Van Niekerk (2014:35, 38).

Findings and discussion

International Organisation for Standardisation (ISO) standards typically have a part and/or section for definitions and concepts explanation. Other standards and frameworks would have a definition section and/or a glossary. It is naturally expected that assets, types of assets, information, and information assets would be defined in the standards, frameworks, and regulations dealing with them.

In this section, the findings of the four themes (assets, types of asset, information, and information asset) across standards, frameworks, and regulations (listed earlier in the methodology) are presented. The birds-eye view of the research finding is shown in Figure 3.

In the interests of space, the detailed findings for the four themes are only summarised in this article. It is intriguing to note that whereas assets are not defined across the board in the standards, frameworks, and regulations, types of assets, on the other hand, are listed and/or implied across a number of them.

Research findings: Asset definition

In order to look at information assets, a natural starting point would be information and assets. We look at the definition of assets across financial, information security and other standards, frameworks, and regulations.

The findings outlined in Table 1, indicate a dearth of definitions across the board.

Asset definition trending the line of financial international accounting standards board or international financial reporting standards

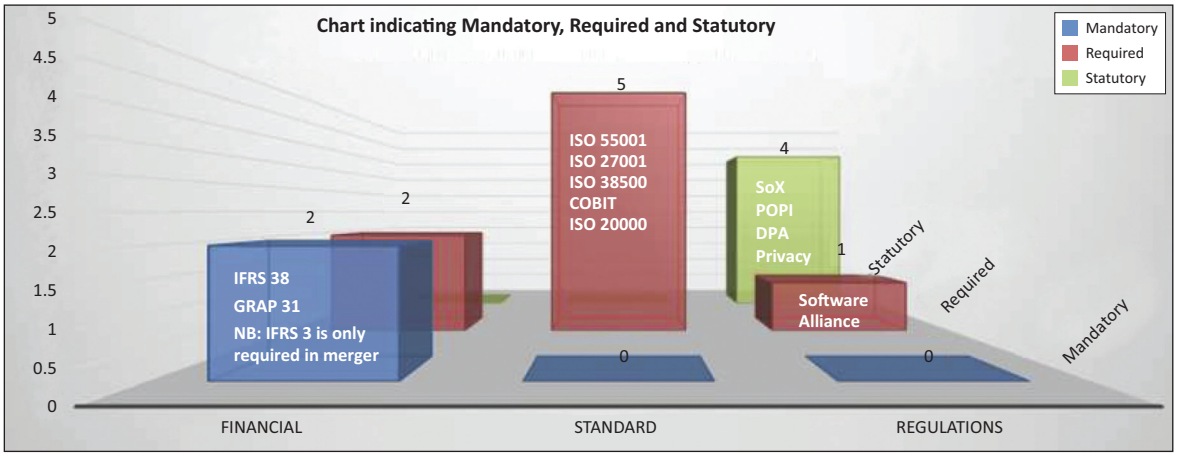
It was noted that a common trend across financial standards, frameworks, and regulations is the reliance on the International Accounting Standards Board/International Financial Reporting Standards (IASB/IFRS) definition of an asset. The financial IASB conceptual framework defines an asset as a *resource controlled by the entity, as a result of past events, and from which future economic benefits are expected to flow to the entity*.

Information Technology Infrastructure Library's asset definition linking financial and information technology

In Information Technology Infrastructure Library 2011 (ITIL2011) (in its service strategy), an asset is seen as any

FINANCIAL:	
IFRS38 (IAS38)	Asset Definition, Intangible Asset Recognition
IFRS 3	Business Combination Reporting, Intangible Asset
King III	Governance, Control over Asset
GRAP 31 (ASB South Africa)	Intangible
STANDARDS:	
ISO55001 (PAS55)	Enterprise Asset Mgt, Deriving Value
ISO27001	Information Asset, Asset Register, Risk Assessment
ISO38500	IT Governance, Strategy
COBIT	IT Acquisition, Control, Mamgement
ISO 20000 (ITIL)	IT Service Management, CMDB, CI
REGULATIONS:	
Sarbanes Oxley	Mandatory Control over Financial ⇔ Software Licensing
Software Alliance	Software licensing Piracy – www.bsa.org
POPI (SA)/DPA (UK)/US Privacy	Personal Info, Mandatory Disclosure

*ISO27001 is classify as *required,* as it is neither *mandatory* nor *statutory*, though highly regarded.
In some sectors, such as banking in Nigeria, it is mandated by the Central Bank.



Source: Authors' careful analysis of the listed standards and regulations

FIGURE 2: Comparative study asset definition across financial, standards and regulations.

resource or capability. A service provider's assets include anything that could contribute to the delivery of a service (AXELOS 2011:5). Although this might initially be viewed to be at variance with the financial world that stipulates specific criteria for asset recognition (uniquely identified material over one financial year), it nonetheless tallies with the IFRS/IASB *resource* view of asset. Although missing in the current standard, in ISO27001:2009, asset was seen as anything that is of value to an organisation (asset 2.3). This resonates well with the financial IASB view of an asset as a resource. Therefore, one can deduce that ITIL's view of an asset is the link between the financial and IT worlds. An asset, as envisaged by ITIL2011, need not necessarily be included on a balanced sheet, or have a book value. However, the asset needs to be safeguarded in order not to have unintended incident.

Research findings: Types of assets

An asset is not defined across the board in the standards, frameworks, and regulations; on the other hand, types of assets are listed and/or implied across a number of them, according to the summary in Table 2.

Distinct categorisation of assets

The major focus of ISO55000 is on the traditional physical property, plant and equipment (PPE); whereas information assets and intangible assets are clearly indicated not to be the main focus of the standard, as discussed below. The focus naturally shifts to financial assets, especially IASB (to which other financial related standards and frameworks refer, or imply), ISO27000 and Software Asset's ISO19770. In the case of IASB, the various types of assets are delineated in three main categories: physical, monetary, and intangible.

Much attention is paid to the recognition of assets in section 4.44 of the IASB, with a particular emphasis on physical (PPE) and monetary aspects. Intangibles are rather treated under notes or auxiliary standards, such as IAS38, IFRS3 and in South Africa, in the Generally Recognised Accounting Practice (GRAP 31). An intangible asset as a type of asset is defined in GRAP31, as an identifiable non-monetary asset without physical substance. One category of intangible asset that has gained prominence (notably after the Enron's saga, and hence the introduction of Sarbanes–Oxley Act 2002) is software. The ISO19770 that focuses on software asset management provides further insight into this type of asset (whether executable or non-executable software). ISO19770's software and record type of assets map well with ITIL2011 (and ISO20000) types of configuration items.

Legend
● Defined ≈ Implied ⊙ In context ○ Not Defined

Asset Definition and Classification Across Standards, Frameworks and Regulations	Asset Definition	Types of Area	Information Define	Information Asset	Asset Identification
ISO270Ox - Information Security	○	≈	○	○	●
COSO - Internal Control	○	○	○	≈	●
IFRS/IAS - Accounting	●	●	≈	≈	●
GRAP 31 (102) - Intangible Asset South Africa	IFRS/ IAS	≈	≈	≈	●
King III/ISO38500 - Governance	IFRS/ IAS	●	●	≈	IFRS/ IAS
ISO5500x - Asset Management	●	●	⊙	○	●
ISO2000x/ITIL2011 - Service Management	≈ refer CI	≈ per CI	≈	⊙ (Service)	●
COBIT5 - IT Controls, Risks, Values and Governance	≈ info	○	●	≈ info/IT	●
POPI - Protection of Personal Information South Africa	○	○	⊙ electronic	⊙ personal info	⊙ for use
ISO19770 - Software Asset Management	IFRS/ IAS	IFRS/ IAS	IFRS/ IAS	⊙ related	●
Sarbanes Oxley 2002	○	IFRS/ IAS	○	≈ (software)	IFRS/ IAS

Source: Authors' viewpoint and collation of the findings across the different standards, frameworks and regulations

FIGURE 3: Summary of information asset definition findings across board based on authors' thematic content analysis and comparative study.

Intangible information assets remain tangible particular emphasis on physical assets still

With the value attributed to software (chiefly that of its licensing), financial IASB, SOX, and ISO19770 have found a way to 'tangibilise' the intangible software. When the real value of software is considered, it can be seen that its real value is in its function, that of the processing of information within an IT asset (Moody & Walsh 1999:10). Yet, assets even in the knowledge economy, are still defined largely from the financial PPE point of view. Has ISO5500x, just like ISO19770, missed a golden opportunity to cater for the asset of the future?

Research findings: Information

Information assets have been affirmed to be a type of asset; nonetheless, the challenge faced is in quantifying it, along with the rest of tangible and intangible assets. Underpinning information assets is information. The efficient flow and use of information are of strategic importance to an organisation's well-being.

King III (2009) and the ISO38500 IT Governance standard (2009) have taken cognisance of this. Indeed, King III para 36: 'information management' indicates that information records

TABLE 1: Comparative study of asset definition across financial, standards and regulations, based on the authors' content analysis of asset definition.

Standard/framework/regulation	Asset definition	Comment
ISO/IEC 27000:2012(E)	**Define**	Sec 2.4 any item that has value to the organization
ISO/IEC 27000:2014(E)	Not defined	Asset: not defined
COSO (integrated framework)	Not defined	Asset: not defined (seems to rely on SEC financial reporting, hence IASB)
IASB/IFRS	**Define**	Asset: IASB conceptual framework 2010 (4.4a, 4.8)
GRAP 31	Implied	(South Africa ASB – intangible asset) asset: refer to IFRS/IAS
ISO5500x	**Define**	Asset: define (physical intended)
ISO19770	Implied	(Software asset management) asset: financial definition (IFRS/IAS implied). Closely related IAITAM's Best Practice library (IBPL) 12 KPAs indicate that IBPL (like ISO5500x and ISO19770) is focused on physical IT assets, its components (ITIL's CIs) and software licenses
SOX (US Sarbanes-Oxley 2002)	In context	Asset: no (financial IFRS/IAS implied)
King III/ISO38500	Implied	Asset: implied IFRS/IAS (King III para 14.1, 35)
ISO2000x/ITIL2011	Implied	Asset: Implied (reference to configuration Item (CI) – uniquely identified, traceable, auditable)
COBIT5	Implied	Asset: implied (Information)
POPI	Not defined	(South Africa Protection of Personal Information) Asset: Not define

TABLE 2: Comparative study of types of assets across financial, standards and regulations.

Types of asset	Standard/framework/regulation	Comment
Physical (tangible)	IASB, ISO55000, ITAM	PPE: Property, plant, equipment. See IASB section 4.44
	ITIL/ISO2000	In ITAM, IT asset is seen mainly from physical point of view while information, records et al are seen as supporting more from an information system point of view
Intangible	IASB, ISO17990, GRAP31	Largely software. IAS38 (IASB) and South Africa's GRAP31 focus mainly on intangible asset. OECD is assisting with classification of intangibles
	ISO27000	Primarily information asset. OECD sees information as an increasingly asset of importance in the (and beyond the) knowledge economy
Information asset (Intangible)	ISO27001, King III, Cobit5	Recognised as asset that is information in nature. A key driver and strategic asset of an organisation. In South Africa's POPI, it is seen from a personal information point of view

are the most important information assets, as they are evidence of business activities. Apart from King III, only COBIT®5 has a definition for information amongst the standards, frameworks, and regulations that were reviewed as summarised in Table 3.

What is remarkable is that ISO27000:2014, a standard for information security, does not have any definition for information. Considering that no definition for assets exists in ISO27000:2014, there is a concern that a standard that stipulates the safeguarding of information assets and provides a control mechanism has neither information nor assets defined! Typically, ISO standards use conjugations to define compound terms. For example, if an asset is defined as anything that has value, then an information asset would be an asset of the type of information that has value. Nonetheless, ISO27000:2014 was explicit that all types of information assets, including financial information, intellectual property, and employee details, or information entrusted to the care of an organisation by their customers or third parties, must be safeguarded (ISO 27000:2014 2014:0.1 Overview).

Research findings: Information assets

The ISO2000x standard and ITIL® framework both recognised the importance of service management as a capability platform in the knowledge economy and beyond. Service, innovation, and wisdom are products in these economies. We note that intangibles, and notably information assets, are key assets of this economy and beyond.

A definition for information assets resides in the past only

Though King III and ISO38500 implied a definition for assets from the financial world (IASB/IFRS implied), it was observed that IT assets, information assets, and private information (privacy) are explicitly recognised as types of assets. A number of other standards, frameworks, and regulations, as shown in Table 4, implied information assets as forms of intangible assets or simply 'financial record'. In fact, in earlier editions of ISO27000:2009, information asset (2.18) was explicitly defined as knowledge or data that has value to the organisation. What then is intriguing is *the omission of any definition for assets, information, and information assets*, in the current ISO2700x family of standards.

We assumed that the IT Security Techniques standardisation subcommittee (SC27) of the ISO/IEC Joint Technical Committee is possibly aware of the IASB ongoing redefinition effort of its 2010 Conceptual Framework (IASB 2010), to redefine an asset and a liability as a 'resource'. It is noted though that IASB's asset definition might change, when the ongoing review of IASB 2010 Concept Framework is completed. The OECD, likewise, is facing challenges in its ongoing task of classifying intangible assets of which an information asset is a part (OECD 2011).

TABLE 3: Comparative study of information definition across financial, standards and regulations.

Standard/framework/regulation	Information definition	Comment
ISO/IEC 27000:2012(E)	Implied	Section 0.1 Overview and section 2.4 Asset
ISO/IEC 27000:2014(E)	Not defined	Section 0.1 Overview
COSO (integrated framework)	Not defined	Rely on SEC financial reporting, hence IASB
IASB/IFRS	Implied	Financial reporting implied
GRAP 31	Implied	Financial reporting, intellectual property (as a form of intangibles)
ISO5500x	Not defined	Information for the asset management system!
ISO19770	Implied	Records, information for management system
SOX (US Sarbanes-Oxley 2002)	In context	Financial reporting (IFRS/IASB implied)
King III/ISO38500	**Define**	Glossary of Terms
ISO2000x/ITIL2011	Implied	ISO20000-1: 3.8 document – information and its supporting medium (ISO9000:2005)
COBIT5	**Define**	Oral, paper or electronic business intangible asset
POPI	Implied	Electronic communication, record

TABLE 4: Comparative study of information assets across financial, standards and regulations.

Standard/framework/regulation	Information asset	Comment
ISO/IEC 27000:2012(E)	Implied	Last defined in ISO27000:2009
ISO/IEC 27000:2014(E)	Not defined	Sections 3.1, 3.2.1, 3.2.5, 3.2.3/3.5.5 (identified information assets!), 3.2.4 (organization's information assets), 3.4/2.68 (associated risks), 3.6 (protect information assets), 0.1 (security of information assets)
COSO (integrated framework)	Implied	SEC financial reporting, hence IASB
IASB/IFRS	Implied	Intangibles (IAS38, IFRS3)
GRAP 31	Implied	Intangibles (IP, software)
ISO5500x	In context	Intangibles explicitly out of scope
ISO19770	**Define**	Records, software related assets (media, documents, data)
SOX (US Sarbanes-Oxley 2002)	Implied	Software (SEC, IFRS/IASB)
King III/ISO38500	Implied	King III Principle 5.6, paragraph 36
ISO2000x/ITIL2011	In context	CI relating to service, security and other documentations
COBIT5	Implied	Information and/or IT assets
POPI	In context	Personal information, public records, special personal information

ISO, International Organisation for Standardisation.

Nonetheless, an organisation must implement a framework for managing the security of their information assets (ISO/IEC 2014, sec. 0.1 Overview and sec 2.68 Risk – Note 6). The starting point for this is the identification for the assets. We posit that the effectiveness of the identification process is premised on proper understanding of the assets to be identified.

Research findings: Birds-eye view of information assets definition across board

Contrary to expectations, the findings (summarised in Figure 3), present a rather worrisome picture.

It was found that only King III and COBIT®5 have definitions for information amongst the standards, frameworks, and regulations that were reviewed. In line with literatures, King III and COBIT®5 both defined information as an asset that is essential to an enterprise's business. On the flip side, ISO27000:2014, a standard for information security, does not have any definition for information. It nonetheless define information asset as knowledge or data that has value to the organisation.

Information and information assets were found not defined; or at best, they were simply implied in a number of standards, frameworks, and regulations. However, across all of them, they all required assets (in this instance intangible information assets) to be identified and safeguarded.

The question remains: *How then can risks to assets' value be safeguarded when the asset is not well defined*?

Research discussion: Implications of incoherent definition across the board

The significant findings in this research have confirmed that there is an incoherent definition across the standards, frameworks, and regulations reviewed. The implication of this is that it can then be shown that our earlier assertion of a lack of coherent definitions for information assets holds true.

Given that the hitherto unknown contributory factor to the lack of commensurate safeguarding of IT assets has been premised on: (1) The lack of understanding of the hybrid nature of an IT asset, and hence its value; and (2) an improper understanding of its information asset, which is the inherent underlying carrying value of an IT asset; it can then be said that the lack of, or the incoherent definition, of an information asset could result in information assets not being identified and adequately valued. Although there are other contributory factors, as alluded to under the review section, that result in the lack of adequate safeguarding, the lack of coherent definition has unfortunately been grossly overlooked.

What could then be said to be the implications of these findings?

Property, plant, and equipment assets that have formed the bulk of critical assets to most organisations might provide some clarity in this regard. It is a known fact that PPE assets have been well defined, identified, managed, and safeguarded. To a large extent, IT assets and investments in IT (Kim, Poon & Young 2011:2) have traditionally been treated along the lines of PPE. Hence, the book value recorded in balance sheets (when done at all) and the asset value considered in risk analysis, have typically been based on IT assets' tangible value. In most cases, there is a variance occasioned by the approaches of practitioners who rely on subjective determination!

However, in the knowledge economy and beyond, information assets (and the containing IT assets) are increasingly becoming important and critical to the sustenance of organisations. The purchase of WhatsApp by Facebook Inc. (reported by the Times as US$22 billion in cash and stock) is a case in point. Likewise, the demise of DigiNotar (Charette 2011) in 2011 is another! What we have at the moment, and which is not appropriate for the knowledge economy and beyond, is that the traditional PPE and evolving intangible approach has not yet taken into due consideration, nor has it addressed the intrinsic nature of information assets and the hybrid nature of the container (IT assets). We therefore posit that the challenge faced in defining – and the difficulty in the safeguarding of information- related assets – is because information assets are not well understood, as they ought to be.

Without a definitive definition for an information asset, or any explicit reference to its inherent and intrinsic nature (attributes), the safeguarding of information-related assets could be subjective. The logical implication of this would then be that the containing IT assets would not be valued properly. This would then result in a possible mismatch between the value of the IT asset and the safeguarding controls being applied to the IT asset.

Research discussion: Information assets' identification and safeguarding

With information assets not being adequately defined, which has been linked to it being not properly understood, the identification and safeguarding thereof can only be in danger. Consequently, effective and efficient safeguarding of (information) assets, which refers to protecting such assets against the unauthorised and wilful acquisition, use, or disposal of (information) assets, cannot be achieved as it ought to be.

The COSO framework is primarily used along with others, by practitioners, for enterprise-risk management and internal controls. As indicated in the earlier discussion relating to ISO2700x, risk assessment (and by inference risk management) cannot be as effective as it ought to be when the 'item' to which risk refers to is not properly understood and/or identified. The accurate identification of an asset is a critical requirement in IASB (section 4.44: recognition of assets), ISO27000 (3.2.3/3.5.5: identified information assets), and ISO27005 (Risk Management). COSO (2013:3, 4), with its focus on controls, expectantly takes risk assessment seriously,

as part of the components of internal control: 'Risk assessment forms the basis for determining how risks will be managed'.

Rethinking information assets definition

In this section, before concluding this article, a definition for information assets will be proposed and the essence of a redefinition discussed.

In order to be able to look at the appropriateness of control(s) over information assets, and to determine whether assets are well defined, it is imperative to look at the internal control requirements of an asset. This we will do, from an audit assertion viewpoint, which also provides a basis for redefinition.

Audit assertion over information assets

The key components of audit assertion: classification, completeness, valuation, and allocation, are also viewed as: completeness, existence, and accuracy (Srivastava & Kogan 2010).

Classification is referred to as ensuring that transactions and events have been recorded in the related accounts properly (Srivastava & Kogan 2010:269). For information assets, we are of the view that a definition should include events having material impact on the carrying information value of the information asset, and by inference its' containing IT asset. Therefore, a definition for information assets and IT assets must consider their inherent attributes.

Completeness is the state of ascertaining that all the assets, interests, and obligations of an entity requiring recording, have been recorded in the financial statements. When information assets are not fully understood, we assert that they cannot be identified and recorded properly.

Valuation and allocation According to Srivastava and Kogan (2010:269), all the assets, obligations, and equity interests have to be valued appropriately; and if any allocation was needed, then it has to be done on the basis of the identification and valuation having been already done. Applying this to information assets, we maintain that if information assets are not properly identified, they cannot be properly valued; and the commensurate control cannot be applied. Furthermore, the best value cannot be derived from them.

The audit assertion of classification, completeness, and valuation has further affirmed that appropriateness of control over information assets can only be ascertained if information assets are well defined and understood. Otherwise, safeguarding of information assets (and their containing IT assets) would be an exercise in futility. The vast array of internal controls technologies/mechanisms and regulations would continue to inappropriately safeguard information assets; as is currently being evidenced.

The need for a rethink of a definition for Information assets

So far, the research study presented here has shown that contrary to 'expectations', information assets (the core of IT assets) are not well defined in standards, frameworks, and regulations. Furthermore, it has been suggested that misunderstanding can be attributed to the lack of an exact or coherent definition. Conversely, this poor definition is a result of, and leads to misunderstanding of the information asset.

To further the thematic content analysis and comparative study across a number of standards, frameworks, and regulations, a look at audit assertion (Srivastava & Kogan 2010:269) shows that a good understanding assists with definition of information assets, and how these assets should be safeguarded.

Information: A redefinition for corporate information

King III (2009, sec. Glossary) defines information as:

> The raw data that [*have*] been verified to be accurate and timely; [*and that are*] specific and organised for a purpose, [and are] presented within a context that gives meaning and relevance, and which leads to [*an*] increase in understanding and [*a*] decrease in uncertainty.

Information is defined in COBIT®5, as an asset that, like other important business assets, is essential to an enterprise's business; and it can exist in many forms: printed or written on paper, stored electronically, transmitted by post or electronically, shown on films, or spoken in conversation (ISACA 2012, sec. COBIT5 Glossary).

In this article, from the transposition of King III, COBIT®5 and ISO27000, information can then be defined as:

> A critical corporate asset produced by processing raw data (whether printed or written on a medium, stored electronically, transmitted by post or electronically, or spoken in conversation), accurately, timeously, and organised for a specific organisational purpose, which is presented within a context that gives it meaning and direct relevance, and leads to an increase in understanding and a decrease in uncertainty, thereby assisting in gaining competitive advantage.

This proposed definition of (corporate) information is apt for a key driver, enabler, and definer of the knowledge economy and beyond. It further differentiates between personal/private information (discussed earlier) and corporate information (that is being redefined here).

Information assets redefined

In the previous section, information was redefined; and information assets were shown to be: (1) critical business information assets; (2) identified and valued properly; and (3) an organisational resource that needs to be safeguarded appropriately.

The redefinition of information and information assets' characteristics have provided a platform to now redefine *information assets* as:

> Intangible assets consisting of information having no physical form that could be identified singly or collectively, which when arranged systematically or logically could, give an organisation a competitive advantage and the necessary leeway to innovate.

It can then be reasonably assumed that an IT asset as a container of information assets, can be said to be a resource (of the type of hardware, software, data, or derivatives) with definable cost or value within the information channel, which is used to process, transmit, or store information; or a resource having the capability of performing, or which performs an IT function, that has the potential to bring economic benefit to an organisation.

It is hoped that the redefinition would provide further clarity on information assets and IT assets.

Essence of information assets redefinition

It has been shown that an IT asset is a container of physical IT devices, and also a processor/storer of information to which internal control mechanisms can be applied, in order to safeguard both the tangible physical assets and the intangible information assets of which it consists. As a processor, control(s) can be applied to the process. For internal control purposes, the control(s) to be applied are expected to be commensurate with the value of the asset being safeguarded (Poller *et al*. 2014:71).

With the proposed redefinition, we reasonably expect a better understanding of the asset of the knowledge economy and beyond. This we can see on two fronts. Information assets are identifiable singly or collectively; although they are abstract in nature. Secondly, IT assets are resources that consist of tangible and intangible parts. This then implies that the nature of information assets and IT assets could be far better understood, and their attributes could be outlined.

The redefinition as proposed also provides fresh view to the already held notion of information assets simply being data, information, and knowledge that are inputs to a production system. It also contextualises the classes of information assets considered to be databases, documents, published contents, uncaptured, tacit expertise, and experience resident in individual workers (Evans & Price 2014:114; Ladley 2010:397, 456).

Conclusion

The assertion of Haider *et al.* (2006:288) that one cannot manage what one cannot measure readily comes to mind. Organisations would continue to 'fire-brigade' this evolving asset of the knowledge economy bringing forth contemporary issues to management and the board, and finding it difficult to address stakeholders' concerns.

This article has identified a major defect in most standards, frameworks, and regulations dealing with the safeguarding and management of information assets (and IT assets). It has established from the review carried out that information assets have not been properly defined across the board. Beyond this significant finding, it was further shown that the principle of risk (assessment) across the board requires the identification of the asset that needs to be controlled.

However, an often overlooked aspect in the information risk quagmire is the *lack of proper understanding of the very (information) asset to be identified and safeguarded*. Hence, it was *argued* and *deduced* in this article that the effectiveness, efficiency, and reliability of internal control and compliance with applicable laws/regulations would not be appropriate if the (information) assets to be controlled are not:

- properly understood
- properly defined
- properly identified
- properly controlled
- properly retired.

In effect, when the very foundation is shaky, the structure is inevitably defective. Poller *et al*. (2014:70) refer to this as *purely patching a concept that is fundamentally flawed*. Information assets and the associated containing IT assets will continue to be undercontrolled (per internal control), undervalued or overvalued, disposed or retired improperly and finding their way to the wild (unintended public space) until they are understood. A challenge with understanding is that what is not understood might not be defined properly; and conversely, what is not defined properly, might not be understood properly. With a proposed redefinition and the possible applicability to internal control and risk scenarios, further empirical research could assist in defining valuation metrics for information assets, and thereby reduce the over-reliance on subjective valuation.

Although we have not focused on defining information in its entirety across financial, economics, information science, information technology, and the related fields, we have contributed to the body of knowledge with our comparative content analysis study of information assets across a number of frontline standards, frameworks, and regulations that have evidenced incoherent definition. The missing link of incoherent definition of an information asset, misunderstanding of an information asset, and its containing IT asset (frequently overlooked) when applying control over IT assets has been highlighted in this research. We posit that this missing link can possibly lie in the inherent attribute of an IT asset in itself (its hybrid physical tangible asset and intangible information asset).

In the knowledge economy and beyond, information assets will increasingly become distinct and prominent! The inability to properly understand its intrinsic nature and/or to isolate this physical IT asset from its inherent intangible information asset could result in undervaluing both the

information asset and IT asset's financial value, and lead to the underallocation of information security controls to be safeguarded. This intrinsic nature requires further research in order to explicitly classify these attributes.

Gazing into our crystal ball, we postulate that it is a matter of time (6–10 years) before firms will be required to disclose more precise information and/or additional specific disclosure and recognition of separately identified intangible assets (information asset being chief). Already, there is an increasing demand for corporate governance's sustainability reporting that addresses the integrity, reliability, and relevance of financial reporting.

By looking beyond the immediate financial gain, a company protects its reputation – its most significant asset powered by information – and builds trust. Even so, with the advent of sustainable governance and holistic financial reporting that takes social and environmental issues into due consideration (King 2009, sec. 17).

The International Association of IT Asset Managers (IAITAM) has gained prominence in IT assets management. It is recommended that IAITAM's Best Practice Library (IBPL), as well as Asset Disposal and Information Security Alliance's IT asset disposal standard be included in future definitions comparative studies. This could lead to more insights into the challenging terrain of IT assets' dynamic-changing characteristics across the asset's lifecycle: Acquisition, Identification, Provision, Managing, Compliance, and Disposal.

Another further research that might arise from the limitation of this article is the acknowledgment that definition alone (by itself) cannot solve the subjective challenges faced in risk management, and to some extent, in internal control. What has been shown in this research is an aspect of the uncertainty that has to do with the asset leg of risk (comprising the possibility of threats to assets). It has been affirmed that a relook, a rethink, and a redefinition for the information assets (and IT assets) of the future is required. More work in this area would bring to the fore, the very dual contrasting nature of these assets of the future: what threats they would be faced with; how to model these threats; and possibly devise the necessary countermeasures.

Acknowledgements

Competing interests

The authors declare that they have no financial or personal relationships which may have inappropriately influenced them in writing this article.

Authors' contributions

A.K.A. an information security specialist, IT auditor, and lecturer, carried out the underlying research arising from industry observation and primary research for his PhD IT. R.v.S. was the project leader, and along with R.A.B. gave conceptual contributions and research validity of the article. In addition to their research prowness, R.V.S. brought his vast information risk experience to reshape the article and R.A.B., an I.T.I.L. expert, critically reviewed the process flow and ITIL alignment.

References

Ahmad, A., Bosua, R. & Scheepers, R., 2014, 'Protecting organizational competitive advantage: A knowledge leakage perspective', *Computers & Security* 42, 27–39. http://dx.doi.org/10.1016/j.cose.2014.01.001

Arlitsch, K. & Edelman, A., 2014, 'Staying safe: Cyber security for people and organizations', *Journal of Library Administration* 54(1), 46–56. http://dx.doi.org/10.1080/01930826.2014.893116

Australian Parliament, 1988, *Privacy Act 1988*, Australian Parliament, California, Australia, viewed 3 June 2014, from http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s6.html

AXELOS, 2011, 'ITIL ® glossary and abbreviations', in A. Hanna (ed.), pp. 1–93, AXELOS Limited, viewed 3 August 2013, from http://www.itil-officialsite.com/InternationalActivities/ITILGlossaries_2.aspx

Babbie, E., 2012, *The practice of social research*, 13th edn., Cengage Learning, Belmont, CA, viewed 24 January 2014, from http://books.google.com/books?id=-YoJAAAAQBAJ&pgis=1

Buera, F.J. & Kaboski, J.P., 2009, 'The rise of the service economy', *American Economic Review* 102(6), 2540–2569. http://dx.doi.org/10.1257/aer.102.6.2540

Burdon, M., 2010, 'Contextualizing the tensions and weaknesses of information privacy and data breach notification laws', *Santa Clara Computer & High Technology Law Journal* 27(1), 63–129, viewed 4 June 2014, from http://digitalcommons.law.scu.edu/chtlj/vol27/iss1/3/

California Senate, 2002, *California Senate Bill SB 1386 ref paragraph SEC. 2 1798.29. (e)*, California Senate, CA, viewed 3 June 2014, from http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

Charette, R., 2011, 'DigiNotar certificate authority breach crashes e-Government in the Netherlands', *IEEE Spectrum*, viewed 13 March 2014, from http://spectrum.ieee.org/riskfactor/telecom/security/diginotar-certificate-authority-breach-crashes-egovernment-in-the-netherlands

COSO, 2013, *Internal control–integrated framework (framework)*, in Committee of Sponsoring Organizations of the Treadway Commission (ed.), American Institute of Certified Public Accountants, viewed 3 November 2013, from http://www.coso.org/documents/coso2013icfrexecutive_summary.pdf

European Parliament, 1995, *Protection of personal data – Directive 95/46/EC*, EU: Ec.europa.eu, viewed 3 June 2014, from http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Evans, N. & Price, J., 2014, 'Responsibility and accountability for Information Asset Management (IAM) in organisations', *Electronic Journal Information Systems Evaluation* 17(1), 113–121, viewed 25 November 2015, from http://www.ejise.com/issue/download.html?idArticle=943

Gates, C. & Matthews, P., 2014, 'Data is the new currency', in *Proceedings of the 2014 Workshop on New Security Paradigms Workshop – NSPW*, ACM Press, Victoria, BC, Canada, pp. 105–116. http://dx.doi.org/10.1145/2683467.2683477

Goede, M., 2011, 'The wise society: Beyond the knowledge economy', *Foresight* 13(1), 36–45. http://dx.doi.org/10.1108/14636681111109688

Haider, A., Koronios, A. & Quirchmayr, G., 2006, 'You cannot manage what you cannot measure: An information systems based asset management perspective', in J. Mathew *et al*. (eds.), *Engineering Asset Management,* pp. 288–300, Springer, London. http://dx.doi.org/10.1007/978-1-84628-814-2

IASB, 2010, *The conceptual framework for financial reporting*, International Accounting Standards Board: IFRS Foundation Publications Department, viewed 18 August 2013, from http://eifrs.ifrs.org/eifrs/bnstandards/en/2012/framework.pdf

ISACA, 2012, *COBIT 5: A business framework for the governance and management of enterprise IT*, ISACA, Rolling Meadows, IL, viewed 17 April 2014, from http://books.google.com/books?hl=en&lr=&id=1iLKVlOIg9EC&pgis=1

ISO/IEC, 2009, *SANS 38500:2009 South African National Standard Corporate governance of information technology*, 1st edn., SANS 38500:2009, ISO/IEC, Pretoria, South Africa.

ISO/IEC, 2014, *ISO/IEC 27000:2014(E) Information technology — Security techniques — Information security management systems — Overview and vocabulary*, 3rd edn., ISO/IEC 27000:2014(E), ISO/IEC, Geneva, Switzerland.

Jones, A., 2009, 'Lessons not learned on data disposal', *Digital Investigation* 6(1–2), 3–7. http://dx.doi.org/10.1016/j.diin.2009.06.017

Kim, S., Poon, S. & Young, R., 2011, 'Issues around firm level classification of IT investment', in P. Seltsikas et al. (eds.), *Proceedings of the 22nd Australiasian Conference on Information Systems ACIS 2011*, pp. 81, Australasian Conference on Information Systems, Sydney, Australia, viewed 15 September 2014, from http://aisel.aisnet.org/acis2011/81

King, M.E., 2009, *King Report on Governance for South Africa 2009*, Institute of Directors, Johannesburg, South Africa, viewed 14 April 2014, from http://african.ipapercms.dk/IOD/KINGIII/kingiiireport/?Purge=true

Krippendorff, K., 2012, 'Content analysis: An introduction to its methodology', in A. Virding (ed.), *Language arts & disciplines*, 3rd edn., Sage, Thousand Oaks, CA, viewed 03 April 2014, from http://www.abebooks.com/book-search/isbn/0761915451/

Ladley, J., 2010, *Making Enterprise Information Management (EIM) work for business: A guide to understanding information as an asset*, Morgan Kaufmann, viewed 25 November 2015, from https://books.google.com/books?hl=en&lr=&id=ck4BVZuw_jcC&pgis=1

Laney, D., 2014, *The hidden shareholder boost from information assets, technology,* Forbes, viewed 17 March 2015, from http://www.forbes.com/sites/gartnergroup/2014/07/21/the-hidden-shareholder-boost-from-information-assets/

Laskowski, N., 2014, *Infonomics treats data as a business asset, CIO decisions: The new infonomics reality – Determining the value of data*, TechTarget, viewed 17 March 2015, from http://searchcio.techtarget.com/feature/Infonomics-treats-data-as-a-business-asset.

Leavitt, H.J. & Whisler, T.L., 1958, 'Management in the 1980's', *Harvard Business Review* 36(6), 41–48, viewed 17 April 2014, from http://hbr.org/1958/11/management-in-the-1980s/ar/1

Moody, D. & Walsh, P., 1999, 'Measuring the value of information: An asset valuation approach', in *7th European Conference on Information Systems (ECIS'99)*, 7th edn., pp. 1–17, ECIS, Copenhagen. PMID:9316228.

Naidoo, V. & Van Niekerk, B., 2014, 'Strategic information security management as a key tool in enhancing competitive advantage in South Africa', *Journal of Contemporary Management* 11, 33–46, viewed 17 April 2014, from http://hdl.handle.net/10520/EJC148885

OECD, 2011, 'New sources of growth: Intangible assets', in OECD (ed.), *OECD project report 2011,* OECD, viewed 03 July 2014, from http://www.oecd.org/science/inno/48918196.pdf

Okere, I., van Niekerk, J. & Carroll, M., 2012, 'Assessing information security culture: A critical analysis of current approaches', in H.S Venter, M. Loock, & M. Coetzee (eds.), *Information Security for South Africa (ISSA), 2012*, pp. 1–8, IEEE, Johannesburg, South Africa. http://dx.doi.org/10.1109/ISSA.2012.6320442

Parliament of the Republic of South Africa, 2013, *Protection of Personal Information Act, 2013, National Gazettes, No 37067*, Government Gazette of the Republic of South Africa, Cape Town, South Africa, viewed 3 November 2014, from http://www.gov.za/documents/download.php?f=204368

Poller, A., Türpe, S. & Kinder-Kurlanda, K., 2014, 'An asset to security modeling? Analyzing stakeholder collaborations instead of threats to assets', in *Proceedings of the 2014 Workshop on New Security Paradigms Workshop – NSPW*, pp. 69–82, ACM Press, Victoria, BC, Canada. http://dx.doi.org/10.1145/2683467.2683474

Rajasekar, S., Philominathan, P. & Chinnathambi, V., 2013, 'Research methodology', *Physics education*, arXiv:phys, p. 23, viewed 04 June 2014, from http://arxiv.org/abs/physics/0601009

Silva, C., 2012, 'Blue Cross Tenn. pays $1.5 million for HIPAA violation', *Nashville Business Journal*, viewed 13 August 2014, from http://www.bizjournals.com/nashville/news/2012/03/13/blue-cross-tenn-pays-15-million-for.html

Srivastava, R.P. & Kogan, A., 2010, 'Assurance on XBRL instance document: A conceptual framework of assertions', *International Journal of Accounting Information Systems* 11(3), 261–273. http://dx.doi.org/10.1016/j.accinf.2010.07.019

Susanto, H., Almunawar, M.N. & Tuan, Y.C., 2011, 'Information Security Management System standards: A comparative study of the big five', *International Journal of Electrical & Computer Sciences* 11(5), 21–27, viewed 8 August 2014, from http://www.ijens.org/IJECS Vol 11 Issue 05.html

Walton, D., 2013, *Methods of argumentation*, 1st edn., newbooks-services.de, Cambridge University Press, New York, viewed 17 September 2014, from http://dx.doi.org/www.cambridge.org/9781107677333

Warner, J., 2011, 'Understanding cyber-crime in Ghana: A view from below', *The International Journal of Cyber Criminology* 5, 736–749, viewed from http://www.cybercrimejournal.com/warner2011ijcc.pdf