

https://dspace.org/

Implementation of Online Assessments in Tertiary Institutions in South Africa

Rooi, Shellaine

2018
https://hdl.handle.net/10539/31562

Downloaded from a DSpace repository. https://dspace.org/

Implementation of Online Assessments in Tertiary Institutions in South Africa

Shellaine Rooi

1532631

A research article submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Business Administration

Johannesburg, 2018

Protocol number: (WBS/BA1532631/137)

DECLARATION

I, Shellaine Rooi, declare that this research article is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration in the Graduate School of Business Administration, University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

SHELLAINE ROOI

Signed at ……

On the …….. day of …… 2018.

DEDICATION

Firstly all the praise and gratitude goes to God the Almighty, for the wisdom, grace and strength to be able to complete this research.

To my husband Jacob and daughter Mandi-lee as without your support, guidance and love, this would not be possible.

Lastly to my daughter Amy for her caring, kindness and pep talks. She has been my pillar of strength in times of doubt and without her unfailing and constant motivation I could not have done this.

ACKNOWLEDGEMENTS

I will be forever grateful to my family and friends for the interest and moral support.

To my colleagues that listened to me, gave me advice and help, I will never be able to repay.

To all the Universities staff members and students that provided the data my deep-felt appreciation.

Lastly to my supervisor, Prof Shahed Nalla, I am grateful for your support and guidance on this journey. Your constant optimism and belief in me has been encouraging. I thank you.

SUPPLEMENTARY INFORMATION

Nominated journal:	South Africa Journal of Human Resources
Supervisor / Co-author:	Prof Shahed Nalla
Word count †:	13 661

ABSTRACT

Implementation of Online Assessments in Tertiary Institutions in South Africa

Orientation: The South African tertiary landscape has been fraught with problems over the past few years, for example, student demonstrations regarding the increase in tuition fees resulted in the disruption of academic activities. A proposed alternative method could be an online assessment as it could be a useful tool for measurability and accountability, as well be an ongoing process for learning and research.

Research purpose: The research aims to investigate, through qualitative analysis, the security and implementation of online assessments within tertiary institutions in South Africa.

The motivation for the study: Alternative solutions to traditional assessments should be investigated within the South African context not only to avoid the high cost of disruptions to the academic calendar but also to embrace technology.

Research Design, Approach, and Method: The survey method was used and a questionnaire was sent to the identified South African Universities where online assessments are currently taking place. This was supported by qualitative data obtained through semi-structured interviews with relevant stakeholders.

Main Findings: Most of the tertiary institutions are using online assessments. There are challenges especially with the cheating of students in the form of dishonest behaviours. The security of the online assessment systems appears to be not such a big factor, but proper authentication is deemed advisable. The effectiveness of the online assessments seems to be very good with training being provided in the use of the online assessments.

Practical and managerial implications: The research could be used to determine the tertiary institutions within South Africa that have implemented online assessments and the challenges encountered. Awareness of these challenges that the tertiary institutions

experienced could be valuable, as well as the security measures that have been implemented to curb cheating and fraud.

Contribution/Value-add: South African tertiary institutions are embracing technology in the form of online assessments and there are various types of online assessments available that could be utilised within institutions.

Keywords: online assessment, security measures, cheating; academic ethics, academic integrity

INTRODUCTION

Background to the study

South African tertiary education has been fraught with problems over the past few years, for example, student demonstrations regarding the increase in tuition fees resulted in the disruption of academic activities and destruction of institutional infrastructure at many Higher Education Institutions (HEI's). This was illustrated with the #FeesMustFall campaign in the latter part of 2015. The #FeesMustFall started mid-October 2015 at the University of the Witwatersrand, Johannesburg when the University announced their increase in tuition fees. From there it spread to the University of Cape Town and Rhodes University before spreading to the other universities nationwide. The protests eventually came to a standstill after the South African Government declared that there will be no increase of tuition fees in 2016 (Baloyi & Isaacs, 2015; Cryptomatic, 2018; Gernetzky & Madibogo, 2015). The commitment to Free Higher Education (HE) promised by the Former President Zuma in November 2017 resulted in the atmosphere which could be described as "quiet with volatility". This announcement has however resulted in challenges now related to finding the optimum implementable funding model for free HE education.

One of the universities that suffered extensive damage was the University of Johannesburg, where a group of student activists illegally gained entry into the ABSA auditorium at the Auckland Park campus, and set it alight. The fire also spread to the upper floor and damaged computer laboratories, as well as career assessment facilities. The total cost to rebuild the auditorium was estimated to be over R100 million (Phaladi, 2016).

The student-led disruption of academic activities resulted in the brief discontinuation of academic activities including lectured classes, practicals and tutorials. This resulted in students demanding that examinations be postponed, to which most universities acceded to these demands. Examinations were postponed to either later in the same academic year or, in some cases, to the beginning/first three months of the following academic year. This obviously impacted the academic activities of the current and subsequent years. When assessments cannot take place, it leads to major problems for the institution, least of which questions the quality of the qualifications on offer (Henard & Leprince-Ringuet, 2008). At the

institutions where examinations continued, these had to be written off-site to ensure the safety of the students and staff.

This had financial implications for Universities, as these off-site venues costs were not budgeted for. In order to mitigate a recurrence of such disruption, Universities were tasked to consider alternative ways of teaching and assessing and also determine what was available, feasible and implementable. The traditional examinations e.g. necessitate invigilation and assessment material costs plus external moderation costs (Rowe, 2004) which could lead to budgetary problems for Higher Education Institutions.

A proposed alternative method is an online assessment or "e-assessment" as it could be a useful tool for measurability and accountability to assess teaching and learned objectives, as well be an ongoing process for further teaching, learning and research. Online assessments are known to be much more simplified in delivery and can be useful to assess both formative and summative assessments (Rowe, 2004). Formative assessments are used to assess student's understanding of the work during a lesson whereas Summative assessments are used to evaluate a student's comprehension at the end of a year or semester (Education Reform, 2014).

The security related to assessments are always considered vital in ensuring its validity (Rowe, 2004). The mode of the online assessment as an alternate form of assessment is the focus of this research paper. When considering online assessments, there needs to be an equivalent, or higher level, of security as compared to that employed for the on-site or contact form of traditional assessments with associated invigilation. Academic fraud is a reality and the temptation to commit fraud would be high for students who have the knowledge and skills to be able to access information systems, for example, via hacking into the system used by HEI's. Universities will have to ensure that they make provision to protect against attempts at Information Technology (IT), enabled fraud and security tampering of assessment systems (Love & Cooper, 2004).

One of the University's core functions is to teach module content, and thereafter academics need to evaluate whether students understand and retain concepts and learned knowledge.

As assessments form a vital part of the learning process within a tertiary institution, it would be wise to investigate all possible means of assessments.

Therefore, it would make sense to use the available technologies to undertake assessments as well. Another added benefit to online assessments is that it improves learning abilities Shute (2009), and that assessments are done first to decide on how to collect information to make an informed decision and secondly to inspire students to learn (R. Stiggins, 2008). The use of technology in teaching (online offerings) and assessment forms the strategic push for many national and international HEIs.

With globalisation and the focus on technology, universities should be embracing e-learning technology as it is considered a necessity in higher education (Volery & Lord, 2000). While embracing e-learning technology, consideration will have to be given to online assessment or e-assessments. The definition of e-assessment as stated by the JISC (Joint Information Systems Committee, 2009), is: "The end-to-end electronic assessment processes where ICT is used for the presentation of assessment and the recording of responses".

Since universities will have to look at alternate sources of income, and online courses are one of the forerunners for income generation, it would be practical to investigate all sources of online assessments as well. This would also have the effect and impact on alleviating the burden of limited venues to hold assessments, the cost of invigilation, the security of the student's well-being and the lessening of the potential risk of damage to property (Stiggins, 2008).

Security related to online assessments is a universal challenge faced by most tertiary institutions. Fraud and quick fixes are the order of the day with the ethics of students being almost non-existent (Kennedy, 2012). The South African Government has been cutting the subsidies given to Universities over the years, and the Universities having no recourse but to increase the University fees. This resulted in student protests and thus alternative solutions to traditional assessments should be investigated within the South African context.

Purpose of the study

The purpose of this research project was to evaluate online assessment systems and tools with a key focus on security surrounding online assessments.

This study attempted to investigate security regarding online assessments by asking the following questions;

- Which online assessment systems are currently being utilised at South African Higher Education Institutions?
- How effective have they implemented measures to curb fraud?
- What online assessment systems are available, and how effective are they in ensuring the security of online assessments?

Potential value-add of the study

As the Head of the Assessment Division, at the University of Johannesburg, this study will be of value and use within my workspace. The University is currently investigating online courses and online assessments will form an integral part of these courses.

The long-term vision is that the online assessments will not only be applicable for online courses, but that it will be extended to the extracurricular courses that are assessed at offsite venues, and start implementing it for the curricular courses that have been using traditional assessment methods. Online assessments will also mitigate any challenges that may result from any future student's attempts at fraud.

The study could be helpful to most tertiary institutions, as they will have to look at alternative ways of assessment, which will include online assessments (Love & Cooper, 2004).

Delimitations

The difficulty in investigating all possibilities on how to overcome the security related to online assessments recognised as well as the inventive ways that students will cheat in assessments. Every year, there are new software, hardware, and toolkits available on how

to hack and break into computer systems to bypass security measures (Bailie & Jortberg, 2009). It will not be feasible to look at all the latest available technology and systems as possible solutions to online security risks, therefore this study will focus on a few technology systems e.g. Respondus, Securexam, Lon-Capa and SMART Sync.

The type of online assessment systems, as well as the effectiveness of their systems that tertiary institutions within South Africa use, is not the focus of this study and is not intended to be a promotional tool for any online assessment system.

The following assumptions are made regarding this study:

1. That the University's staff who have completed the questionnaire where online assessments are in place will be open and forthcoming regarding the problems and issues that they are facing or have faced and;

2. That the interviewees will be willing to participate; and

3. The tertiary institutions are all making use of online assessments in some form or other.

LITERATURE REVIEW

Universities have always had to be at the forefront of technology as one of the core functions has been to make education accessible to everyone (alive2green, 2016). This is stressed by the fact that improving the quality of the student learning experience is important for tertiary institutions and e-assessments will add to this (Dermo, 2009). New opportunities with the increased use of mobile phones and tablet devices have made it easier to have e-assessments (Shute, 2009). This would include people that live in remote rural communities and who have part-time employment. Therefore the shift has been to look at online distance learning, including online assessments, as a means to reach this target group (Dermo, 2009).

Overview of security of online assessments

The benefits of online learning and assessments are that there are now more opportunities for lifelong learning, the automatic marking of assessment papers and the ability to have immediate feedback (Apampa, Wills, & Argles, 2010). Furthermore, it is cost effective, there is control over the format, quick and remote access to students, the widened participation of the students and that its attraction to certain populations (Vosylis, Žukauskienė, & Malinauskienė, 2012). It also fosters a paperless office Wang and Sun (2014), with the associated cost savings and more importantly, the reduction of demands on the environment.

The disadvantages of online assessments are the risks related to academic integrity such as cheating and plagiarism, the cost of creating high-quality assessments, verification, and authentication protocol to ensure security (Aly, 2011). It also increases the levels of anxiety and worry from students not skilled in ICT, digital illiteracy, provision of training and the infrastructure unavailability (Attia, 2014).

Security is very important in the context of an education environment and improving the security around e-learning and e-assessment is the fundamental responsibility of the tertiary

institution. In order to assess if tertiary institutions are security conscious, they need to understand cyber-attacks so that they can put “security design factors” in place (Miguel, Caballé, Xhafa, & Prieto, 2014).

Specific security issues like “virtual assignments and exams, security monitoring, authentication and authorization services” were investigated and recommendations were given to minimise threats (Miguel et al., 2014). Digital certificates were also researched to ensure student identification, integrity, and authorship (Miguel et al., 2014).

Consideration has to be given to ensure that basic security measures are in place which is “authenticity, access control, confidentiality, integrity, availability, and non-repudiation” (Luminita, 2011).

There are two types of security categories in e-assessments, namely web security and e-assessment security (Marais, Argles, & von Solms, 2006). They further indicate that although web security has been extensively researched, it is not sufficient to deal with e-assessments (Marais et al., 2006). 73.6% of students feel that it is easier to cheat in an online course than the more traditional exams (King, Guyette Jr, & Piotrowski, 2009) and furthermore, it is suggested that the user security process needs to be further researched (Klett & Pharow, 2006). The result of this is that there is a possibility of increased academic fraud risk with the online assessments (King et al., 2009). The authors also suggest that impersonation is considered a major concern, as students can give their login details to another person, where it is not so easy with traditional methods, as a student has to be validated with his student card by the invigilator (King et al., 2009).

E-assessments rationality and motivation

The delivery of a secure end-to-end session between a student and the tertiary institution's e-learning platform is considered the role of security (Raitman, Ngo, Augar, & Zhou, 2005). Furthermore, the students focus are different as they are more concerned with collaboration and interactions with other students. There have to be tools in place to ensure that the trust

of the system and privacy of the individuals are maintained (Raitman et al., 2005). There is also an expectation that the online environment should be better than the traditional environment. Measurement of this is done by the criteria of confidentiality, integrity, and availability (Raitman et al., 2005). The students would also want the assurance that online submitted assignments and tests will only be seen by the relevant lecturer and that it will not be destroyed, or damaged after submission, and lastly that the online resources will be available as it is needed (Raitman et al., 2005).

Concerns with online assessments

1. Cheating

According to Cizek (1999), Lathrop and Foss (2000), and Sheard and Dick (2003), cheating in assessments is considered a reality. Studies have shown that as a student matures, they are more prone to partake in cheating. When students feel disconnected from their lecturer, they are more inclined to cheat due to the nature of online assessments whereby no personal interaction between student and lecturer can be obtained. The authors further elaborate by stating that many of the students are at ease with a computer and therefore are aware of the potential of computers as a cheating mechanism. To limit the cheating, focused assessment instruments like multiple-choice and calculation questions could be utilised (Rowe, 2004).

There are two types of cheaters, the unintentional cheater who under stress will resort to finding ways to cheat and the intentional cheater who will deliberately go and find inventive ways of cheating (Sewell, Frith, & Colvin, 2010). Some deliberate ways that are mentioned are for a proxy to take the assessment, to send an SMS to someone for answers during exams and disguising notes in one's possessions, e.g. in water bottles or as hidden notes on electronic devices brought into an evaluation venue during a traditional contact assessment (Sewell et al., 2010).

Yet in a study done on academic dishonesty (Stuber-McEwen, Wiseley, & Hoggatt, 2009), less academic misconduct than anticipated was found. Plagiarism involves “premeditated” cheating, but the author concedes that preserving academic integrity is difficult, irrespective of the type of assessment (Heberling, 2002). Peer disapproval reduces the cheating behaviour of students when honor codes and self-reporting tools are in place (McCabe, Trevino, & Butterfield, 2002). A suggestion is to use supervised computer laboratories to thwart cheating as well as to ensure that the assessment is taken by the correct students (Llamas-Nistal, Fernández-Iglesias, González-Tato, & Mikic-Fonte, 2013).

2. Fraud

Many higher education institutions have academic regulations and guidelines which are not currently equipped to react and respond to online fraud (Love & Cooper, 2004). The most profitable business today is internet fraud (Australian Computer Society, 2016). This is surprising as the technology of online security is reasonably mature with the technological developments in other industries, for example, online share trading, online banking, and online retail (Love & Cooper, 2004). With students being more technological savvy, it would be easy for some of them to commit fraud by logging in as the lecturer to determine answers to assessments (Australian Computer Society, 2016). As most assessment software is only protected by a short password, students can use “cracker” software which according to BusinessDictionary (2017), is software used when a person deliberately break into a computer to destroy information and to guess a lecturers password. If they cannot determine the lecturer's password, they can use "social engineering" methods to scam lecturers into revealing their passwords, for example, phone calls claiming to be ICS staff or claiming to change your password to test the system (Mintz, 2002).

As most lecturers are not security specialists they can easily fall prey to some scams into revealing their passwords (Rowe, 2004). The author furthermore states that students can also use “spyware” which is software installed secretly into a computer to obtain sensitive data (Dictionary.com, 2017), to see how and what other students are answering during an assessment, or worse, to see what the lecturer is typing on their computer (Rowe, 2004).

Students can also use “sniffers” which refers to a software tool to monitor data in real time over the internet (LifeWire, 2018) to decipher the message packets of a local-area network containing data of fellow students or the instructor and thereby read their answers or passwords (Scambray & McClure, 2001). Other ways of committing fraud are to use computer-forensics tools that read the memory on lecturer's keyboards and then they retrieve the information (Scambray & McClure, 2001). An example is that a lecturer working on an assessment paper can leave the memory in the cache of their Web browser (Rowe, 2004). Another fraudulent activity especially using WebCT and Blackboard is that students can retake an assessment multiple times if the server software is not designed properly. The students break the connection to the server, then declare that the computer lost power and that they need to retake the assessment (Rowe, 2004). This gives them additional time to either look up the answers or collaborate with others on the correct answers (Rowe, 2004).

Students are able to delete information deliberately (either the information is no longer needed or it is offensive, but there still remains concern about the student who may abuse the environment (Raitman et al., 2005). Students are using “wikis” which is a server program for working together with others so that it forms a web content (WhatIs.com, 2017), to collaborate with each other and to share information. These wikis are backed up every night, but there are concerns that they could lose their work or other members defaming the database or website (Raitman et al., 2005). author also confirms that a time stamp can be faked by a student, so as to appear that a submission is on time, even when it is past the deadline (Mays, 2012).

3. Security

There are various types of attacks that can be done to access institutions’ security firewalls and one of them is called the “brute force attack” (Luminita, 2011). A brute force attack is when someone tries every way possible to access the institution's security firewalls using codes, combinations or password until they achieve success (Sheo Kumar & Dutta, 2011). It is used to guess the password or username. In order to guestimate the password, several demands are sent to the web server with an empty cookie field to ensure that the login failure is reset to zero (Sheo Kumar & Dutta, 2011). Password management is reinforced in the

study done by (Kruger, Steyn, Dawn Medlin, & Drevin, 2008), as they state that students should not be able to access systems where test and examination marks can be adjusted and where the assessment papers can be obtained before the start of the assessments. It is important for all stakeholders to keep their passwords secure and not easily obtainable or easy to guess (Kruger et al., 2008).

Another form of hacking is the "Session hijacking attack" which is the "act of taking control of a user session after successfully obtaining or generating an authentication session ID" (Luminita, 2011). Session hijacking tries to seize control of a user's web application session while they are busy and then uses the cookie which is a file stored on a user's computer that is designed to hold specific information (What Are Cookies.com, 2018), to take control of the session (Luminita, 2011). This can be prevented if institutions make use of Secure Socket Layer (SSL), protocol. Biometrics that include fingerprint scanning, voice recognition, facial features have been introduced to protect systems and data and for authentication (Jain, Ross, & Pankanti, 2006). However, the username and password are used the most for the protection of data (J. Sun, Ahluwalia, & Koong, 2011). They are also of the opinion that it is not always in the best interest to enhance security measures, as it can cause resistance if the users feel that the security is too arduous and unnecessary (J. Sun et al., 2011).

4. Social Media Networking

Sites have now caught on to the trend of sharing tests and notes on multiple courses (Mays, 2012). These sites include www.postyourtest.com, www.sharenotes.com, www.mycollegeexams.com, and www.coursehero.com. These websites all deal in a selection of information that students can upload which can include lectures, assessment papers, and assignments (Mays, 2012). Other sites that have sprung up works are the Ponzi model where students can only access others shared resources if they upload their own (Mays, 2012).

Challenges with online assessments

1. Technology

There is a gap of technology knowledge and skills between students and their lecturers as students are using new technologies in all kinds of ways and therefore lecturers have to keep abreast of modern technology (Mohammad & Gütl, 2008). A case in point is how tertiary institutions are going to incorporate the Internet of Things to the education platform (Bandyopadhyay & Sen, 2011). Furthermore, most of the e-assessment tools are only applicable to certain parts of the assessment cycle or limited to certain types of assessments (Mohammad & Gütl, 2008).

It would be prudent to investigate e-assessment tools that support the entire lifespan of the assessment by making use of various kinds of automatic and semi-automatic methods (Mohammad & Gütl, 2008). This is supported by Saikkonen, Malmi, and Korhonen (2001) who advocates the use of assessments without any human involvement using automatic assessment methods. A challenge in the use of technology is that as it becomes more pervasive other tactics need to be used to counteract the social, cultural and historical ways of assessment (DePaula, 2003). With the increased use of technology, assessment systems have become more complicated, as they have to increasingly serve more purposes (Webb, Gibson, & Forkosh-Baruch, 2013). Another challenge is to develop the assessment literacy of the academic (R. J. Stiggins, 1995).

The advantage of technology is that teaching and learning for both student and lecturer are simplified and easy (Usang, Archibong, Aji, Eyong, & Bassey, 2018).

2. Authentication

Passwords are used as a measure of authentication to gain access, but it is not a proper use for addressing authentication (Morris & Thompson, 1979). This concern is strengthened by the fact that most people choose weak passwords (Katz, Ostrovsky, & Yung, 2009), which is compounded by the fact that password authentication is most often inadequate (Clarke &

Furnell, 2007). There are various approaches to authentication namely “something he/she knows (i.e. secret knowledge), something he/she has (e.g. a physical token), or something he/she is (e.g. a biometric)” (Furnell, 2007). A single authentication method has been the rule over the years, and this posed challenges as people make use of simple dictionary words, they write down their passwords, they use the same password across multiple devices and share their passwords with colleagues (Levy, Ramim, Furnell, & Clarke, 2011). Combining passwords with smart cards for authentication is advocated as this has been in the financial industry sometime now (Weir, Douglas, Carruthers, & Jack, 2009). The use of multi-biometric (fingerprint scanner, facial recognition, and audio surrounding) authentication will be able to pass the toughest identification tests (Z. Sun et al., 2010).

Preventative Measures

There are multiple ways of preventing cheating which includes student's signing a code of honor, an enquiry into students with significantly improved performances and trying to make passwords hard to guess (Cizek, 1999). This is reinforced by Strom and Strom (2007) that if they are caught cheating, there should be consequences spelled out in a tertiary institutions code of conduct, for example, disciplinary hearings with possible expulsions.
Another suggestion is to install software so that the academic is able to see the screens of the computers and with the ability to be able to lock down access to other applications (Rogers, 2006). Regular update of server software and anti-virus software and that copies of marks need to be kept in case of students hack into the system to change the mark (Cizek, 1999).

A rule must be made that no handheld devices to be used during assessment opportunities and investigating online invigilation. Finally, the lockdown of the internet during online assessments is advised (Cizek, 1999).

Furthermore, it is recommended that lecturers have to plan for the unexpected by ensuring that there is a plan B in case of technology problems (Rowe, 2004). Another preventive measure is to only make the test available when the assessment is being written and only

to the students that have the correct password (Sewell et al., 2010). Other measures include open book assessments where it is clearly stated which tools are available (Sewell et al., 2010). When staff members are aware of their University policies regarding student misconduct, they can implement preventive measures to minimise cheating (Hard, Conway, & Moran, 2006). With each assessment, there should be a disclaimer at the beginning whereby students have to state that they will not be dishonest or fraudulent (Strom & Strom, 2007).

E-assessment systems

In the study done by Harmon and Lambrinos (2008), they found that cheating will be more likely to take place when exams are not proctored. This is reinforced by studies done by (Edling, 2000); (Rovai, 2000), and (Deal, 2002). The study, therefore, has to look at what systems are currently available to curb cheating. An integrated assessment system that will cater for assessments and for learning, which serves both the learner and the teacher is an ideal (Birenbaum et al., 2006).

Assessment systems are moving towards more web-based systems. Systems like Blackboard which is used at the University of Johannesburg and at most tertiary institutions in South Africa provided "automatic grading of multiple choice and True/False questions" and other systems like QUIZIT, WebCT, ASSYST, and PILOT also possess the ability to conduct online testing and grading (Rowe, 2004). Another few assessment systems of internet surf lock vendors that are on the market are Vision Classroom Management Software® - using surf lock, Respondus LockDown Browser Powerlink® (www.respondus.com/), and Securexam Browser Powerlink® www.softwaresecure.com/browser.htm (Sewell et al., 2010).

1. ProctorU

The system available from the website (www.proctoru.com) is a fully automated artificially intelligence based platform with identity verification (ProctorU, 2017). Video recordings are done of the students and their activity during assessments. If there are incidents, they are flagged with a timeline and timestamp to make reviewing much easier. They also have integrity violation and post-exam reports immediately available after each assessment

opportunity. According to their website, administrators can view all students live while they are doing the assessment and they state that not one of their competitors can do this (ProctorU, 2017).

2. Respondus

This is a third-party software package who have partnered with various publishers to make it easier to download and to customise the test bank of textbooks (Virginia Commonwealth University, 2017). Respondus works with Blackboard and has developed the Respondus LockDown Browser (www.respondus.com/products/lockdown.shtml) that is customised with Microsoft Internet Explorer and is able to lock down the testing environment. With the LockDown browser, students are unable to use the internet, print, copy or access any URL, as well as any other applications (Wankel & Wankel, 2012).

3. Lon-Capa

Lon-Capa (Learning Online Network – Computer Assisted Personalised Approach is a "distributed network system" which allows for the sharing of assessments and learning within an institution, as well as with other participating ones. It is used by students especially in the Sciences and Mathematics as it has the ability to write complex problem types (Virginia Commonwealth University, 2017).

4. Securexam Remote Proctor

This is by the company Software Secure (www.softwaresecure.com) and it offers a browser with restricted functionality to regulate printing and access to the internet. It also included a device that has a biometric fingerprint scanner, a camera, and a microphone, that connects to a student's computer. The biometric fingerprint scanner will only give access to the online assessment to the authorised student and with the camera, a proctor is able to have a 360-degree view of the exam area (Mays, 2012).

5. SMART Sync

The software available at (www.smarttech.com) is part of the SMART classroom suite and gives you thumbnail views of all the computers in a classroom. This makes it easier to monitor, as well as controlling the computers by means of locking access. It provides the

ability of the academic to connect and interact with individual students and groups (Mays, 2012).

6. Examity

Examity makes use of live proctors in a controlled supervised invigilation centre (Schauffhauser, 2017). They have various levels of proctoring available namely automated authentication as well as live authentication (Schaffhauser, 2017). As per their website www.examity.com, they have proctors that watch all students ensure that there are no violations. As they doing this, they are able to make comments and flag issues which are time-stamped (Examity, 2017). They have a flag system which they use for authentication and completion of the assessment. Green flags indicate no incidents occurred, yellow flags show that there was a minor violation and red flags are used to show that cheating was involved. They also have blue flags to show that there were technical issues (Examity, 2017).

7. Other Systems

Other systems are Angel and WebCT that was attained by Blackboard; WebCT; Blackboard (blackboard.com); Desire2learn (www.desire2learn.com); Pearson's ecollege (www.ecollege.com/index.learn); Instructure (www.instructure.com); Moodle (moodle.org); and ims qti (www.imsglobal.org) (Mays, 2015). Most of the e-learning platforms make provision for online evaluation and assessment within their structure with automatic assessment rectification (Llamas-Nistal et al., 2013). The aim of most of the platforms is to attain automatic assessments (Llamas-Nistal et al., 2013).

Summary of the Literature Review

As discussed in this chapter, there have been several studies done on security aspects around online assessments, however, the security and advances in technology will remain a hindrance block. It is evident that South Africa is in need of advancing with the offering of online courses and the relevant online assessments.

Tertiary institutions must learn from one another's online systems and the focus should be on evolving and keeping up to date with the latest technology to try and be one step ahead of "computer criminals". Academic fraud is on the increase and we have to educate our students on the repercussions of cheating and fraud and advocate honesty and doing the right thing.

RESEARCH APPROACH

The study adopted both the qualitative and quantitative data gathering techniques known as the Mixed Methods Procedure. The Mixed Methods Research is a methodology that is used when accumulating, analysing and assimilating both quantitative (surveys) and qualitative (interviews) research (FoodRisc Resource Centre, 2017). By using the Mixed Methods Procedure it can make the most of the strengths of both qualitative and quantitative research (Creswell & Clark, 2017). The author goes further to say that more insight can be gained by using both than by using either one of the two (Creswell & Clark, 2017; Creswell & Creswell, 2017). Furthermore, the authors state that there are four important aspects to this method namely timing, weighing, mixing and theorizing (Creswell & Clark, 2017). With the *timing* aspect, the researcher will have to decide whether the research should go in phases or which method of either qualitative or quantitative must go first. The *weight* and priority given to the research method must also be decided at that time, on which method should be given more weight or priority. With *mixing* the study has to decide where and when the two sets of data will be connected. Lastly, with the *theorizing* aspect, the study has to decide what principles, theories, structures, and instincts to bring to the inquiry and if it must be mentioned or not (Creswell & Clark, 2017).

The strategy that was used is called the sequential explanatory strategy and it is characterised by the assembling and scrutiny of the qualitative data in the initial phases that also builds on the results of the earlier quantitative results (Fleisch, 2008). The author is of the view that qualitative research is able to balance the findings of quantitative research and would provide a better understanding for making decisions (Fleisch, 2008).

The survey method was used and a questionnaire was sent to the identified South African Universities where online assessments are currently taking place. This was supported by qualitative data obtained through semi-structured interviews with relevant stakeholders. The researcher conducted interviews with staff members at the University of Johannesburg who are currently dealing with online assessments. The survey method of questionnaires and

the semi-structured interviews will best serve to answer the questions and the purpose of this study.

Population and sample

Population

A *population* is a group of individuals that are sharing the same characteristics and who is the main focus of a study (Hasson, 2016). Since research cannot be done on the whole population due to the cost and the time, the study focussed on making use of sampling techniques. There are two types of population in research namely a *target population* and an *accessible population* (Hasson, 2016). The target population in this research were the individuals selected who met certain selection criteria so that the sample can be used to see if the conclusion will be reached. The accessible population for this study, for both the qualitative and quantitative methods, comprises of staff members within tertiary institutions that are either working with online courses and assessments or non-academic staff maintaining the secure online systems and students that are dealing with online assessments.

Sample and sampling method

In some instances, the population could be small enough so that the researcher can include them in the study, but in other cases, the study may have a large population that cannot all be studied and a portion of the population that is going to be studied is called a *sample* of the population (Nworgu, 2006). A purposive sampling technique was used as the researcher determined who to send the questionnaire to, as well as who to interview. Purposive sampling also tries to “capture the range of views/experiences, pursue saturation of data and draw theory from data” (Sunday, 2014). It is commonly used in qualitative research to identify and select information (Patton, 2005) and it should be people that are experts in the field that are investigated (Creswell & Clark, 2017). The sample in this study will be all of the Universities within South Africa, as it cannot be determined who are dealing with online

assessments or not. South Africa has 26 Universities and of them, a smaller group of Universities are offering online courses with the accompanying online assessments. Questionnaires were emailed to those Universities and once feedback was received, interviews were undertaken. Table 1 below shows who the questionnaires were emailed to.

Questionnaire - Email Recipients

Table 1: Email Recipients for Questionnaire

Tertiary Institution	Females	Males
Cape Peninsula University of Technology	3	7
Central University of Technology	2	1
Durban University of Technology	5	4
Limpopo University	3	8
Mangosuthu University of Technology	0	1
Nelson Mandela University	2	0
Northwest University	0	3
Rhodes University	1	0
Sol Plaatjie University	2	0
Stellenbosch University	1	0
Tshwane University of Technology	4	2
UNISA	3	0
University of Cape Town	1	1
University of Fort Hare	1	1
University of Johannesburg	6	8
University of KwaZulu Natal	1	2
University of Mpumalanga	0	1
University of Pretoria	1	0
University of the Witwatersrand	1	1

University of Venda	1	0
University of Zululand	1	2
Vaal University of Technology	3	1
Walter Sisulu University	1	1
University of the Free State	1	0

Research method

As mentioned in the previous section the mix method was considered to be the best method to obtain the best results. To facilitate the process a questionnaire was designed consisting of 21 close and open-ended questions divided into three sections. Section 1 consists of the respondent's personal information, Section B probed the depth of the tertiary institutions use of online assessments, and finally, Section C looked at the challenges and security measures in place at their institutions. The questionnaire was emailed to tertiary institutions that are actively participating in online assessments. With the semi-structured interviews, a few sample questions sent with the request for an interview. The sample for the questionnaire consisted of academic staff, as well as students, and the interviews were a mixture of academic staff and support staff.

The rationale for the use of a questionnaire

Surveys that use questionnaires are “the most widely used data-gathering technique in research” (Anderson & Shaw, 1999), which is correborated by Mathers, Fox, and Hunn (2007) & Slattery et al. (2011). The questionnaire used is important in the development of human resources, such as behaviour, attitudes, beliefs, opinions, characteristics, expectations and so on. Therefore, the design of the questionnaire was appropriate for testing the sample population's knowledge of the security around online assessments. The advantages of a questionnaire were considered namely cost-effective; timely; more people can be reached; ensures anonymity; people could think about their answers and the data could be pre-coded. The disadvantages of the questionnaire such as low response rate;

incomplete answers, clarification of answers were considered (Denscombe, 2003; Robson, 2002); (Brynard & Hanekom, 1997); (Sameer Kumar & Phrommathed, 2005). The disadvantages were deliberated and were not thought to be much of a hindrance. The contact details of the researcher were made available to ensure that respondents are able to contact her for clarity on questions, if necessary. The questionnaire was emailed to respondents as this ensured that the cost is not too high.

Some of the disadvantages, for example, the low response rate, were addressed by means of a follow-up email to request a response, but others like poorly completed answers affected the study negatively. Since the sample population is all within South African Universities, which are locally based, the cost element will not be a factor to be considered as a disadvantage.

Questionnaire design

A questionnaire is a list of carefully structured questions, which goes through a pre-testing phase, to ensure that reliable responses are received from the chosen sample (Brace, 2018). The aim of a questionnaire is to determine what the sample thinks or feels. Interviews are the spoken dialogue between two people with the objective of getting the applicable information for the purpose of research (McNamara, 2009). The researcher can probe for more information and the interview can also be used as a follow-up with participants. The interview will be an alternative method of collecting data survey (Hesse-Biber & Leavy, 2010), and should be useful in obtaining information and learning from stakeholders that are currently going through the process of online assessments (Walliman, 2016).

There are a few types of interviews namely personal, telephone, focus group, depth and projective techniques (Hasson, 2016). The study's primary focus will be on personal interviews as it is a face to face interaction. It was conducted in a semi-structured way with a set of planned questions, but with the leeway of being able to clarify points. If time was the enemy, then the secondary focus will shift to telephone interviews, with the same set of questions, and the ability to probe and request more information.

Some of the advantages of interviews are that more probing of the questions could be done; the responses are guaranteed and it produces more detailed results, and additional advantages would be the immediate feedback as there is no limit to the length of the interview unless the time is pre-determined. This method ensures that there is a high participation rate (Logic Consulting, 2017).

Some of the disadvantages to this method is the cost, and since they are either in a face to face situation or telephonically, the participants cannot claim anonymity. There is sometimes also a need for a call back session which increases the cost. Interviewees might also not disclose full information for fear of reprisals. The culture and gender can be a factor for a participant's willingness to participate in an interview (Logic Consulting, 2017).

Procedure for data collection

Data collection can be different as it depends on the method of open-ended versus closed-ended responses (Creswell & Creswell, 2017). Some forms of data such as interviews can either be quantitative or qualitative as it is determined by how open (qualitative), or closed (quantitative), the reaction might be.

A survey research method was used in the form of a questionnaire, to try to address the research questions. The questionnaires were sent via email to the Universities directly to the chosen sample for the study. The survey data was obtained through pre-determined questions.

Once the data was collected, it determined the questions that were asked during the interview phase. The semi-structured interview will also try to address the research questions through data collection of pre-determined questions during the interview process (Creswell & Creswell, 2017).

Data analysis and interpretation

A normal distribution was not possible because of the smaller sample. Content analysis is the "procedure for the categorization of verbal or behavioural data for the purpose of classification, summarisation, and tabulation (Sunday, 2014). After the questionnaires were completed, an analysis was done to determine if there are similarities and from that, the data were analysed further to see the commonalities. Content analysis can be used on two levels, namely Descriptive with the question being asked “What is the data?” and with Interpretative “What is meant by the data”? (Sunday, 2014).

With the analysis of the interview data the researcher used narrative analysis which in effect means ‘transcribed experiences’. Once the interviews were conducted the researcher sorted the data and reflected on it. It was then augmented and presented within the study. One of the main activities in a narrative analysis is to show the common thread that is weaved from people’s different experiences and context (Sunday, 2014).

The second order analysis was to see if there is a theme that is repeating as well as seeing if there are patterns within the data. The data was analysed so that the study can answer the research questions and from there develop a hypothesis (Sunday, 2014).

The limitations of this study are namely;

- Time Limit, as the questionnaire and interviews were done within a short period of time. If tertiary institutions do not adhere to the deadlines, a follow up was made.
- Sample Constraints, as the study is limited to universities within South Africa and specifically to universities offering online assessments. This study did not cover any international tertiary institutions.
- The scope of the research will only focus on the implementation and security aspect of online assessments and the assessment systems that they are using.

Validity and reliability

“Validity is often defined as the extent to which an instrument measures what it purports to measure” (Kimberlin & Winterstein, 2008). Content validity refers to the extent to which an instrument pertains to the factors under study. To achieve this the questionnaire included a variety of questions that determined the extent of the sample population's knowledge of security around online assessments.

Face validity was obtained by ensuring that the questionnaire was sent to experts who will make recommendations on the content of the questionnaire. Questions were asked based on the information that is gathered during the literature review so that no unnecessary data were collected. Questions were written in layman’s terms to ensure that there is no misunderstanding and miscommunication. It was also kept short and to the point so that it did not become onerous to complete. Instructions were clear to avoid ambiguity.

External validity

The questionnaire was sent to a few selected specialists in this field, to determine if the study meets the requirements of fulfilling the brief and whether the questions are appropriate and valid. The questionnaire was structured with checkboxes where the respondents have to choose the applicable choice. It was difficult to obtain subjects who were willing to participate in a study, especially if it takes up the valuable time of the sample. The study, therefore, had to be planned to limit the time demands on the subject so that they would be more willing to participate.

Internal validity

Internal validity is mostly concerned with the similarities of the research findings with the reality of the study (Zohrabi, 2013). It also “deals with the degree to which the study observes and measures what is supposed to be measured” (Prochaska, 2016). To strengthen the validity of the data and findings, the researcher collected data from various sources namely interviews and questionnaires. To collect data from one source can be

flawed and open to biases. The internal validity determined if the research is believable and true, and evaluating what it is supposed to evaluate (Prochaska, 2016). Studies that have high internal validity will produce results that are not as flawed, where the low internal validity is the opposite (Campbell & Stanley, 2015).

Through triangulation, the study could get qualitative and quantitative data that can substantiate the findings (Zohrabi, 2013). With the interviews, the researcher checked the results and interpretations with the participants so that the findings could be corroborated. This ensured the plausibility and truthfulness of all the information in the study. Lastly, all researchers have their bias and the data collection, analysis and interpretation were as impartially as possible. The researcher was as non-judgemental and principled as possible, to ensure that the findings are reflected as honestly and accurately (Zohrabi, 2013).

Factors that threatened the internal validity of the study is the passage of time as technology advances at a rapid rate, and what implementation of online assessments and security measures could be relevant today can be obsolete tomorrow. The researcher had to also be attentive to the biases of the sample population, as people have their own hidden agendas (Zohrabi, 2013).

Reliability

The reliability of the study is if the questionnaire would yield the same result each time (Hesse-Biber & Leavy, 2010). To get the information in quantitative research it is easier as the data is in numerical format. However, in qualitative research, the data is in narrative form and subject to interpretation (Zohrabi, 2013).

Reliability can be guaranteed by trying to reduce “sources of measurement error” like data collector bias. The bias was removed by ensuring that the researcher does the administration of the questionnaires and standardising the conditions to show similar personal traits to all participants, e.g. friendliness, collegiality, and support (LeCompte & Goetz, 1982).

FINDINGS

This chapter will focus on the findings and the analysis of the data obtained from the research.

QUESTIONNAIRES

Section A - The characteristics of the respondents

The questionnaire was sent to 24 of the 26 universities with 44 of the email recipients being female and 44 male. From this, a total of 16 responses were received from the targeted 88 potential respondents, which constitutes an 18% response rate for the questionnaire.

The questionnaire was divided into three sections with Section A being the socio-demographic information, Section B was investigating the depth of the institution's use of online assessments and Section C the challenges and security measures that exist at the tertiary institutions. The analysis is based on the academics and students at various tertiary institutions within South Africa who have responded. Figures and diagrams have been used to facilitate a simplistic reader-friendly reporting of the results/findings.

Personal Information

The section below covers the socio-demographics of the respondents by listing the type of tertiary institution the respondents were working at; their position at the institution; the Faculty and Department/Division; age; how long they are dealing with online assessments; and how many students they have registered. Although it was not central to the study, the personal data helped to contextualise the findings and develop suitable recommendations in the use of online assessments.

The type and tertiary institutions that responded

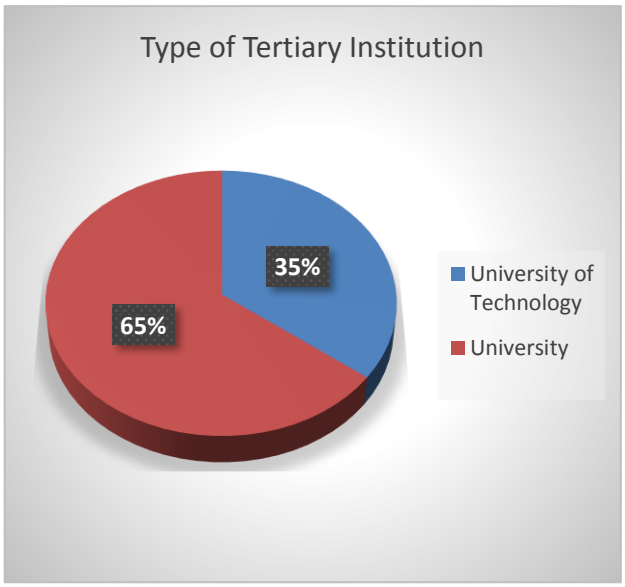


Figure 1: Responses received from the different type of tertiary institutions

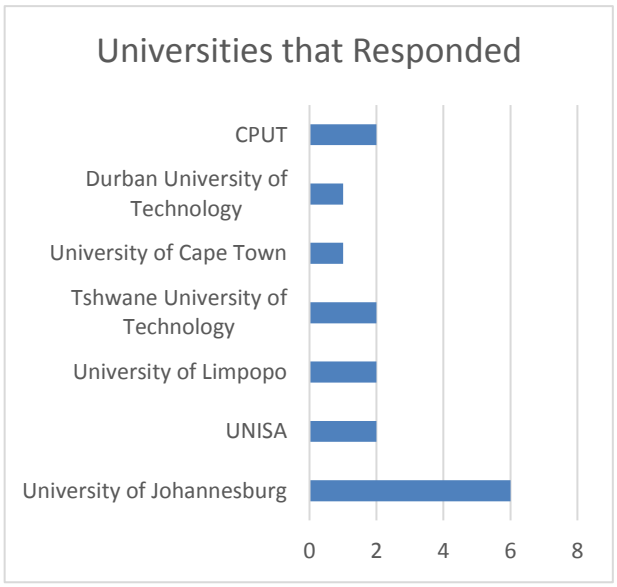


Figure 2: Responses received from the tertiary institutions

Based on Figure 1 above, 65% of the respondents are from a University and 35% are from a University of Technology.

Figure 2 illustrates the tertiary institutions that participated in the study with the University of Johannesburg having the most respondents namely six, with DUT and UCT having the least namely one respondent.

The respondents' position/title within the tertiary institution

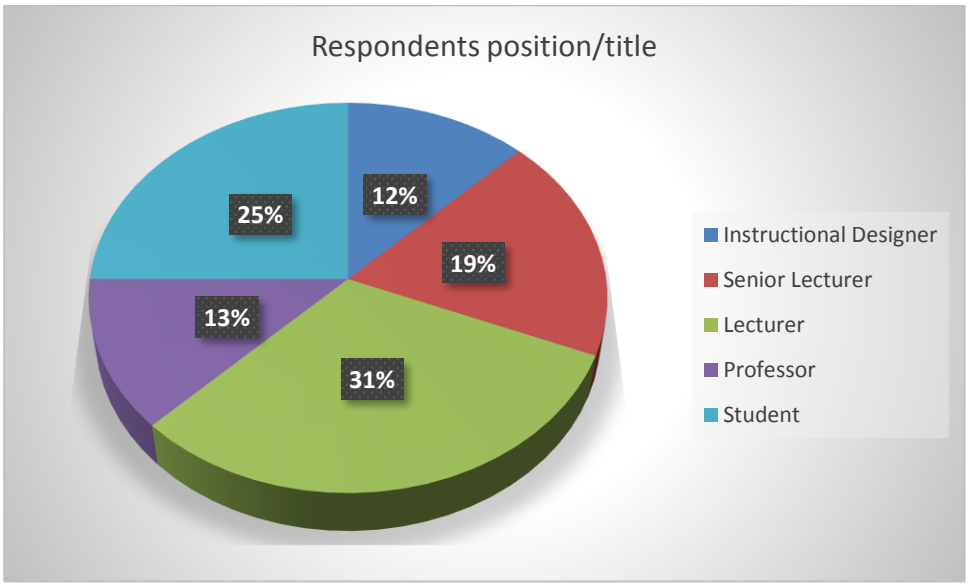


Figure 3: The respondent's position/title within the tertiary institution

As indicated above in Figure 3, 31% were made up of lecturers with 25% being students with the rest being senior lecturers (19%) professors (13%) and instructional designer (12%). This represented a fair distribution of positions within a tertiary institution.

The Faculty where respondents originate from

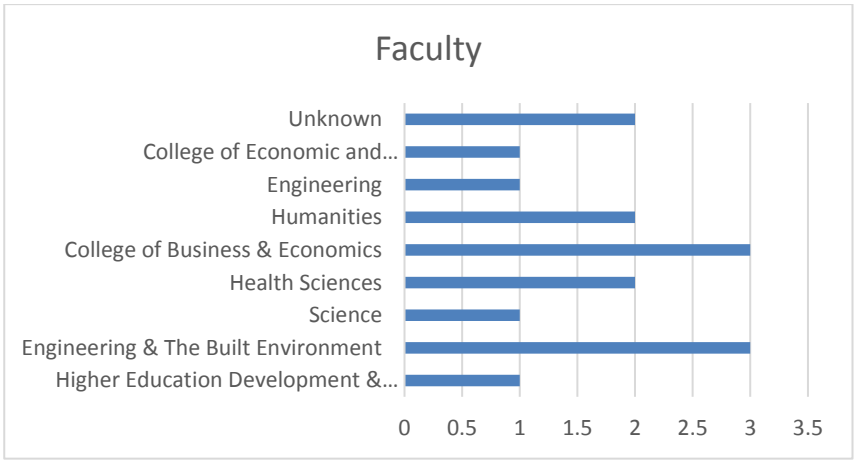


Figure 4: The Faculty's where the respondents originate from

Figure 4 shows that the majority of the respondents 19% were from the College of Business and Economics as well as the Faculty of Engineering and the Built Environment. 13% of

the respondents were from the Faculty of Humanities and 13% of the respondents did not indicate their faculty. This gave a fair distribution of the Faculties where the respondents were based.

Departments and Division where respondents are based

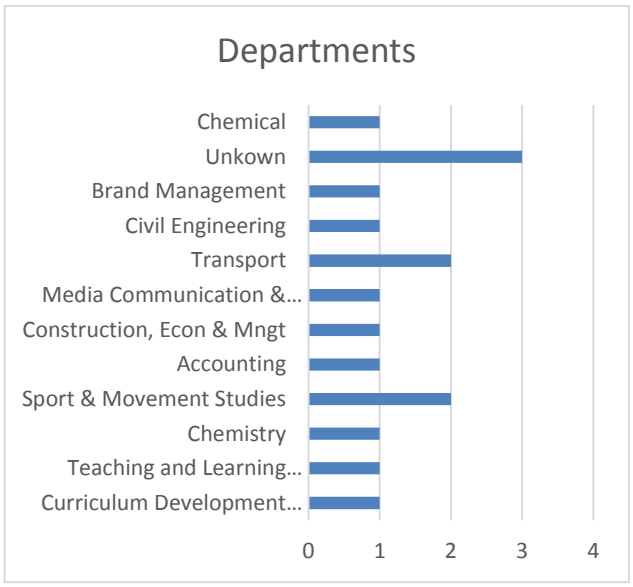


Figure 5: The Departments where the respondents are based

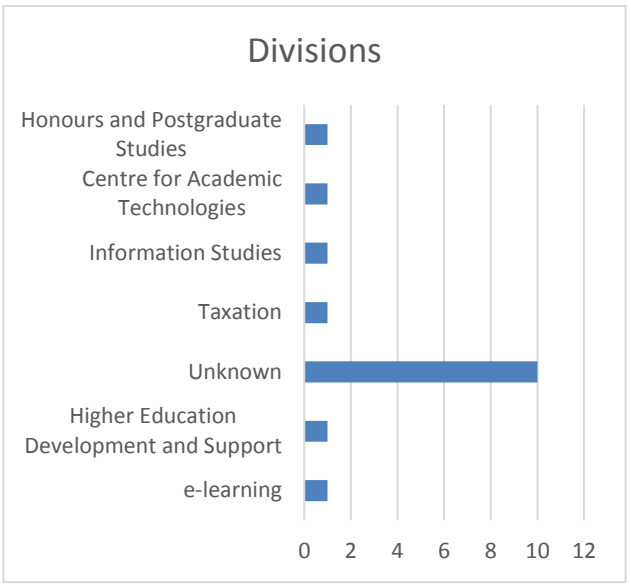


Figure 6: The Divisions where the respondents are based

The majority of the respondents 19% did not indicate their Department as per Figure 5. This could be an indication that they are not based in a Department or that they have chosen to omit their Department's information. Thereafter, 13% of the respondents were from the Department of Transport and the Department of Sport and Movement Studies, while the remaining 6% were all based in various departments.

As shown in Figure 6, the majority of the respondents (10 of the 16 (63%) did not complete this section. The rest of the respondents (37%) were all from various divisions.

Gender and Age of Respondents

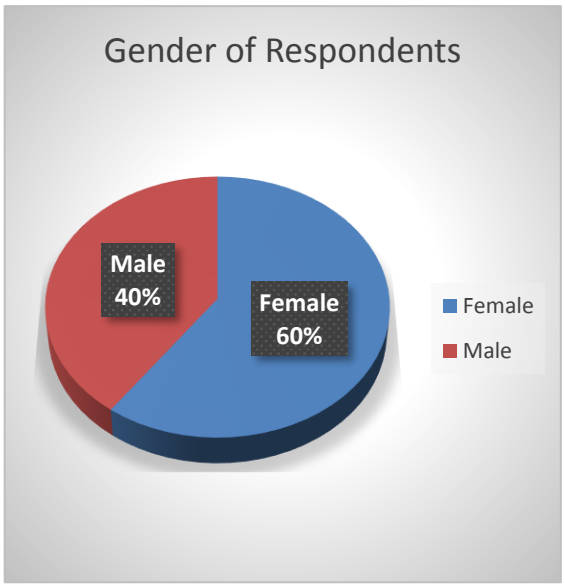


Figure 7: The Gender of the Respondents

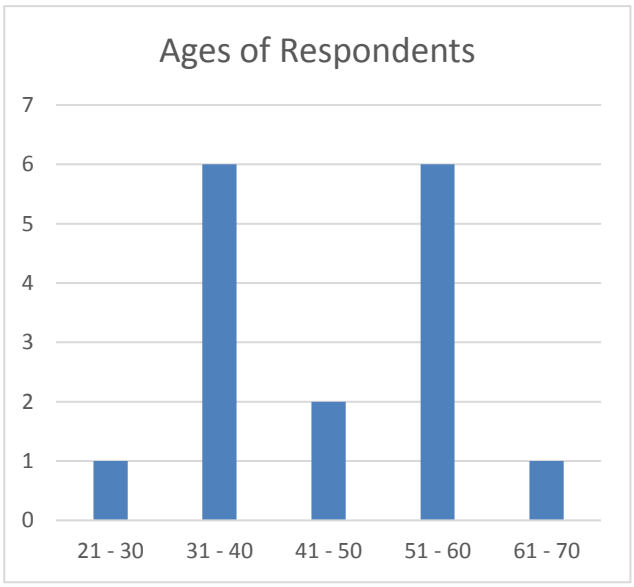


Figure 8: The Age of the Respondents

In Figure 7 the bulk of the respondents were females namely 60%. This ties in with research that shows that more women are likely to complete questionnaires than their male counterparts ((Curtin, Presser, & Singer, 2000); (Moore & Tarnai, 2002); (Singer, Van Hoewyk, & Maher, 2000)).

In Figure 8 the ages of the respondents also varied with the majority of them in the 51-60 and 31 – 40 age group (38%). The respondents with the least amount of responses were in the age group 21-30 and 61-70 namely 6% respectively.

How long are Respondents Using Online Assessments?

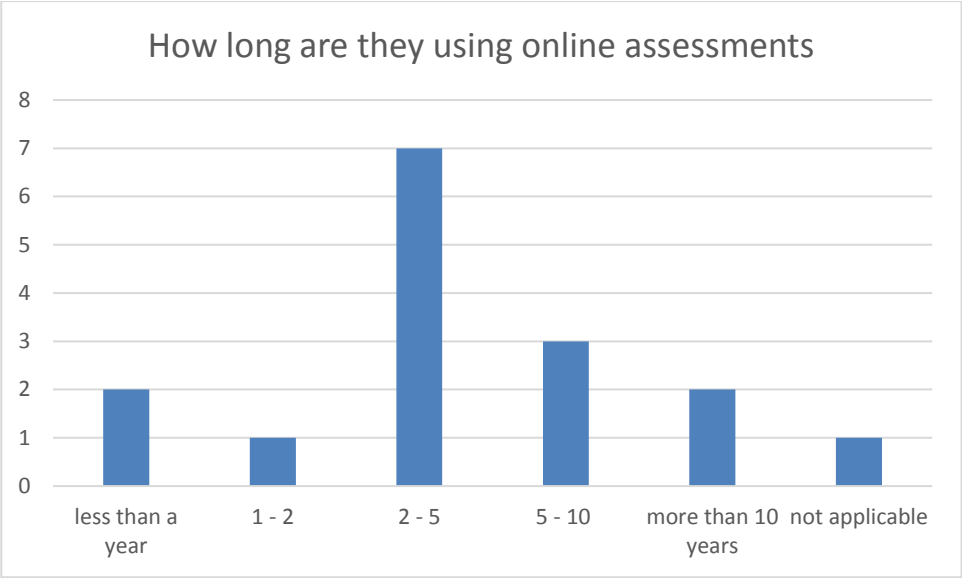


Figure 9: How long are the respondents using online assessments?

In Figure 9, 44% of the respondent's tertiary institutions were making use of online assessment for 2 – 5 years. The respondents (6%) that were the least in terms of years, were only using online assessments for 1 – 2 years and the others did not use online assessments at all (6%).

How many Students at Respondents University

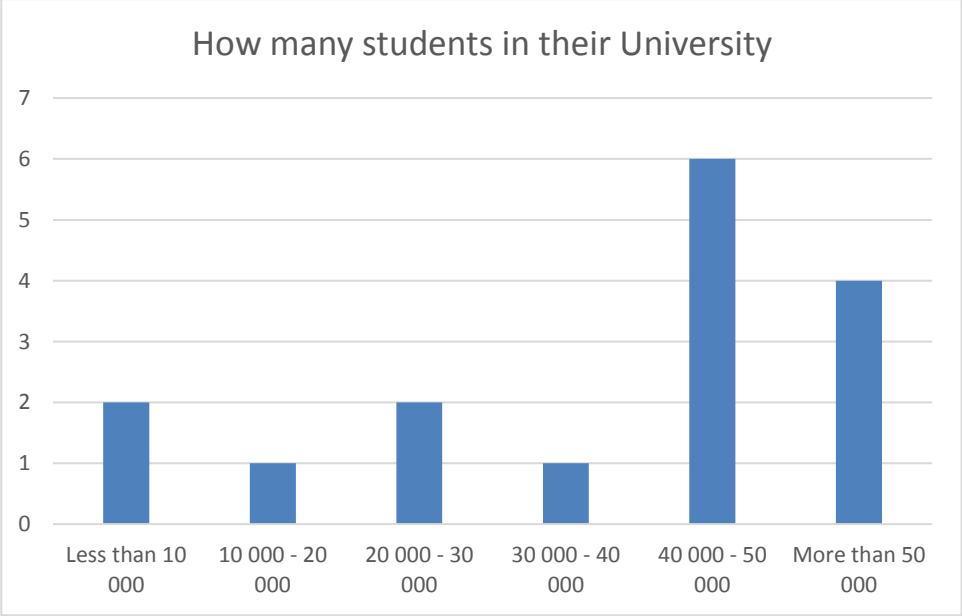


Figure 10: How many students at respondents' tertiary institution

Figure 10 illustrates the students' numbers per tertiary institution. More than 38% of the tertiary institutions had student numbers in the region of 40 000 – 50 000. The respondents with the least numbers of 10 000 – 20 000 and 30 000 – 40 000 accounted for 6%.

Section B – The depth of the tertiary institutions use of online assessments

In this section, the researcher asked specific questions on the respondent's depth of use of online assessments and how they are using it.

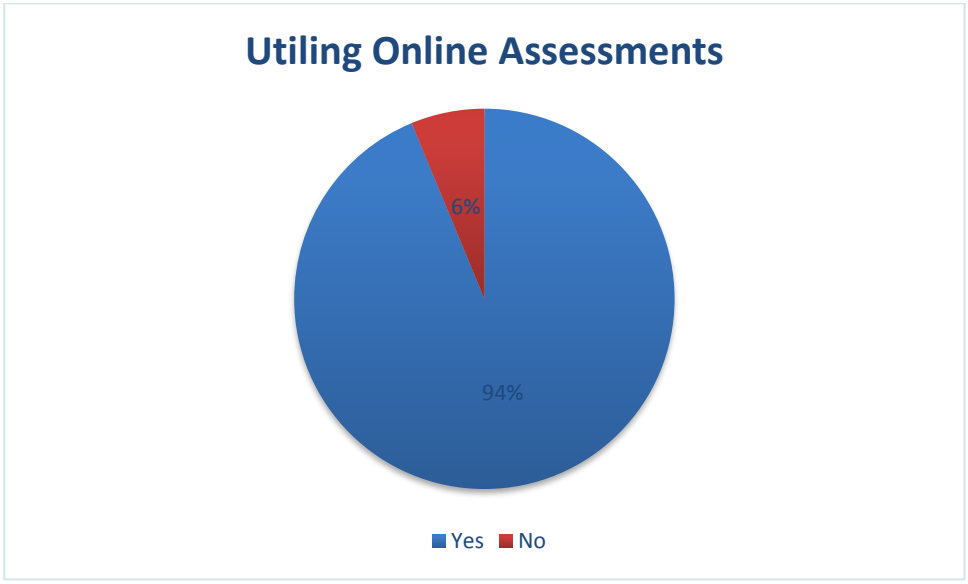


Figure 11: Are the respondents utilising online assessments?

It seems that the majority of the respondents are using online assessments at their tertiary institutions as it came to 94% with 6% of the respondents stating that they are not using online assessments at their institutions.

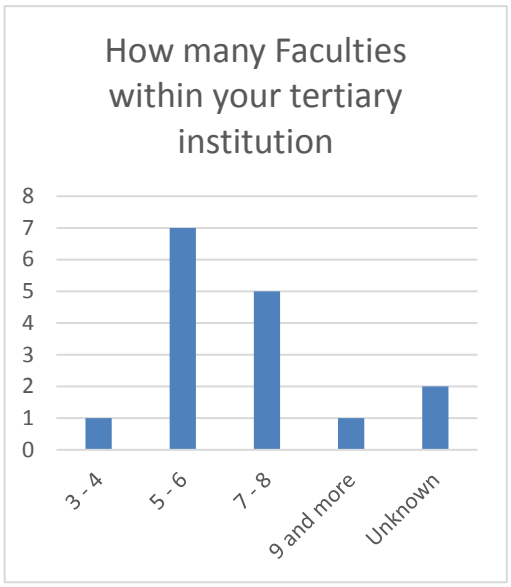


Figure 12: How many faculties are within the tertiary institution?

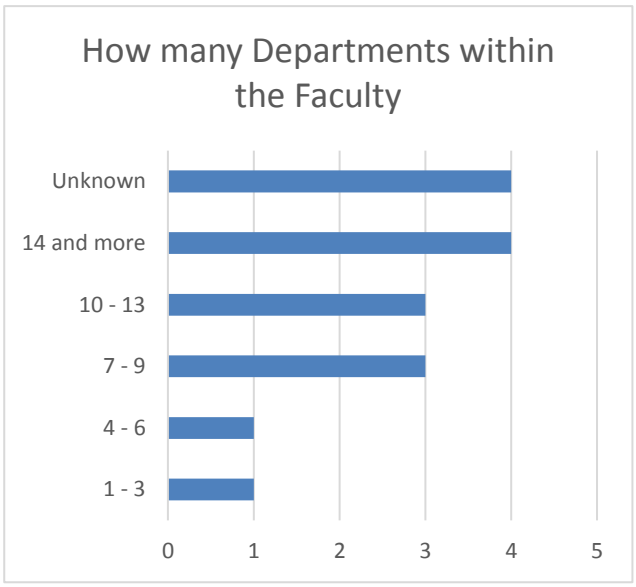


Figure 13: How many Departments within the Faculty

The bulk of the tertiary institutions (44%) seem to have 5 – 6 Faculties within the tertiary institutions with the least (6%) having 3 – 4 faculties and 9 and more respectively.

Figure 13 it shows that most of the Faculties had 14 and more departments (25%). The remaining 25% of the respondents did not complete this section.

.

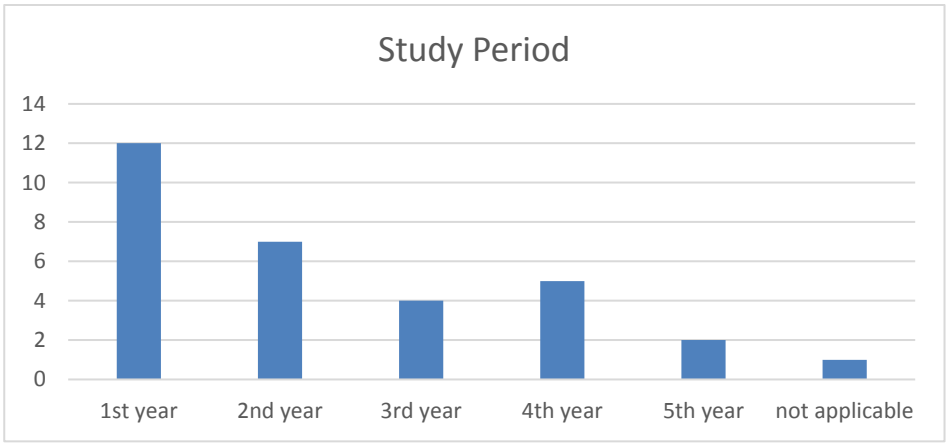


Figure 14: Study Period where online assessments take place

The respondents were making use of online assessments from the 1st year to the 5th year. 12 of the respondents (75%) were using it in the first year with the 5th year (13%) which is probably tutored Masters being the least utilised.

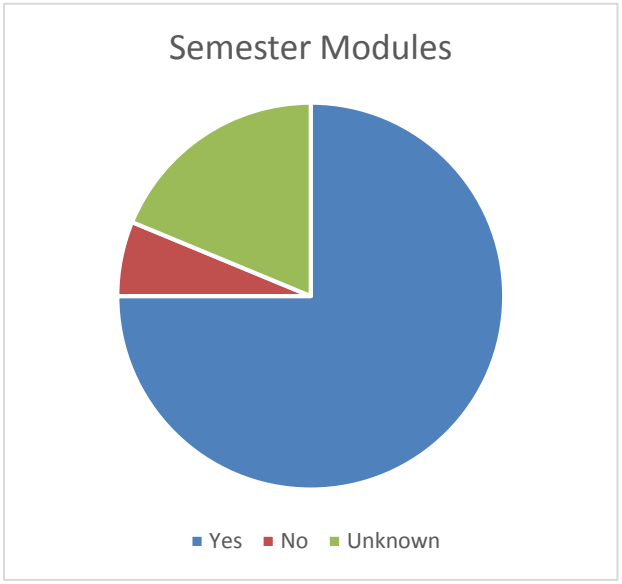


Figure 15: Is the Online Assessments Semester Modules?

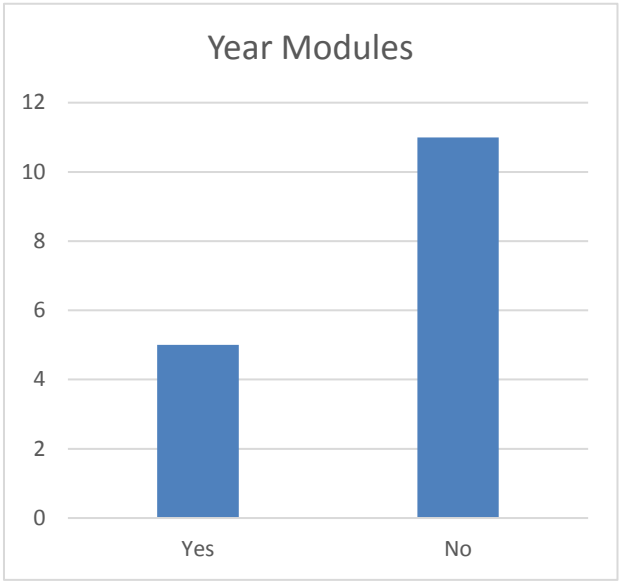


Figure 16: Year Modules where online assessments are done

In Figure 15 75% of modules are semester modules and this is reflected in Figure 16 with 69% of the respondents indicating that the modules are not year modules.

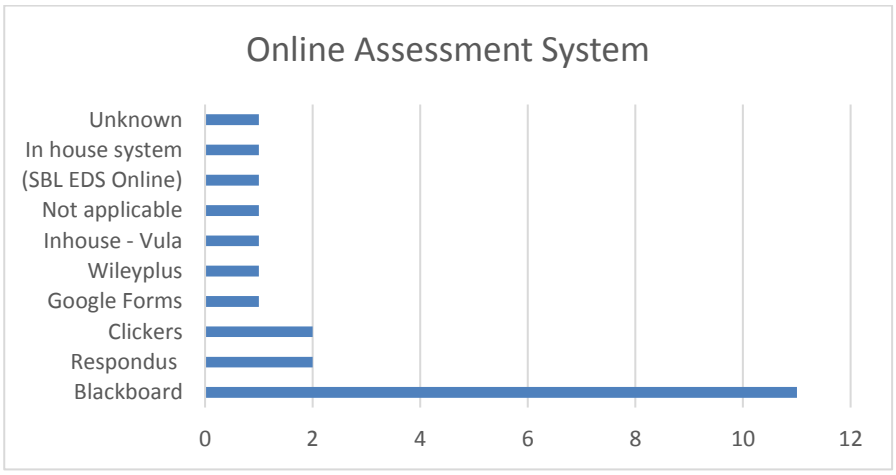
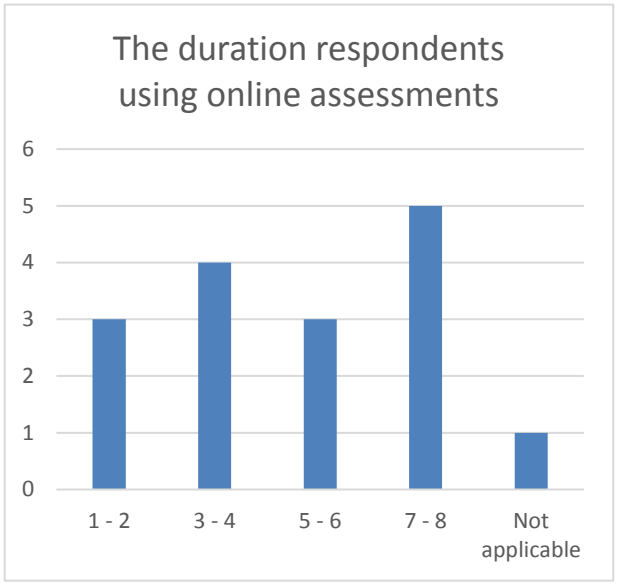


Figure 17: The type of Online Assessment Systems that respondents use

Most of the tertiary institutions' respondents (69%) are using Blackboard for their online assessments while most of the other respondents have an in-house system in place.



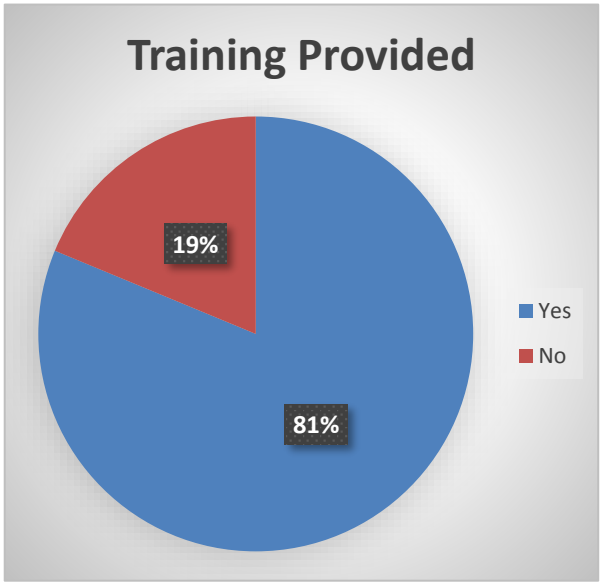


Figure 18: The duration respondents are using online assessments

Figure 19: Were training sessions provided for the online assessment system

The majority of the respondents (32%) in Figure 18 have been using the online assessment system for 7 – 8 years. In Figure 19, 81% of the respondents indicated that training on the use of online assessments has been provided. Their level of competence as shown in Figure 20 shows that the majority (50%) of them specified "Very Good".



Figure 20: Respondents level of competence with the online assessment systems

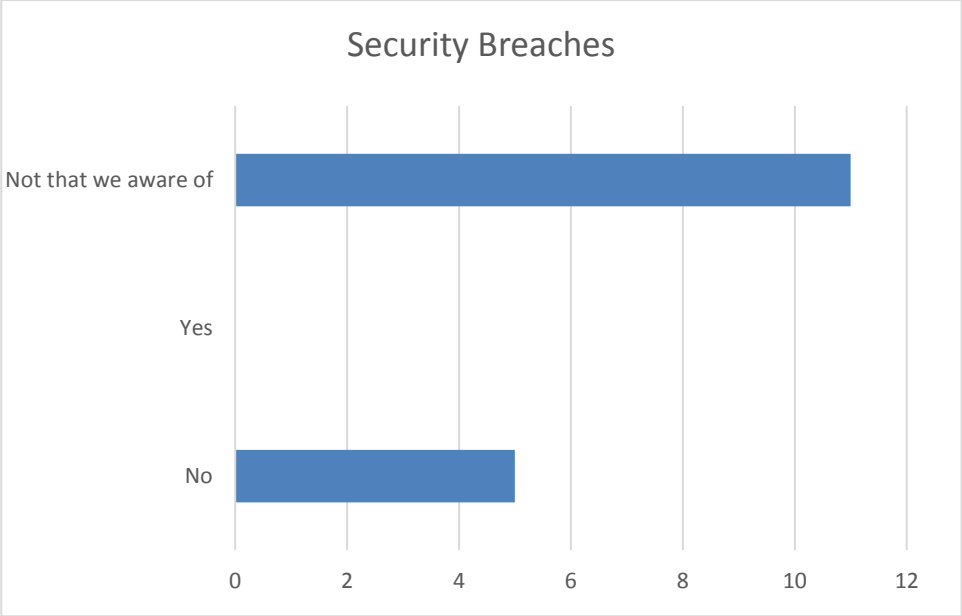


Figure 21: Were there any security breaches with the online assessment system

Most of the respondents (69%) were not aware of any security breaches while they are using the online assessment system. Not one of them indicated that there were security breaches while they were utilising online assessments.

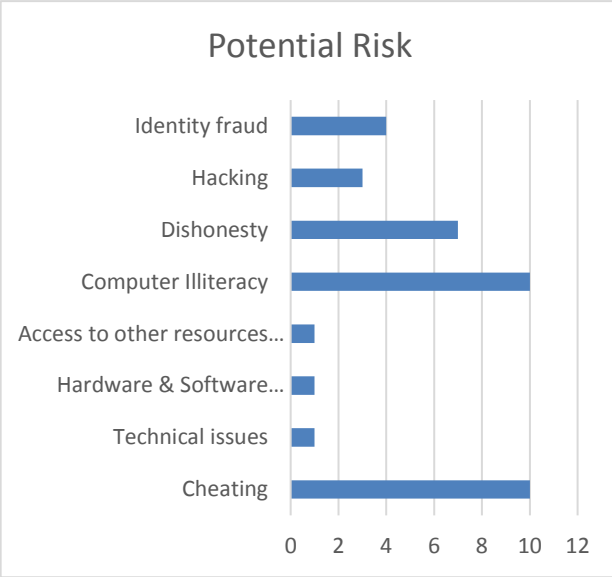


Figure 22: Potential Risks identified by respondents

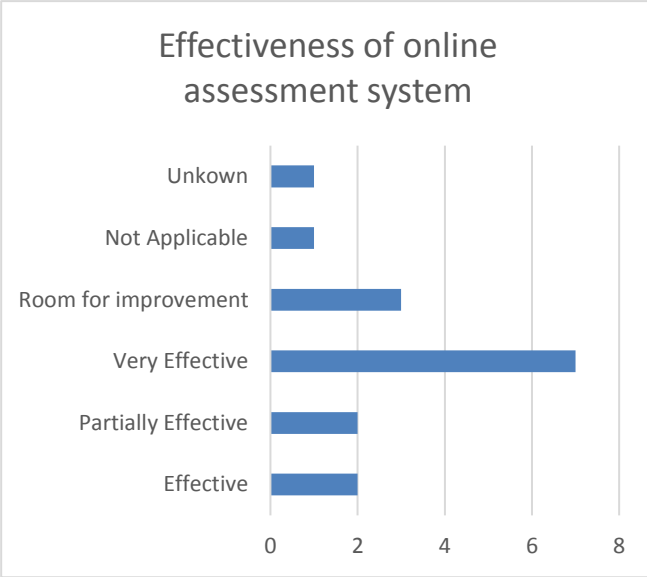


Figure 23: The effectiveness of the online assessment systems used by respondents

The respondents have identified potential risks to the online assessment system with Computer Illiteracy and Cheating (63%) being the forerunner. In Figure 23, the respondents have indicated the effectiveness of the online assessment systems with the majority of them (44%) feeling that their systems were “Very Effective”.

Section C - The challenges and security measures that respondents experienced with their online assessments

Challenges

Cheating

A common thread that ran through this section of the questionnaire was that a challenge for the larger amount of respondents were possibilities for cheating.

Respondent 2: *"Cheating; online searching"*
Respondent 3: *"There is a possibility for cheating and dishonest behaviour amongst the students"*
Respondent 5: *"The only challenge we have is cheating"*

Most of the respondents felt that the close proximity of computers lent itself to cheating. The fact that there is a system like Respondus in place to curb cheating does not seem to act as a determent, but for tertiary institutions that do not have this in place, it is definitely possible for students to do an online search while conducting the assessment. Another challenge received from the respondents is that if students are left alone, they might get help from someone else.

Another challenge that was mentioned was that students can take or conduct assessments on behalf of one another, sometimes through payment which again comes down to cheating and dishonesty. It was also felt that there are no measures in place to ensure that the actual student is the one doing the assessment.

Respondent 14: *"Anyone can complete an assessment on your behalf and put in the output as your own".*
Respondent 16: *"Since the students log in using their username and password, there are no measures in place to ensure that the "actual" student (based on the username and password used) is completing the assessment and not another student on their behalf".*

There are various assessment online assessment systems available and some of the online proctoring systems like Respondus and Examity are being used. It seems to be effective in the curbing of the cheating behaviour as shown in the respondent's responses below.

Respondent 4: ***"****Now that we are able to use RESPONDUS the security for the assessments have improved".*
Respondent 9*: "Various system software available on the market has been demonstrated and trailed and possible solutions have been found that would assist in curbing cheating. I.e. Palm scanning, retinal tracking, typing tracking, and behaviour".*

Respondent 10: ***"****For fully online programmes we will use online proctoring (invigilation software) – Examity"*

Cyber Retrieval of Information & Monitoring of Students

The respondents felt that there is a possibility that the information of the assessments can be lost in cyberspace, and they will not be able to retrieve the information. Another concern is that due to technical issues information cannot be retrieved. It was also a concern that students, with their knowledge of technology, could be able to access the computers of the academics to retrieve information like assessment papers. In part, this could be due to the negligence of the academic with regard to security measures they have in place.

Respondent 7: *"Also ensuring that the information is not lost"*

The monitoring of the students, whether in a controlled environment or not, remains a challenge, as well as the volume of the students that are partaking in the online assessment.

Respondent 7: *"The electronic tests/assignments takes places in a monitored environment. All rooms are monitored during the assessment period".*
Respondent 9: *"Monitoring masses of students at once is a challenge every institution face that have implemented online assessments. This, in my view, is the biggest challenge. You may have the best security in place to verify that a student that has logged on to do an online assessment is, in fact, the said student but multiplied by thousands at once would be a challenge".*
Respondent 12: *"Monitoring submissions; Small venues make it easy to cheat"*

Security measures in place

Most of the tertiary institutions that have responded have the basic security measures in place namely a lockdown browser, identity verification and a password on the e-assessments. Some of the lockdown browsers will not allow the student to close the assessment until it is completed. It seems to be the norm to randomise the questions and

response options in order to prevent the same set of questions in the same order. There also seems to be restrictions in place on the availability duration of the assessment.

Another security measure that was mentioned is that there are more invigilators inside the venue where the e-assessment takes place. The number of students at a tertiary institution also seem to be a factor, as huge classes definitely have an impact on the monitoring of the assessment.

Respondent 1: *" Lock down browser; Identity verification; Password on the e-assessment; Randomising questions and response options; Shuffle the order of questions; Restrict availability; Display questions all at once on a separate window; more invigilators during the online assessment:*

Respondent 3: *"We use algorithmic based questions (all students get the same type of question, but with different values). We also randomize questions as well as randomize answers within certain types of questions to prevent dishonest behaviour. A browser that does not allow students to minimize or exit until they have completed an assessment".*

Respondent 8: *"Students are required to bring students cards or some form of identification to venues".*

Respondent 12: *"more tests are set up for separate release"*

Computer Literacy of Students

A common thread seems to be the computer literacy of the students, but it was not clearly spelled out whether it was too advanced or too low. If it is too low, more must be done to ensure that the standards of the student computer skills are upgraded. If it is too high, then more security measures must be put in place to curb the dishonest behaviour.

INTERVIEWS

The responses of the semi-structured questions were recorded and then the interview questions were systematically worked through by first presenting the responses to the interview questions, and then it was followed up with a discussion on the responses.

Presentation of the semi-structured interview data

Question 1: *What challenges do you think Higher Education is facing around the security and implementation of online assessments?*

In the words of one of the interviewee's "the security challenges are huge". They were "very sceptical (negative) about real online assessments" and they further reiterated that "Identification and Authorization of students and constant monitoring is a big problem, specifically if students are allowed to work from individual unsupervised environments".

In the Blackboard environment, the security challenges experienced by one of the interviewee's is to ensure that the controlled environment is manageable. This can be done by making sure that the following security measures are in place - the lockdown of the computer; students not allowed to insert a memory stick; restricting access the internet; students not able to do a screenshot, print or save notes on a machine.

Another interviewee said that the tertiary institution should be concentrating on continuous evaluation as an assessment tool and that a "formal exam should only constitute 20% of the marks". Technology seems to be a challenge as an interviewee says "The technology will

be redefined in the next few years and more role players will step into this field". A positive spin on this is that as more role players step into this field, the cost will decrease.

A recommendation by one of the interviewees is that a tertiary institution "must have a strong IT division; they must have a learning management system like Blackboard and the academics must be skilled and have the necessary knowledge".

Capacity building is needed for the academics in the use of the online assessments. How to use the online tools for assessment purposes, how you structure the test, feedback provided, how you scaffold the students, how many opportunities you allow the students states another interviewee. Furthermore, they say that "to drive change you have to change the habits of the academics".

A major challenge for one of the interviewees is "appropriate contextual staff development". Which tools and services are suitable for each kind of assessment?

Question 2: *What security measures do you think tertiary institutions must put in place to curb cheating?*

An interviewee felt that in an unsupervised environment they “do not see any proper secure solution at this time”. Another one feels that authentication is a problem, but in a controlled environment, namely a computer lab, the problem is lessened. However, when an academic goes fully online using a system, for example, Examity, it is the responsibility of the system to do online proctoring, which takes the control away from the tertiary institution. The respondents felt that a tertiary institution should also enforce 12 character and more passwords to make it more difficult to hack into academics Blackboard credentials.

An interviewer has built-in scaffolding in their module which they called "milestone tasks" which ensures that students cannot cheat, as all of the "tasks" before are needed as "scaffolding" to ensure that the final tasks can be done. Group component assignments are also used as a variety of online tools – collaboration classes. A metacognitive process has been built in (thinking of the tasks you have done and then critically reflecting on it). This is done via journaling which is an additional layer on the assessments.

Question 3: *What online assessment systems are your tertiary institution investigating for implementation?*

One of the interviewees feels that Blackboard will still be around a few years, and that Blackboard is aware that they have to innovate and keep up with the latest technology, hence they have come up with Blackboard Ultra which will be launched soon. Other systems that are being investigated is Moodle, Canvas, Google Classroom, Microsoft, and SAP, but Blackboard is used the most in the Western world.

Other systems have been investigated but it is expensive states one of the interviewee's. Examity seems to be the cheapest option as they have the "most functionality for the best price". It is also able to integrate with Blackboard.

Question 4: *What in your opinion is the best platform/tools for online assessment?*

"The learning pedagogy is changing worldwide in that the shift and focus are going to more on machine learning" commented one of the interviewee's. Machine Learning is a subsection of artificial intelligence that says systems are able to learn from data, can see patterns from it and they are able to make decisions without any human interaction (SAS, 2018). A recommendation by one of the interviewees is the flipping of the classroom by continuously testing the student using case applications. Other online tools like Cahoot Google Forms and keeping of a journal are used as additional assessment tools with a link provided to via the Blackboard system. The Blackboard system is then used to capture the mark of the various online assessment tools.

Question 5: *What in your opinion is the advantages and disadvantages of online assessment?*

Advantages of online assessments

“If you can forego a formal exam, a lot of the processes are then redundant, like the printing of exam papers, the cost of physical invigilation and the use of exam venues” states one of the interviewee’s. Another positive of online assessments is that it can be “written all over the world, the system is able to mark the bulk of the assessments and it can be done in a specified time-frame”. You can save a lot of money and time, at-risk students can be identified much quicker and due to advances in technology the online assessment systems cost will decrease.

As per one of the interviewee’s a positive to online assessments is a “pedagogy driven assessment”, which is another form of blended learning which combines online technology assessments with the traditional classroom activities (Panopto, 2018). The benefits of a blended learning model are that students learning is enriched, the active learning strategies are heightened and it could potentially increase the students learning outcomes (Pizzi, 2014).

Another interviewee states that you have to ensure that there is no fraud from the student's side via authentication. The storage on the tertiary institution's servers has to be secure and access has to be restricted. Biometric authentication then becomes more important to ensure that the student is who he claims to be. The digital signature also comes into play which is the ability to “access, view and sign documents online” (Cryptomatic, 2018). Furthermore, it also has the ability to identify keystrokes and is able to authenticate the authenticity of the person (Cryptomatic, 2018).

The value proposition to the academics is the collecting of data on the various assessments tools. In addition to the “scholarship of teaching and learning the lecturer can derive publications from the set of data provided”. This angle is used to sell the use of online assessments to the academics. The data can be used to advance the academics teaching strategy, as well as improving their teaching and learning.

Disadvantages of online assessments

A concern raised by one of the interviewees was that tertiary institutions must ensure that everything that goes to a social media platform cannot be hacked with Digital Badging. A digital badge is an authenticated display of a student's qualification via online websites (Hastac, 2018).

If a curriculum is poorly designed it will frustrate both the student and the lecturer. A lot of thought must go into the planning of the assessment. Not all of the academics possess the necessary capacity and skills to do this.

One of the interviewees thinks that “it is very risky and dangerous if not controlled properly” and that they “do not know how it can be done in an unsupervised environment”.

Another con of online assessments is that it is not fully developed to handle questions that require paragraph answers. You can do a keyword search, but it is not fail-proof.

Most of the online assessment systems are not based locally, but mostly in the United States of America, in cities like Washington and Natick hence the cost due to the exchange rate.

The sharing of credentials remains a risk and has to be monitored via a tertiary institution's online policy and through a strong ICT department.

Question 6: *What are the barriers to online assessment at your institution?*

An interviewee felt that computer literacy of the academic staff is a barrier to online assessments, as most of the lecturers are using Blackboard as a "dumping site" instead of properly utilising the full potential of the system. The interviewee feels that you have to be "tech savvy" and that there is lots of help available online if an academic struggle. According to the interviewee, only a "select few are using Blackboard to its full capacity". In America, academics are required to undergo a training session before they are allowed to access Blackboard. At the interviewee tertiary institution, it is not compulsory, you can access the help manuals and then if you struggle, there is a helpline available.

An interviewee states that they are “looking at other channels of assessments for example “couplet modules”; continuous evaluations; and if your semester mark is a certain

percentage there is no need to write the exam. A “couplet module” is a first-semester module followed by the second-semester module where the content of the second-semester module is dependent on the content of the first-semester module, subject to a minimum of 40% obtained for the first-semester module to progress to the second-semester module (UJ Academic Rules and Regulations, 2018).

One of the interviewee’s felt that security is a major barrier to online assessments.

Another interviewee stated that barriers at the tertiary institution are "cost, the need for a specialised system and that the cultural appetite must be ready". A tertiary institution will also get criticism from CHE and SAQA as the qualification has been submitted with different types of assessments. The Higher Education bodies will have to do an audit on how the assessments have changed.

Another barrier is the varying levels of the staff capacity. As per one of the interviewee’s when their faculty implemented teaching-learning strategies one of the strategies was to have learning design consultants in the form of honours students. This lead to academics having to accept the support of the students in co-designing an online assessment module. The power relations had to be addressed and it took time to get a baseline of everyone being on the same page with regard to the Blackboard and assessment environment. The online assessment was designed from the student perspective – what they value and what they do not value. This lead to an improvement in the rigor of the assessment.

A concern raised by an interviewee is the case of plagiarism. The interviewee’s Faculty are using Safeassign and Turnitin as a developmental tool, as it highlights the student’s grammar and spelling in their draft reports. The concern is that not all academics are knowledgeable and trained enough to set up the system to detect plagiarism.

Suggestions and recommendations

- Some of the respondents felt that there should be a time limit placed on the assessment to minimise the risk. But at the same time, if there are technical issues, the time limit could be a hindrance.

- The training of academics on the Blackboard system needs to be relooked at and a suggestion is given that Blackboard must be capable of being able to do more of a “search engine” help.
- Assignments need to be checked for plagiarism using online assessment tools like Turnitin and Safeassign.
- Tertiary institutions have to do research on what the rights of the computer are according to IIS standards.
- In context training to be provided to the academics which is specialised training that is geared towards a specific faculty needs.
- The building in of ‘just-in-time’ support on Blackboard for the academics.
- The focus should be more on the learning experience and a special focus on the student to make the learning experience more enjoyable with the added benefit of improving the throughput rate.
- Tertiary institutions to go on a journey with the academics with special focus groups and learning design consultants to ensure standards of online assessments are met.
- Academics must be encouraged to use Safeassign and Turnitin as an assessment tool and that training must be provided.

DISCUSSION

Introduction

The primary objective of this study was to determine the implementation and security of online assessments. A summary of the research is presented, and the findings of the study will be discussed and analysed. Some limitations to the study have been identified and recommendations and suggestions for further research will follow.

Summary

The focus of this study was to determine which online assessments systems are currently being utilised at South African Higher Education Institutions, how effective have they implemented measures to curb fraud, which online assessment systems are available, and how effective are they in ensuring the security of online assessments?

Socio-demographics

The socio-demographics have shown that there were more respondents from a University than from a University of Technology. South Africa has 26 universities with nine universities of technology, six comprehensive universities and 11 traditional universities (Business Tech, 2015). This ties in with the findings that only about a third of the respondents were from universities of technology.

The bulk of the respondents were from the academic field whether their position was Professor, Senior Lecturer, Lecturer or Instructional Designer.

The findings on the ages of the respondents show that the majority of them were in the age group 51 – 60 and 31- 40. This was interesting as the mistaken belief is that the older adults do not use or do not want to use technology (Olson, O'Brien, Rogers, & Charness, 2011).

The average practice of respondents using online assessments is in the category of 2 – 5 years. This shows the trend that South Africa is moving towards the utilisation of online assessments.

Online Assessment Systems

Various online assessments systems have been researched, but the majority of the tertiary institutions are making use of the Blackboard system for their online assessments. Other systems that are in use are Clickers and Respondus, but it seems that most of the institutions have created their own in-house systems, for e.g. SBLEDS Online, Vula and Wiley Plus.

Although Blackboard is the learning management system of choice, it does not look like it is used to its full capacity by the academics. Although most of the respondents have indicated that training has been provided and that they are effective in the use of online assessments, the interviewee's, when probed, state that extensive training on the Blackboard system should be embarked on.

The effectiveness of the security of online assessment systems

It seems that most of the online assessments take place in the 1st year with semester modules being the norm. It is then easier to expand it to the 2nd year students as they progress to the next level of study. The bulk of the respondents stated that training has been provided and that most of the respondents have been dealing with online assessments for more than 7 – 8 years hence their level of competence seem to be "Very Good".

What could be taken from this research is that the security of the online assessments seem to be effective as most of the respondents are not aware of security breaches? This could also be interpreted that they are confident of the security measures their institutions have put in place for their online assessments.

It appears that most of the tertiary institutions are using online assessments for tests and assignments and not for any formal exams. The majority of the interviewees are concerned that when tertiary institutions move to the more formal type of exams, there have to be better security measures in place with regard to biometric scanning and more upgraded authentications than passwords. There are online proctoring systems available, but most of them are expensive and the packages include that institutions have to pay per student. This means that tertiary institutions with the high volumes of students cost are increased.

Challenges Experienced with online assessment systems

Cheating which includes dishonest behaviour seems to be a theme throughout the findings. Most institutions are concerned that although they put security measures in place, students will still find a way to cheat. It could be impersonating another student, cribbing or cheating online, therefore, the behaviour of the students has to be addressed as a preventative measure.

The monitoring of the students whether in a supervised or unsupervised environment remains a challenge as some tertiary institutions have higher volumes of students than others. In a controlled environment, for example, in a computer lab, security measures could be put in place to curb dishonest behaviour via the computer, as well as with more invigilators in the venue. The unsupervised environment is still fairly new to the tertiary education field, as it seems that the Respondus online system is only used at one university. As one of the interviewee's indicated online proctoring is very expensive, and with the limited financial resources some of the universities find themselves in, due to underfunding of the education sector for years, it will be difficult to implement (Business Tech, 2016).

Limitations of the study

- The sample size of the respondents was too small, and the experiences could be different at other tertiary institutions within South Africa. The lack of responses to the email requests, in spite of numerous follow-ups, was disheartening.
- Due to various factors including time constraints, the interviews could only be done by the University of Johannesburg staff members. This could be interpreted as being bias and only a one-dimensional view was obtained.

Recommendations

The following recommendations are derived from the findings on the implementation and security of online assessments.

- Since the sample size was too small, it is recommended that the research is expanded and that more tertiary institutions participate so that a broader perspective could be obtained.
- The computer illiteracy of the students remain a concern, so a recommendation is made that students are tested at the beginning of their 1st year to determine their computer literacy. If they do not meet the standard, that additional computer training is given to them after their classes, to bring them up to par with their fellow students.
- ICT skills must be a requirement in the teaching qualifications of academics. In addition to a teaching qualification, an academic must be able to prove their computer literacy. By increasing the academics computer literacy, it would increase their use of online assessments, as well as the willingness to experiment with different types of online assessments.
- Other types of online assessments, for example, open book assessments, portfolios and take-home exams are recommended, so that the pressure on physical exam venues are reduced.
- Tertiary institutions must develop a strategy that if there are resources available, to invest in technology. The intention then is that the tertiary institution keeps abreast of the latest technology, and so increase their competiveness within the market.
- Colllabaration between universitities with the sharing of information on the challenges they are experiencing with online assessments.

Suggestions for further research

Listed below are the recommendations for future research within this area

- More research emphasises should be given to the security aspect of online assessments as technology is constantly changing and tertiary institutions must be able to keep abreast of the latest security hacks.

- The focus of this research was only on universities and universities of technology within South Africa. If colleges within South Africa are also incorporated it could further increase the research on online assessments and if their challenges are similar to Universities.

- The research could also be expanded to include tertiary institutions within Africa to get an overview of African institutions, or it could be expanded to international tertiary institutions, to get a grasp of where South African institutions are with regard to their international counterparts.

- Further research could be conducted on the effectiveness of the online assessment systems that tertiary institutions are using.

- Online proctoring effectiveness and if it curbs cheating is another avenue for research.

Conclusion

The implementation of online assessments, and the security around it, at tertiary institutions, is relevant in South Africa today. Due to the advances in technology today, South African institutions must look at alternative ways of assessment which includes online assessments. The research shows that South African tertiary institutions are embracing technology in the form of online assessments. Most of the respondents indicated that they have implemented online assessments for two years and more.

There are barriers and challenges experienced in the implementation of it, but it is not insurmountable. Cheating and dishonest behaviour of the students is a real concern for the successful implementation of online assessments. Most of the tertiary institutions are concerned about the computer illiteracy of the students, and this must be overcome if the implementation of online assessments is going to be sustainable.

The security of the online assessments are a concern for most of the tertiary institutions with all the latest hacking toolkits out on the World Wide Web, but in spite of it, they are forging ahead and gaining valuable experience in the implementation of online assessments. Most of the tertiary institutions are using Blackboard for online assessments and the usage of it could be expanded with advanced training.

The effectiveness of the online assessment systems seems to be on par with international institutions and some of the institutions have incorporated online proctoring systems already, although most of the tertiary institutions are using online assessments within a supervised environment.

South Africa still has a way to go for online assessments. The tertiary institutions started with online tests, so the next step would be to start with online exams. There has been advances within the online proctoring, and therefore tertiary institutions should embrace technology with systems for example UProctor and Examity. This is itself, will throw up different challenges and more security measures that have to be in place.

REFERENCES

alive2green. (2016). SA has the means to make higher education more accessible. Retrieved from http://alive2green.com/sa-means-make-higher-education-accessible/

Aly, E. (2011). *Student's Perceptions towards Computer Based Tests: The Case of Science College* Paper presented at the Edulearn11 Proceedings.

Apampa, K. M., Wills, G., & Argles, D. (2010). User security issues in summative e-assessment security. *International Journal of Digital Society (IJDS), 1*(2), 1-13.

Attia, M. A. (2014). Postgraduate students' perceptions toward online assessment: The case of the faculty of education, Umm Al-Qura university. In *Education for a Knowledge Society in Arabian Gulf Countries* (pp. 151-173): Emerald Group Publishing Limited.

Australian Computer Society. (2016). Cybersecurity - Threats, Challenges, Opportunities. Retrieved from https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

Bailie, J. L., & Jortberg, M. A. (2009). Online learner authentication: Verifying the identity of online users. *Journal of Online Learning and Teaching, 5*(2), 197.

Baloyi & Isaacs. (2015). #FeesMustFall: What are the student protests about? Retrieved from http://edition.cnn.com/2015/10/27/africa/fees-must-fall-student-protest-south-africa-explainer/index.html

Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58*(1), 49-69.

Birenbaum, M., Breuer, K., Cascallar, E., Dochy, F., Dori, Y., Ridgway, J., . . . Nickmans, G. (2006). A learning integrated assessment system. *Educational research review, 1*(1), 61-67.

Brace, I. (2018). *Questionnaire design: How to plan, structure and write survey material for effective market research*: Kogan Page Publishers.

Brynard, P., & Hanekom, S. (1997). *Introduction to research in Public Administration and related academic disciplines*: JL van Schaik Academic.

Business Tech. (2015). Here are South Africa's 26 universities. Retrieved from https://businesstech.co.za/news/general/101412/here-are-south-africas-26-universities/

Business Tech. (2016). 16 universities in South Africa in financial distress. Retrieved from https://businesstech.co.za/news/general/134432/16-universities-in-south-africa-in-financial-distress/

BusinessDictionary. (2017). cracker. Retrieved from http://www.businessdictionary.com/definition/cracker.html

Campbell, D. T., & Stanley, J. C. (2015). *Experimental and quasi-experimental designs for research*: Ravenio Books.

Cizek, G. J. (1999). *Cheating on tests: How to do it, detect it, and prevent it*: Routledge.

Clarke, N. L., & Furnell, S. (2007). Advanced user authentication for mobile devices. *computers & security, 26*(2), 109-119.

Creswell, J. W., & Clark, V. L. P. (2017). *Designing and conducting mixed methods research*: Sage publications.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*: Sage publications.

Cryptomatic. (2018). What is a Digital Signature - What it Does, How it Works. Retrieved from https://www.cryptomathic.com/news-events/blog/what-is-a-digital-signature-what-it-does-how-it-works

Curtin, R., Presser, S., & Singer, E. (2000). The effects of response rate changes on the index of consumer sentiment. *Public opinion quarterly, 64*(4), 413-428.

Deal, W. F. (2002). Distance learning: Teaching technology online. Resources in Technology. *Technology Teacher, 61*(8), 21-26.

Denscombe, M. (2003). The good research guide Maidenhead. In: Open University Press.

DePaula, R. (2003). *A new era in human computer interaction: the challenges of technology as a social proxy.* Paper presented at the Proceedings of the Latin American conference on Human-computer interaction.

Dermo, J. (2009). e-Assessment and the student learning experience: A survey of student perceptions of e-assessment. *British Journal of Educational Technology, 40*(2), 203-214.

Dictionary.com. (2017). spyware. Retrieved from http://www.dictionary.com/browse/spyware?s=ts

Edling, R. J. (2000). Information technology in the classroom: experiences and recommendations. *Campus-Wide Information Systems, 17*(1), 10-15.

Education Reform. (2014). Formative Assessment Definition. Retrieved from http://edglossary.org/formative-assessment/

Examity. (2017). Online Proctoring Poised to go Mainstream. Retrieved from https://examity.com/

Fleisch, B. (2008). *Primary education in crisis: Why South African schoolchildren underachieve in reading and mathematics*: Juta and Company Ltd.

Furnell, S. (2007). An assessment of website password practices. *computers & security, 26*(7-8), 445-451.

Gernetzky & Madibogo. (2015). Damage caused by arson attack at UJ estimated at R100 million. Retrieved from https://www.timeslive.co.za/news/south-africa/2016-05-16-damage-caused-by-arson-attack-at-uj-estimated-at-r100-million/

Hard, S. F., Conway, J. M., & Moran, A. C. (2006). Faculty and college student beliefs about the frequency of student academic misconduct. *The Journal of Higher Education, 77*(6), 1058-1080.

Harmon, O. R., & Lambrinos, J. (2008). Are online exams an invitation to cheat? *The Journal of Economic Education, 39*(2), 116-125.

Hasson, M. (2016). Research Population. Retrieved from https://www.academia.edu/5563491/Research_Population

Hastac. (2018). Digital Badges. Retrieved from https://www.hastac.org/initiatives/digital-badges

Heberling, M. (2002). Maintaining academic integrity in online education. *Online journal of distance learning administration, 5*(2).

Henard, F., & Leprince-Ringuet, S. (2008). The path to quality teaching in higher education. *Paris: OCED Publication.–2008*.

Hesse-Biber, S. N., & Leavy, P. (2010). *The practice of qualitative research*: Sage.

Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: a tool for information security. *IEEE transactions on information forensics and security, 1*(2), 125-143.

Joint Information Systems Committee. (2009, 2017). JISC. Retrieved from https://www.jisc.ac.uk/

Katz, J., Ostrovsky, R., & Yung, M. (2009). Efficient and secure authenticated key exchange using weak passwords. *Journal of the ACM (JACM), 57*(1), 3.

Kennedy, K. A. (2012). An Analysis of Fraud: Causes, Prevention, and Notable Cases.

Kimberlin, C. L., & Winterstein, A. G. (2008). Validity and reliability of measurement instruments used in research. *American Journal of Health-System Pharmacy, 65*(23), 2276-2284.

King, C. G., Guyette Jr, R. W., & Piotrowski, C. (2009). Online exams and cheating: An empirical analysis of business students' views. *Journal of Educators Online, 6*(1), n1.

Klett, F., & Pharow, P. (2006). *How to Achieve User Satisfaction in Complex E-Learning Environments.* Paper presented at the Information Technology Based Higher Education and Training, 2006. ITHET'06. 7th International Conference on.

Kruger, H., Steyn, T., Dawn Medlin, B., & Drevin, L. (2008). An empirical assessment of factors impeding effective password management. *Journal of Information Privacy and Security, 4*(4), 45-59.

Kumar, S., & Dutta, K. (2011). Investigation on security in lms moodle. *International Journal of Information Technology and Knowledge Management, 4*(1), 233-238.

Kumar, S., & Phrommathed, P. (2005). *Research methodology*: Springer.

Lathrop, A., & Foss, K. (2000). *Student cheating and plagiarism in the Internet era. A wake-up call*: ERIC.

LeCompte, M. D., & Goetz, J. P. (1982). Problems of reliability and validity in ethnographic research. *Review of educational research, 52*(1), 31-60.

Levy, Y., Ramim, M. M., Furnell, S. M., & Clarke, N. L. (2011). Comparing intentions to use university-provided vs vendor-provided multibiometric authentication in online exams. *Campus-Wide Information Systems, 28*(2), 102-113.

LifeWire. (2018). What Is a Network Sniffer? . Retrieved from https://www.lifewire.com/definition-of-sniffer-817996

Llamas-Nistal, M., Fernández-Iglesias, M. J., González-Tato, J., & Mikic-Fonte, F. A. (2013). Blended e-assessment: Migrating classical exams to the digital world. *Computers & Education, 62*, 72-87.

Logic Consulting. (2017). Research Techniques. Retrieved from http://www.logicconsulting.co.uk/uploads/1/0/4/2/10429881/1362994_orig.png?698

Love, T., & Cooper, T. (2004). Designing online information systems for portfolio-based assessment: Design criteria and heuristics. *Journal of Information Technology Education: Research, 3*, 65-81.

Luminita, D. C. (2011). Information security in E-learning Platforms. *Procedia-Social and Behavioral Sciences, 15*, 2689-2693.

Marais, E., Argles, D., & von Solms, B. (2006). Security issues specific to e-assessments. *The International Journal for Infonomics*.

Mathers, N., Fox, N., & Hunn, A. (2007). Surveys and questionnaires. *Trent: RDSU*.

Mays, M. (2012). Chapter 12 Misbehavior in Online Testing. In *Misbehavior Online in Higher Education* (pp. 243-260): Emerald Group Publishing Limited.

McCabe, D. L., Trevino, L. K., & Butterfield, K. D. (2002). Honor codes and other contextual influences on academic integrity: A replication and extension to modified honor code settings. *Research in higher Education, 43*(3), 357-378.

McNamara, C. (2009). General guidelines for conducting interviews. Retrieved January 11, 2010. In.

Miguel, J., Caballé, S., Xhafa, F., & Prieto, J. (2014). *Security in online learning assessment towards an effective trustworthiness approach to support E-learning teams.* Paper presented at the Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on.

Mintz, A. P. (2002). *Web of deception: Misinformation on the Internet*: Information Today, Inc.

Mohammad, A.-S., & Gütl, C. (2008). Past, present and future of e-assessment: Towards a flexible e-assessment system. *Institute for Information Systems and New Media (IICM), TU-Graz, Austria*.

Moore, D. L., & Tarnai, J. (2002). Evaluating nonresponse error in mail surveys. *Survey nonresponse*, 197-211.

Morris, R., & Thompson, K. (1979). Password security: A case history. *Communications of the ACM, 22*(11), 594-597.

Nworgu, B. G. (2006). Educational research: Basic issues and methodology. *Nsukka: University Trust Publishers*, 45-49.

Olson, K. E., O'Brien, M. A., Rogers, W. A., & Charness, N. (2011). Diffusion of technology: frequency of use for younger and older adults. *Ageing international, 36*(1), 123-145.

Panopto. (2018). What is Blended Learning? Retrieved from https://www.panopto.com/blog/what-is-blended-learning/

Patton, M. Q. (2005). *Qualitative research*: Wiley Online Library.

Phaladi. (2016). UJ fire to cost the University R100m. Retrieved from https://citizen.co.za/news/south-africa/1117855/uj-fire-to-cost-the-University-r100m/

Pizzi, M. A. (2014). Blended learning pedagogy: the time is now! *Occupational therapy in health care, 28*(3), 333-338.

Prochaska, F. (2016). Internal & External Validity. Retrieved from www.sjsu.edu/...prochaska/.../ScWk-240-Week-5-2nd-Set-Slides---Internal-and-Exter...

ProctorU. (2017). Online Exam Proctoring for Academic Institutions. Retrieved from https://www.proctoru.com/academic-institutions

Raitman, R., Ngo, L., Augar, N., & Zhou, W. (2005). *Security in the online e-learning environment.* Paper presented at the Advanced Learning Technologies, 2005. ICALT 2005. Fifth IEEE International Conference on.

Robson, P. (2002). *The economics of international integration*: Routledge.

Rogers, C. F. (2006). Faculty perceptions about e-cheating during online testing. *Journal of Computing Sciences in Colleges, 22*(2), 206-212.

Rovai, A. P. (2000). Online and traditional assessments: what is the difference? *The Internet and Higher Education, 3*(3), 141-151.

Rowe, N. C. (2004). Cheating in Online Student Assessment: Beyond Plagiarism. *On-Line Journal of Distance Learning Administration, Summer*.

Saikkonen, R., Malmi, L., & Korhonen, A. (2001). *Fully automatic assessment of programming exercises.* Paper presented at the ACM Sigcse Bulletin.

SAS. (2018). Machine Learning - What it is and why it matters. Retrieved from https://www.sas.com/en_za/insights/analytics/machine-learning.html

Scambray, J., & McClure, S. (2001). *Hacking Exposed Windows 2000: Network Security Secrets and Solutions*: McGraw-Hill Professional.

Schauffhauser. (2017). Indiana U High School Adopts Examity for Online Proctoring. Retrieved from https://thejournal.com/articles/2017/12/14/indiana-u-chooses-examity-for-online-proctoring.aspx

Sewell, J., Frith, K. H., & Colvin, M. M. (2010). Online assessment strategies: A primer. *Journal of Online Learning and Teaching, 6*(1), 297.

Sheard, J., & Dick, M. (2003). *Influences on cheating practice of graduate students in IT courses: what are the factors?* Paper presented at the ACM SIGCSE Bulletin.

Shute, V. J. (2009). Simply assessment. *International Journal of Learning and Media, 1*(2), 1-11.

Singer, E., Van Hoewyk, J., & Maher, M. P. (2000). Experiments with incentives in telephone surveys. *Public opinion quarterly, 64*(2), 171-188.

Slattery, E. L., Voelker, C. C., Nussenbaum, B., Rich, J. T., Paniello, R. C., & Neely, J. G. (2011). A practical guide to surveys and questionnaires. *Otolaryngology--Head and Neck Surgery, 144*(6), 831-837.

Stiggins, R. (2008). A call for the development of balanced assessment systems. *Assessment Manifesto). Portland, OR: ETS Assessment Training Institute*.

Stiggins, R. J. (1995). Assessment literacy for the 21st century. *Phi Delta Kappan, 77*(3), 238.

Strom, P. S., & Strom, R. D. (2007). Curbing cheating, raising integrity. *The Education Digest, 72*(8), 42.

Stuber-McEwen, D., Wiseley, P., & Hoggatt, S. (2009). Point, click, and cheat: Frequency and type of academic dishonesty in the virtual classroom. *Online journal of distance learning administration, 12*(3), 1-10.

Sun, J., Ahluwalia, P., & Koong, K. S. (2011). The more secure the better? A study of information security readiness. *Industrial Management & Data Systems, 111*(4), 570-588.

Sun, Z., Paulino, A. A., Feng, J., Chai, Z., Tan, T., & Jain, A. K. (2010). *A study of multibiometric traits of identical twins.* Paper presented at the Biometric Technology for Human Identification Vii.

Sunday, C. (2014). QUALITATIVE DATA ANALYSIS (QDA). Retrieved from https://www.uwc.ac.za/Students/Postgraduate/.../Qualitative%20data%20analysis.pdf

UJ Academic Rules and Regulations. (2018). Couplet Module. Retrieved from https://www.uj.ac.za/about/Documents/University-of-Johannesburg-Academic-Regulations.pdf

Usang, A. I., Archibong, D. O., Aji, E. E., Eyong, C., & Bassey, O. A. (2018). Assessment of influence of student perception, knowledge, and area of specilization on ICT utilization for academic purposes in College of Health Technology, Calabar. *International Journal of Medicine and Medical Sciences, 10*(3), 36-41.

Virginia Commonwealth University. (2017). The Center for Teaching and Learning Excellence. Retrieved August 18, 2017, from https://ctle.vcu.edu/about/assessment-evaluation/. Retrieved from https://ctle.vcu.edu/about/assessment-evaluation/

Volery, T., & Lord, D. (2000). Critical success factors in online education. *International journal of educational management, 14*(5), 216-223.

Vosylis, R., Žukauskienė, R., & Malinauskienė, O. (2012). COMPARISON OF INTERNET-BASED VERSUS PAPER-AND-PENCIL ADMINISTERED ASSESSMENT OF POSITIVE DEVELOPMENT INDICATORS IN ADOLESCENTS'SAMPLE. *Psichologija/Psychology, 45*.

Walliman, N. (2016). *Social research methods: The essentials*: Sage.

Wang, Z., & Sun, Y. (2014). E-education in an open distance university.

Wankel, L. A., & Wankel, C. (2012). *Misbehavior online in higher education*: Emerald Group Publishing Limited.

Webb, M., Gibson, D., & Forkosh-Baruch, A. (2013). Challenges for information technology supporting educational assessment. *Journal of Computer Assisted Learning, 29*(5), 451-462.

Weir, C. S., Douglas, G., Carruthers, M., & Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. *computers & security, 28*(1-2), 47-62.

What Are Cookies.com. (2018). What Are Cookies explained. Retrieved from http://www.whatarecookies.com/

WhatIs.com. (2017). wiki. Retrieved from http://searchmicroservices.techtarget.com/definition/wiki

Zohrabi, M. (2013). Mixed method research: Instruments, validity, reliability and reporting findings. *Theory and Practice in Language Studies, 3*(2), 254.