A CASE FOR CURRICULUM RENEWAL: DEFICIENCIES IN THE TRAINING OF PROSPECTIVE AUDITORS IN A TECHNOLOGY ERA

R. Rudman*
e-mail: rjrudman@sun.ac.za / https://orcid.org/0000-0002-3789-2386

N. D. Sexton*
e-mail: nsexton@sun.ac.za / https://orcid.org/0000-0002-5885-0441

*School of Accountancy
Stellenbosch University
Stellenbosch, South Africa

ABSTRACT

The information revolution, where the evolution of technology has a pervasive impact on all aspects of life and business, is upon us. The private sector has embraced new technologies, presenting opportunities while also giving rise to new risks. Although slow to start, organisations (or audit clients – auditees) have started implementing specialist information technology (IT) governance frameworks to mitigate the risks attributable to IT. Just as organisations have changed, it is expected that external auditors (auditors), and their education and training, would also have adapted their audit approaches to account for the impact of evolving IT on auditees. This has not necessarily been the case. The standards do not provide the necessary detail guidance on IT required by auditors. The university curriculum as well as supplementary text have neither kept up to date with the rapid changes in technology or the changes in governance frameworks. The objective of this research was to perform a curriculum audit of the sufficiency of the auditing text (i.e. International Standards on Auditing (ISAs) and supporting guidances and textbooks as required by the competency framework) used in the audit specialisation of training prospective CAs (i.e. the curriculum relating to IT as part of the audit process) in ensuring graduates (i.e. future auditors) are relevant in an ever-evolving IT-driven environment The study found that although several areas of the audit curriculum are appropriate, there is in fact a gap within the current curriculum relating to IT internal controls and risks that exist at a technology level. The study calls for curriculum renewal within the audit specialisation, giving specific consideration to technology or operational-level controls within the framework of general and application IT internal controls taught.

Keywords: curriculum renewal, accounting education, auditing, IT governance

INTRODUCTION

Training of chartered accountants (CA) in South Africa includes tertiary education, professional examinations and practical training over seven years to achieve a core set of technical and

professional competencies as set out in the competency framework of the South African Institute of Chartered Accountants (SAICA) (SAICA 2010). These competencies aim to ensure that CAs, as professionals, remain relevant to the roles they do and will perform. As future auditors, professionals and business leaders, students need to be prepared for advances in business, how business operates and its global and local context. Digital technologies (such as the internet of things, machine learning, artificial intelligence and big data) are disrupting the ways in which businesses operate (Gartner 2015). Organisations are relying on information technology (IT) systems, with varying degrees of dependence and complexity, to record, process, store and report financial and other pertinent company information (Yang Liming Guan 2004). Linked to this disruption are changes in corporate governance, where the latest King Report on Corporate Governance (2016) (King IV) requires governing bodies of organisations to take responsibility for the strategic as well as operational implementation of IT (Institute of Directors Southern Africa (IODSA) 2016). This has caused businesses to implement risk management, governance and internal control frameworks for the implementation of advanced technologies. Audit practices globally have acknowledged that there is a growing use of IT, which influences external auditing when considering data analytics and the impact of mobile, cloud and cognitive computing on the auditor as well as the audit client (auditee) (Anderson 2017; Miles 2016; SAICA 2017). At a training level, SAICA is in the process of enhancing the competency framework (as part of the CA2025 project) (SAICA 2018) for the required set of skills required by the future CA. This may include different and more comprehensive competencies for future CAs. This process is however not yet complete.

In training future professionals, universities strive to remain aware and abreast of and improve with the world in which their graduates will function and attempt to prepare them for the future. Advances in IT and the manner in which IT is being used and controlled by businesses have raised questions about the whether the current curriculum taught at universities is comprehensive and sufficient enough to prepare them for their world of work. Specifically in South Africa, the skills accounting students learn at university are of great importance, as the sizes of audit firms and their access to specialised IT related skills and resources (where future CAs do the practical element of their professional training, known as training offices) vary significantly. The majority of audit firms are small and medium in size (Independent Regulatory Board for Auditors (IRBA) 2016) and may not have specialist IT auditors on their audit teams. This means that as the IT architecture of all their auditees is becoming more complex, they may be at a disadvantage with knowledge limited to IT risks and controls that were taught within the university curriculum. Lastly, a disconnect exists with the challenges that arise, as IT architects, leadership of organisations and auditors do not fully understand the differences

between the objectives, terminology and outputs that each uses regarding IT (Julisch et al. 2011). These differences, advances in technology and the specific South African context presented the question as to *whether the current curriculum is sufficient*? This article is structured as follows:

1. Research objectives and contributions, which set out the objective of the article and its contribution to teaching future chartered accountants.
2. Research methodology conducted in three stages: literature review and the GAP analysis, performed on the current curriculum.
3. Literature review which presents the relevant literature to the study
4. Findings which focusses the GAP analysis
5. Conclusion, which presents the impact of the results of the study and the areas where advancements in the curriculum are required in the future.

RESEARCH OBJECTIVE AND CONTRIBUTIONS

The objective of this research was to perform a curriculum audit of the sufficiency of the auditing text (i.e. ISAs and supporting guidances and textbooks as required by the competency framework) used in the audit specialisation of training prospective CAs (i.e. the curriculum relating to IT as part of the audit process) in ensuring graduates (i.e. future auditors) are relevant in an ever-evolving IT-driven environment.

This research is important, as it adds to the discussions currently taking place in the profession on the impact of technology on auditors. It highlights shortcomings in the material used both to train future CAs and in practice (particularly in small and medium-sized firms). Further, it creates a case for academia to reconsider the manner in which technology and its impact on the audit are taught at universities. Lastly, it shows that within higher education in South Africa, when training professionals, faculty need to remain abreast of the changing contexts. By embracing elements of rapid curriculum renewal, graduates can continue to meet industry needs and remain relevant and do not have to wait for their governing body (such as SAICA) to react.

RESEARCH METHODOLOGY

In positioning the research methodology, the research focused on *Element 3: Curriculum audit* of the rapid curriculum renewal framework (as depicted in Figure 1), proposed by Desha, Hargroves and Smith (2009). In order to achieve the objective of this study, the qualitative research design included a literature review followed by a detailed gap analysis to identify

deficiencies in the auditing text compared to a comprehensive IT governance framework that can be applied in a complex IT environment.

Step 1: Literature review

A systematic review of the existing literature, employing a concept-centred approach, as suggested by Webster and Watson (2002), using four of the five stages suggested by Sylvester, Tate and Johnstone (2013), was conducted to determine how private organisations address IT risk management and IT governance and other topics related to the research objective. Initially, a broad selection of literature was reviewed and the selection was refined using the University of Arizona's search strategy builder tool (University of Arizona 2016). Search terms included SAICA competency framework; How we teach CAs; External audit; Risk identification and response; Impact of IT on financial reporting and audit; Business and IT governance; IT internal control framework; IT governance frameworks; and General and application IT controls. The application of the concept centric four-stage process in conducting the systematic review provided scientific rigour to the study. The review was performed to confirm that the use of IT governance frameworks by the private sector has evolved with IT and that there is a need for the auditing profession and curriculum to follow suit.

Step 2: Gap analysis

In order to identify whether there are areas in the current auditing text and curriculum that need to be amended in terms of the impact of evolving IT on external audit, a gap analysis was performed, comparing the detailed general and application IT control areas in the integrated framework (Goosen and Rudman 2013) to those in the auditing text. The detailed mappings are available on request. The gap analysis identified deficiencies in the core concepts/areas.

LITERATURE REVIEW

The aim of the literature review is to position the research within accepted curriculum renewal processes. It explains the scope of the current curriculum by considering the broad requirements of the SAICA prescribed competency framework (2010) (*i.e. What we teach*) which is detailed in the International Standards on Auditing (*i.e. What auditors should do* – the basis for the curriculum). Lastly, it considers what business does regarding IT governance and frameworks making the case for curriculum renewal.

Time lag dilemma

When training professionals in any area of specialisation, the regulatory requirements and

industry expectations, as well as changing contexts, drive what universities teach; however, the process of making enhancements to the curriculum can be reactive rather than proactive. The timeframe and red tape to amend competencies and degree outcomes and upskill lecturing staff (faculty) also delay change. This presents itself in a concept referred to as the *time lag dilemma* (Desha et al. 2009). Desha, Hargroves and Smith (2009) recommend that faculty embrace a more rapid approach to curriculum renewal, where a continual process of awareness and understanding of the environment in which students will be employed drives enhancements of graduate attributes and competencies, leading to curriculum audits and course renewal in consultation with industry, and ultimately campus integration of the new curriculim. Figure 1 presents an overview of the rapid curriculum renewal process proposed by Desha, Hargroves and Smith (2009).

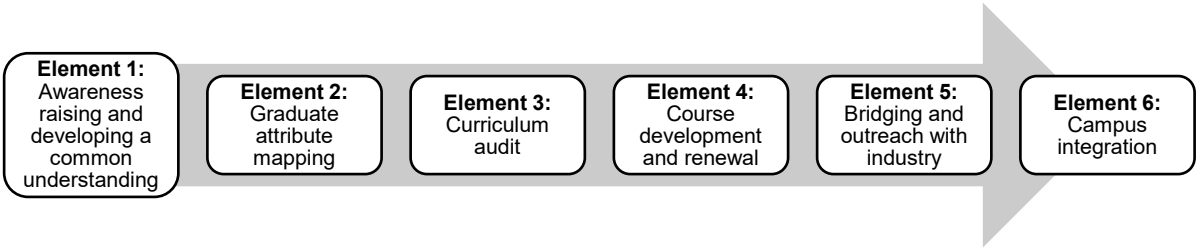

Figure 1: Elements for rapid curriculum renewal (Desha et al. 2009)

In response to the risks presented by the time lag dilemma and the recommendations for rapid curriculum renewal by Desha, Hargroves and Smith (2009), the lecturers at a SAICA-accredited university considered the influence these risks and recommendations may have on what is being taught in relation to IT in the subject area of auditing.

Changes in IT driving rapid curriculum renewal

Advances in technologies and digitisation are taking place at an exponential rate, with many arguing that the world is entering a Fourth Industrial Revolution (IODSA 2016). The evolution of IT can be categorised into various stages: *Data processing*, where functionality of applications was initially driven by singular activities or tasks that were not integrated; thereafter *batch processing*, which updated separate databases for each functional area within the organisation. *Shared databases* emerged with a clear separation between databases and applications. Functionality was business process-driven rather than task-driven; shared applications and shared databases introduced the need for database management systems. Organisations used shared databases for applications across functional areas within *networks*. Networks extended across geographic locations, connecting all functional areas of the business; in some cases, communicating and linking with external organisations, whether by means of

internet connection or extended or virtual enterprise. From an audit perspective, the infrastructure was relatively standard and function-specific. The move to a mobile environment was among the first significant departures to technology where the demands for instant, reliable, anywhere anytime information and functionality on various platforms were the key drivers (Gartner 2015). The Gartner Hype Cycle for emerging technologies places emphasis on moving towards digital business and the convergence of people, business and things, where the lines between the physical and digital world are blurred (Gartner 2015; Luchetti 2015). An emerging technology gaining traction is *autonomous computing*, where IT is able to provide human-like or human-replacing capabilities to an organisation (Gartner 2015; Luchetti 2015). The evolution in IT impacted users, businesses and the governance thereof. Organisations responded by changing business models and governance frameworks, embracing the changes in technology together with the opportunities and risks that IT presents. As technology has progressed through the stages of the IT evolution, so too has the manner in which organisations rely on IT systems, with varying degrees of dependence and complexity to record, process, store and report financial and other pertinent company information. The leadership of organisations and legislators have acknowledged this by building IT into overall corporate governance structures.

Within the context of training CAs as future auditors, many universities consider IT as a support subject and not a core skill of a CA. The curriculum currently taught at institutions of higher learning accredited to train CAs does not include more complex IT governance frameworks such as COBIT 5 (Control Objectives for Information Technology), International Organisation for Standardisation (ISO) or Information Technology Infrastructure Library (ITIL) or their application to advance in technology (Stellenbosch University 2016). As these frameworks are complex and onerous, in order to obtain the necessary understanding of these frameworks, an auditor is expected to enrol in further studies. However, perhaps with the changes in industry expectations, curriculum renewal for these new complex IT environments is required. As such, a clear and detailed understanding of the current curriculum initiates the assessment of the appropriateness thereof.

Competency framework: What we teach

The basis for what is taught in the university curriculum in training CAs is the competency framework (SAICA 2010), which outlines the key professional and technical competencies required by a future CA. Within the competency framework there are varying levels of proficiency that a future CA is required to demonstrate. These proficiency levels (referred to as "competency levels") range between "awareness", "basic knowledge at a contextual level",

"daily use and application" and "advanced application". The level of proficiency is linked to the competency. As the focus of this study was on the impact of evolving IT on the auditing curriculum, all the competencies relating to IT are summarised into broad categories (linked to the level of proficiency required) in Table 1.

Table 1: IT competencies and required competency level

Broad categories of competency	Proficiency/Competency level
Management and decision making	Awareness
Governance model (including the IT strategy)	Basic knowledge, broad contextual level
Internal control	Advanced application
Audit procedures	Advanced application
Daily IT functionality	Daily use and application

With the focus on what is taught (relating to IT in auditing), a more in-depth investigation into the broad categories of "internal control" and "audit procedures" is discussed in the sections to follow. The competency framework requires an "advanced application" level of proficiency for these two competencies. These competencies relating to IT and internal control can be broken into (i) using a framework for control evaluation, (ii) understanding internal control systems (ICS), (iii) testing the design and implementation of internal control systems, (iv) assessing weaknesses in internal controls, (v) considering IT security and (vi) IT systems and processing internal controls. All these competencies (relating to IT) as part of the audit specialisation are taught based on the International Standards on Auditing (ISAs). This requires a discussion of the detail contained in the ISAs relating to IT, specifically relating to internal controls, which is included in the following section.

International Standards on Auditing: What auditors should do – the basis for the audit curriculum

The ISAs outline the audit process that an external auditor must follow to effectively give an opinion on the financial position and performance of an organisation (IAASB 2015b, para. 3). The ISAs guide the auditor through the audit process to enable him/her to express an opinion on the financial statements (i.e. historical financial information). The audit process includes pre-engagement activities, planning activities, execution of audit procedures and reporting. The key considerations within the "advanced application" proficiency required to be achieved within the internal controls competency are presented in Table 2. Table 2 presents an overview of the impact of IT in relation to internal controls in the planning and execution phases of the audit. A summary outlining the impact of IT on each of the phases of the audit process is available on request.

Table 2: ISAs considerations relating the IT controls within the planning and execution phases of the audit process

Phase of the audit process	Key considerations per the ISAs
1. Planning activities	
1.1 Understanding the organisation and its environment	Impact of IT on the auditee in the auditee's internal (e.g. strategies, business structure, processes) and external (e.g. industry, legal environment) context
1.2 Understanding the organisation's internal control	Use of IT within the client's financial reporting processes General and application IT internal controls implemented
1.3 Assessing audit risk and developing an audit approach	Decision on which IT internal controls are relevant to the audit and should be tested for operating effectiveness based on the control objectives per the ISAs (completeness, validity, accuracy and data integrity)
2. Execution (performing the planned audit procedures)	Testing the operating effectiveness of the IT internal controls that are relevant to the audit and the impact on the final assessment of control risk

Within the planning activity *Understanding the organisation and its environment* (Table 2), the ISAs guidance on the impact of IT together with the risks these impacts present to the audit is comprehensive and can be applied without additional guidance no matter the size of the auditee. Areas for consideration include the nature of the industry and the client's objectives and strategies, financing structure and accounting framework, the regulatory environment and governance structures (IAASB 2015a) that are documented. However, when delving into the detail of *Understanding the organisation's internal control* (Table 2), the ISAs give limited detail of the considerations and actions the auditor must take regarding how the client captures, records, stores and reports financial information, together with the related internal controls. The auditor's considerations are summarised as follows:

- The auditor needs to obtain an understanding of internal controls relevant to the audit, which include both the manual and the automated procedures that are used to initiate, record, process and report transactions that are relevant to the performance of the audit (IAASB 2015a, 12, 18, A60–A61).
- The use of IT presents several opportunities to strengthen internal control, for example where large volumes of transactions are processed or ensuring segregation of duties where clear security controls are implemented in applications, databases and operating systems (IAASB 2015a, A62).
- The use of IT exposes the organisation to additional risks that need to be addressed in the governance of IT by management as well as by the auditor (IAASB 2015a, A63).
- The auditor is to consider certain situations where reviewing manual internal controls may be less suitable than reviewing the IT controls, such as when high-volume recurring

transactions are being processed (IAASB 2015a, A65).

- The auditor is required to understand those control activities that the organisation uses to respond to its risks arising from IT (IAASB 2015a, 21). These control activities are considered effective when they maintain the integrity of information and the security of data, achieving the specific control objectives of completeness, validity, accuracy and data integrity. The explanatory material for this paragraph expands these control activities to include general as well as application IT controls (IAASB 2015a, A103–105). This is supported by the guide for using the ISAs in the audits of small and medium-sized firms, which also provides broad guidance, stating the requirement to use professional judgement when considering the general and application IT controls (International Federation of Accounts (IFAC) 2011). However, no further guidance is given as to what control areas general IT controls and application IT controls comprise of, or to a general approach that the auditor can apply in understanding them.

The information gathered in understanding the organisation and its internal control directly influences the assessment of audit risk (the risk that the auditor expresses the incorrect opinion) and the audit procedures performed to gather audit evidence. The auditor requires additional guidance when assessing the impact of IT on a client in the planning phase of the audit process, specifically when understanding the organisation and its general and application IT internal controls. This guidance comes from the teaching material that is included in the university curriculum for future auditors.

Prescribed text: What auditors know – the detail of the audit curriculum

The guidance in the ISAs is broad, written in general terms, to allow auditors to tailor the content to a specific client using their professional scepticism and judgement. In the era of evolving IT, the auditor requires supplementary guidance in terms of detailed control areas within the general and application IT controls and which of these controls are relevant to the audit. Currently, the tertiary auditing curriculum expands these principles based on auditing textbooks that explain these principles. Audit textbooks, including those by Von Wielligh et al. (2014); Marx, Van der Watt and Bourne (2014); Boynton and Raymond (2006); and Arens and Loebbecke (1980), have over time categorised the general and application IT controls into control areas. They further link the control areas to the control objectives they may achieve to assist the auditor in identifying IT controls that may be relevant to the audit (Singleton 2010a; Singleton 2010b). A review of these textbooks showed that they tend to focus on generic technology and hardly address modern technology referred to in section

1. Introduction. The control areas presented by these authors overlap and address similar focus areas despite the time lapse between them. As the detailed control areas highlighted in *Auditing Fundamentals in a South African Context* by Von Wielligh et al. (2014) addressed all the areas of overlap between the other supporting texts, their book was selected to form the basis to understand the control areas within general and application IT controls, the detail of which was used for the curriculum audit.

In considering whether the curriculum is appropriate, it is necessary to investigate how IT has changed how auditees responded to evolving IT and govern IT from a strategic to an operational level to identify and manage their risks and implement their strategies.

IT governance frameworks: What business does

Advances in IT have allowed IT governance to gain prominence within corporate governance structures. King III Report on Governance for South Africa (2009) was the first South African governance publication that acknowledged the pervasive impact that IT has had on every area of the organisation (IODSA 2009). King III defined IT governance as a framework that supports effective and efficient management of IT resources to facilitate the achievement of the company's strategic objectives (IODSA 2009). For boards of directors to fulfil their corporate and IT governance responsibilities, they can utilise internal control frameworks and methodologies that relate to the organisation as a whole, commencing with strategic IT governance and then filtering down to include operational elements of the ever-evolving IT system. King IV (2016) expanded the responsibilities of the governing body (as opposed to the board of directors) of an organisation regarding IT governance to include integrating people, technologies, information and processes in the digital business value chain and cyber security risks to keep up with the evolution of IT (IODSA 2016). In order to address these risks, many organisations rely on IT governance frameworks, such as COBIT, ISO and ITIL (Information Systems Audit and Control Association (ISACA) and Protiviti 2015). Each IT governance framework addresses a different purpose.[1] When utilised individually, there is a risk that the IT systems and related internal controls that are implemented are not in line with the organisation's unique strategic objectives and strategies (Goosen and Rudman 2013). To address this, Goosen and Rudman (2013) created a framework that integrated the control areas in COBIT with the control areas in ITIL and ISO 27001 and ISO 27002 to assist management in achieving alignment and eliminating areas of overlap between the four frameworks (referred to as an integrated framework). These control areas were used in the curriculum audit performed as part of the study.

Need for curriculum change

The ISAs follow a principle-based approach to allow the auditor flexibility in customising the audit process to the specific requirement of the auditee; however, these have not been modernised for evolving technologies and frameworks (Hoogwerf 2018; IRBA 2018). It is up to the auditor, and his/her knowledge (developed while at university) of detailed systems and internal control techniques, to identify risks and design tests of controls. The International Accounting and Assurance Board (IAASB) is in the process of reviewing and enhancing elements of the ISAs for evolving IT (Hoogwerf 2018). While this process is still incomplete, it implies that there have also not been significant changes to the way universities teach auditing to account for evolving IT and the impact on internal controls. Therefore, as what universities currently teach is based on the ISAs together with the prescribed text (hereafter referred to as the "auditing text"), it is also necessary to consider how the curriculum must change to equip graduates for their future audit roles in the IT era.

FINDINGS

Overview

Using the core concepts highlighted in the research methodology and literature review, a high-level comparison between the curriculum taught (from the auditing text) and the integrated IT governance framework that businesses are using (and which has evolved with IT to address the risks) was done. This comparison is summarised in Figure 2, where it shows the shortcomings (gap) in the current curriculum (Gap: broad), and provides the detail aspects that need to be considered at a technology level to address the shortcomings (Gap: detail), which address the fact that the ISAs have not evolved with IT.

To structure the mapping in the gap analysis into comparable control areas, the detailed analysis was performed within the control areas at a general and then application IT control level.

General IT controls

General IT controls are those policies and procedures that relate to all the applications used by the IT systems and support the effective functioning of all applications (Julisch et al. 2011).

Within the auditing text, these include oversight controls and then key areas of the IT environment. The detailed general IT control areas are organisational controls and personnel practices; system development and acquisition control; program change controls; access controls; business continuity controls; operating controls; and system maintenance controls

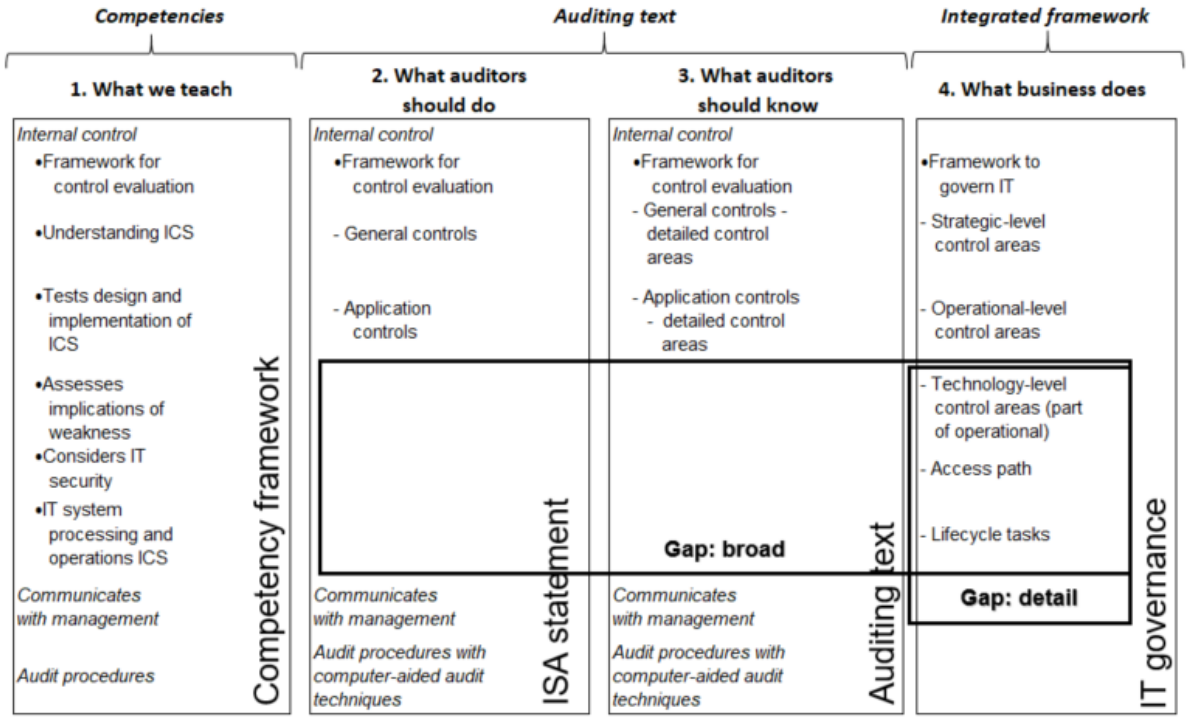

Figure 2: Overview of the gap analysis performed

(Arens and Loebbecke 1980; Boynton and Raymond 2006; Gheorghe 2010; Huang et al. 2011; IAASB 2015a, A103–A105; Jackson and Stent 2016; Marx et al. 2014; Rubino and Vitolla 2014; Sayana 2002; Von Wielligh et al. 2014; Yang 2004). These control areas have been broken down further in Table 3.

The integrated framework does not refer to general IT controls; however, those control areas included at a strategic level, address similar control areas included in the general IT controls. The strategic-level detailed IT control areas of the integrated framework (Goosen and Rudman 2013) focus on aligning IT resources, systems and operations with the business strategies. The detailed control areas are determining business policies and strategies; implementing business IT alignment procedures; service-level management; implementing accurate IT resource management; procurement management; access controls/security management; acquisition and development of an information system and maintenance controls; project management; implementation of an information management system; financial management; risk management processes; change, release and deployment management; human resource security; problem management; business continuity management; compliance requirements; and configuration management through access paths (Goosen and Rudman 2013).

The gap analysis at the general IT control level in the form of a mapping between the

auditing text and the integrated framework is contained Table 3.

Table 3: General IT control mapping between the auditing text and the strategic control areas in the integrated framework

Auditing text (the current curriculum)			**Integrated framework**
General IT controls per ISA315	**General IT controls (Von Wielligh et al. 2014)**	**General IT control areas per auditing fundamentals (Von Wielligh et al. 2014)**	**Strategic Control areas contained in the integrated framework (Goosen and Rudman 2013)**
Oversight controls	Organisational controls and personnel practices	Responsibility levels and reporting lines	Determining business policies and strategies
			Implementing business IT alignment strategies
			Service-level management procedures
			Implementing accurate IT resource management
			Financial management
			Human resource security
		Segregation of duties	Human resource security
		Staff practices	Human resource security
		Staff supervision and review	Human resource security
Data centre and network operations	Operating controls	Scheduling and production runs and processing	Access path Configuration controls – operate
		Operating activities and use of assets	Access path Configuration controls – operate
		Library controls	Business continuity management
		Business continuity controls	Problem management Business continuity management
System software acquisition, change and maintenance Application system acquisition, development and maintenance Program change	System development and acquisition controls Program change controls System maintenance	Request and needs assessment	Procurement management
			Change, release and deployment management
		Project management	Project management
		Planning and design Development and testing Implementation Post-implementation review	Change, release and deployment management
			Acquisition and development of an information system and maintenance controls
			Implementation of an information management system
			Configuration management
			Compliance requirements
Access security	Access controls	Security and management policy	Access controls / security management
			Risk management processes
		Physical access controls: facilities, system, data	Access controls / security management
		Logical access controls	Access controls / security management
Other*	Business continuity controls	Operating environment: physical dangers, non-physical dangers	Business continuity management
		Repair and disaster recovery: back-ups, disaster recovery plan	Problem management
* These control areas are not specifically mentioned in ISA 315; however, as the supporting guidance suggests, no IT system as a whole will function effectively without business continuity.			

The mapping in Table 3 shows that all of the detailed control areas in the auditing text align to the integrated framework, which confirms the appropriateness of the current curriculum taught regarding general IT controls.

Application IT controls

Application IT controls are those controls (manual or automated) that usually operate at a business process level that apply to the processing of transactions by individual applications (IAASB 2015a, A103–A105). The auditing text highlights that application IT controls are dependent upon the operating effectiveness of the general IT controls and are only relevant to the external audit when the general IT controls are operating effectively. Presently, the auditor focuses on the application IT controls that relate to the financial reporting systems (Center for Audit Quality 2014). Application IT controls are four categories of controls relating to functions within individual applications: input controls, processing controls, output controls and masterfile change controls (Arens and Loebbecke 1980; Boynton and Raymond 2006; Chang et al. 2014; Flowerday and Von Solms 2005; Marx et al. 2014; Rubino and Vitolla 2014; Sayana 2002; Von Wielligh et al. 2014). The integrated framework does not refer to application IT controls; however, Goosen and Rudman (2013) argue that should all of the strategic-level control areas be addressed, governing bodies will have achieved IT governance at a strategic level, but not at an operational or technology level in the actual hardware and software components that are included within the IT system. To do so, Goosen and Rudman (2013) propose a process to identify the access paths in an IT system, which then reaches the application IT controls within the auditing text. A user performs computerised activities by activating an access path. An access path is formed by the various IT components that need to be activated in order for a typical user (business, IT or otherwise) request (functionality, data or otherwise) to be executed, to access computer-controlled resources (Boshoff 1990) and consider the individual components therein and then implementing configuration controls for each of the components identified. Configuration controls (also referred to as IT lifecycle tasks) include the functions of each component of the access path (Goosen and Rudman 2013) and can be compared to the application IT controls in the auditing text. The IT lifecycle tasks are computer hardware build; computer software build; setup or installation of programs; configuration of computer software; operating a computer; and computer maintenance. Using the components of the access path and the supporting configuration controls will enable management to implement IT governance at an operational or technology level (Goosen and Rudman 2013) and address each system risk. This was a departure from conventional thinking at the time, which is why the curriculum is also being questioned now. The gap analysis in the

form of a mapping between the auditing text and the integrated framework at an application IT control level is presented in Table 4.

Table 4: Application IT control mapping between the auditing text and the operational control areas in the integrated framework

Auditing text (the current curriculum)		**Integrated framework**
Application IT controls per ISA315	**Application IT controls (Von Wielligh et al. 2014)**	**Operational control areas contained in the integrated framework (Goosen and Rudman 2013)**
Application IT controls to be reviewed for individual applications identified by the auditor to address the potential risk of significant misstatement*	Input controls	Access path – only the application itself Configuration controls – configure, operate and maintain
	Processing controls	Access path – only the application itself Configuration controls – configure, operate and maintain
	Output controls	Access path – only the application itself Configuration controls – configure, operate and maintain
	Masterfile amendments controls	Access path – only the masterfile itself Configuration controls – configure, operate and maintain
*The question that arises is whether the applications selected for the review of the application IT controls relating to one application, generally in the financial application, in isolation will address all the IT control risks that arise from the each of the technological components of the access path(s) to that financial application.		

The mapping in Table 4 shows that although each of the categories of application controls are accounted for in the auditing text, this is in general limited to individual applications that have a direct impact on financial reporting, which confirms what is taking place in practice (Center for Audit Quality 2015). In terms of the ISAs, auditors assess the input, processing, output and masterfile amendment controls. When these controls outlined in the ISAs are compared to the operational- or technology-level controls of the integrated framework Goosen and Rudman (2013) (refer to Table 4), only certain elements of the access path are considered and further, only the "operate" configuration control is considered. When this comparison is broadened to the general IT controls assessment, the "configure, operate and maintain" (refer to Table 4) controls for all applications can be included. However, there is a risk that other hardware and software within the access path to the specific accounting application and its underlying data can expose the organisation to additional risks of material misstatement that are relevant to the audit and the curriculum. With the migration in business to accounting processing and financial reporting applications that are cloud-based and accessed from traditional as well as mobile IT platforms (Anderson 2017; Miles 2016), the scope of the elements of the access path together with their lifecycle tasks included in application IT control assessment subsequent to the general IT control assessment is not broad enough. The evolution of IT and its pervasiveness have heightened this risk and the cyber security risk within the entire IT system presents a very real

threat for organisations today. This supports the need to increase the auditor's scope over the lifecycle tasks of more components within the IT system after the general IT controls assessment (Center for Audit Quality 2014; 2017; IODSA 2016). This shows that the current curriculum needs to be broadened to include technology-level control areas.

CONCLUSION

IT influences all organisations, irrespective of size, and graduates who aspire to be CAs and future auditors need to be equipped to function in a world driven by the IT evolution. This means they need to be able to respond to the impact of the IT evolution when preforming audits, either by taking the auditee's technology into account or by using IT to gather data. This study questioned whether the current curriculum relating to the impact of evolving IT on the audit specialisation taught at university equips graduates with the skills required in industry. The study was positioned within the framework of the principles of rapid curriculum renewal (Desha et al. 2009) when training professionals. The findings presented the auditing text taught at university from the competency framework to the broad guidance available to the auditor in the ISAs when assessing the impact of IT on the auditee throughout the audit process. The ISAs, which are broad, are supported by the prescribed text that defines the control areas of the control environment, which are in the form of general and application IT controls. In order to execute the curriculum audit, these control areas from the auditing text were compared with an integrated framework, which can be used by auditees today to account for evolving IT risks. This was based on the premise that if organisations can use a comprehensive IT governance framework to address all the IT risks they are exposed to and assist management to achieve the control objectives, it should also form the basis for the auditor when identifying IT controls relevant to the audit. When the comparison was performed, a mismatch was identified at a technology level. Certain IT-related risks that present themselves because of the various IT hardware and software elements of the access path, subsequent to initial configuration, are not considered within the application IT control areas. This is due to the focus by auditors and by default the auditing text on the financial application. At a minimum, academia must incorporate an approach to design internal controls for an advanced technology system that extends past the financial system, similar to the concepts underlying the access path recommended by Goosen and Rudman (2013). It is recommended firstly that auditors who solely apply the ISAs and supported text extend their assessment of IT controls to include the components of the access path together with their lifecycle tasks, after the initial "build, setup and configure" that would have been included in the general IT controls. Secondly, it is recommended that the curriculum be updated. Historically, accounting academia have not taken the lead in this process, but the

time lag dilemma creates a risk for the auditing profession. Academia need to lead the way with new teaching tools and material and further consideration should be given to the required competencies that should be developed in graduates to address the gap that exists between the:

- current core content (auditing text) taught to trainees;
- competencies (competency framework) prescribed by the professional body of accountants; and
- detail contained in frameworks (integrated framework) used by auditees.

The findings of this research have a broader reach across higher education in South Africa, where several professions have an element of their training that is concluded at university. The professions and academia, where professional bodies set curriculum, cannot rely on professional bodies alone before they react. The industries in which professionals will function will remain abreast of advancements, as auditees have remained abreast of technological developments. Academia should remain abreast of advances in industry, continue to question the *status quo* and respond with rapid curriculum redesign and renewal in anticipation of changes in professional spheres in which graduates will find themselves.

An area for future research is a focus on the latter stages of rapid curriculum renewal in the form of course development and renewal, with a focus on which additional control areas and/or frameworks need to be included in the curriculum. The competency of faculty to effectively teach the new curriculum could also be investigated.

NOTE

1. COBIT addresses the IT system in its entirety, from strategic alignment, daily operations and IT system development to service delivery and support (ISACA 2014).
   ITIL addresses areas including service strategy, design, transition, operations and continual improvement (Goosen and Rudman 2013; Sanker 2013).
   The ISOs, specifically ISO 27001 and ISO 27002, address risk management policies and preventative internal controls to ensure security over the entire management information system (Goosen and Rudman 2013).

REFERENCES

Anderson, A. 2017. “4 Keys to the future of audit.” Thompson Reuters Checkpoint. https://tax.thomsonreuters.com/wp-content/private/pdf/checkpoint/whitepapers/Checkpoint-Al-Anderson-Whitepaper.pdf (Accessed 15 April 2019).

Arens, A. A. and J. K. Loebbecke. 1980. *Auditing: An integrated approach.* 2nd Edition. Englewood Cliffs: Prentice-Hall.

Boshoff, W. H. 1990. A path context model for computer security phenomena in potentially non-secure environments. PhD diss., University of Johannesburg.

Boynton, W. C. and N. J. Raymond. 2006. *Modern auditing: Assurance services, and the integrity of financial reporting.* 8th Edition. New York: Wiley.

Center for Audit Quality. 2014. CAQ member alert: Cybersecurity and the external audit. 2014(3) Alert. http://www.aicpa.org/interestareas/centerforauditquality/newsandpublications/caqalerts/2014/downloadabledocuments/caqalert_2014_03.pdf (Accessed 4 March 2016).

Center for Audit Quality. 2015. Selecting audit considerations for the 2015 audit cycle. 2015 Alert. http://www.thecaq.org/docs/default-source/alerts/select-auditing-considerations-for-the-2015-audit-cycle.pdf?sfvrsn=2 (Accessed 4 March 2016).

Center for Audit Quality. 2017. Cybersecurity: How CPAs and their firms are addressing a dynamic and complex risk. Cybersecurity factsheet. http://www.thecaq.org/cybersecurity-how-cpas-are-addressing-dynamic-and-complex-risk (Accessed 11 May 2017).

Chang, S.-I., D. C. Yen, I.-C. Chang and D. Jan. 2014. Internal control framework for a compliant ERP system. *Information & Management* 51(2): 187–205.

Desha, C. J., K. Hargroves and M. H. Smith. 2009. Addressing the time lag dilemma in curriculum renewal towards engineering education for sustainable development. *International Journal of Sustainability in Higher Education* 10(2): 184–99. https://doi.org/10.1108/14676370910949356

Flowerday, S. and R. von Solms. 2005. Real-time information integrity=System integrity+data integrity+continuous assurances. *Computers & Security* 24(8): 604–613.

Gartner. 2015. Hype cycle for emerging technologies identifies the computing innovations that organizations should monitor. http://www.gartner.com/newsroom/id/3114217 (Accessed 20 June 2016).

Gheorghe, M. 2010. Audit methodology for IT governance. *Informatica Economică* 14(1): 32–42.

Goosen, R. and R. Rudman. 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 & Economics Research Journal* 12(7): 835–854.

Hoogwerf, H. B. 2018. Feedback on exploring the growing use of technology in the audit. *Accountancy SA* April: 56–59.

Huang, S. M., W. H. Hung, D. C. Yen, I. C. Chang and D. Jiang. 2011. Building the evaluation model of the IT general control for CPAs under enterprise risk management. *Decision Support Systems* 50(4): 692–701.

IFAC *see* International Federation of Accountants.

International Federation of Accountants. 2011. Guide to using ISAs in the audits of small- and medium-sized entities. Volume 2: Practical guidance. 3rd Edition. https://www.ifac.org/publications-resources/guide-using-international-standards-auditing-audits-small-and-medium-sized-18 (Accessed 15 May 2019).

IODSA *see* Institute of Directors Southern Africa.

Institute of Directors Southern Africa. 2009. King Code of Governance for South Africa. http://www.ngopulse.org/sites/default/files/king_code_of_governance_for_sa_2009_updated_june_2012.pdf (Accessed 15 May 2019).

Institute of Directors Southern Africa. 2016. King IV Report on Corporate Governance for South Africa. https://cdn.ymaws.com/www.iodsa.co.za/resource/collection/684B68A7-B768-465C-8214-E3A007F15A5A/IoDSA_King_IV_Report_-_WebVersion.pdf (Accessed 15 May 2019).

IRBA *see* Independent Regulatory Board for Auditors.

Independent Regulatory Board for Auditors. 2016. Annual Report 2015/2016. https://www.irba.co.za/upload/ANNUAL%20REPORT%202016%20final.pdf (Accessed 15 April 2019).

Independent Regulatory Board for Auditors. 2018. Exposure draft: Proposed international standard on auditing 315 (Revised): Identifying and assessing the risks of material misstatement. *Communiques* 26, 25 July 2018. https://www.irba.co.za/upload/report_files/26.-ED-ISA-315_Revised.docx (Accessed 4 September 2018).

ISACA *see* Information Systems Audit and Control Association.

Information Systems Audit and Control Association. 2014. COBIT 5 Process Reference Model – Processes for Governance of Enterprise IT. http://www.isaca.org/COBIT/Documents/COBIT-5-Enabling-Processes-Laminate_res_Eng_0812.pdf (Accessed 15 October 2015).

Information Systems Audit and Control Association and Protiviti. 2015. A global look at IT audit best practices: Assessing the international leaders in an annual ISACA/Protiviti Survey. http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/a-global-look-at-it-audit-best-practices.aspx (Accessed 4 March 2016).

Jackson, R. D. C. and W. J. Stent. 2016. *Auditing notes for South African students.* 10th Edition. Southern Africa: LexisNexis.

Julisch, K., C. Suter, T. Woitalla and O. Zimmermann. 2011. Compliance by design: Bridging the chasm between auditors and IT architects. *Computers and Security* 30(6/7): 410–426.

Luchetti, J. P. 2015. Why Gartner's hype cycle matters to companies and developers. DeveloperTech.com. http://www.developer-tech.com/news/2015/aug/20/why-gartners-hype-cycle-matters-companies-and-developers/ (Accessed 20 June 2016).

Marx, B., A. van der Watt and P. Bourne. 2014. *Dynamic auditing.* 11th Edition. Durban: LexisNexis.

Miles, D. 2016. 5 Ways technology is transforming accounting. rogercpareview.com. https://www.rogercpareview.com/blog/5-ways-technology-transforming-accounting (Accessed 24 July 2017).

Rubino, M. and F. Vitolla. 2014. Internal control over financial reporting: Opportunities using the COBIT Framework. *Managerial Auditing Journal* 29(8): 736–771.

SAICA *see* South African Institute of Chartered Accountants.

South African Institute of Chartered Accountants. 2010. C*ompetency framework: Competencies of a Chartered Accountant (SA) at entry-point of the profession.* Johannesburg.

South African Institute of Chartered Accountants. 2017. SAICA Comment letter on the IAASB's request for input: Exploring the growing use of technology in the audit, with a focus on data analytics. https://www.saica.co.za/Portals/0/Technical/assurance/Data_Analytics.pdf (Accessed 16 May 2017).

South African Institute of Chartered Accountants. 2018. The future CA 2025. https://www.saica.co.za/Portals/0/documents/SAICA_CAW_Future_CA_2025_Layout_v4.pdf (Accessed 15 April 2019).

Sanker, G. 2013. What is ITIL: A simple explanation. http://itsmtransition.com/2013/05/what-is-itil-a-simple-explanation (Accessed 1 June 2016).

Sayana, S. A. 2002. Auditing General and application controls. *ISACA Journal* 5: 1–3. http://www.isaca.org/Journal/archives/2002/Volume-5/Pages/Auditing-General-and-Application-Controls.aspx (Accessed 3 September 2015).

Singleton, T. 2010a. The minimum IT controls to assess in a financial audit (Part I). *ISACA Journal* 1: 1–3.

Singleton, T. 2010b. The minimum IT controls to assess in a financial audit (Part II). *ISACA Journal* 2: 1–5.

Stellenbosch University. 2016. Unpublished Auditing undergraduate and Honours curriculum. Stellenbosch.

Sylvester, A., M. Tate and D. Johnstone. 2013. Beyond synthesis: Re-presenting heterogeneous research literature. *Behaviour & Information Technology* 32(12): 1199–1215.

University of Arizona. 2016. Search strategy builder. //www.library.arizona.edu/help/tutorials/searchBuilder.html (Accessed 18 June 2016).

Von Wielligh, P., P. Prinsloo, G. Penning, R. Butler, D. Nathan (Josset), R. Kunz, V. Motholo, G. O'Reilly, R. Rudman and H. Scholtz. 2014. *Auditing fundamentals in a South African context.* Cape Town: Oxford University Press.

Webster, J. and R. T. Watson. 2002. Analysing the past to prepare for the future: Writing a literature review. *MIS Quarterly* 26(2): xiii–xxiii.

Yang Liming Guan, D. C. 2004. The evolution of IT auditing and internal control standards in financial statement audits: The case of the united states. *Managerial Auditing Journal* 19(4): 544–555.

International Standards on Auditing

IAASB *see* International Auditing and Assurance Standards Board.

International Auditing and Assurance Standards Board. 2015a. Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and its Environment. ISA315 (Revised), Effective December 15, 2013. http://www.irba.co.za/upload/IAASB-2015-Handbook-Volume-1_0.pdf (Accessed 15 April 2019).

International Auditing and Assurance Standards Board. 2015b. Overall objectives of the independent auditor and the conduct of an audit in accordance with international standards on auditing. ISA200, Effective December 15, 2009. http://www.irba.co.za/upload/IAASB-2015-Handbook-Volume-1_0.pdf (Accessed 15 April 2019).