COBIT 5 compliance: best practices cognitive computing risk assessment and control checklist

Jana van Wyk and Riaan Rudman
School of Accountancy, Stellenbosch University Faculty of Economic and Management Sciences, Cape Town, South Africa

Received 9 April 2018
Revised 18 September 2018
20 February 2019
31 May 2019
4 June 2019
Accepted 19 June 2019

Abstract

Purpose – The purpose of this paper was to develop a comprehensive best practices checklist that can be used by governing bodies to identify and evaluate an enterprise's risk exposure around cognitive systems (CSs) and formulate mitigating internal controls that can address these risks.

Design/methodology/approach – COBIT 5 was scrutinised to identify the processes which are necessary for the effective governance of CSs. The applicable processes were used to identify significant risks relating to cognitive computing (CC), as well as to develop a best practices control checklist.

Findings – The research output developed was a best practices checklist and executive summary that would assist enterprises in evaluating their CC risk exposure and assess the adequacy of existing controls. The first checklist highlights the incremental risk exposure which needs to be addressed. To evaluate the effectiveness of the cognitive computing control structure, a best practices checklist was developed that can be used by internal auditors and risk and audit committees. An executive summary was developed to highlight the key focus areas that governing bodies need to consider.

Practical implications – The checklist provides a tool to assess the enterprises' risk exposure, evaluate the existing CC control mechanisms and identify areas that require management attention.

Originality/value – The checklists and executive summary developed provides enterprises with a comprehensive checklist that can be used, while at the same time allowing them to discharge their responsibility in terms of King IV.

Keywords Cognitive systems, Cognitive computing, Governance framework

Paper type Research paper

1. Introduction and research objective

1.1 Introduction and background

Cognitive computing (CC) refers to individual technologies (*inter alia* machine learning, natural language processing, data analytics, deep learning, etc.) that when combined into a cognitive system (CS) have the ability to think, learn and reason like a human brain (Hurwitz *et al.*, 2015). CSs use computerised models to simulate the human cognition process by synthesising data from various information sources, and weighing context and conflicting evidence to find solutions to complex situations where the answers may be ambiguous and uncertain. Cognitive technologies are defined as those technologies underlying CSs.

An increasing number of industries are using the abilities of CSs. For example, in the health industry, CSs are used as medical diagnostic systems that review medical literature and guidelines from world-class experts, and analyse patient data to provide data-driven recommendations to medical practitioners (Bataller and Harris, 2015). CSs are used by biomedical researchers to extract information from scientific literature to automatically identify direct and indirect patterns, thereby accelerating research (Sarkar and Zaharchuk,

Meditari Accountancy Research
Vol. 27 No. 5, 2019
pp. 761-788

2049-372X
DOI 10.1108/MEDAR-04-2018-0325

2015). In the financial services industry CSs are used to automate fraud detection and trade execution (Bataller and Harris, 2015). Deloitte estimates that more than 80 of the world's largest enterprise software companies (by revenues) had already incorporated cognitive technologies into their products by the end of 2016. This is expected to increase to 95 out of every 100 enterprise by 2020 (Willis Towers Watson, 2016). Although the use of CSs creates opportunities for enterprises, problems have emerged. CSs represent an evolution in the use of data and technology, with many enterprises being unaware of the full impact on these two elements (Tarafdar *et al.*, 2017). Risk management, specifically the identification and assessment of risks, as well as the formulation of appropriate controls, is lacking in the governance of CSs. Enterprises require a structured approach to identify and address significant risks pertaining to the use of CSs. Governing bodies are expected to identify and address weaknesses before losses are incurred, but owing to the rate of innovation in and the complex nature of CSs, many enterprises are not equipped to perform an effective analysis of risk exposure and evaluate the control environment. The consequences of this can be severe for those charged with governance, who are ultimately responsible for risk management and IT governance (IODSA, 2016). Generic IT governance frameworks, standards and practices are available to assist organisations with risk management, but they need to be customised to a specific technology to be useful. A tool is needed that can be used by those charged with governance (including internal auditors) to discharge their responsibilities and ask the right questions to those charged with implementation.

1.2 Problem statement and research objective

The purpose of this research was to develop a comprehensive checklist that can be used to identify and evaluate an enterprise's exposure to CC risks and to assist governing bodies in formulating mitigating internal controls that can address these risks.

The fourth King report on corporate governance (King IV) holds governing bodies responsible for risk management and IT governance (IODSA, 2016). Internationally, the UK Corporate Governance Code, ASX Corporate Governance Council's Principles and Recommendations and the Sarbanes-Oxley Act also holds governing bodies responsible for risk management. The board often assigns this responsibility to the risk or audit committee, which in turn relies on the reports of the internal audit function to evaluate risks and assess the effectiveness of controls relating to specific business areas or technologies. Owing to the rate of innovation in and the complex nature of CC, these committees, and in some cases the internal audit functions, are not equipped to perform an effective evaluation of the control environment. Generic IT governance frameworks, standards and practices are available in assisting enterprises in risk management, but these frameworks need to be customised to a specific technology to be useful. The findings of the research is of value to enterprises that intend to use CC because the output of the research was the development of a best practices tool or checklist and executive control summary that can be used by governing bodies to evaluate the control environment in a comprehensive manner based on widely used governance frameworks, such as COBIT. The checklist is already customised to the technology. Organisations can use the checklist to develop their own checklist based on context, including their environment, existing risk management policies and strategies, while relying on their existing risk rating scale and maturity. The checklist will provide governing bodies, as well as internal auditors, as the function tasked with providing assurance to the board of directors, with a tool to i) provide a greater understanding of the role of the CC of the enterprise in the business processes and assess the resulting risk exposures; evaluate the existing CC control structure; and identify areas that

require management attention. Accounting and accounting related subject research has historically focused around the four professional subjects (accounting, auditing, management accounting and taxation). With the growing importance of information technology, and specifically advanced technologies such as CC, the study adds to growing body of interdisciplinary research (Enslin, 2012; Kruger, 2012; Sahd and Rudman, 2017; Bishop, 2018) in the field of auditing and information technology.

This research only concentrated on significant risks relating to the implementation of a CS as well as significant internal control techniques. It was not the purpose of this research to identify the entire spectrum of risks to which enterprises are exposed or all internal controls, because the CS interacts with other technologies and systems. The research did not intend to address the technical complexities of CC, such as the data science and engineering of each core component of the CS. The core components included data, data access, metadata, natural language processing (NLP), deep learning, corpus, advanced analytics, hypothesis, machine learning, infrastructure and enabling technologies. The virtualisation and application components were excluded from this research because they hold their own risks. Similarly, CS development poses its own challenges, therefore this article only highlights some of the significant development risks and appropriate control techniques that can be directly linked to the CS.

2. Research design and methodology

The research is positioned as positivism paradigm, relying on an inductive reasoning approach. The output of the research is a control checklist, as well as an executive summary which can be used by those charged with governance (including internal auditors) to perform risk assessments and develop controls. The best practices checklist was developed following a non-empirical, qualitative approach used by Enslin (2012), Sahd and Rudman (2017) and other authors. The approach was modified to include a systematic literature review. The approach consisted of the following steps:

Step 1: The five-stage systematic process suggested by Sylvester *et al.* (2013) was used to conduct a literature review to obtain an understanding of the technology underlying CC and possible governance frameworks, which could be used. The initial search is broad and inclusive with minimal evaluation, and as the stages progress, the search will narrow and become more focused. Only four of the five stages were considered relevant to this study and were used:

(1) *The searching stage*: The initial search criteria to identify and select relevant literature was deliberately diverse and with a broad scope. The terms used in the initial search included: "cognitive computing", "cognitive technologies", "cognitive analytics", "cognitive computing and big data analytics", "artificial intelligence", "business value of cognitive computing", "IT governance", "corporate governance", "control frameworks", "risks related to cognitive computing", "big data analytics" and "big data". The sources used in the search include printed books and e-books, organisational articles and white papers, theses, scholarly articles published in local and international academic journals, electronic databases (IEEE, Elsevier, Emerald, Scopus) and Web articles. CC as a new generation technology has limited research available, therefore the literature reviewed was not evaluated or discarded based on the quality, academic focus or the reputation of the sources. Seeing as big data, big data analytics and cognitive computing were included in the search, it yielded 323 articles, books and white papers.

(2) *The mapping stage*: The mapping stage focuses on narrowing the scope by identifying recurring themes, keywords and phrases. The themes, keywords and phrases identified during this stage included "data and information governance", "COBIT", "ITIL", "COSO", "cognitive computing systems", "IBM's Watson", "machine learning", "big data analytics", "big data analytics and related risks" and "data privacy and security". A more detailed review of the abstracts, introductions and conclusions were performed to obtain a clear understanding of the extent to which each theme will be included in the research. Based on this review the collection of literature was reduced to 129 relevant articles, books and white papers.

(3) *The appraisal stage*: During this stage the refined selection of articles, books and white papers were read, analysed and the contributions to the identified concepts were linked. The studies were summarised according to common themes throughout the studies. Important concepts underlying CC and CS were identified, categorised and grouped to obtain an understanding of CC and its underlying technologies while identifying the core components of a CS. Key studies performed by *inter alia* Hurwitz *et al.* (2015) and Digital Reasoning Systems (2015) were considered. Although not the focus of the research, consideration was also given to the significant risks enterprises are exposed to given to the implementation of a CS and the related mitigating control techniques, which would assist in better explaining the proposed risk and mitigating control techniques.

Furthermore, literature relating to IT governance and governance frameworks were also considered. The content, scope, benefits and limitation of a selection of governance frameworks (COBIT 5 [Control Objectives for Information and Related Technology version 5]), IT Information Library [ITIL] and Committee of Sponsoring Organizations [COSO 2013]) were analysed to identify the most appropriate governance framework. Professional guides such as the Institute of Internal Auditors' Artificial Intelligence Auditing Framework and Global Technology Audit Guides, were also considered; however, the Artificial Intelligence Auditing Framework was not selected for further review because it has a narrow focus on Artificial intelligence. The Global Technology Audit Guides consists of various guides, which provide detailed guidance for conducting internal audit activities and can be used as the foundation to build a framework. However, the purposes of this study is to use an established, well-known governance framework to create a checklist thereby improving alignment when using the checklist with existing IT governance frameworks. Furthermore, the problem with guides developed by professional bodies are that the methodology they apply are in most cases not scientific methods (Rajcoomar, 2017) and as such may not be complete. This does however create future research opportunities.

(4) *The synthesis stage*: During this stage the available literature from the previous stages are synthesised to enable a consistent approach in reaching conclusions and assists in creating a clear and structured final document.

Step 2: To ensure the academic rigour and completeness of the checklist, an internationally accepted and well-known governance framework was selected and used as the foundation of the checklist. Validity and rigour are added to qualitative research in the positivism paradigm by anchoring the research in theory or a framework. Although other guides

developed by professional bodies are available, a specific framework was selected to ensure that all the control objectives pertaining to the implementation of the technology are identified thereby ensuring that the checklist is complete. From the literature review performed in Step 1 above COBIT was selected as the most appropriate governance framework to achieve the research objective. COBIT 5 is the most comprehensive approach to IT governance and therefore supports the development of a comprehensive checklist. According to Rubino *et al.* (2017), COBIT 5 is a business goal orientated framework and as such other management and IT control frameworks do not provide a complete reference on IT-control to support firm processes in the same manner as COBIT 5 does. COBIT 5 provides an internationally recognised comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. The framework helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use. COBIT 5 is generic, has a broad scope and can be customised for enterprises of all sizes. It allows managers to focus on integrating, aligning and linking process:

- The detailed processes of COBIT 5 were scrutinised to identify the processes that will enable the governance of a CS. Using the knowledge gained about CC from the literature review performed in step 1 above, the applicable processes were used to identify significant risks relating to the core components of a CS.
- The control processes and related significant risks were used as a basis to develop a best practices control checklist to assist enterprises and others in either designing systems of internal control or evaluating the CS. A mapping between the significant risks and related controls is available on request from the authors.

Step 3: An executive summary was also developed.

3. Literature review

3.1 Review of prior research

The majority of research on CC have been conducted by organisations such as IBM Corporation (Drury *et al.*, 2015; Fox *et al.*, 2015; Sarkar and Zaharchuk, 2015; etc.), Accenture (Bataller and Harris, 2015) and Deloitte (Danson *et al.*, 2015). IBM focused much of their research on IBM Watson, while Accenture offers a perspective on CC challenges and presents a framework for understanding how CC can deliver value (Bataller and Harris, 2015). A review of prior research showed that initial CC literature focused on a general overview of CC, CSs and cognitive technologies (Kelly and Hamm, 2013; Ronanki and Steier, 2014; Hurwitz *et al.*, 2015). Hurwitz *et al.* (2015) provided an overview of cognitive analytics and big data analysis, defining CC, the elements within a CS and the underlying technologies. At the same time they provide case studies from the financial, healthcare, and manufacturing industries which address the design and testing of CS. Kelly and Hamm (2013) introduce the world of CS to general audiences and investigate the future of cognitive computing. Academic research has also been conducted. Wang (2011 and 2009) explored the theoretical foundations of cognitive computing in terms of cognitive informatics, denotational mathematics, and neural informatics. A survey by Wang (2011) focused on a theoretical framework, architectural techniques, and conceptual models of cognitive computing. The focus expanded to include the capabilities of the CS as well as the opportunities and challenges enterprises are exposed to because of the use of a CS (Bataller and Harris, 2015; Sarkar and Zaharchuk, 2015).

Other literature focused on CC as a multidisciplinary field that combines neurobiology, cognitive informatics, cognitive psychology and artificial intelligence, with specific focus on

developing computational models (Gutierrez-Garcia and López-Neri, 2015). The latest literature focuses on domain-specific cognitive applications. The research examined the opportunities for the development of applications, as well as the risks regarding the implementation of applications (Chen *et al.*, 2016; Tarafdar *et al.*, 2017). The literature review established that prior research discussed the underlying technologies, as well as the general challenges relating to CC. These were presented in an *ad hoc* manner. Prior research did not present a systematic, comprehensive approach to identify specific risks pertaining to the different components of a CS, nor were these studies conducted with reference to a recognised governance framework. This research proposed to address this gap by providing a structured approach to identify significant risks pertaining to the implementation of a CS, with a specific focus on identifying controls to mitigate the risks. This will ensure that a complete list of risks and controls is presented. Before presenting the checklist, it is necessary to discuss the key concepts underlying the technology (Sections 3.2 and 3.3) and the importance of governance, specifically IT governance, in bridging the IT gap (Section 3.4).

3.2 Cognitive computing and cognitive systems

The evolution of IT and computing consists of three eras. The first and second era encompassed instruction-driven computing, while the third is focused on data-driven computing. The first era, known as the *tabulating era*, comprised of computers which automated the process of logging numbers and performing calculations. In the second era, known as the *programmable computing era*, computers perform tasks, such as calculations and storing of information, based on a set of instructions embedded in software. Programmable computers are still used today, but not all support the enormous amounts of data generated daily by digital technologies (Kelly and Hamm, 2013; Wladawsky-Berger, 2013). CC, the third era in the evolution, and is characterised by a collaboration between humans and machines (Kelly and Hamm, 2013) where systems extract meaning from data and solve problems in the same manner as the human brain does (Chen *et al.*, 2016). Kelly and Hamm (2013), Zaino (2014), Hurwitz *et al.* (2015), Noor (2015), Zhou *et al.* (2017) and highlight the fact that CC consists of several components that, when combined, have various capabilities. The fundamental capabilities of a CS that differentiate CC from other computing include the following (Zaino, 2014; Bellisimo, 2015; Hurwitz *et al.*, 2015; Noor, 2015; Sarkar and Zaharchuk, 2015):

- *Discover*: The CS uses context-driven dynamic algorithms to discover patterns and insight in vast amounts of data. The CS extracts meaning and makes sense of unstructured text data through NLP and extracts features from non-text data (images, videos, voice and sensors) through deep learning tools.
- *Reason and learn*: The CS generates, evaluates and scores contradictory hypotheses. The CS is unbiased and probabilistic, therefore it presumes that there are multiple correct answers for a hypothesis and selects the most appropriate answer based on the applicable data. The CS learns from experience and based on this experience, the system is able to improve its knowledge and its performance without direct programming.
- *Create*: The CS constructs a model of a domain, which includes internal and external data, in the corpus and creates assumptions to determine what learning algorithms are required to enable the system to learn.
- *Engage*: The CS is highly interactive, facilitating advanced communication between human and computer. The system offers expert assistance by gaining deep domain-specific insights and providing this information in a timely, natural and usable format.

The CS contains four phases that consist of core components. Some of these components are fundamental to CC, while others may differ depending on the objective of the CS as well as the approach used to design the CS. The four phases are:

(1) *Phase 1 – structured, semi-structured and unstructured data*: The CS requires large quantities of structured, semi-structured and unstructured data to discover insights, generate hypotheses for decision-making capabilities and engage with humans.

(2) *Phase 2 – data access, feature extraction, NLP, deep learning and metadata*: The function of these components within the CS is to extract features, meaning and context from unstructured data in preparation for ingestion into the corpus, in essence making it machine-readable.

(3) *Phase 3 – corpus and advanced analytics*: The corpus is the body of knowledge of the CS and consists of comprehensible data about a specific domain. Advanced analytic algorithms are applied to the information provided by the corpus to identify new patterns and relationships to increase insight into data and to generate new data for hypotheses.

(4) *Phase 4 – hypothesis generation and scoring, and machine learning*: CC uses three classes of machine learning algorithms to understand and correlate all of the information discovered and generated in the other phases and ultimately manipulate the collection of concepts and relationships to answer questions. The classes of machine learning algorithms used include:

- *Supervised learning*: This refers to an approach where the CS is trained by humans using sample data to detect patterns in a data set. Supervised learning is used where large data sets with known patterns are available, and regression or classification problems must be solved.
- *Reinforcement learning*: This refers to an approach where the CS improves its "thought process" and refines future hypotheses based on feedback received on its performance. The system learns and discovers, through trial and error, which actions yields the greatest rewards and uses this as the basis for its next actions. Reinforcement learning is used when it is too complicated to create a representative training data set.
- *Unsupervised learning*: This refers to an approach that uses inferential statistical modelling algorithms to discover rather than detect (Hurwitz *et al.*, 2015) patterns or relationships in data (Oberlin, 2012). It learns through experience by identifying new patterns and not by matching patterns which it learned through human training. It is used when representative relationships or question-answer pairs are not available to train the CS. The objective is to explore the domain instead of detecting known patterns (Hurwitz *et al.*, 2015).

The core components of the CS depend on a distributed environment supported by an agile and flexible infrastructure. Moreover, the functioning of the CS is dependent on enabling technologies such as Hadoop, cloud computing and big data.

3.3 Application of cognitive computing

According to Bataller and Harris (2015), cognitive computing capabilities can be divided into four types of activity models. Each model uses the CS in a different manner to create value for the enterprise. The following activity models can be implemented:

(1) The *efficiency model* provides consistent, low cost performance for routine, predictable, rule-based activities. In this model the CS senses, comprehends and acts, while humans monitor the accuracy of the results, and determine how the rules need to evolve as conditions change (Bataller and Harris, 2015). Call centres use CS to provide relevant and accurate automated responses to enquiries posed in natural language, thereby improving call center productivity as well as customer satisfaction (Fox *et al.*, 2015). Financial services use CS to assist customers in making better investment decisions. They search large quantities of data to deliver evidence-based recommendations (Drury *et al.*, 2015). The auditing profession can use CS to identify fraudulent behaviour.

(2) An *effectiveness model* provides integration for routine, predictable rule-based activities. However, the data is more complex in comparison with the efficiency model because of an increase in volume and unstructured data. The CS acts as a personal assistant which assist in scheduling, communicating, monitoring and executing activities (Bataller and Harris, 2015). Examples include agents such as Siri, and Alexa, while in a corporate situation, virtual agents will answer routine questions of a customer service center (Bataller and Harris, 2015) for account management, security management and identity management in the banking sector.

(3) An *expert model* provides specialised expertise for ad-hoc, unpredictable, judgment-based activities. The CS makes inferences and recommendations based on the knowledge obtained during the exploration of various data sources. The humans will make the final decision based on recommendations (Bataller and Harris, 2015). A medical diagnostic system is an example of an advisory CS. The CS analyses patient data, medical literature and guidelines from experts to provide data-driven recommendation (Bataller and Harris, 2015). The CS provides advice and experience to customers in the wealth management sector. (Drury *et al.*, 2015).

(4) The *innovation model* enhances ideas and creativity by identifying alternatives and optimising recommendations based on unstructured and more complex data because of an increased volume. The CS enhances creativity and ideas of biomedical researchers, fashion designers, chefs, musicians and entrepreneurs (Bataller and Harris, 2015).

3.4 Governance of cognitive computing

Corporate governance is a structure of policies and procedures by which enterprises are controlled, directed and organised (Zalewska, 2014). IT governance is an integral part of corporate governance and enables the effective management of IT (ISACA, 2012a; Goosen and Rudman, 2013). The third King Code of Corporate Governance for South Africa (King III) specifically includes IT governance principles, emphasising that IT has become a pervasive part of business and as such became a strategic asset that needs to be governed (IODSA, 2009). King IV further confirms this point by highlighting the governance of technology as one of its 17 core governance principles (IODSA, 2016). IT governance is achieved through leadership and organisational structures as well as a framework of best practices for both users and administrators to direct, manage and maintain IT investments and use (Rudman, 2008). Governing bodies must take reasonable steps to generate business value and mitigate risks by adapting international guidelines to the specific technology deployed (IODSA, 2009; Juiz and Toomey, 2015). King III recommends using international

guidelines set by ITGI, ISACA and ISO authorities to support IT governance (IODSA, 2009). A framework should be implemented that provides structures and processes that align business and IT, and should be customised to all relevant risk areas pertaining to the implementation of the specific technology deployed (Goosen and Rudman, 2013). This will ensure that an active, flexible strategy and a cross-functional governance structure are put in place.

An essential element of the IT governance principles is that the board and management should obtain an understanding of the laws and regulations applicable to the CS. Principle 7 of King III makes it necessary for an enterprise to give consideration to data-protection laws and regulations, such as the Protection of Personal Information Act No. 4 of 2013, which prescribes data-protection practices that align South Africa's data privacy and protection legislation with global best practice (De Bruyn, 2014).

Within an organisation, the board is responsible for the implementation of an IT governance framework, while IT specialists are responsible for the implementation of control techniques as indicated by the governance framework. This is problematic, seeing as those charged with governance have insufficient knowledge with regard to the technology and technical design driving the technological infrastructure, while the IT specialists, charged with the implementation of the technology, lack understanding of the governance framework (Rudman, 2010). The IT gap causes a misalignment between business and IT strategies, which in turn creates risks and weaknesses in an IT system. To bridge the gap, the governing body must focus on integrating business and IT strategies by using a framework that enables alignment and is customised to a specific technology (Rudman, 2010).

3.5 Governance frameworks

Governance frameworks make IT governance achievable by providing governing bodies with a framework to systematically, comprehensively and effectively govern IT systems and the background against which controls can be implemented. Governance frameworks provide the basis for addressing risks related to IT, but still need to be adapted to a specific business or technology to ensure that risks are comprehensively identified and addressed. Moreover, enterprises need to consider their approach to the implementation of controls. They can either implement multiple frameworks in an integrated manner or select and customise the most appropriate framework that addresses all the governance areas affected by a specific technology. There are numerous established standards, frameworks and best practices available to govern IT. According to Zhang and Le Fever (2013), governance frameworks can be separated into business-focused (COSO, Statement of Auditing Standards [SAS]), IT-focused (ITIL, ISO/IEC 17799:2000, ISO/IEC 27000) or business–IT alignment-focused (COBIT) governance frameworks. One framework from each category was selected and a review of the scope and content of the frameworks as well as available literature identified specific benefits and limitations (Huang *et al.*, 2011; ITIL, 2011; ISACA, 2012a; D'Aquila, 2013; Rubino and Vitolla, 2014). Figure 1 provides an overview of the benefits and limitations of each framework.

COBIT is a globally accepted and widely used comprehensive framework that seamlessly integrates IT governance into enterprise governance (Huang *et al.*, 2011; Rubino and Vitolla, 2014) and incorporates other frameworks such as Val IT and Risk IT. COBIT was also specifically mentioned in King III. The objective of this framework is to find a balance between the benefits and risks of IT, while considering the interests of all stakeholders (ISACA, 2012a). ITIL is a comprehensible framework of best practices in IT service management and supports the governance, management and control of IT services (ITIL, 2011). COSO is the most widely applied internal control framework for designing,

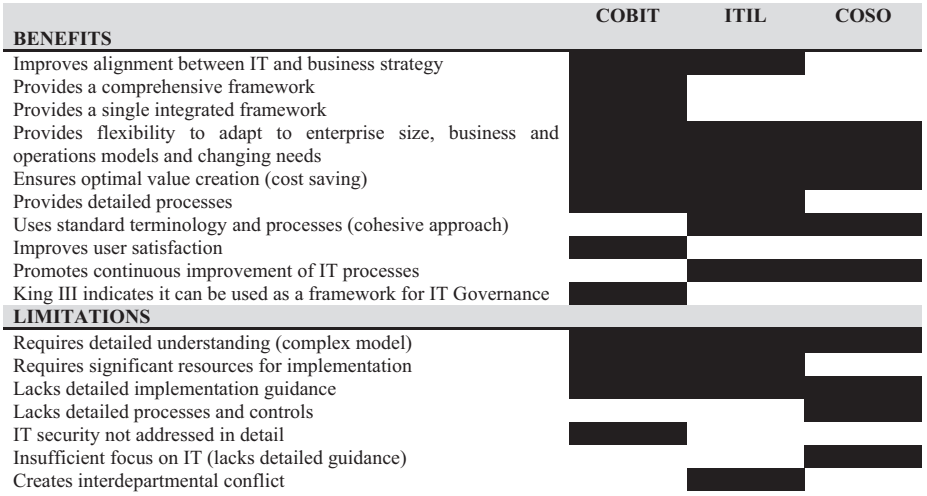


Figure 1.
The benefits and limitations of COBIT, ITIL and COSO

implementing, and managing internal controls, as well as evaluating the effectiveness of these controls (Rubino and Vitolla, 2014). Figure 1 shows that COBIT 5 has more benefits than ITIL and COSO and the same number of shortcomings. This, in the context of the research objective, influenced the selection of the framework. The review of the scope, content, benefits and limitations also showed that COBIT 5 has been updated to be in accordance with ITIL practices (Rubino and Vitolla, 2014) and that COSO, being a broad framework, does not explicitly consider internal control concepts related to IT which COBIT addresses by providing IT specific detail not provided in COSO. Therefore COBIT was selected as the most suitable framework. In addition COBIT has supplementary guidelines (COBIT 5 for Assurance, Information Security and Risk) which can be used in conjunction with the control checklist developed in this study (Table III). The control checklist is customised to address CC risk and mitigating controls and the supplementary guidelines can provide additional detail in specific areas using the COBIT 5 process number as a reference. COBIT 5 for Assurance can be used with the control checklist developed when planning and performing assurance reviews, whereas, COBIT 5 for Information Security can be used with the control checklist developed to provide additional detail regarding information security specific services, infrastructure and application. COBIT 5 for Risk can be used with the control checklist developed to provide more detail on concepts such as risk aggregation and response.

COBIT is focused on the following five key principles (ISACA, 2012a):

(1) meeting stakeholder needs by creating business value by transforming business objectives into IT-related objectives;

(2) incorporating governance and management of information and related IT into enterprise-wide governance;

(3) applying a single, integrated framework by aligning appropriate standards and frameworks to function as an overarching framework for governance;

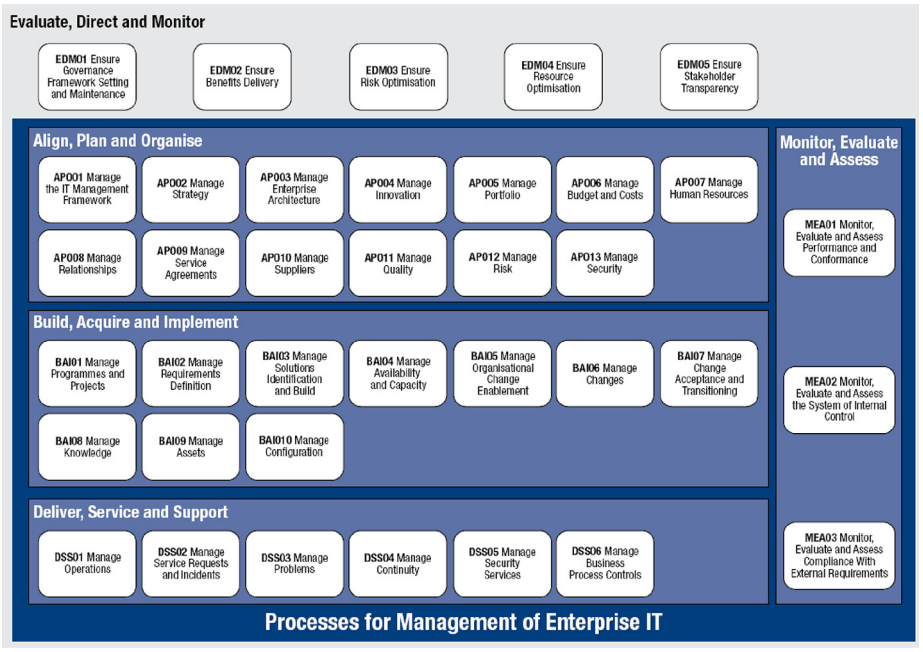
(4) enabling a holistic approach through the use of enablers (i.e. policies and processes) to create efficient and effective governance and management of IT; and

(5) separating governance from management by distinguishing between the different types of activities, organisational structures and goals.

COBIT groups 34 IT processes into five domains, which were used to formulate the control objectives that were used to identify the risks arising from CC (Figure 2). COBIT provides indications for each process which include a process purpose statement, process description, IT-related goals, best practices to be followed and detailed activities (ISACA, 2012b; Rubino *et al.*, 2017).

4. Evaluation of risks pertaining to cognitive systems

A CS interacts with its surrounding environment and as such cannot be governed and managed in isolation. To apply a structured approach to the risk identification process, the detailed processes of COBIT were used to identify risks. The CS components identified during the literature review (Kelly and Hamm, 2013; Digital Reasoning Systems, 2015; Hurwitz *et al.*, 2015) were mapped against the 34 detailed processes of COBIT to identify applicable control objectives. The detailed processes and process requirements were obtained from the COBIT 5: Process Reference Guide. Based on the mapping the significant risk pertaining to a CS were identified. The relevant process requirements and the specific risk exposures are summarised in Table I. The risk exposures are formulated in generic terms to retain the flexibility of the governance framework. This table can serve as a checklist to the internal audit function as well as governing bodies in reporting on an entity's risk exposure and areas requiring management attention. Table I presents the risks in terms of COBIT processes; however, the manner in which this is reported will depend on a particular organisation's reporting and governance practices, and will differ between organisations. Organisations can report in terms of conventional *control objectives* (of confidentiality, integrity and availability), *risk ratings* (of high, medium or low risk) or *risk*



Source: ISACA (2016)

Figure 2.
Processes for governance of enterprise IT

Processes	Risk(s) identified
Evaluate, direct and monitor (EDM): Setting responsibilities for evaluating, directing and monitoring IT usage to create value by establishing a governance framework; assigning responsibilities for value delivery, risk factors and resources; as well as maintaining transparency to stakeholders	
EDM01	CC strategies and policies are inadequately addressed in the enterprise's governance structures, principles and processes
	CC strategies and policies are not comprehensive, effective or well documented
	There is poor implementation of policies and procedures, as well as a lack of stewardship and ownership of CC strategies and policies
	There is inadequate involvement from the board, cascading down to lower management structures and resulting in a poor culture of governance
	There is insufficient monitoring of CC governance for effectiveness
EDM02	The cost of the investments in CC and use there off exceeds the value it contributes to the enterprise
	There is insufficient management and monitoring of value realisation from the CS
EDM03	Not all risks relating to the utilisation of a CS are identified or mitigated appropriately to reduce risk to an acceptable risk tolerance level. Therefore, the risk management process is ineffective
	All governance and legal requirement (relating to the use of personal data, ownership and storage of data) are not identified and mitigated
	There are inadequate business resilience arrangements
EDM04	The CS and resources utilised are not effectively managed and used
	Misallocations of resources occur and are not identified, resulting in under- or over-utilisation of resources
	The current and future need for resources are not continually investigated
EDM05	Reporting to and communication with the stakeholders involved in the investment in and use of the CS are not complete, timely and accurate
Align, plan and organise (APO): Addresses how IT can contribute to achieve business objectives through IT strategy, enterprise architecture, innovation and management of cost, human resources, relationships, quality, risks and security	
APO01	CC objectives are not aligned with enterprise objectives, resulting in a misalignment between strategy and operations (i.e. daily activities)
	The necessary organisational structures are not established
	Ownership of CC policies and procedures is not assigned
	CC policies are insufficient
	CC investments do not create value
	Data ownership of new data and information produced by the CS is not established or controlled
	Continual improvement of the CS and procedures is hampered by insufficient monitoring and management
APO02	The CC road map for the use of the CS is inadequate
	The infrastructure supporting the CS is not sufficient, scalable or compatible
	EDM05
APO03	The CS infrastructure and components are not sufficient for the achievement of the CC objective
	New investments in CS components are not managed effectively, leading to excessive costs
	CC infrastructure (including storage, access, processing, management and transmission) is not scalable and cannot integrate
	Opportunities to advance enterprise operations are missed because of ineffective management
	The algorithms used in the CS are not scalable
	There is insufficient technical and semantics interoperability
APO04	New solutions and opportunities are missed because of ineffective management
APO05	*EDM04, APO01, APO03*

(*continued*)

Table I.
Cognitive computing risks identified using COBIT processes

Processes	Risk(s) identified
APO06	The costs related to the investment in infrastructure and management of the CS components are excessive and deviate from the budgets. These costs include: The initial investment required to develop the CS Investment in experts, personnel changes and retraining Investment in additions, modifications and upgrades to infrastructure Costs required to ensure security and privacy of the CS
APO07	There is ineffective allocation of IT personnel to tasks, without them having the necessary skills and experience There is a shortage of experts, scientists and other IT personnel with the required technical skill sets and experience (i.e. machine learning experts, NLP scientists and data scientist), manifesting in difficulties in recruiting staff and retaining staff
APO08	*APO01*
APO09	Service providers and suppliers do not provide the required skill set or services in accordance with enterprise requirements The IT services provided do not meet user requirement or are insufficient
APO10	Service providers do not have adequate privacy and security policies, procedures and controls Outsourcing services limit the control enterprises have over data *APO09*
APO11	There is insufficient management of data quality The data (i.e. large quantities of data from various sources and spread across various systems) ingested into a CS are inaccurate, manipulated, falsified or outdated, resulting in incorrect outcomes Insecure programs corrupt data, resulting in incorrect results Ingested data cannot be validated, creating data integrity issues
APO12	*EDM03*
APO13	There are inadequate policies and management of sensitive data *DSS05*
Build, acquire and implement (BAI): Improves IT strategy by identifying requirements for IT and management of the IT investment. These include management of capacity, organisational change, IT changes, acceptance, knowledge, assets and configuration	
BAI01	There are inadequate software development processes: The development procedures do not adhere to the enterprise's development standards Third parties involved in the development do not adhere to contractual obligations and enterprise development standards The changes during the development process are not authorised and monitored The different stages of the development process are not controlled and monitored for effectiveness and performance *EDM04*
BAI02	The CS infrastructure and components do not meet enterprise and user requirements *APO09*
BAI03	The corpus is inadequate, as the algorithms are too narrowly defined and do not include the right combination of relevant data External sources are trimmed or cleaned before they are imported into the corpus, limiting discovery The incorrect algorithms are used Inconsistencies occur in the ontology or taxonomy development The CS is not trained correctly There is a lack of integration between the different CS components There is insufficient technical and semantic interoperability *APO02, APO03, APO08, BAI02*

(*continued*)

Table I.

Processes	Risk(s) identified
BAI04	The enterprise has insufficient resources to support the CC strategy
BAI05	Changes during the development and deployment of the CS are not authorised and monitored
BAI06	*BAI05*
BAI07	*BAI01, BAI05*
BAI08	*APO11*
BAI09	There is interference, modification or destruction of the CS by partial infrastructure breaches Challenges in establishing access control across the distributed environments are experienced, including physical security of CS components Software are not updated regularly
BAI10	There is insufficient documentation of system configurations There are inadequate configuration controls
Deliver, service and support (DSS): Focus on the delivery and support of services required to meet strategic plans. Covers the management of operations, service requests, incidents, security, continuity and business process controls	
DSS01	Insufficient monitoring of CS components will leave additional requirements for the CS unidentified, and as such hamper continual improvement *APO09, APO10*
DSS02	*APO02, DSS01*
DSS03	Incorrect solutions and hypotheses occur because of: A low level of quality of data owing to instrumental errors, changing work parameters, falsified data or hacked accounts, etc.; lack of sufficient quality data; bias in training; and CC models that do not capture relationships between data
DSS04	Interference, modification or destruction of the CS occur and lead to significant disruptions. The business continuity plan is inadequate
DSS05	Unauthorised access occurs to sensitive, confidential and personal data, which could result in reputational risk, loss of data, legal liability, etc. because of the following: Intentional security breaches through hacking, malware and phishing Inability to restrict access of all the access points and data sources Distributed infrastructure that leads to security vulnerabilities through: leakage of confidential data owing to malfunctioning computing nodes; eavesdropping on confidential data by adding rogue nodes; interference, modification or destruction of parts of the system or the entire system by a partial infrastructure breach owing to high levels of connectivity and dependency; the number of access across the distributed environments, as well as physical security of data infrastructure, data networks, data applications and data; or operational inefficiency owing to the fact that implementing several security controls across a diverse enterprise IT infrastructure may be complex, time-consuming and costly Non-compliance with regulation Insider breaches by privileged users, resulting in lost, stolen or unauthorised sharing of privileged credentials Inadequate management of security internally and at service providers Inadequate validation of data, affecting the integrity of data Re-identification of individuals as a result of the data manipulation process Use, processing or disclosing of personal data without consent Use of data for a secondary purpose without obtaining consent Violation of individual participation rights to refuse usage, revoke consent and request corrections to their personal data There is a lack of a breach notification plan to inform individual of unauthorised access to personal data
DDS06	*APO01, APO11, DSS05*

Table I.

(*continued*)

Processes	Risk(s) identified
Monitor, evaluate and assess (MEA): Ensures the assessment of performance and conformance, evaluation of internal controls and monitoring of regulatory compliance.	
MEA01	*APO09, APO10*
MEA02	*EDM01*
MEA03	There is legal exposure in multiple geographical jurisdictions regarding the protection of private information and storage of private information Inadequate notice of data collection, use, disclosure and restoration policies is given New knowledge produced from the CS creates uncertainty about data ownership and intellectual property rights

Source: Authors' own construct

Table I.

maturity (ranging from risk-naïve to risk-enabled). Column 1 contains the COBIT 5 process reference, while Column 2 contains the risk derived from the research.

The potential risk exposure of each process in Table I was considered assigning a risk rating and a list of significant risks was identified by means of content analysis. These significant risks are summarised in Table II, with significant strategic-level risks being divided into inadequate governance and management of the CS and inadequate human skills and resource management. Significant risks at an operational or technological level were divided into groups, being risks that affect, either or the objective of the CS; and the ability of the CS to function effectively.

To better explain and define the risks, the literature review was extended to include *inter alia* ISACA (2012b), Géczy (2014), Kitchin (2014), Kshetri (2014), CA Technologies (2015), Hurwitz *et al.* (2015), Sarkar and Zaharchuk (2015), ISACA (2016), Fang *et al.* (2017), Zhou *et al.* (2017) and Raguseo (2018).

5. Evaluation of cognitive control environment

Controls governing a specific technology are typically configured by the IT department or a service provider, while the internal audit function is typically responsible for evaluating the risk exposure and assessing which controls are present and operating effectively. Despite the significance of CS risks, the controls addressing these risks are often not methodically planned and implemented. According to ISACA (2016), internal controls are policies, processes and practices developed to provide reasonable assurance that undesirable events (risks) are prevented, detected and corrected. While some enterprises are establishing comprehensive policies and processes in accordance with COBIT, others are using *ad hoc* approaches (Sarkar and Zaharchuk, 2015). Enterprises using a CS as a strategic platform are exposed to significant risks. To mitigate these risks, the enterprises must implement a governance framework to ensure that comprehensive controls are deployed to govern and manage the CS in a comprehensive manner, rather than implementing controls in an *ad hoc* manner.

To develop a comprehensive best practices checklist for evaluating the control structure, the detailed processes of COBIT were first applied to a CS to identify the specific risks, as outlined in the previous section. A risk or weakness is a control objective not being met. These potential weaknesses were then used by the researcher to formulate the most relevant and practical internal controls needed to mitigate these risks. Literature by *inter alia*

Risks at a strategic level	
Inadequate governance and management of the CS	The absence of an effective governance framework and comprehensive governance strategies results in a misalignment between CC objectives and the entities' objectives (Rubino and Vitolla, 2014), investments in CC exceeding the expected return, misallocation of resources (Suer and Nolan, 2015) and CC risks not being addressed (Hurwitz *et al.*, 2015)
Shortage of human skills	A shortage of people with the technical skills (e.g. machine learning experts, NLP and data scientist) required to develop and deploy the CS exists (Kitchin, 2014; Sarkar and Zaharchuk, 2015)
Risks at an operational level	
Risks that affect the objective of the CS	
Increasing cost	Implementing the CS may have significant cost implications; because the majority of the CS require in-house development or vendor collaboration, additional investment is required to obtain and retain staff with specialised skill. Additional investment and payment of unforeseen costs may be necessary to support infrastructure modifications
Breach of privacy	The deployment of CC introduces the following significant privacy risks (De Bruyn, 2014; Kitchin, 2014; Kshetri, 2014; CA Technologies, 2015; Hurwitz *et al.*, 2015; Fang *et al.*, 2017): *Re-identification risk*: The CS integrates data from various sources to identify new connections, thereby increasing the risk of semi-anonymous information or personally non-identifiable information becoming identifiable *Transparency risk*: Personal data may be used, processed or disclosed without consent from the affected individual because aggregated data from various data sources may not have enough identifiers to trace the data back to the source in order to obtain consent. The CS also creates secondary data that may be used for a purpose other than for the original consent obtained *Violation of individual participation rights*: CSs are continually updated with newly generated information. Individuals may not be able to update or remove personal information included in the newly generated information *Unauthorised access:* Unauthorised access to sensitive data increases in the CS because data are obtained from various sources that are aggregated in one place *Compliance risk*: CC exists in a data-rich environment that is highly regulated, particularly personally identifiable information; as such, a risk of financial and other legal consequences exists due to non-compliance
Security	Challenges to secure data against disclosure to unauthorised users, unauthorised modification and inaccessibility in a CS include (Paryasto *et al.*, 2014; CA Technologies, 2015; Hurwitz *et al.*, 2015): *Unauthorised access* (refers to privacy risks) *Intentional security breaches* through hacking, malware, viruses and denial of service *Distribution risk* due to the distributed nature of infrastructure that increases the number of access points, thereby increasing the risk of malicious attacks going undetected *Non-compliance* (refers to privacy risks) *Insider breaches* where there is a risk of lost, stolen or unauthorised sharing of privileged credentials by privileged users and administrative accounts *Insecure computation* where an insecure program that has access to confidential data in the CS corrupts the data, leading to incorrect results as well as denial of service to the CS *Outsourcing risks* owing to the enterprise using service providers, thereby limiting the enterprise's control over confidential information
Assignment of ownership and risks	In a CC environment, the new knowledge produced by the system creates uncertainty about data ownership and intellectual property rights (Hurwitz *et al.*, 2015)

(*continued*)

Table II.
Significant risks relating to cognitive computing

Risks that affect the ability of the CS to function effectively	
Lack of scalability	The inherent limitation of algorithms in the CS creates the risk that the algorithms will not be able to scale as data and computational resources increases. Some machine learning algorithms and NLP specifically have scalability problems (Chen and Zhang, 2014; Zhou *et al.*, 2017). Moreover, the data infrastructure supporting the CS also contains inherent limitations that will restrict the performance levels of the CS
Poor integration	Integration risk encompasses both data integration, and system and infrastructure integration *Incompatible data from diverse sources*: Diverse data sources produce data with various formats and semantics that may be incompatible. If the CS does not obtain a common representation when integrating data, the links between the data can be poorly defined, resulting in invalid outputs (Kitchin, 2014; Knoblock and Szekely, 2015) *Incompatible infrastructure*: The variety and complexity of data in a CS require diverse storage capacity, processing power, management mechanisms and network technologies (Chen *et al.*, 2015). If these different infrastructure components do not integrate seamlessly, there is a risk that the system will not deliver the desired results (Géczy, 2014)
Lack of inter-operability	The two main threats for a CS are technical and semantics interoperability (Janssen *et al.*, 2014). Technical interoperability entails the risk that the different components of the CS will be unable to communicate. Semantics interoperability entails the risk that the CS interprets data inconsistently, resulting in the misinterpretation of data, correlations between data not being recognised or incorrect associations being made
Errors in data, training and hypothesis (i.e. veracity)	The risk exists that low levels of data quality will result in lower levels of data quality within the CS, thereby weakening the validity of the results of hypotheses and prohibiting the identification of correlations and nuances between similar data sources (Wigan and Clarke, 2013; Kitchin, 2014). The quality and veracity of data within a CS may also be weakened due to bias of experts involved in the development of supervised machine learning algorithms
CC life-cycle risks that affect both the objective of the CS and the ability to function effectively	
Life-cycle risk	In the development phase of the life cycle, an inadequate high-level CC road map will compromise the ability of the system to function effectively. The risk that the development of cognitive components will be ineffective because of problems with logic increase if: the contents of the corpus are too narrowly defined, limiting the problems that can be solved; the corpus does not include the right combination of relevant data resources; the data from the external sources are cleaned before they are imported, thereby limiting the generation and scoring of hypotheses; the inappropriate machine learning algorithms is used; or the taxonomy or ontology is poorly developed Insufficient monitoring of the core CS during the use/operate phase will leave additional requirements for the CS unidentified, and as such will hamper continual improvement. An inadequate change management plan may impact the workings of a CS

Source: Authors' own construct

Table II.

Rudman (2010), ISACA (2012a), ISACA (2012b), Sudarsan (2013), Kitchin (2014), CA Technologies (2015), Danson *et al.* (2015), Hurwitz *et al.* (2015), Terzi, Terzi and Sagiroglu (2015), Zikopoulos, deRoos, Bienko, Buglio and Andrews (2015), ISACA (2016) and Fang *et al.* (2017), Zhou *et al.* (2017) were used to clarify the description of the internal control techniques. The comprehensive list of controls, as set out in Table III, can be used as a best practices checklist to identify omissions and weaknesses in existing control structures. Column 1 contains the COBIT 5 process reference, while Column 2 contains the checklist developed from the research. The checklist can either be used in its entirety, or can focus on the high-risk areas identified in Table I.

From Table III it is apparent that at a strategic level, the enterprise should develop a CC governance strategy accompanied by a list of comprehensive policies to provide practical guidance for implementation and a human resources strategy, while at an operational or technological level, the enterprise should implement techniques to detect and mitigate risk exposure. These include data controls, infrastructure controls, supplier controls and lifecycle controls.

6. Executive summary of cognitive system controls

In assessing and reporting on the effectiveness of an entity's CC control structure, the internal audit function can use the best practices checklist as formulated in Table III. The best practices have been summarised in an executive summary in two parts, in Table IV and V that can serve as a toolkit to educate board level committees on CC management. The summary is also useful as a final checklist that all significant areas of CC exposure have been addressed. The summary highlights that a comprehensive CC control structure includes controls at two levels: strategic and operational.

7. Conclusion

The exponential growth of data, advances in enabling technology and the ability of CC to realise significant business value have accelerated the growth and use of CC. However, enterprises are unaware of the risks the deployment of the CS creates (Tarafdar *et al.*, 2017). Given that governing bodies, responsible for oversight and implementation of governance, are often unaware of these risks, they are not implementing a system of internal control in accordance with an appropriate governance framework to mitigate these risks. The objective of this research was to assist enterprises with this problem by providing a structured approach using COBIT to identify the significant risks the enterprise is exposed to owing to the deployment of the CS. By applying the relevant processes of COBIT control objectives and related significant risks, appropriate internal control techniques were formulated. Using COBIT, the following significant risks were identified: inadequate governance, insufficient human skills and resourcing, cost, privacy, security, scalability, integration, interoperability, veracity, ownership and lifecycle risks. Through the implementation of the COBIT detailed processes, various internal control techniques can be implemented to address risks. These include the following:

- *strategic level controls* – establishing a CC governance framework and implementing human skills and resources controls; and
- *operational or technological level controls* – implementing CC lifecycle controls to provide management with information on how to develop and maintain a CS. This includes the design and implementation of detailed internal control techniques on a data control level, infrastructure control level and supplier control level.

The research output developed was a best practices checklist and executive summary that would assist enterprises in evaluating their CC risk exposure and assess the adequacy of controls implemented. The first checklist contained in Table I highlights the incremental risk exposure, as a result of the nature of the technology that needs to be addressed. To evaluate the effectiveness of the CC control structure, a best practices checklist was developed (Table III) that can be used by internal auditors and risk and audit committees. From the comprehensive best practices detailed in Table III, an

Processes	Control(s) to mitigate the risk(s)
Evaluate, direct and monitor	
EDM01	The board must take ownership for the governance of CC within the enterprise and must design and implement a governance framework that ensures that: all stakeholders are identified and their requirements are obtained and documented; comprehensive CC governance policies are established; governance policies and procedures are reviewed and monitored to enable improvement; responsibility regarding the investment in and use of CC is established and communicated; and formal reporting lines are established to ensure accountability Design and implement a system to monitor the effectiveness of the governance policy and procedures
EDM02	Compile a comprehensive cost-benefit analysis and budget to measure and manage the investment in and return from the CS
EDM03	Develop and implement a risk management system that: establishes a risk committee to take ownership for risk management and monitoring; establishes and documents processes for risk identification, risk assessment and risk response; assigns and communicates the responsibility for the identification of risks; addresses legal and regulatory compliance risks; and addresses the management of changes in risks and disaster recovery
EDM04	Perform a resource gap analysis to establish whether sufficient resources are available to implement an effective cognitive solution Establish ownership and accountability for resource investment Establish performance policies and measures to evaluate and monitor the optimisation of allocated resources, as well as the alignment between resource allocation to the CC strategy and the business strategy
EDM05	Identify all stakeholders, establish their requirements and develop communication policies
Align, plan and organise	
APO01	Define enterprise and CC strategies and objectives and ensure alignment between the strategies and objectives by performing a detailed mapping Establish CC policies and procedures to support alignment Communicate the CC strategy and policies to the stakeholders and establish their responsibilities Establish and implement data provenance standards and rules throughout the data lifecycle in the CS Implement a system of continuous monitoring and improvement of the strategy, policies and procedures
APO02	Design a CC road map that defines the objective of the CS, establishes user requirements, identifies the required CC components and establishes a development plan Establish the IT infrastructure required to support the CC strategy Perform a maturity analysis to assess the ability of the current infrastructure Perform a gap analysis to identify shortcomings between the current and required infrastructure
APO03	Define and implement procedures and controls to manage and monitor the IT infrastructure, cognitive components and related services Implement a change management process and an infrastructure migration plan Use CC platforms, cloud computing platforms and data platforms to increase scalability and integration
APO04	Develop procedures for the identification of new areas of innovation Establish a Centre of Excellence (CoE) to facilitate the mobilisation of resources for the CC initiatives Evaluate the data resources the enterprise owns and which additional data resources are required to create new opportunities for insight
APO05	*EDM04, APO01, APO03*

(*continued*)

Table III.
Best practises control checklist formulated using COBIT processes

Processes	Control(s) to mitigate the risk(s)
APO06	Use CC platforms, cloud computing platforms and data platforms to reduce and control development cost, infrastructure cost, human skills cost, and security and privacy costs
	Determine the resources and investment necessary to create the appropriate IT infrastructure to support the CS and prepare a budget
	Establish performance measures to evaluate and monitor the optimisation of resources
APO06	Reduce cost by integrating the CS with the existing IT environment and extending current controls and processes into system
APO07	Include human skills and resource requirements in the CC strategy and governance programme
	Appoint a chief information officer with the appropriate experience
	Perform a gap analysis to identify potential skill and resource gaps
	Provide targeted training for existing employees
	Hire new talent and leverage consulting firms
	Form partnerships with vendors involved in CC and invest in higher education systems
APO07	Establish a CoE to facilitate: the development of cross-functional team, which will include analysts, domain specialists, data engineers and data scientists; cross-training of personnel; communication between experts and IT teams; and culture of trust and collaboration
	Develop policies for the assessment, training and development of staff
APO08	*APO01, APO02*
APO09	Determine whether the CS will be developed in-house, outsourced or by means of a cognitive platform
	Establish a usage policy, which identifies which components of the CS should be supported by services from service providers
	Establish performance measures for outsourced services, compile and review service level agreements, assign responsibility within the enterprise to monitor compliance with the service level agreement and establish controls to address security, change management and access rights
APO10	*APO09*
APO11	Control data quality through pre-processing data by using: data cleaning software that identifies and corrects potential data-quality issues by standardising data based on historic data captured; data-quality software that ensures that data and meta-data elements are represented in the same manner throughout the CS; standardisation that normalise data into defined standards by creating a consistent representation of data by parsing free-form data into single-domain data elements; data profiling that allows the system to validate data against technical rules; and metadata management that provides a metadata definition and a glossary to facilitate data quality, data provenance and data governance
	Map, link, match and filter data in the corpus with the use of taxonomies, analytics and NLP
	Standardise data into a universal form to facilitate effective data integration in a CS. This can be done by leveraging mature data integration tools or third-party products (Hadoop), or by using the interpretation level in the CS (NLP, text analytics)
APO12	Establish risk management procedures for the continuous identification, monitoring and evaluation of new and emerging risk relating to the CS
	Identify, monitor and manage supplier risks to ensure that the supplier has the ability to continuously provide secure, efficient, effective and reliable service delivery
APO13	Establish data classification policies that define the purpose, ownership and sensitivity of data types to ensure that sensitive information is managed according to the risks it poses to the enterprise

Table III. (*continued*)

Processes	Control(s) to mitigate the risk(s)
	Establish privacy policies that defines sensitive data and personally identifiable information and addresses securing the data, transparency of usage, receiving and revocation of consent *DSS05*
Build, acquire and implement	
BAI01	Manage the development process by: assigning ownership of the project; establishing a development methodology that aligns with enterprise development standards; implementing quality assurance processes; implementing project risk management processes; and implementing change management processes Develop a training and testing strategy *APO09*
BAI02	*APO02, APO09*
BAI03	Determine the objective of the CS and the type of question it will have to solve Define the domain area for the CS and based on the definition determine the domain experts needed to train and test the system Establish the user requirements Evaluate the data resources the enterprise owns and which additional data resources are required to create new opportunities for insight Determine the right combination of relevant data resources (internal and external) needed Determine the lifecycle for each data source to establish which sources must be updated regularly and create a process to ensure that the updates are made on a timely basis Determine whether data from the external sources should be cleaned or transformed before they are imported Validate the ingested data to ensure that the data are readable, comprehensible and searchable Monitor the data ingestion process to ensure that the deletion of records for security purposes has been done Identify which machine learning algorithms and analysis techniques are best suited for the specific domain question which must be solved Determine whether a taxonomy or ontology is available for the domain or whether a new taxonomy or ontology must be developed Monitor the development of the ontology or taxonomy to identify any inconsistent assumptions, beliefs and practices that may affect the corpus Determine the correct combination of algorithms that will enable the corpus to update and maintain the corpus itself
BAI04	*EDM04*
BAI05	Implement change management processes Implement policies and procedures that identify new innovation areas within the CC solution
BAI06	*BAI05*
BAI07	*BAI01, BAI5*
BAI08	*APO11*
BAI09	Establish an access control list to limit the access rights of system users and assign the proper access rights Use access control models, such as role-based access control or attribute-based access control
BAI09	Implement physical security controls Establish policies to control inbound and outbound data traffic by using network filtering mechanisms such as firewalls, anti-malware and intrusion detection software
BAI10	Establish and maintain a logical model for the configuration of infrastructure items as well as regular software updates

(*continued*)

Table III.

Processes	Control(s) to mitigate the risk(s)
Deliver, service and support	
DSS01	Service level agreements must clearly define service requirements Monitor and review service to ensure it aligns with the service level agreement Identify which controls are relinquished to the provider and determine the specific monitoring controls that must be implemented because of this relinquishment Validate the control activities of the provider to ensure that they align with the enterprises risk appetite Periodically verify if the controls maintained by the provider are effective through independent reviews Assess and monitor the ability of the supplier to provide adequate incident response and procedures to address system disruption and security breaches Assess and monitor the ability of the supplier to restore operations in the event of a disaster Establish an incident response plan and business continuity plan to support the suppliers' plans Integrate key internal IT management processes with those of suppliers, specifically change, configuration, incident, security and business continuity management
DSS02	*APO02, DSS01*
DSS03	Improve the accuracy of answers and hypotheses provided by: adding glossaries and ontologies to the corpus; testing sample data; and continually acquiring new data to update the corpus
DSS04	Establish an incident response plan and business continuity plan to support the suppliers' plans *EDM03*
DSS05	Implement the following privacy controls techniques: *Anonymisation*: De-identifies all data that can be linked to an individual by removing personally identifiers through the use of *AES symmetric key encryption, adaptive utility-based anonymisation and sub-tree anonymisation* *Pseudonymisation*: De-identifies most identifying fields within a data by replacing it with one or more artificial identifiers, or pseudonyms *Privacy preferences*: Enable individuals to tag their data or information with privacy preferences. Software is then used to track the usage of the data by means of metadata *Masking*: Disguises sensitive data by substituting real data with realistic-looking fictitious data. Static data masking or dynamic data masking can be used *Tokenisation (data scrubbing)*: Replaces sensitive data with tokens obtained from a token table which enables only authorised users who has access to the token table to restore the data Implement privacy and security management, including the following: *Proactive management*: Ensures security of personal information and sensitive information, as well as compliance with legislative requirements by proactively identifying, understanding and responding before processing occurs *Data lifecycle control*: Manages data from collection to retirement by documenting policies for data retention and disposition, which specifically address the manner in which collected data are preserved in their original format, and how the data are destroyed in a manner that creates a verifiable data disposition audit trail *Monitoring system model*: Ensures security during data collection, integration, analysis and interpretation by means of security and network logs and data integration processes (e.g. data filtering and classifying) *Data activity monitoring*: Ensures that data access is secure by continuously monitoring activities in real time, using pattern-based policies to identify unauthorised, suspicious and/or malicious activity (internal and external), which terminates the request and subsequently alert key personnel

Table III. (*continued*)

Processes	Control(s) to mitigate the risk(s)
	Implement security controls such as the following: *Authentication*: Identification of users with e-mail, passwords, digital signatures and two-factor authentication *Encryption*: Secures transmission of data by scrambling sensitive data *Anti-malware software*: Eliminate the threat of malicious infections of both inbound and outbound data transmissions by using anti-spy and anti-virus software *Access control list*: Limits the access rights of system users and assigns the proper access rights. The enterprise should also use access control models, such as role-based access control (grants permission to users based on their roles within the enterprise) and attribute-based access control (makes a context-aware decision to grant access to the system based on multiple attributes) *Key establishment scheme*: Secures data by using cryptographic virtual mapping to create separate data paths that are located at different storage providers, with information encryption *Secure group key transfer protocols*: Secure communications between multiple groups through key freshness, key authentication and key confidentiality. This protocol includes an online key generation centre (based on Diffie–Hellman key agreement) and linear secret sharing scheme *If-assuring system*: Prohibits the user from proceeding with a task or accessing data if the system classifies the user as suspicious Use the following data management and monitoring controls to ensure secure communication: *Privileged access management solutions*: Manage privileged users, such as system and network administrators, vendors and business partners, by establishing privileged user authentication, privileged user credential management and privileged user session management *Intrusion detection and prevention architecture*: Secures data through security monitoring architecture that stores and processes data in distributed sources through data correlation schemes. Uses a maliciousness likelihood matrix to identify whether a domain name, packet or data flow is malicious *Data encryption security server*: Administers, manages and controls encryption policies and keys, as well as access to unencrypted data
DDS06	*APO01, APO11, DSS05*
Monitor, evaluate and assess	
MEA01	*APO09, APO10*
MEA02	*EDM01*
MEA03	*EDM03, DSS05*

Source: Authors' own construct

Table III.

Governance	Implement a governance framework and develop a governance system for CC Develop and implement a CC strategy Develop and implement CC policies Provide employees with training on the use of CC and the related output
Human resources and skills	Include human skills and human resource requirements as part of the IT governance programme Standardise human resource management Perform a skills gap analysis Cultivate existing talent with targeted training on the skills required to operate a CS Address the skills gap by employing new talent and leveraging off consulting firms Enter into partnerships to gain access to skills resources Establish a CoE

Source: Authors' own construct

Table IV.
Executive summary of cognitive computing controls at strategic level

Lifecycle controls	Develop a CC roadmap
	Define the objective and domain of the CS
	Determine which experts are required to train the CS
	Establish user requirements
	Evaluate data sources, determine the right combination and perform regular updates
	Determine which data should be cleaned and transformed
	Validate ingested data and monitor the ingestion process
	Identify the best algorithms for the domain and the right combination
	Determine whether taxonomies and ontologies are available and monitor the development process
	Develop a training and testing strategy
	Test sample data on a regular basis
	Continuously add glossaries and ontologies to improve the CS
	Implement best practices to manage the CS and software development process
Data controls	De-identify personally identifiable information using anonymisation techniques
	Allow individuals to tag personal data with privacy preferences
	Implement masking techniques as well as tokenisation techniques
	Perform proactive management to identify risks and develop protocols that address the risks
	Manage data throughout their lifecycles, placing reliance on data lifecycle controls
	Implement a monitoring system model to detect breaches in the system
	Implement data activity monitoring to ensure secure data access
	Use Hadoop standard security controls
	Use data cleaning software to ensure data quality
	Use data quality software to ensure data quality
	Standardise data to defined standards
	Use data profiling to validate data
	Implement metadata management to ensure data quality and provenance
	Obtain legal advice regarding privacy matters and data storage and usage
	Implement data provenance standards to allow traceability
Infrastructure controls	Perform a needs assessment to identify the IT infrastructure required for a CS
	Perform a gap analysis and maturity analysis to access current IT infrastructure
	Develop an IT infrastructure solution to address the gaps identified during the gap and maturity analysis
	Manage and monitor the IT infrastructure
	Implement change management, disaster recovery and business continuity plans
	Implement physical security
	Implement and maintain configuration and software updates
	Implement authentication techniques.
	Implement encryption techniques
	Use anti-malware software
	Implement access control
	Secure data by implementing a key establishment scheme
	Implement secure group key transfer
	Implement secure group data sharing
	Establish a secure communication channel for data transmission
	Implement a self-assuring system to prohibit suspicious tasks and users
	Establish privileged access management
	Monitor the system through intrusion detection software

(*continued*)

Table V.
Executive summary of cognitive computing controls at operational level

Service provider controls	Establish service level agreements with key service providers
	Manage and monitor service provider risks
	Define service requirements in service delivery agreements
	Monitor and review service delivery
	Implement monitoring controls (service provider control management)
	Request independent reviews to evaluate controls implemented by service providers
	Assess and monitor service providers' incident responses
	Assess and monitor service providers' disaster recovery plans
	Establish incident response and business continuity plans to support service providers' plans
	Integrate key IT management processes with service providers' processes

Source: Authors' own construct

Table V.

executive summary was developed in Tables IV and V to highlight the key controls necessary to govern CC at a governance, management and operational level, which can be used by management. These checklists were developed using COBIT to ensure completeness and rigour. These checklists can be used either as a complete checklist or to rate the risks to identify high-risk areas that require attention. Thereafter, the COBIT reference can be used to identify which controls must be implemented to mitigate the relevant risks. Because prior research studies were performed without the use of a governance framework as a completeness benchmark, findings were incomplete. In a business environment where greater reliance is being placed on IT, future research that focuses on methods to mitigate risk in a comprehensive manner is needed. For further research, an expert review can be performed on the governance framework or the framework can be used as a best practice benchmark in a real-world setting to evaluate its appropriateness. The research could also be extended to include applications controls, which have been excluded from this study. Other frameworks and professional guides, for example the Global Technology Audit Guides, can be used to design the application controls.

References

Bataller, C. and Harris, J. (2015), "Turning cognitive computing into business value today", available at: www.accenture.com/t20150521T005731__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_8/Accenture-Turning-Cognitive-Computing-Business-Value-Today.pdf (accessed 15 June 2015).

Bellisimo, J. (2015), "What's the future of cognitive computing? IBM Watson", available at: www.forbes.com/sites/ibm/2015/02/23/whats-the-future-of-cognitive-computing-ibm-watson/#7a2e74085e2e (accessed 5 April 2015).

Bishop, W.A. (2018), "A project management framework for small-and-medium-sized entities: Accounting software implementation", *Journal of Economic and Financial Sciences*, Vol. 11 No. 1, pp. 1-11.

CA Technologies (2015), "How can I defend my hybrid enterprise from data breaches and insider threats?", available at: http://docs.media.bitpipe.com/io_12x/io_128619/item_1283253/EC-solutionbrief-privilegedaccessmanagement-Final.pdf (accessed 9 February 2016).

Chen, Y., Argentinis, E. and Weber, G. (2016), "IBM Watson: how cognitive computing can be applied to big data challenges in life sciences research", *Clinical Therapeutics*, Vol. 38 No. 4, pp. 688-701.

D'Aquila, J. (2013), "COSO's internal control integrated framework updating the original concepts for today's environment", *The CPA Journal*, Vol. 83 No. 10, pp. 22-29.

Danson, F., Pierce, D. and Shilling, M. (2015), "Amplified intelligence, power to the people", available at: www2.deloitte.com/insights/us/en/focus/tech-trends/2015/tech-trends-2015-amplified-intelligence.html (accessed 5 April 2015).

de Bruyn, M. (2014), "The protection of personal information act: impact on South Africa", *International Business and Economics Research Journal (Iber)*, Vol. 13 No. 6, pp. 1315-1340.

Digital Reasoning Systems (2015), "Introduction to SYNTHESYS", available at: https://vimeo.com/digitalreasoning (accessed 21 December 2015).

Drury, N., Harper, A., Marshall, A. and Sarkar, S. (2015), "Breakthrough banking", available at: www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&htmlfid=GBE03713USEN&attachment=GBE03713USEN.PDF (accessed 22 July 2016).

Enslin, Z. (2012), "Cloud computing adoption: control objectives for information and related technology (COBIT) - mapped risk and risk mitigating controls", *African Journal of Business Management*, Vol. 6 No. 37, pp. 10185-10194.

Fang, W., Wen, X.Z., Zheng, Y. and Zhou, M. (2017), "A survey of big data security and privacy preserving", *IETE Technical Review*, Vol. 34 No. 5, pp. 544-560.

Fox, B., Lala, R. and Coelho, O.C. (2015), "Dialing in a new frequency: your cognitive future in the communications industry", available at: www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&htmlfid=GBE03722USEN&attachment=GBE03722USEN.PDF (accessed 22 July 2016).

Géczy, P. (2014), "Big data characteristics", *The Macrotheme Review*, Vol. 3 No. 6, pp. 94-104.

Goosen, R. and Rudman, R. (2013), "An integrated framework to implement IT governance principles at a strategic and operational level for medium-to large-sized South African businesses", *International Business and Economics Research Journal (Iber)*, Vol. 12 No. 7, pp. 835-854.

Gutierrez-Garcia, J.O. and López-Neri, E. (2015), "Cognitive computing: a brief survey and open research challenges", Paper Presented at the 3rd International Conference on Applied Computing and Information Technology and the 2nd International Conference on Computational Science and Intelligence, 12-16 July, Okayama, available at: http://ieeexplore.ieee.org.ez.sun.ac.za/stamp/stamp.jsp?tp=&arnumber=7336083 (accessed 3 June 2016).

Huang, S.M., Hung, W.H., Yen, D.C., Chang, I.C. and Jiang, D. (2011), "Building the evaluation model of the IT general control for CPAs under enterprise risk management", *Decision Support Systems*, Vol. 50 No. 4, pp. 692-701.

Hurwitz, J.S., Kaufman, M. and Bowles, A. (2015), *Cognitive Computing and Big Data Analysis*, John Wiley and Sons, Indianapolis, IN.

IODSA (Institute of Directors Southern Africa (2009), "King code of governance for South Africa 2009", available at: www.Iodsa.Co.Za/?Kingiii (accessed 7 April 2016).

IODSA (Institute of Directors Southern Africa (2016). "King IV: Report on corporate governance for South Africa 2016", available at: https://c.ymcdn.com/sites/www.iodsa.co.za/resource/resmgr/king_iv/King_IV_Report/IoDSA_King_IV_Report_-_WebVe.pdf (accessed 19 July 2017).

ISACA (2012a), "COBIT 5: a business framework for the governance and management of enterprise IT", available at: www.isaca.org/cobit/pages/cobitLiteRegistrationdownload.aspx?RegID=72492e8e-70a1-4ee6-91a4-fcb5e3f37539 (accessed 11 August 2015).

ISACA (2012b), *COBIT 5: Process Reference Guide*, ISACA, Rolling Meadows, IN.

ISACA (2016), "Internal control using COBIT 5", available at: www.isaca.org/knowledge-center/research/researchdeliverables/pages/internal-control-using-cobit-5.aspx (accessed 17 March 2016).

ITIL (2011), "An introductory overview of ITIL 2011", available at: www.doc-developpement-durable.org/file/Projets-informatiques/cours-&-manuels-informatiques/ITIL/An_Introductory_Overview_of_ITIL_V3.pdf (accessed 6 August 2016).

Juiz, C. and Toomey, M. (2015), "To govern IT, or not to govern IT?", *Communications of the Acm*, Vol. 58 No. 2, pp. 58-64.

Kelly, J.E.I.I. and Hamm, S. (2013), *Smart Machines: IBM's Watson and the Era of Cognitive Computing*, Columbia University Press, New York, NY.

Kitchin, R. (2014), "The data revolution: Big data, open data, data infrastructure and their consequences", available at: http://srmo.sagepub.com.ez.sun.ac.za/view/the-data-revolution/n9.xml (accessed 22 December 2015).

Kruger, W. (2012), "Strategic business–IT alignment of application software packages: Bridging the information technology gap", *South African Computer Journal*, Vol. 49, pp. 1-11.

Kshetri, N. (2014), "Big data's impact on privacy, security and consumer welfare", *Telecommunications Policy*, Vol. 38 No. 11, pp. 1134-1145.

Noor, A.K. (2015), "Potential of cognitive computing and cognitive systems", *Open Engineering*, Vol. 5 No. 1, pp. 75-88.

Oberlin, S. (2012), "Machine learning, cognition, and big data", available at: www.ca.com/us/~/media/files/articles/ca-technology-exchange/machine-learning-cognition-and-big-data-oberlin.aspx (accessed 3 June 2015).

Raguseo, E. (2018), "Big data technologies: an empirical investigation on their adoption, benefits and risks for companies", *International Journal of Information Management*, Vol. 38 No. 1, pp. 187-195.

Rajcoomar, A. (2017), "A framework for the implementation and practice of professional bodies", Unpublished Phd dissertation, University of South Africa, Pretoria.

Ronanki, R. and Steier, D. (2014), "Cognitive analytics, tech trends 2014", available at: www2.deloitte.com/insights/us/en/focus/tech-trends/2014/2014-tech-trends-cognitive-analytics.html?id=us:el:dc:dup565:cons:tt14:awa (accessed 5 April 2015).

Rubino, M. and Vitolla, F. (2014), "Corporate governance and the information system: how a framework for IT governance supports ERM", *Corporate Governance: The International Journal of Business in Society*, Vol. 14 No. 3, pp. 320-338.

Rubino, M., Vitolla, F. and Garzoni, A. (2017), "The impact of an IT governance framework on the internal control environment", *Records Management Journal*, Vol. 27 No. 1, pp. 19-41.

Rudman, R. (2010), "Framework to identify and manage risks in web 2.0 applications", *African Journal of Business Management*, Vol. 4 No. 13, pp. 3251-3264.

Rudman, R.J. (2008), *IT Governance: A New Era*, Accountancy SA, pp. 12-14.

Sahd, L. and Rudman, R.J. (2017), "Best practices mobile technology risk assessment and control checklist", *Southern African Journal of Accountability and Auditing Research*, Vol. 19, pp. 129-145.

Sarkar, S. and Zaharchuk, D. (2015), "Your cognitive future: how next-gen computing changes the way we live and work", available at: www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&appname=CB_BU_B_CBUE_GB_TI_USEN&htmlfid=GBE03641USEN&attachment=GBE03641USEN.PDF (accessed 15 June 2015).

Sudarsan, S. (2013), "An ecosystem of innovation: creating cognitive applications powered by Watson", available at: https://developer.ibm.com/watson/wp-content/uploads/sites/19/2013/11/An+Ecosystem+Of+Innovation+-+Creating+Cognitive+Applications+PoweredByWatson.pdf (accessed 7 March 2015).

Sylvester, A., Tate, M. and Johnstone, D. (2013), "Beyond synthesis: Re-presenting heterogeneous research literature", *Behaviour and Information Technology*, Vol. 32 No. 12, pp. 1199-1215.

Tarafdar, M., Beath, C.M. and Ross, J.W. (2017), "Enterprise cognitive computing application: opportunities and challenges", *IT Professional*, Vol. 19 No. 4, pp. 36-44.

Terzi, D.S., Terzi, R. and Sagiroglu, S. (2015), "A survey on security and privacy issues in big data", Paper Presented at the 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015), 14–16 December, London, available at: http://ieeexplore.ieee.org.ez.sun.ac.za/stamp/stamp.jsp?tp=&arnumber=7412089 (accessed 1 June 2016).

Wang, Y. (2009), "On cognitive computing", *International Journal of Software Science and Computational Intelligence*, Vol. 1 No. 3, pp. 1-15.

Willis Towers Watson (2016), "TechTalk: cognitive computing", available at: www.willis.com/documents/publications/Industries/Technology_and_Telecomm/15644%20PUBLICATION_TMT%20Cognitive%20Computing.pdf (accessed 16 July 2016).

Wladawsky-Berger, I. (2013), "The era of cognitive computing", available at: https://blog.irvingwb.com/blog/2013/07/the-dawn-of-a-new-era-in-computing.html?cid=6a00d8341f443c53ef0192abaa12af970d (accessed 23 August 2015).

Zaino, J. (2014), "Bringing clarity to the topic of cognitive computing", available at: www.dataversity.net/bringing-clarity-topic-cognitive-computing/ (accessed 17 June 2015).

Zalewska, A. (2014), "Challenges of corporate governance: twenty years after Cadbury, ten years after Sarbanes-Oxley", *Journal of Empirical Finance*, Vol. 27, pp. 1-9.

Zhang, S. and Le Fever, H. (2013), "An examination of the practicability of COBIT framework and the proposal of a COBIT-BSC model", *Journal of Economics, Business and Management*, Vol. 1 No. 4, pp. 391-395.

Zhou, L., Pan, S., Wang, J. and Vasilakos, A. (2017), "Machine learning on big data: opportunities and challenges", *Neurocomputing*, Vol. 237, pp. 350-361.

Zikopoulos, P., deRoos, D., Bienko, C., Buglio, R. and Andrews, M. (2015), "Big data beyond the hype: a guide to conversations for today's data center", available at: www.ibm.com/developerworks/community/blogs/SusanVisser/entry/big_data_beyond_the_hype_a_guide_to_conversations_for_today_s_data_center?lang=en (accessed 10 July 2015).

Further reading

Chen, K., Li, X. and Wang, H. (2015), "On the model design of integrated intelligent big data analytics systems", *Industrial Management and Data Systems*, Vol. 15 No. 9, pp. 1666-1682.

Chen, C.L. and Zhang, C. (2014), "Data-intensive applications, challenges, techniques and technologies: a survey on big data", *Information Sciences*, Vol. 275, pp. 314-347.

Janssen, M., Estevez, E. and Janowski, T. (2014), "Interoperability in big, open and linked data: organizational maturity, capabilities, and data portfolios", *Computer*, Vol. 47 No. 10, pp. 44-49.

Knoblock, C.A. and Szekely, P. (2015), "Exploiting semantics for big data integration", *AI Magazine*, Vol. 36 No. 1, pp. 25-38.

Paryasto, M., Alamsyah, A. and Kuspriyanto, B.R. (2014), "Big-data security management issue", Paper Presented at the 2014 2nd International Conference on Information and Communication Technology, 28-30 May Scon, Bandung, available at: http://ieeexplore.ieee.org.ez.sun.ac.za/stamp/stamp.jsp?tp=&arnumber=6914040 (accessed 8 April 2016).

Suer, M. and Nolan, R. (2015), "Using COBIT to deliver information and data governance", available at: www.isaca.org/cobit/focus/pages/using-cobit-5-to-deliver-information-and-data-governance.aspx (accessed 6 August 2015).

Wang, Y. (2011), "Towards the synergy of cognitive informatics, neural informatics, brain informatics and cognitive computing", *International Journal of Cognitive Informatics and Natural Intelligence*, Vol. 5 No. 1, pp. 75-93.

Wigan, M.R. and Clarke, R. (2013), "Big data's unintended consequences", *Computer*, Vol. 46 No. 6, pp. 46-53.

Corresponding author
Jana van Wyk can be contacted at: janavw@sun.ac.za