Critical Spective Reflectivity on Open and Distance Learning (ODL) Assessment Rigidity: Keeping Pace with Security Measures of Assessment Modalities

J. Nyoni
Department of Educational Leadership and Management
South Africa. nyonij@unisa.ac.za

Segue B. A.
Department of Curriculum and Instructional Studies
South Africa. segoeba@unisa.ac.za

Doi:10.5901/mjss.2013.v4n3p101

Abstract

Critical spective reflectivity draws on very different ways of thinking about reality as well as a different way of thinking about securing assessment modalities in open and distance learning (ODL). We use the praxis: the need for self-conscious and ethical action based on a critical questioning of past actions and future possibilities to critically explore how secure assessment instruments in ODL are in order to keep up with security measures given the availability of a plethora of information communication technologies (ICTs) affordances. This article looks at the concept of critical spective self-reflectivity as a basis for an inquiry into what could be alternative methodologies of security. We suggest that reflective processes could offer important alternatives to the existing dominant and rigid security tools used for securing examination tools or instruments. In this article we do not seek to question the existing security tools, but to explore new ways of thinking about the need for appropriate stringent, adaptive security tools that can be used for protecting the reliability and integrity of those examination tools in an attempt to minimise the possibilities of compromising and breaching security in ODL.

Keywords: spective critical reflectivity; open and distance learning (ODL); conventional rigidity; summative and informative assessment methodologies.

1. Introduction

Open distance learning (ODL) is considered to be the most viable means for broadening educational access while improving the quality of education, advocating peer-to-peer collaboration and giving the students/learners a greater sense of autonomy and responsibility for learning (Calvert, 2006; Peters, 1998; Keegan, 1993; Knowles, 1978; Holmberg, 1989). From a postmodern, critical point of view, we believe that, new technology comprises the world of computers (mainframe and personal computers and computer networks), communication systems and further inventions of electronics, “What counts is no longer raw muscle power, or energy, but information” (Bell, 1976: 127). This has already changed many work processes structurally and will continue to do so. As production will increasingly make use of more efficient communication networks, ‘the physical location of an enterprise is no longer really important’ (Norman, 1975: 321). In addition, the work place of an employee can be chosen at leisure (Peters, 1989: 73) – with the help of computer terminals it can also be at his or her place of residence. This development has already begun. Perhaps the change from industrial technology to new technology will be as fundamental as the change from the craftsman's technology to industrial technology.

However, we strongly believe (given the rapidity of digitising ODL mediation processes and introducing appropriate mediation tools in post-industrial societal developments; and postmodern changes in values using industrialised processes) that ODL institutions are engaged in large-scale ODL operations; labour is divided into interdependent subunits; and tasks are assigned to various staff members who work in conjunction to achieve institutional goals as Peters (1989) had predicted. One fundamental prediction peddled by Peters (1989) and supported by Taylor (2002) is the fact that post-industrialised societal developments would be dominated by information and communication technologies (ICTs). However, ODL assessment tools have remained conventionally rigid despite the rapid growth of the student body and the availability of tools that could be used for assessing the knowledge, skills and performance of students. The critical reflectivity theory helps us to acknowledge the rigidity of conventional assessment which regards exit summative
assessment as the most preferred assessment methodology in ODL despite the availability of other more appropriate and effective e-assessment tools that can equally provide a holistic picture of the students’ achievements. Using the same critical perspective reflectivity theory, we simultaneously analyse security measures designed to collate and secure examination instruments given the exponential growth of students and ICTs designed to handle such processes. We critically reflect on institutional security measures around generating, producing, storing and dispatching open examination hard copies between the examining entity and examination centres directly or indirectly involved with examination at an ODL institution.

How could ODL higher educational institution examinations be generated and secured to avoid breaches, compromises or leaks?

Theoretical framework underpinnings

According to Dewey (1933), “reflective thinking, involves (1) a state of doubt, hesitation, perplexity, mental difficulty, in which thinking originates, and (2) an act of searching, hunting, inquiring, to find material that will resolve the doubt, settle and dispose of the perplexity” (Dewey, 1933: 12) Invariably the entire process of ‘reflection’ is aimed at a solution for the perplexity by exploring in the realm of the security of assessment practices in the case of our study. Reflective practice is the: “capacity for thinking about innovative actions while involved with the rigors of security of assessment practices. This active consideration of one’s knowledge and behaviour assists in reconfiguring the building blocks of practice, and enables the professional to cope more successfully with novelty and uncertainty of security of assessment practices for a more appropriate response” (Mott, 1994: 12).

Reflection as used in the context of open and distance learning (ODL) is actually closer to what Schon (1983, 1988) refers to as “reflection-for-action:” a combination of “reflect-on-action”, undertaken after the fact, and “reflection-in-action”, spontaneously occurring in the midst of action itself. With the prime goal of improving examination security practice, reflection-for-action enables practitioners to determine the efficacy of their actions, and is a precursor to practice interventions, theories-in-use, or “adjustments-in-action” (Mott, 1994).

It is in this state of reflection-for-action that inquiry and reflective theory building begins. According to Schon, (1988: 34) theories-in-use represent the synthesis of both formal and explicit theories; and the informal and incidental knowledge that guides the action of practitioners. In “unfamiliar situations when the problem is not initially clear and there is no obvious fit between the characteristics of the situation and the available body of theories”, theories-in-use are constructed by the practitioner to fill the gaps and extend one’s technical knowledge. An important element in the promotion and use of reflective theory building is, of course, a sufficient level of expertise; one of firmly understanding and applying the tenets of one’s practice reflectively “to develop and test new forms of understanding and action where familiar categories and ways of thinking fail” (Schon, 1988: 40, 1992).

Lecturers use a range of assessment techniques to ensure that assessment is educationally sound and appropriate to the discipline or field of study; that all outcomes are assessed; and that the criteria of validity, reliability, authenticity and feasibility are met. No single assessment method can fully assess a student’s learning. It is necessary to use a set of assessment methods to achieve consistent and fair results. The total assessment package for a module/learning programme should be carefully designed to cover all the learning outcomes. The assessment type(s) used will also be suited to the underlying teaching/learning principles outlined in the tuition policy, the learning students need to evidence the level of the module and diverse student abilities, learning styles, and contexts. The constraints of ODL and the particular tuition model should be considered as well. Summative assessment will measure, record and report on the achievement of exit-level outcomes. It may take a form other than an examination such as the submission of a portfolio of evidence or reports from workplace mentors. Reflectivity theory makes it easier and appropriate for practitioners to evaluate how such assessment instruments are secured to protect the integrity and credibility of the outcomes.

Assessment in open and distance learning (ODL)

In South Africa, and in other countries, the most common assessment methodologies in open and distance learning (ODL) are formative and summative; e-assessments are utilised on rare occasions. Formative assessment helps students and staff to identify strengths, weaknesses and ways of improving and enhancing learning attainment; whereas summative assessment provides information to judge the extent to which a student has achieved objectives relevant to the graduate qualities in a course or programme. However, the advent of technological advancement has not triggered
the need of ODL institutions to adapt their assessment methodologies to exploit some e-assessment methodologies. Assessment instruments are usually generated at institutional level. These instruments normally go through a number of interrelated systems and/or sub-systems before they are produced and dispatched to different centres for examination processes. Before the processes can unfold, the generation of examination instruments, proofreading, production and dispatch follow a systematic approach (see Figure 1 with checks and balances in each systemic step).

The adaptability of a systems approach to enhance credibility, reliability and dependability of assessment methodologies in ODL

Figure 1: Critical spective reflectivity serves as a mirror that constantly reflects a systems approach as an orderly process that helps to reflect on the security measures on which institutions embark from time to time. A systems approach also recognises that all the components of the system are interrelated. A change in one component will bring about changes in the others – hence, the need to do risk assessment from time to time to tighten any loopholes and inadequacies. Institutions use cyclic reflective risk assessment to continuously monitor and improve on security measures in order to ward off security risks and threats.

The examining institution is, therefore, obliged to take reasonable steps in order to protect the integrity of the examinations and guard against unauthorised access, use, modification or disclosure and misuse. This obligation includes the management of the examination process, the submission of examination tasks which include the utilisation of cover sheets, the sorting of examination papers, the management of examination processes at examination venues and the provision of results and feedback to students. Critical reflectivity theory helps to revisit these processes in order to tighten security minimising chances for breaching and compromising security systems.

Examination management systems

Academic dishonesty has always been a major concern for many universities, because it cuts through the heart of the pursuit of knowledge and the purpose of higher education (Lambert, Hogan and Barton, 2003). Many researchers in higher education institutions of various countries have studied this social phenomenon in detail (Whitley, 1998; McCabe, Butterfield & Trevino, 2006). It involves the use of unauthorised devices or processes while doing e-assessment and paper-based assessment.

Unauthorised devices would mean using cellphones, texting, or having a standby tablet or computer while doing an online assessment; and having another window open or script tools running in the same online assessment environment. Those who are more competent would even venture to hack a course site and adjust the computer clock to make it look like emails were sent much earlier than they were actually sent.

Cyclic spective reflective risk assessment model

Underpinned by reflectivity theory, ODL institutional risk assessments must be undertaken periodically to ascertain whether security measures are still adequate enough to secure assessment processes. Assessment policy guidelines
should provide clauses or a framework for institutions to perform periodic risk assessments and adjust their control mechanisms as appropriate in response to changing internal and external security threats.

The purpose of the security measures for assessment processes is to reinforce the risk management framework and update the policy expectations regarding assessment authentication, layered security, or other controls in the increasingly hostile ICT environment. The cyclic, reflective risk assessment model reiterates and reinforces the expectations contained in security policies that direct institutions to perform periodic risk assessments considering new and existing threats to online interactivities; and adjust their assessment authentication, layered security, and other controls appropriately in response to identified risks. It establishes minimum control expectations for certain online communication activities and identifies controls that are less effective in the current environment. It also identifies specific minimum elements that should be part of an institution’s risks awareness and education programme for the assessors.

As new information becomes available, ODL institutions should review and update their existing risk assessments prior to implementing new electronic financial services at least every twelve months. Updated risk assessments should consider the following factors (but should not be limited to it):

- changes in the internal and external threat environment, including those discussed in the Appendix to this supplement
- changes in the customer base adopting electronic banking
- changes in the customer functionality offered through electronic banking
- actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry

Layered security is characterised by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of another. Layered security can substantially strengthen the overall security of internet-based services and can be effective in protecting sensitive customer information, preventing identity theft and reducing account takeovers and financial losses. It should be noted that other regulations and guidelines also specifically deal with the responsibilities of financial institutions in order to protect customer information and prevent identity theft. Financial institutions should implement a layered approach to security for high-risk internet-based systems.

Methodological underpinnings

The interview schedule comprised six sections grouped around themes such as: obtaining access to examination control centres at institutional level, the security of examination instruments from primary source (examiners), security measures at examination centres, security at production centres, security at the examination storage vault, and the dispatch and collection of scripts. The semi-structured interviews contained several questions to participants. These semi-structured interviews involved three administrators, six primary lecturers and two personnel members from the examination control centre of the Department of Student Assessment and Administration (DSAA)

Table 1: Semi structured interview strategy

<table>
<thead>
<tr>
<th>Units</th>
<th>Number of participants</th>
<th>Frequencies and duration of structured interviews</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foundation phase</td>
<td>2</td>
<td>Two sessions of 40 minutes each for each participant</td>
</tr>
<tr>
<td>Inclusive education</td>
<td>2</td>
<td>Two sessions of 40 minutes each for each participant</td>
</tr>
<tr>
<td>Language education, arts and culture</td>
<td>2</td>
<td>Two sessions of 40 minutes each for each participant</td>
</tr>
<tr>
<td>Departmental administrators</td>
<td>3</td>
<td>one session of 30 minutes each per administrator</td>
</tr>
<tr>
<td>Examination directorate</td>
<td>2</td>
<td>one session of 40 minutes for each participant</td>
</tr>
<tr>
<td>Total</td>
<td>11</td>
<td></td>
</tr>
</tbody>
</table>

Guided by the critical reflectivity theory (partly conceptualised by Schon (1988) to mean “reflection-for-action;” a combination of “reflection-on-action”), we sought to do a risk assessment of examination security measures designed to secure authenticities and credibilities of exit examinations at institutional level to avoid tempering with examinations and compromising the security thereof.

The interviews were discontinued after the first or second interview section and resumed at a later date for reasons such as tiredness, lack of communication, network disconnection, as well as constraints on participants’ time.

Ethical approval for the research was gained from the Ethics Committee of the University of South Africa and the research was conducted according to the guidelines of the Ethics Committee. Pseudonyms were used to ensure the
anonymity of participants during the write-up. Any information that could identify them was either removed or substantially altered. Once each interview was completed, the participants were sent a copy of their transcripts to read through and make additions, alterations or exclusions as desired. The exercise empowered the participants to make changes and play a significant role in retaining the integrity of the interview and securing the participants’ ownership of data.

**Discussion of findings**

The rationale behind utilising critical reflectivity was the author’s concern with fraudsters that increasingly use sophisticated and malicious techniques to thwart existing authentication controls, gain control of students’ assessments portfolios, and disclose illicitly gained examination instruments, in whatever form, to potential examinees for financial gains. Security risk analysis methods and tools were regarded as tools to help researchers make security risk decisions. Critical spective reflective methodology assisted in incorporating the uncertainties and variability in the views of various participants. However, these methods should not be used to shift the focus of security risk assessment to overall numerical summaries at the expense of information on the qualitative differences. We contextualise the use of spective reflection to mean an introspective look at what we are doing in terms of adopting security measures for examinations.

In this article risk assessment is defined as, “the process of estimating and evaluating risk, understood as the possibility of beneficial and harmful outcomes and the likelihood of their occurrence in a stated timescale” (Titterton, 2005: 83). Two models of risk assessment have been identified (Davis, 1996):

- the risk-taking model (risk is normal and positive and the assessment focuses on security measures and systems in place, abilities, examination generation; and examination paper trail)
- the risk minimisation model (targeting those processes most at risk and the assessment focuses on security and control of examination instruments in ODL).

Thematic findings of the semi-structured interviews was underpinned by the following question to participants; How are ODL higher education institution examinations generated and secured to avoid breaches, compromises or leaks? Thematic analysis is the most common form of analysis in qualitative research. It emphasises the pinpointing, examining, and recording of patterns (or themes) in data (Creswell, 2013). Themes are patterns across data sets that are important to the description of a phenomenon and are associated with a specific research question (Creswell, 2013). The themes become the categories for analysis. Thematic analysis was done by coding in six phases to create established, meaningful patterns, namely familiarising oneself with data, generating initial codes, searching for themes among codes, reviewing themes, defining and naming themes, and producing the final report.

1.1 **Gaining access to examination control centres at institutional level**

From observations and through semi-structured interviews we discovered that workers from different departments and units were permitted to enter examination centres without being subjected to security checks despite the fact that examination papers were piled on the tables for processing. In the Department of Student Assessment and Administration (DSAA), two respondents were unable to tell what the acronym DSAA stood for. On closer analysis it was evident that the two employees had never taken time to familiarise themselves with the sensitivities of the operations in the department.

1.2 **Security examination generation and paper trails**

The primary examiners generate examination instruments (examination papers) in consultation with external examiners and moderators. Examination papers are then electronically forwarded to the administration employees who capture the examination papers on the system. Some primary examiners retorted that the administrator checks for typing errors and do not conduct quality assurance:

> “I do not know why should question papers be sent to admin officers...the question papers go through too many hands”

We also noted that security breaches or compromises could occur between the examiner and the administrators before examination papers are conveyed to the DSAA for further processing. The departments did not ensure that new, temporary or contractual academic and administrative staff members are fully briefed about the department’s procedures for securing and delivering examination papers and material during the induction process. It would appear that it was not the case with the DSAA and the departments that participated in the research.
Drafts of examination scripts were not sent by encrypted email, secure fax, memory sticks or on CDs. When making use of e-mail, good practice would be to encrypt the data before sending it. This can be done in many ways, but the most common ways would be to use Word's option for encrypting a document, or an encrypted pdf file, or to send the document as a ZIP file and encrypt it. The recipient can be given the password to decrypt the message via a telephone or other non-computer-based method; thereafter messages can be sent using the same password. There was no evidence that such processes were followed. Administrators also decried the logic behind the idea of relaying examination scripts via their offices:

"Lecturers must format the question papers themselves ...not us. This will help to minimise leakages"

We also noted that it was possible for administrators to come across examination papers that directly link them to their studies. Under such circumstances the integrity of the paper is compromised and it is possible for the particular individual to copy the examination paper before forwarding it to DSAA.

1.3 Security measures at DSAA

If there is a remote possibility that draft or final examination papers might have been seen by unauthorised people, it may be necessary to reset such papers. Before doing so, departments should consult with the relevant authorities to establish whether it is necessary, or whether small changes could be made to core sections of the examination papers that could identify academic misconduct. Where anyone has access to a machine for a required period, it is always possible to read the data from such a machine unless it is encrypted, even if a machine has been switched off or if it has a screensaver that requires a password. Where possible, the data should be stored on a network disk (one of the IT Service’s rented file stores; or a similar storage offered by a department). The study indicated that this was not the case. Data was not physically stored elsewhere and access to the desktop machine mattered much less. The other great advantage of doing this is that it should ensure that the data is backed-up. Administrators were not instructed to take printed copies in sealed envelopes:

"When I take the hard copy to exam... it is not sealed....this poses a high risk"

"Some of us who format question papers are more than likely to come across the examination question paper we are going to write...this is a real blunder"

Their comments were supported by what DSAA employees who said:

"This whole thing does not work...I advised...and advised that we should be provided with a paper scanner so that no person should leave the room with some paper in his/her possession"

The implications of these quotations are that there are minimal/no adequate security checks and balances at DSAA. Employees can simply walk in and out of the centre without being subjected to a security search and/or some form of identity before access is allowed.

1.4 Security at production and dispatch

The DSAA submits examination papers to the production unit where the required number of scripts is printed. The findings pointed to a security lapse at the production unit, because it is possible to generate more examination papers than required. Soon after production, the examination papers are returned to the DSAA for packing and storing the papers before they are distributed to the various examination venues. In this regard one of the officials stated as follows: “We normally/sometimes invite local invigilators to come and assist with counting and packing of examination scripts.” Examination processes could be compromised at this point as the invigilators are trusted with the information. Employees made the following comment in this regard.

"The question papers leak at the exam section....not here"
"I am not sure about control measures at production. Who checks there?"

There appears to be an attempt on the part of DSAA employees to absolve themselves from any blame.
1.5 Security at the examination storage vault

From production, examination scripts are counted and sorted according to examination venues, before they are securely stored in the vault. DSAA employees were adamant that once examination scripts land on their tables, security measures are strictly followed and as pointed earlier, security breaches and/or compromises do not occur at the DSAA centre.

1.6 Dispatch and collection of scripts

Document analysis revealed that there was no security policy for examination paper production available on request. The policy should be developed and communicated to all staff each year before they commence with the production of examination papers. However, findings show that examination papers are sometimes sent to remote examination venues two weeks before the examination date. One can only wonder how secure some of the storage facilities in remote areas are.

“Some question papers, like in far remote areas, could reach those centres two weeks before the actual exam date. This is risky...who checks the question papers before students write?”

Even those involved in securing examination processes doubted their own processes in place.

Summary of findings

Figure 1 provides a synopsis of the examination script paper trail. The examination question paper is generated by the primary examiner in consultation with external examiners and moderators before it is handed over to the administrator. The administrator checks for errors and formats the paper that goes to DSAA in an unsealed envelope. DSAA processes the examination papers in line with the number of scripts required before forwarding it to production. Scripts are then relayed to DSAA for counting, sorting and storage.

Recommendations

Critical spective reflectivity would require that draft examination papers be treated with confidentiality to avoid compromising the security and validity thereof. Computers are used for drawing up examination papers; therefore, attention must be paid to the security of such computers. Departments are strongly advised to use disks, CDs, secure fax or USB flash drives to manage the drafting of examination papers and to ensure that the setting of examination papers do not involve sharing data via e-mail without encrypting such documents beforehand. One should remember that e-mail attachments are not secure and consultations on examination questions should not be shared in this way. All personal computers used for the production of examination papers must:

• only be accessible via user accounts, and a separate account must be used for each user. guest type accounts must not be used.
• bear the labels of the manufacturer and updated at all times
• use a file system that only allows the author or owner of a file to read it
• not be placed on hard drives that are shared by different authors
Examination generation processes should be confined to the DSAA and the primary examiner to minimise opportunistic tendencies for breaching or compromising. Administrators should be totally excluded from the examination processes.

Conclusion

The risk discourse from an organisational perspective, including the influence of organisational culture, accountability frameworks and inter-agency collaboration should continue at times as critical perspective reflectivity suggest, "action in action". The risk discourse also questions whether the security of examinations is currently operating within a conflictual or cooperative model of risk assessment and management. We conclude the study with a summary of the key findings and suggest ways forward for policy and research. The security of examination materials is of utmost importance and departments will already have procedures in place to communicate with colleagues and external examiners and to store examination papers and scripts during the assessment process. The DSAA and Departmental heads want to remind departments to be vigilant and encourage departments to undertake regular reviews of their processes.

References

Mott, V. W. (1994). The role of intuition in the reflective practice of adult educators. proceedings of the 34th Adult Education Research Council Conference, University of Tennessee, Knoxville, TN.