The African Journal of Information Systems

Volume 8 | Issue 2 Article 2

Spring 4-1-2016

A Framework to Manage Sensitive Information during its Migration between Software Platforms

Olusegun Ademolu Ajigini
University of South Africa, ajigioa@unisa.ac.za

John Andrew van der Poll
University of South Africa, vdpolja@unisa.ac.za

Jan H. Kroeze PhD
University of South Africa, jan.kroeze@gmail.com

Follow this and additional works at: https://digitalcommons.kennesaw.edu/ajis

 Part of the Information Security Commons, and the Management Information Systems Commons

Recommended Citation

Ajigini, Olusegun Ademolu; van der Poll, John Andrew; and Kroeze, Jan H. PhD (2016) "A Framework to Manage Sensitive Information during its Migration between Software Platforms," *The African Journal of Information Systems*: Vol. 8 : Iss. 2 , Article 2.
Available at: https://digitalcommons.kennesaw.edu/ajis/vol8/iss2/2

This Article is brought to you for free and open access by DigitalCommons@Kennesaw State University. It has been accepted for inclusion in The African Journal of Information Systems by an authorized editor of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems

The African Journal of Information Systems

A Framework to Manage Sensitive Information during its Migration between Software Platforms

Research Paper

Volume 8, Issue 2, April 2016, ISSN 1936-0282

Olusegun Ademolu Ajigini
University of South Africa
ajigioa@unisa.ac.za

John Andrew van der Poll
University of South Africa
vdpolja@unisa.ac.za

Jan H. Kroeze, PhD
University of South Africa
kroezjh@unisa.ac.za

(*Received December 2014, accepted September 2015*)

ABSTRACT

Software migrations are mostly performed by organizations using migration teams. Such migration teams need to be aware of how sensitive information ought to be handled and protected during the implementation of the migration projects. There is a need to ensure that sensitive information is identified, classified and protected during the migration process.

This paper suggests how sensitive information in organizations can be handled and protected during migrations, by using the migration from proprietary software to open source software to develop a management framework that can be used to manage such a migration process. The research used a sequential explanatory mixed methods case study to propose a management framework on information sensitivity during software migrations.

The management framework is validated and found to be significant, valid and reliable, by using statistical techniques such as exploratory factor analysis, reliability analysis and multivariate analysis, as well as a qualitative coding process

INTRODUCTION

Information is a resource that has strategic value to an organization, and exists in many forms – such as written or printed documents, electronic files, microfilms and videotapes (Fung & Jordan, 2002). Correct information is expected to support decision-making or to provide service at the appropriate time. Therefore, the integrity of the information cannot be compromised, and data protection is vital, in order

for the users to be assured of their privacy and that the data meets the service provider's integrity requirements (Duri et al., 2004).

The management of sensitive information relating to their business ought to be very important to all organizations (Rakers, 2010). Arai and Tanaka (2009) have highlighted the importance of avoiding information leakage in a computer system's handling of a company's sensitive information – for example, during migration of platforms. Sensitive information is regarded as any information which, if leaked, can lead to the destruction of the person or the organization, and may include personal information as well as the organization's information (Nawafleh et al., 2013).

This paper is about the development of a framework to manage sensitive information during its migration between software platforms. This research involves the development and validation of a management framework for the migration of sensitive information during the migration of platforms by using a sequential explanatory mixed methods case study approach.

The rest of the paper is organized as follows: the t first section explains the background to the study. The following section elucidates the research setting and methodology. The quantitative and qualitative data findings are then presented. This is followed by the section on the management framework on migration of platforms. Lastly, the discussion and conclusion of the research are presented.

BACKGROUND

The study concentrates on South African government departments and parastatals that have performed software migrations. The main focus is the development and validation of a management framework that can be used to protect and handle sensitive information during its migration between software platforms. A good example of such platform migration is from Closed Source Software (CSS) to Open Source Software (OSS) – also known as Free Open Source Software (FOSS).
In South Africa, examples of such platform migrations include, but are not limited to:

a) migrations from proprietary systems to open source systems conducted during the eNaTIS migration by the Department of Transport (IT Web, 2007).
b) State Information Technology Agency (SITA) migration to FOSS (GITOC, 2003).
c) Presidential National Commission (PNC) migration to FOSS (PNC, 2007).
d) National Libraries of South Africa (NLSA) migration to FOSS (Novell Connection, 2009).
e) National Department of Arts and Culture migration to FOSS.
f) South African Department of Public Works migration to an open source asset management system

The following problems are envisioned during the migration of sensitive information across platforms:

a) there is the possibility of intruders trying to gain unauthorized access to the system during such migration process (Crossler et al., 2013).
b) viruses and intruders can also invade the system during the migration process (Huth et al., 2013).
c) data integrity needs to be maintained during the migration, and data corruption has to be prevented (Huth et al., 2013).
d) information leakage (Ahmad et al., 2014; Garfinkel, 2014).
e) information theft (Von Solms & Van Niekerk, 2013).
f) identity theft (Kirda & Kruegel, 2005).

g) phishing is an online identity theft that aims to steal sensitive information e.g. passwords of banking clients and client's credit card information (Kirda & Kruegel, 2005).
h) stealing sensitive information – e.g. account details and cookies, and getting hacked during the process (Gupta, 2010).

The view of these authors is that these problems could be proactively resolved, if an organization uses a management framework on sensitive information during platform migrations to guide their migration project implementation – hence the importance of this study.

RESEARCH SETTING AND METHODOLOGY

The focus of this paper is the development of a management framework to manage information sensitivity during software migrations. The research was conducted in some South African government departments and parastatals, located in Pretoria, South Africa that had migrated from proprietary platform to open source platform. Specifically, the migration from Closed Source System (CSS) to Open Source System (OSS) is used to conceptualize the solution to the research problem.

Research Setting

Data is collected from the following organizations, namely State Information Technology Agency (SITA); South African Revenue Services (SARS), Presidential National Commission (PNC), National Libraries of South Africa, South African Department of Arts and Culture, South African Department of Public Works, and South African Department of Social Development. These organizations have performed platform migrations such as migration from a proprietary platform to an OSS platform. The data is then subjected to quantitative and qualitative analysis, to conceptualize the final management framework.

Research Methodologies

Research methods are techniques used for carrying out the research, while a methodology is the set of methods in a research project. Methodology is a strategy of enquiry guiding a set of procedures, while methods are techniques used in analyzing data to create knowledge (Denzin & Lincoln, 2000; Cresswell, 2009; Petty et al., 2012). The case study methodology is used to carry this research by using multiple cases (data triangulation). The mixed methods approach is used in this research to enhance and validate the management framework on information sensitivity. Mixed methods research has been defined by Johnson and Onwuegbuzie (2004) as an approach requiring the researcher to combine the two paradigms (quantitative and qualitative), methods, concepts or language. They argue that a mixed methods approach draws upon the strengths and perspectives of each method by recognizing the existence and importance of reality and influence of human experience.

Mixed methods research is defined by Tashakkori and Creswell (2007) as the collection and analysis of data, and then integrating the findings by drawing inferences from quantitative and qualitative approaches. Case study research is one of the ways of performing social science research, while experiments, surveys, histories and the analysis of archival information are the others (Yin, 2009). Case study research is conducted in an actual life situation by the researcher, and there is no distinction

between the research phenomenon and the real life context, especially when there is no difference between phenomenon and context (Yin, 2009).

The case study research is used as the methodology in this research work, and it is carried out by using the mixed methods approach. Multiple sources of evidence (data triangulation), as explained by Yin (2003), is followed, to conduct this research. The results from these cases are analyzed, using both quantitative and qualitative data analysis to develop the management framework on information sensitivity during the migration of platforms. The case study research is conducted in some South African government departments and parastatals that have performed platform migrations.

Underlying Philosophical Paradigm

Research strategies in Information Systems (IS) differ in their underlying philosophical paradigms and IS researchers are expected to understand the different paradigms underlying their research strategies (Oates, 2006). IS philosophical paradigms include positivism, interpretivism, critical research and pragmatism (Oates, 2006).

The underlying philosophical paradigm used by the researcher is pragmatism, which substantiates the trustworthiness and dependability of the case study research. This is because both quantitative and qualitative methods, in the form of a mixed methods research approach, are employed in this research.

Data Gathering

Data was gathered in the government organizations and agencies that are mentioned in the introductory section. Data triangulation was used to collect the data, that is, data was collected from many different sources, following Yin's (2003) data triangulation methodology. A questionnaire was developed and forwarded to 250 respondents in various government organizations and agencies. The author of this thesis received 90 completed questionnaires. The responses were then collated using a spreadsheet, and the data was imported into the JMP SAS software for data analysis.

The quantitative research questions were enhanced by the qualitative analysis, by using open-ended and in-depth interviews to validate the preliminary management framework that resulted from the quantitative analysis. The qualitative interviews were recorded on tapes, and were later transcribed. Recording requires consent, and ethical clearance was obtained from the University of South Africa's ethics committee. The transcripts were subsequently imported into the NVIVO version 10 software, for further qualitative analysis.

Data Analysis

Two types of data analysis were performed, namely quantitative data analysis and qualitative data analysis, in order to validate the management framework. There was a pilot quantitative data analysis (item analysis) performed to test the reliability of the questions posed in the questionnaire. During this pilot quantitative data analysis, the questionnaire was validated by testing the reliability of the constructs in the questionnaire using item analysis (Cronbach's alpha).

Twenty-five respondents completed the first version of the questionnaire, then the data was analyzed using statistical techniques to validate the constructs and obtain the final questionnaire. The final questionnaire was analyzed using statistical analysis, namely factor analysis, item analysis, and reliability analysis. Factor analysis was used to identify the constructs in the measuring instrument, while item analysis was used to test the reliability of the constructs in a measuring instrument (Tate, 2003; Wiid & Diggines, 2013).

There are two major types of factor analysis, namely (a) Exploratory Factor Analysis (EFA) and (b) Confirmatory Factor Analysis (CFA) (Thompson, 1992; Kahn, 2006). The EFA is used to identify the constructs in this research. The idea is to identify and eliminate the items that do not measure an intended construct or measure multiple constructs that could be poor indicators of the desired construct (Worthinton & Whittaker, 2006). After the pilot quantitative data analysis, the descriptive and correlation analyses were performed.

During the qualitative data analysis, the audio tapes containing the interviews were transcribed and analyzed using the NVIVO software. A bottom-up approach (content analysis) grounded in data was used to develop the management framework on information sensitivity, inductively. The framework was validated using open-ended and in-depth interviews with government organizations that have performed platform migrations.

QUANTITATIVE DATA FINDINGS

This section covers the quantitative data findings in the study.

Biographical Data Distributions

The Biographical Data is the first component in the questionnaire called component A. Some of the Biographical Data Distributions in the research is explained below:

(i) Type/Nature of Respondent Employment

Figure 1 describes the type/nature of respondent employment. The majority of the respondents were from three government organizations, namely SITA, South African Department of Public Works and South African Department of Social Development.

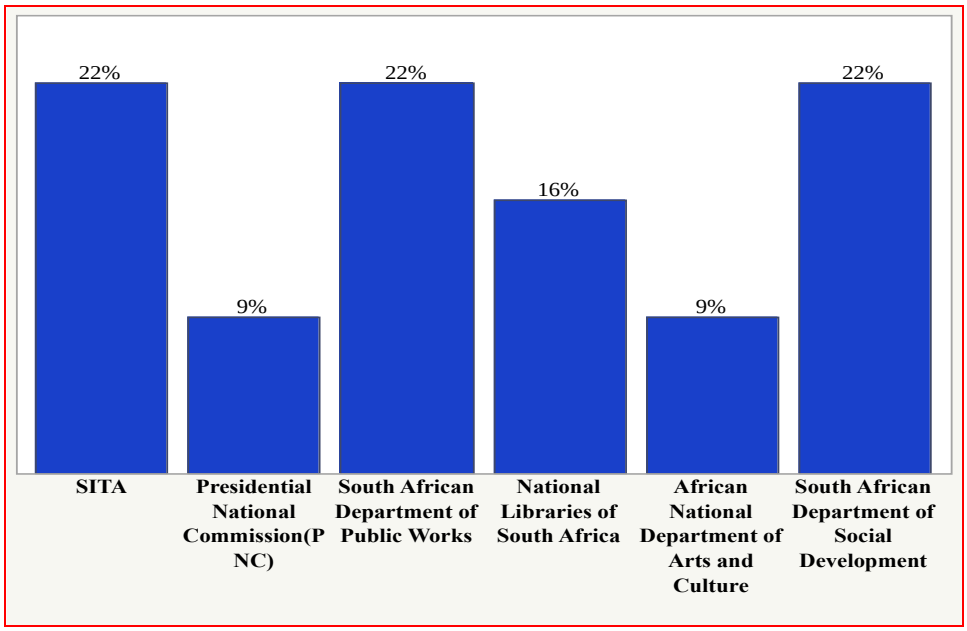


Figure 1. Type/Nature of respondent employment

(ii) Respondent's Post Levels (IT Specialists)

Figure 2 shows the respondents' post levels for the IT specialists. The figure shows that most of the respondents fall into the developers and junior developers (49% and 28% respectively).

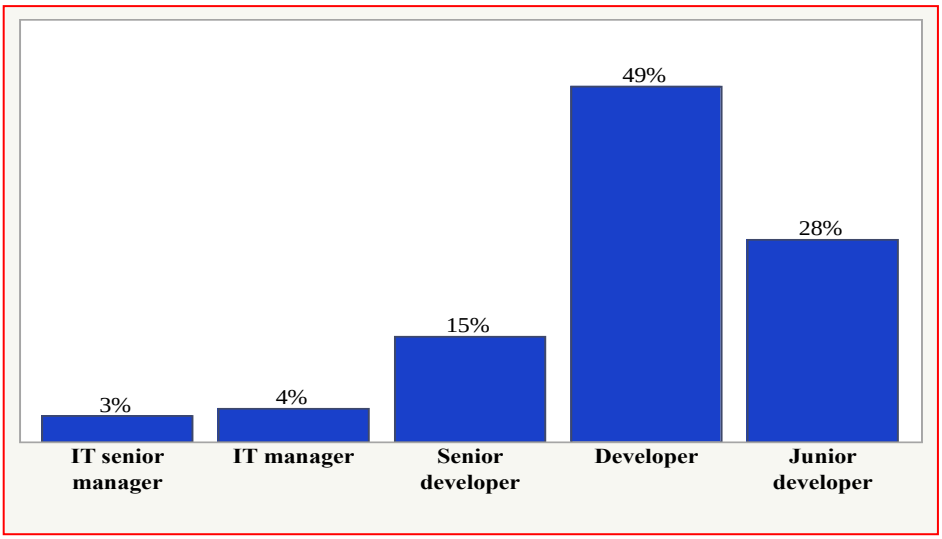


Figure 2. Respondent Post Level (IT Specialists)

(iii) Respondents' Type of Work

Figure 3 depicts the respondents' type of work in their organizations. It shows that most of the respondents work at transferring and loading data/ETL migration and data security/IT security (21% and

34% respectively). This might mean that the majority of the IT respondents are from the data/IT security domain.

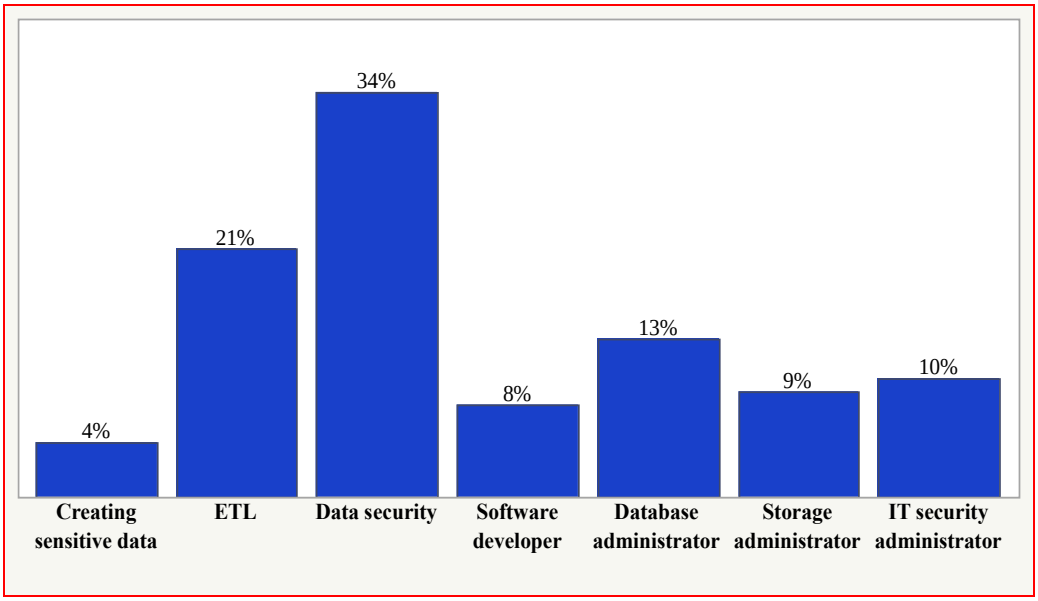


Figure 3. Respondents' type of work

(iv) Respondents' Awareness of Sensitive Data Management Policy

The respondents' awareness of a sensitive data management policy in organizations is depicted in Figure 4. It shows that most of the respondents are aware of a sensitive data management policy in organizations (92%). This shows that there could be an awareness of a sensitive data management policy, among the IT respondents.

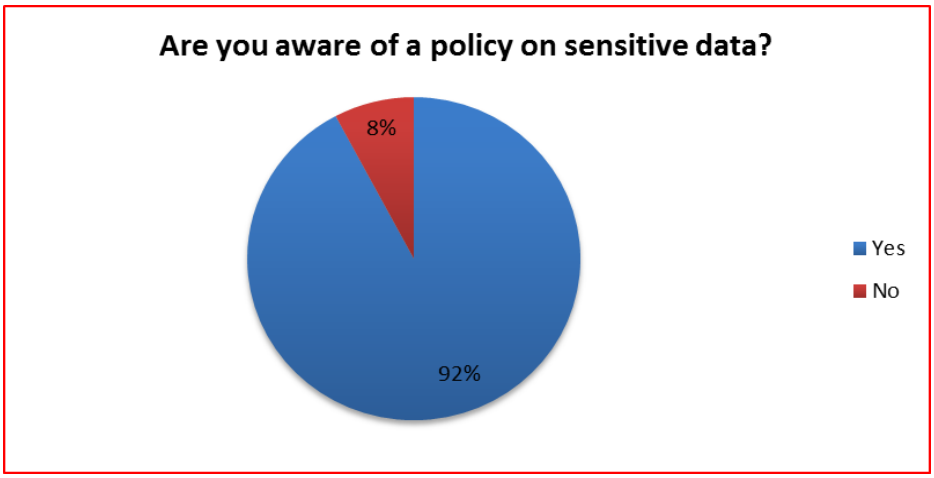


Figure 4.1 Respondents' Awareness of Sensitive Data Management Policy

(v) Respondents' Participation on Platform Migration Projects

The respondents' participation in platform migration projects is shown in Figure 5. This figure reveals that most of the respondents have participated in migration projects (94%). This might mean that most of the respondents have been part of migration projects, and their contributions would be valuable in the research, due to their knowledge in this area.

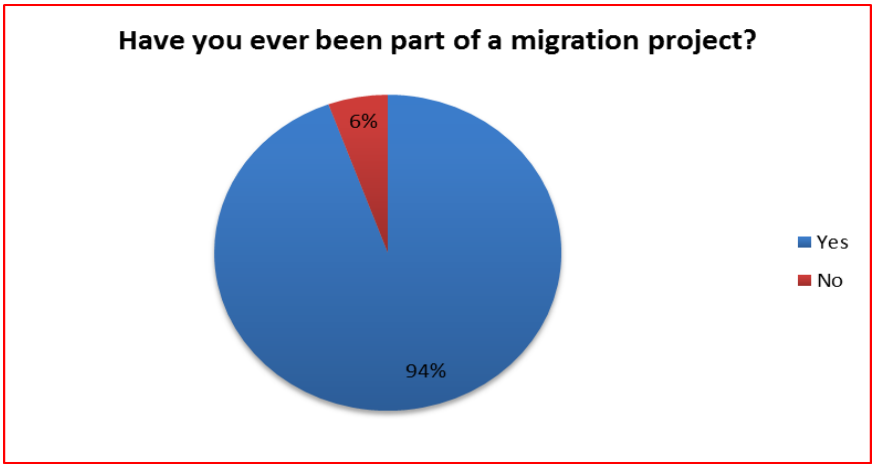


Figure 5.2 Respondents' Participation on Platform Migration Projects

Exploratory and Descriptive Statistics

(a) Exploratory Factor Analysis (EFA)

The original questionnaire is made up of four scales or components (B, C, D and E). Component B is made up of three constructs: employee behavior (construct B1), employee training (construct B2), and employee accountability (construct B3). Component C is made up of four constructs: organizational strategy (construct C1), organizational policies and procedures (construct C2), organizational data (construct C3), and organizational standards (construct C4). Component D is made up of five constructs: data categories and business rules (construct D1), data classification system (construct D2), data protection tools (construct D3), data sensitivity assessment (construct D4), and security models (construct D5). Component E is made up of five constructs: data migration and planning (construct E1), data migration process (construct E2), data migration tools (construct E3), data migration controls (construct E4), and data migration monitoring (construct E5). The questions in each of these components B, C, D and E are regrouped after the EFA has been performed on each of them. Table 1 illustrates the grouping of questions in all the components of the questionnaire.

COMPONENT B			COMPONENT C				COMPONENT D				COMPONENT E				
B1	B2	B3	C1	C2	C3	C4	D1	D2	D3	D4	E1	E2	E3	E4	E5
B1.1	B2.1	B3.1	C1.1	C2.1	C3.1	C4.1	D1.1	D2.1	D3.1	D4.1	E1.1	E2.1	E3.1	E4.1	E5.1
B1.2	B2.2	B3.2	C1.2	C2.2	C3.2	C4.2	D1.2	D2.2	D3.2	D4.2	E1.2	E2.2	E3.2	E4.2	E5.2
B1.3	B2.3	B3.3	C1.3	C2.3	C3.3	C4.3	D1.3	D2.3	D3.3	D4.3	E1.3	E2.3	E3.3	E4.3	E5.3
B1.4	B2.4	B3.4	C1.4	C2.4	C3.4	C4.4	D1.4	D2.4	D3.4	D4.4	E1.4	E2.4	E3.4	E4.4	E5.4
							D1.5		D3.5			E2.5			

Table 1. Grouping of Questions in all the Components of the Questionnaire

Table 2 indicates how the questions were re-grouped in component B, after performing EFA on Component B of the questionnaire, to ensure the validity of the identified constructs.

Factor 1	Factor 2	Factor 3
Question B1.1	Question B2.1	Question B1.3
Question B1.2	Question B2.4	Question B1.4
Question B3.1	Question B3.2	Question B2.2
	Question B3.4	Question B2.3

Table 2. Re-Grouping of Questions in Component B of the Questionnaire

Table 3 indicates how the questions were re-grouped in component C, after performing EFA on component C of the questionnaire, to ensure the validity of the constructs.

Factor 1	Factor 2	Factor 3
Question C1.2	Question C1.4	Question C3.2
Question C1.3	Question C2.1	Question C3.4
Question C2.2	Question C2.3	Question C4.3
Question C3.1	Question C2.4	
Question C3.3	Question C4.1	
Question C4.2		
Question C4.4		

Table 3. Re-Grouping of Questions in Component C of the Questionnaire

Table 4 illustrates how the questions were re-grouped in component D, after performing an EFA on component D of the questionnaire, to ensure the validity of the constructs.

Factor 1	Factor 2
Question D1.2	Question D1.1
Question D2.1	Question D1.3
Question D1.4	Question D5.1
Question D1.5	Question D5.2
Question D2.3	Question D5.3
Question D2.4	Question D5.4
Question D3.1	
Question D3.2	
Question D3.3	
Question D3.4	
Question D3.5	
Question D4.1	
Question D4.2	
Question D4.3	
Question D4.4	

Table 4. Re-Grouping of Questions in Component D of the Questionnaire

Table 5 shows how the questions were re-grouped in component E, after performing the EFA on Component E of the questionnaire, to ensure validity of the constructs.

Factor 1	Factor 2
Question E2.2	Question E1.1
Question E2.3	Question E1.2
Question E2.4	Question E1.3
Question E2.5	Question E1.4
Question E3.1	Question E4.2
Question E3.2	
Question E3.3	
Question E3.4	
Question E4.1	
Question E4.3	
Question E4.4	
Question E5.1	
Question E5.2	
Question E5.3	
Question E5.4	

Table 5. Re-Grouping of Questions in Component E of the Questionnaire

The new constructs and their descriptions after the EFA was performed, are shown in Table 6.

Construct	Description
Construct 1	Awareness Accountability score or (Employee_awareness/information Handling/accountability)
Construct 2	Training handling or (Employee_course type/sensitivity classification)
Construct 3	Consequences of sensitive data or (Employee_Training/Info Non-protection consequences)
Construct 4	General data policies, etc. or (Organization_strategy/culture/communication/data)
Construct 5	Specific sensitive data policy or (Organization_data security Policy/sensitive info identification)
Construct 6	Access to sensitive data or (Data_access/controls/standards enforcement)
Construct 7	General data issues or (Employee_roles/Responsibilities)
Construct 8	Data security model or (Organization_security models)
Construct 9	General control etc. or (Monitor/control_tools/migration issues/risk assessment/migration duration/network bandwidth)
Construct 10	Migration planning or (Migration processes_application identification/time management/servers de-staging/source data Backup/data quality)

Table 6. New Constructs after EFA and their Descriptions

(b) Reliability Analysis

The results of the reliability analysis of the new constructs, obtained as a result of the exploratory factor analysis on the original questionnaire, are presented in table 7. Estimates of internal consistency as measured by Cronbach's alpha, all exceeded 0.80, with the exception of three constructs that are less than 0.70. This indicates good reliability for seven of the ten constructs.

Variables	Items	Cronbach Alpha	Reliability
Construct 1	B1.1;B1.2;B3.1	0.7033	Acceptable
Construct 2	B2.1;B2.4;B3.2;B3.4	0.8443	Good
Construct 3	B1.3;B1.4;B2.2;B2.3	0.6265	Acceptable
Construct 4	C1.2;C1.3;C2.2;C3.1;C4.2;C4.4	0.8922	Good
Construct 5	C1.4;C2.1;C2.3;C2.4;C4.1	0.8342	Good
Construct 6	C3.2;C3.4;C4.3	0.7046	Acceptable
Construct 7	D1.2;D1.3;D1.4;D1.5;D2.4;D3.1;D3.2;D3.4;D3.5; D4.1;D4.2;D4.3;D4.4	0.9658	Good
Construct 8	D1.1;D2.1; D5.1;D5.3;D5.4	0.8630	Good
Construct 9	E2.2;E2.3;E2.4;E2.5;E3.1;E3.3;E3.4;E4.1;E4.3;E5. 1;E5.2;E5.3;E5.4	0.9647	Good
Construct 10	E1.1;E1.2;E1.3;E1.4;E4.2	0.8975	Good

Table 7. Reliability Analysis Results of the New Constructs

(c) Means and Standard Deviations of new Constructs

The comparisons among the new constructs, with respect to the means and the standard deviations of the new constructs, are shown in Table 8.

Construct	Mean	Std Dev
Construct 1	4.49	0.64
Construct 2	4.21	0.88
Construct 3	4.66	0.42
Construct 4	4.50	0.65
Construct 5	4.28	0.77
Construct 6	4.51	0.66
Construct 7	4.21	0.84
Construct 8	4.51	0.53
Construct 9	4.31	0.78
Construct 10	4.57	0.69

Table 8. Means and Standard Deviations of the new Constructs

The knowledge of the data that are collected is obtained from descriptive statistics – e.g. standard deviations, mean values, and scatter plots. The new Construct 3 is the most important one, with a mean of 4.66. Correlation analysis and predictive models are used to relate the quantity from a future activity to an earlier process measurement (Runeson & Host, 2009).

(d) Correlations between the Constructs

Table 9 shows that the correlation of the paired constructs are mostly medium and strong.

Variable	by Variable	Correlation	Count	Lower 95%	Upper 95%	Signif Prob
Construct 2	Construct 1	0.5563	90	0.3947	0.6845	<.0001*
Construct 3	Construct 1	0.4935	90	0.3190	0.6357	<.0001*
Construct 3	Construct 2	0.5429	90	0.3784	0.6742	<.0001*
Construct 4	Construct 1	0.6329	90	0.4901	0.7427	<.0001*
Construct 4	Construct 2	0.5284	90	0.3607	0.6629	<.0001*
Construct 4	Construct 3	0.5169	90	0.3469	0.6540	<.0001*
Construct 5	Construct 1	0.6023	90	0.4515	0.7196	<.0001*
Construct 5	Construct 2	0.7544	90	0.6486	0.8316	<.0001*
Construct 5	Construct 3	0.5013	90	0.3283	0.6418	<.0001*
Construct 5	Construct 4	0.4727	90	0.2945	0.6192	<.0001*
Construct 6	Construct 1	0.2374	90	0.0319	0.4237	0.0243*
Construct 6	Construct 2	0.5805	90	0.4244	0.7031	<.0001*
Construct 6	Construct 3	0.5688	90	0.4100	0.6941	<.0001*
Construct 6	Construct 4	0.4941	90	0.3197	0.6361	<.0001*
Construct 6	Construct 5	0.5201	90	0.3508	0.6565	<.0001*
Construct 7	Construct 1	0.4780	90	0.3006	0.6234	<.0001*
Construct 7	Construct 2	0.7499	90	0.6427	0.8284	<.0001*
Construct 7	Construct 3	0.6583	90	0.5225	0.7616	<.0001*
Construct 7	Construct 4	0.6163	90	0.4690	0.7302	<.0001*
Construct 7	Construct 5	0.7448	90	0.6358	0.8247	<.0001*
Construct 7	Construct 6	0.7009	90	0.5777	0.7929	<.0001*
Construct 8	Construct 1	0.4276	90	0.2419	0.5830	<.0001*
Construct 8	Construct 2	0.5335	90	0.3669	0.6669	<.0001*
Construct 8	Construct 3	0.4438	90	0.2607	0.5961	<.0001*
Construct 8	Construct 4	0.6280	90	0.4838	0.7390	<.0001*
Construct 8	Construct 5	0.4906	90	0.3155	0.6333	<.0001*
Construct 8	Construct 6	0.4763	90	0.2987	0.6221	<.0001*
Construct 8	Construct 7	0.5801	90	0.4239	0.7027	<.0001*
Construct 9	Construct 1	0.4232	90	0.2368	0.5795	<.0001*
Construct 9	Construct 2	0.7286	90	0.6142	0.8130	<.0001*
Construct 9	Construct 3	0.6641	90	0.5299	0.7659	<.0001*
Construct 9	Construct 4	0.5593	90	0.3983	0.6868	<.0001*
Construct 9	Construct 5	0.7152	90	0.5965	0.8033	<.0001*
Construct 9	Construct 6	0.7565	90	0.6515	0.8331	<.0001*

Variable	by Variable	Correlation	Count	Lower 95%	Upper 95%	Signif Prob
Construct 9	Construct 7	0.8811	90	0.8245	0.9203	<.0001*
Construct 9	Construct 8	0.5166	90	0.3465	0.6537	<.0001*
Construct 10	Construct 1	0.4384	90	0.2543	0.5917	<.0001*
Construct 10	Construct 2	0.5597	90	0.3988	0.6871	<.0001*
Construct 10	Construct 3	0.6499	90	0.5116	0.7553	<.0001*
Construct 10	Construct 4	0.4952	90	0.3210	0.6369	<.0001*
Construct 10	Construct 5	0.5795	90	0.4232	0.7023	<.0001*
Construct 10	Construct 6	0.5287	90	0.3611	0.6632	<.0001*
Construct 10	Construct 7	0.7064	90	0.5849	0.7969	<.0001*
Construct 10	Construct 8	0.5095	90	0.3381	0.6482	<.0001*
Construct 10	Construct 9	0.8135	90	0.7292	0.8734	<.0001*

Table 9. The Multivariate Correlations of the Study's Variables

The correlations between the paired constructs in the above correlation table is used to develop a preliminary management framework, shown in Figure 6, which resulted in the final management framework after its validation using qualitative analysis.

QUALITATIVE DATA FINDINGS

This section covers the qualitative data findings in the study.

Interview Narratives

The narratives of some questions posed to the ten interviewees are presented below:

[1] all ten interviewees said that they understood the difference between sensitive information and non-sensitive information, and they all explained the difference between the two types of information. Most of them described sensitive information as *the information that is classified as information that should not be accessible or accessed by any other person except the one that it is intended for, while non-sensitive information is that information that can be accessed by anyone without any repercussions*. One of them said that "… sensitive information is the information that is restricted in terms of who can access it, and it is also to some extent information that, if accessed, can compromise the security policies of that organization".

[2] on the protection of sensitive information during software migration, most of the interviewees mentioned that *encryption techniques should be used, as well as techniques such as Hashing should be used*. Some also mentioned that employees handling sensitive information need to be vetted, and obtain security clearance, to know the type of information they can handle. Others also said that data must be classified first, before migration, so that they can know the kind of protection measures applicable to the various data sensitivity levels. there was a general consensus among all the interviewees that *it is important for organizations to control and monitor their data access by their employees, to avoid data corruption by the employees*. Other

reasons mentioned were to ensure accountability of data, and also to limit data access. One of them said: "… the access to data exposes your data firstly to leakage or to modification or whatever~~,~~ the intent anybody may have. Firstly, ~~by~~ limiting access to data implies that someone does not know what exists and this will not bother them. Therefore, we limit the access to allow them to use what they need to do their job and that will assist avoiding data corruption. If they know there are secret data somewhere in another database and they cannot have access to it, then the possibility of their exploiting that access or using the access is just so much better. Having access to what they need to do their job definitely protects the inner security level that you can enforce on data".

[3] all the interviewees agreed that *the organizational source data be backed up prior to migration*, because if anything goes wrong during the migration process, it would be difficult to roll back to the previous state, and only afterwards can the migration proceeds again. Some suggested keeping the backup copy of sensitive data off-site~~,~~ as a precautionary measure to protect sensitive information. One of the interviewees said that "… this is important so that if something goes wrong, then you can fall back in terms of your operations and your business continuity".

[4] all of them agreed that *proper migration tools and strategies be provided prior to migration of data, so that the planning and the execution process proceeds in a coherent manner*. It should be spelt out in the user specifications requirements at the beginning of the migration project. A strategy is a roadmap, and it includes project monitoring tools in order to ensure a successful migration project.

[5] all the interviewees agreed that *database activities should always be monitored*, since the database is the life of the organization, and therefore it must be secured. Examples of monitoring questions include: who accesses the database? are the database requests normal? what has happened in the database? and, what did they do with the data? Database activities of users, such as modifications, deletions and alterations, can be selectively monitored.

[6] all the interviewees agreed that *organizational data should be classified prior to migration, as part of the security strategy*. This will show who should access the data based on the data classifications and their security level clearance. It will also aid in the protection of sensitive information, since only employees who have security clearance to handle such information will be allowed to do so. One of the interviewees said that: "… Yes ... it is an indication of how that data should be handled. Now if it is classified, then it would be handled according to its classification". This can also aid in knowing which data is more important than the other, and can be used to prioritiz~~s~~e the migration process.

[7] they all agreed that *the flow of sensitive data should be monitored during the migration process,* so that sensitive data arrives at the right destination at the same level of quality. This will avoid sensitive information leakage, and is one of the protection mechanisms of sensitive information migration.

[8] there was a general consensus among the interviewees that *IT standards such as ISO/IEC 17799 should be adhered to during software migrations,* because standards give the best practice baseline for IT governance, since they are the basis of the foundations of information security. Organizational data security policies should be based on such standards~~,~~ to ensure protection of their data during migrations, and to ensure interoperability of information across organizations.

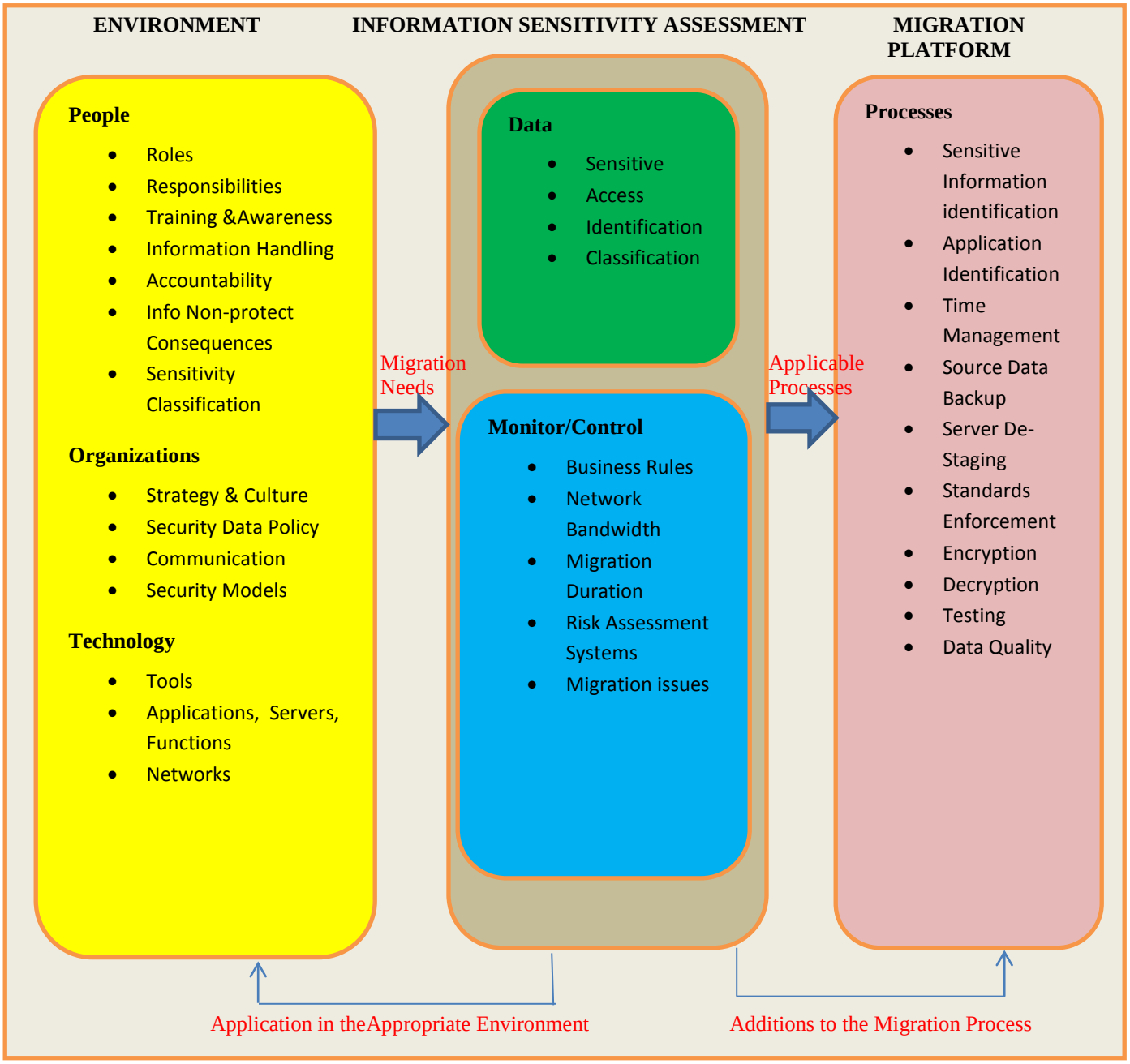


Figure 6. The Preliminary Management Framework after Quantitative Analysis

Word Cloud of most frequently used Words

Figure 7 illustrates the Word Cloud of the most frequently used 100 words obtained from the interview transcripts, with a minimum word length of four.

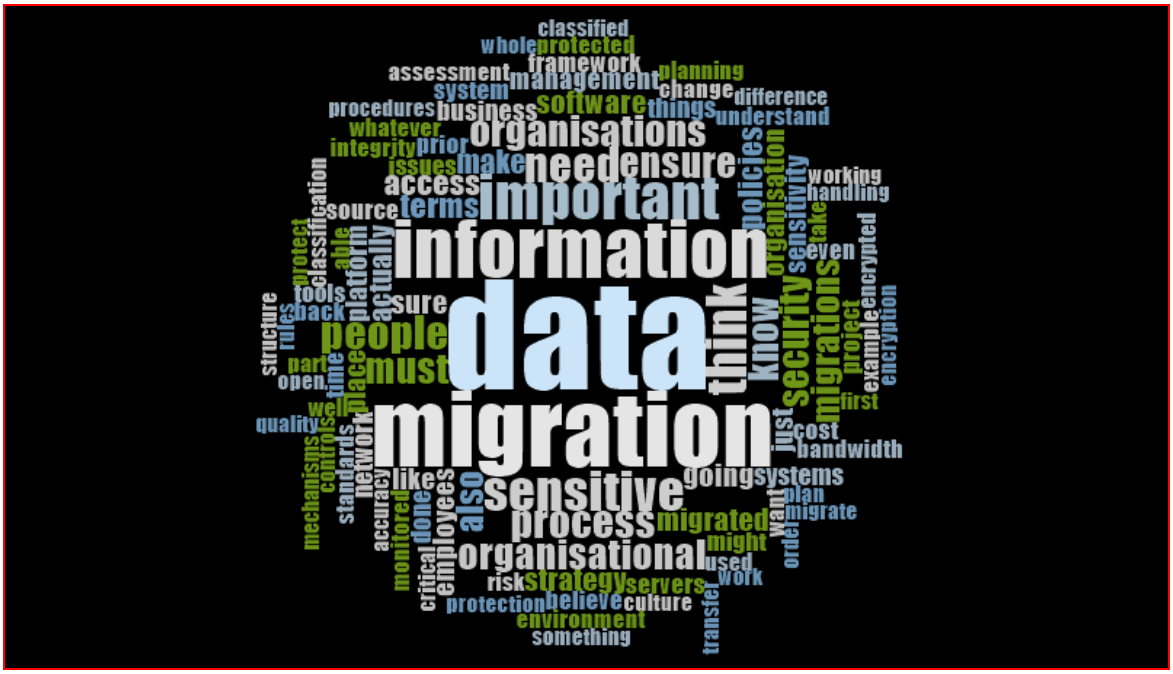


Figure 7.3 Word Cloud Diagram for the Qualitative Data Analysis

The bigger the size of the word, the more frequently it is used in the data – e.g. 'data' is the biggest word, followed by 'migration', 'information' and 'sensitive'; therefore, these are the most frequently used words in the data in Figure 7.

Coding - Model of Nodes (Categories) identified in the Data

Figure 8 illustrates the model of the nodes (categories) identified in the data. The model illustrated in Figure 8 demonstrates the hierarchical diagram of the nodes of the data. The sub-nodes are the children of the nodes, while the sub- sub-nodes are the children of the sub-nodes.

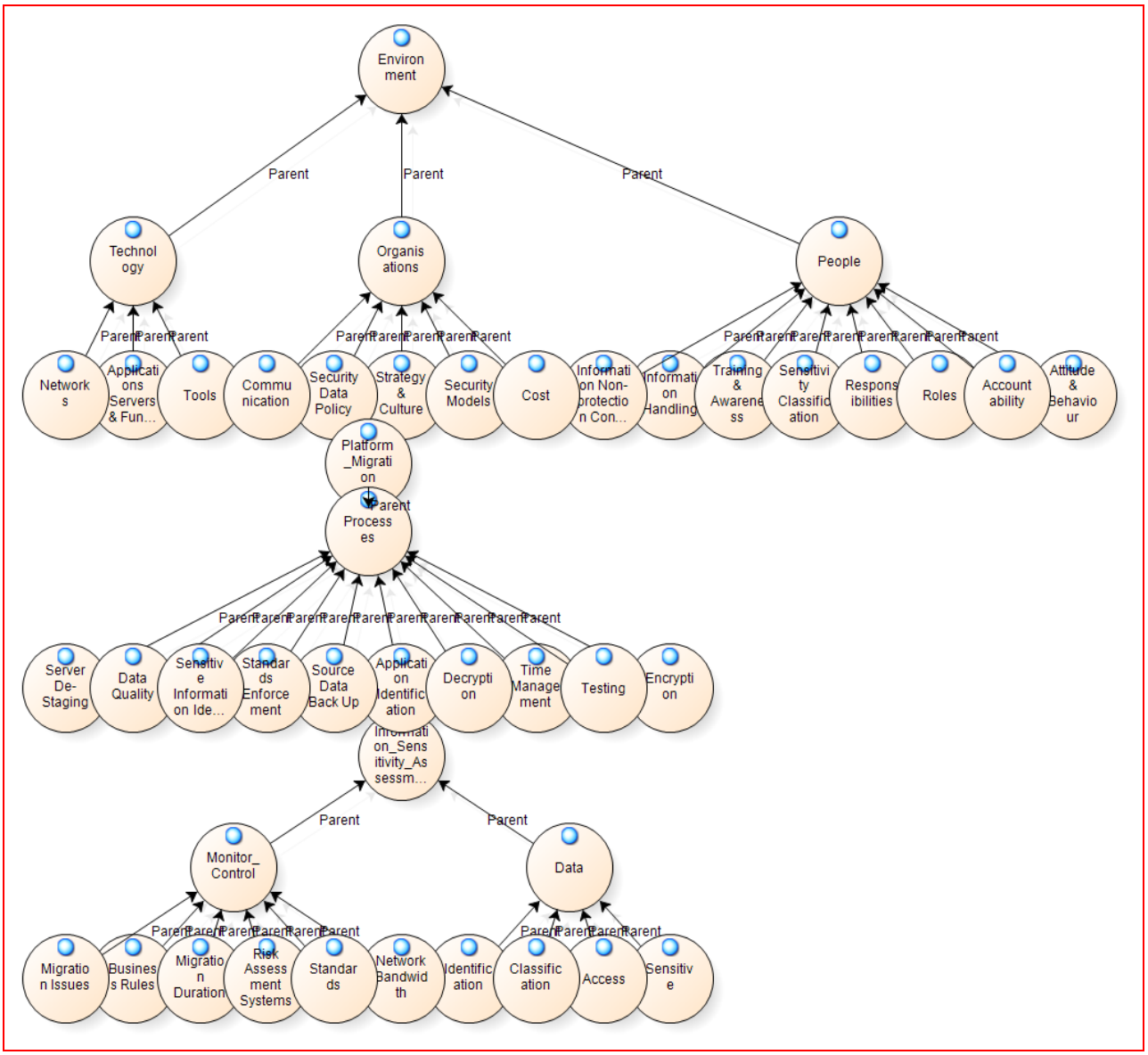


Figure 8.4 Model of the Nodes (Categories) identified in the Data

MANAGEMENT FRAMEWORK ON INFORMATION SENSITIVITY DURING SOFTWARE MIGRATIONS

Figure 9 illustrates the resulting final management framework on information sensitivity during migration of software platforms. This figure is conceptualized from the findings of both the quantitative analysis and qualitative analysis, and it is the enhancement and the validation of the preliminary management framework from the quantitative analysis (Figure 6), after the qualitative analysis has been performed. More discussion follows about the management framework on information sensitivity during software migrations, in the next section.

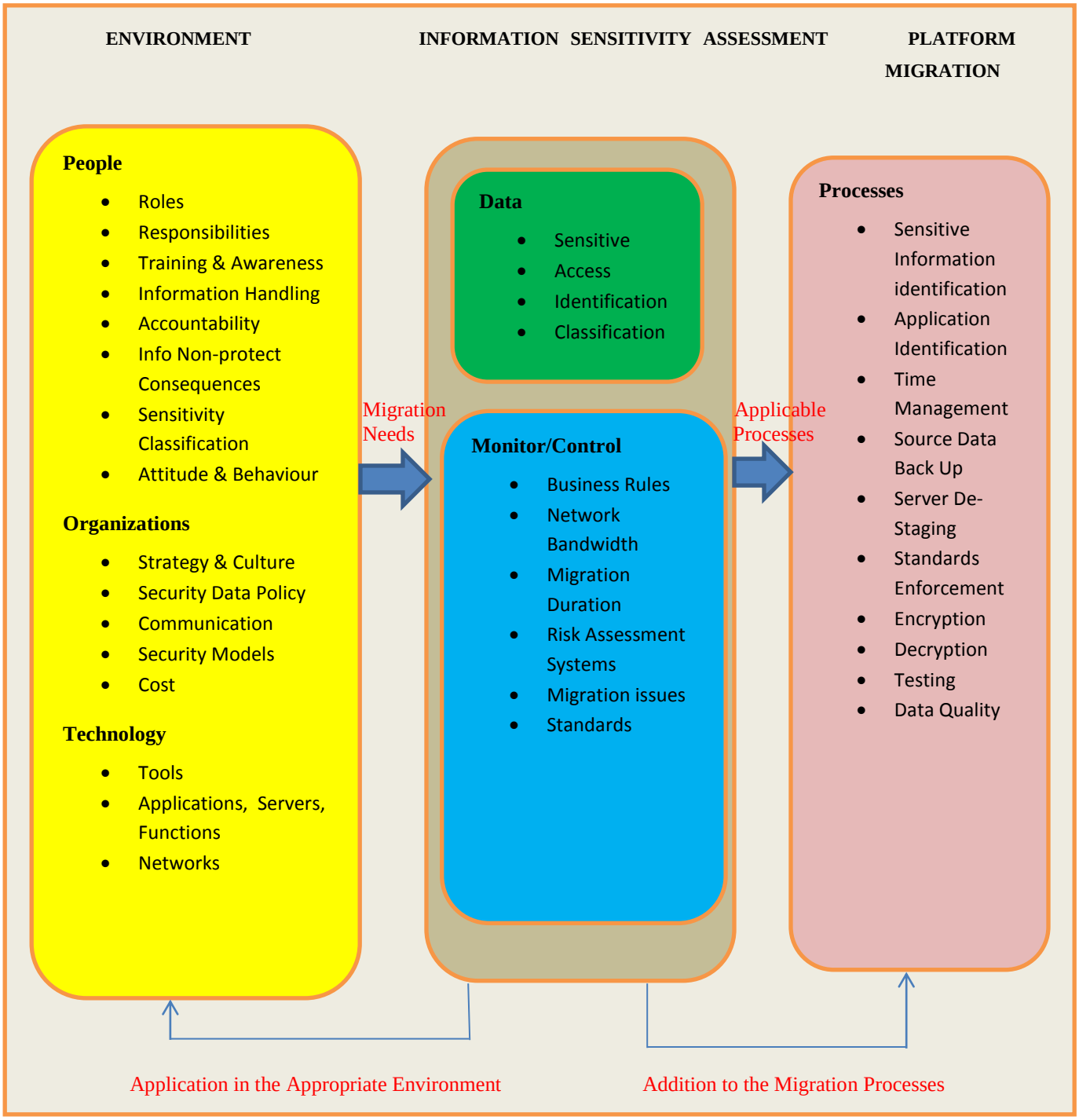


Figure 9.5 Management Framework on Information Sensitivity during Software Migrations

DISCUSSION

The roles and responsibilities of the migration team members should be clearly defined before the commencement of the project. Dhillon and Backhouse (2000) have stressed the importance of the integrity, roles and responsibilities of users as good values of information security management. Users are seen as the weakest connection in the information security chain (Schneier, 2000), so the information security function of each user should be seen as part of information security (Albrechtsen, 2007). This author further reiterates that users should be made to know their role in the total information security process.

Organizations should provide training and awareness of sensitive information protection and handling. Training of employees in detecting manipulative attempts is one of the methods proffered by CPNI (2009) to protect organizations against manipulation and sabotage risks. Security topics and requirements should be part of the normal business behavior, by having a clear policy and educating employees (Colwill, 2009). Induction courses should cover various aspects of the risks attached to the management of sensitive data. The training should spell out the consequences of the misuse of sensitive data, and also the risks in not protecting sensitive data. User awareness of the risks to their organization's information systems, has been identified by Humphreys (2008) to be part of good business practice. This might be in the form of regular awareness briefings, newsletters and circulars, and the organizational awareness program should be re-examined and brought up to date when necessary.

All employees should be educated in the different classification levels, their respective markings, and when to apply them. Employees should value accountability when they handle sensitive data, and handle sensitive information with care – as outlined in their data security policy. They need to be aware of what sensitive information is and how it should be protected, with organizations having a process to identify sensitive information that is worth protecting. Employees working on sensitive data should undergo vetting, in order to ascertain their confidential sensitivity levels. Colwill (2009) states that it is essential for organizations to perform effective employee background checks and vetting, before they start work, and the vetting process should apply to all staff levels, especially to management and employees allocated to roles with powerful privileges – for example, those with access to sensitive information. Members of the migration team must be certified at least up to a secret level.

Organizational strategy should include the protection of sensitive information, and should be aligned with clear objectives on how sensitive data should be handled. Protecting sensitive information should be part of any organizational corporate culture. Some authors have recognized that an organization's security culture is an important factor when maintaining an adequate information systems security level in their organizations (Ruighaver et al., 2007; Nosworthy, 2000; Borck, 2000; Von Solms, 2000; Beynon, 2001). According to Borck (2000), organizsations willing to have effective security must also involve the corporate culture when they deploy the latest technology. Cultural change needs to be managed, as Colwill (2009) indicates, since it can lead to fear, uncertainty and doubt in employees, and these can have an adverse effect on employees' attitudes towards security.

Organizations should have a data security policy which lists data security methods and sensitive data management. These procedures, and the policy, should be regularly communicated to, and enforced among, all staff. There should be a continual update of the data security policy, and data integrity should be the hallmark of any organization. This is also the view of Ross (2008) and Kavanagh (2006), in that organizations should have a policy in place, and the policy, as well as the standards, need to be enforced by the level of management that does the enforcing. Security models should be developed to support

organizational strategy, and such models should ensure confidentiality, integrity and reliability of data, in order to protect sensitive information. Security is related to management change, and the management change should be properly communicated to end users to ensure that they receive it well in their organization (Ashenden, 2008). There should be sufficient communication on information security with end users by management.

The organizational data access by employees should be controlled and monitored, and organizational data should be defined through data discovery and classification. Employees should be given access, based on their job role, to the information they are required to have, in order to perform their duties (Humphreys, 2008). He points out that there should be separation of duties, in order to enhance access protection against the insider threat. Confidentiality, integrity, identifying authorized users, and monitoring access, should be undertaken by organizations, to ensure sensitive data protection. According to McCue (2008), research shows that 70% of computer fraud is perpetrated by insiders, but 90% of security controls and monitoring is concentrated on external threats. Technical controls must be used to prevent unauthorized data access, and they should not be used in an isolated manner (Jones & Colwill, 2008).

Organizations should enforce hardware and software standards in order to eliminate unknown factors that might access their sensitive information. Organizations should have the required tools, applications, databases, servers and data migration strategies in place, in order for them to have a successful migration. Organizational networks should be protected at all times. Proper integration of people, process and technology should be undertaken, in order to facilitate successful information security management (Eminagaoglu et al., 2009). Organizations should provide for continuous management of data sensitivity and risk management. Eminagaoglu et al. (2009) indicate that organizations must always audit, check and measure their tasks within any information security program.

All the data created by users (information creators) should be classified or identified, and proactively marked before they are migrated. Data classification roles and responsibilities (e.g. data creators, data owners, data users, and data auditors) should be clearly defined within the organization. Business rules should be examined, in order to provide a basis for data classification. The flow of sensitive data communication monitoring, as well as database activity monitoring, should be in place.

Enough time should be planned for the data migration process, and all the functions, applications, host servers, and storage impacted by the data migration, should be identified during the data migration. All the data in the servers, memory and buffers, should be de-staged to disc before performing migrations. It is important for organizations to know the timing of migration, the migration duration period, and the system's downtime (if necessary). Scripts (if used) during the migration should be reviewed for reliability and accuracy.

Organizations should use Continuous Data Protection (CDP) technology and Data Loss Prevention (DLP) tools to protect sensitive information during data migrations (Nawafleh et al., 2013). The source data should be backed up prior to data migrations to the destination. Backups should be managed properly, since they can cause critical points of weakness (Humphreys, 2008). Humphreys suggests the encryption of backup tapes, and using e-vaulting of data to protect sensitive information. The issues of data corruption, missed data or data loss, should be considered during migration. Migrated data should be tested and validated after migration, in order to ensure data accuracy and integrity. Technical controls should be in place to ensure effective sensitive data protection during migrations. In addition, the view of Colwill (2009) is that encryption, access control, monitoring, auditing and reporting should be part of the technical controls against insider attacks.

Migrated sensitive data should always be encrypted during and after migration, and should only be decrypted when the data is accessed by the authorized user, for readability. The necessary monitoring and risk assessment systems should be in place. Colwill (2009) has argued that a holistic approach which includes human factors, technical controls and implementing focused risk assessments, are necessary to protect the organization from the malicious insider attacker. The network bandwidth capacity utilization needs to be measured before migration, and there is a need to know the network availability in order to ensure smooth migration. Verification or comparing migrated data with source data should be performed, and if problems persist, then a data quality process should be performed.

The attitude and behavior of the migration team members should be taken into consideration before the composition of the team. The migration team should be composed of dedicated and enthusiastic people who are committed to the success of the project. It is vital that members of the migration team have the right attitude and behavior, and that they also adhere to the organizational security policies and procedures. Albrechtsen and Hovden (2010) highlight that there is a need for user awareness and good behavior to be part of the important aspects of the information security performance. Employee awareness and training are important, but, equally, changing the behavior of employees through targeted training should be employed, by educating employees in identifying unacceptable, and malicious behavior (Sasse et al., 2007). Organizations should reward and reinforce good security behavior (Kavanagh, 2006).

The total cost of ownership of the migration projects should be computed during the migration planning stage, to facilitate the completion of the migration project within its initial budget allocation. The benefits, value, and return on investment must be explored before embarking on the migration project in order to ensure that the migration project is beneficial to the organization.

Standards such as ISO/IEC 17799 should be adhered to when compiling security policies and procedures in order to ensure protection of information during migration. Organizations have applied best information security practice for decades, and many of them are incorporated into the international standards – such as ISO/IEC 27001 and ISO/IEC 27002 (Humphreys, 2008). Such standards can be used to monitor and control the migration processes. The standards would give the best practice baseline for IT governance, since they form the basis of the foundations of information security. Humphreys (2008) emphasizes that due diligence should be performed, to reveal risks and manage them, in terms of information security of organizational assets and their protection. This should be done by implementing effective systems of control, and undertaking regular monitoring and reviews. He maintains that organizations should embark on information security governance, in order for them to protect their information assets.

CONCLUSION

This research contributes to the enrichment of the theory of information systems, with respect to information sensitivity management, by developing a framework to manage sensitive information during software migrations. The resulting management framework can be used to protect sensitive information between software migrations. Additionally, the research work contributes to the ICT theory, by developing and validating the management framework on migration of platforms.

In conclusion, the resulting final management framework, shown in Figure 9 is a fully-fledged, concise, valid and reliable management framework that organizations may utilize to assist them in protecting their classified sensitive information during migrations of software platforms.

REFERENCES

Ahmad, A., Bosua, R. and Scheepers, R. (2014) Protecting organizational competitive advantage: A knowledge leakage perspective, *Computers & Security*, 42, 27 – 39.

Albrechtsen, E. (2007) A qualitative study of users' view on information security, *Computers & Security*, 26, 4, 276 – 289.

Albrechtsen, E. and Hovden, J. (2010) Improving information security awareness and behaviour through dialogue, participation and collective reflection – An intervention study, *Computers & Security*, 29, 4, 432 – 445.

Arai, M. & Tanaka, H. (2009) A proposal for an effective information flow control model for sharing and protecting sensitive information, *Australasian Information Security Conference (AISC), Wellington, New Zealand, Conferences in research and practice in Information Technology (CRPIT)*, Ljiljana Brankovic and Willy Susilo, Eds.

Ashenden, D. (2008) Information security management: A human challenge?, *Information Security Technical Report*, 195 – 201.

Beynon, D. (2001) Talking heads, *Computerworld*, 24, 33, 19 – 21.

Borck, J. (2000) Advice for a secure enterprise: implement the basics and see that everyone uses them, *InfoWorld*, 22, 46, 90.

Colwill, C. (2009) Human factors in information security: The insider threat – Who can you trust these days?, *Information Security Technical Report*, 14, 186 – 196.

CPNI,2009; Insider attacks, retrieved September 4, 2012 from www.cpni.gov.uk/MethodsOfAttack/insider.aspx.

Cresswell, J. W. (2009) Research design, qualitative, quantitative and mixed methods approaches, 3rd edn. Los Angeles: Sage.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. and Baskerville, R. (2013) Future directions for behavioural information security, *Computers & Security*, 32, 90 – 101.

Denzin, N. K. and Lincoln, Y. S. (2000) Handbook of Qualitative Research, 2nd edn. Thousand Oaks: Sage

Dhillon, G. and Backhouse, J. (2000) Information system security management in the new millennium, *Communications of the ACM*, 43, 7, 125 – 8.

Duri, S., Elliott, J., Gruteser, M., Liu, X., Moskowitz, P., Perez, R., Singh, M. and Tang, J. (2004) Data protection and data sharing in Telematics, Mobile Networks and Applications, 9, 693 – 701, Kluwer Academic Publishers, Netherlands.

Eminagaoglu, M., Ucar, E. and Eren, S. (2009) The positive outcomes of information security awareness training in companies – A case study, *Information Security Technical Report*, 223 – 229.

Fung, P. and Jordan, E. (2002) Implementation of information security: A knowledge-based approach.

Garfinkel, S. L. (2014) Leaking sensitive information in complex document files and how to prevent it, *IEEE Computer and Reliability Societies*, 20 – 27.

GITOC, (2003) Using open source software in the South African Government: A proposed strategy compiled by the Government Information Technology Officers' Council, Version 3.3.

Gupta, M. (2010) A new strategy for the protection of intellectual property, *Computer Fraud & Security*, 8 – 10.

Humphreys, E. (2008) Information security management standards: Compliance, governance and risk management, *Information Security Technical Report*, 247 – 255.

Huth, C. L., Chadwick, D. W., Claycomb, W. R. and You, I. (2013) Guest editorial: A brief overview of data leakage and insider threats, *Information Systems Front*, 15, 1 – 4.

IT Web, 2007; Two nabbed for eNaTIS fraud, IT Web News retrieved September 22, 2008 from http://www.itweb.co.za.

Johnson, R. B. and Onwuegbuzie, A. J. (2004) Mixed methods research: A research paradigm whose time has come, *Educational Researcher*, 3, 7, 14 – 26.

Jones, A. and Colwill, C. (2008) Dealing with the malicious insider, In: *9th Australian information and Warfare security Conference.*

Kavanagh, J. (2006) Security special report: the internal threat, Computer Weekly; retrieved June 27, 2011 from www.computerweekly.com/Articles/2006/04/25/215621/security-special-report-the-internal-threat.htm

Khan, J. H. (2006) Factor analysis in counseling psychology research, training and practice: Principles, advances, and applications, *The Counseling Psychologist*, 34, 684 – 718.

Kirda, E and Kruegel, C. (2005) Protecting users against phishing attacks with antiPhish, *Proceedings of the 29th Annual Conference Computer Software and Applications Conference, IEEE*.

McCue, A. (2008) Beware the insider security threat, CIO Jury: retrieved April 8, 2012 from www.silicon.com/management/cio-insights/2008/04/17/beware-the-insider-security-threat-39188671/

Nawafleh, S. A., Hasan, M. Y. F. and Nawafleh, Y. (2013) Protection and defense against sensitive data leakage problem within organisations, *European Journal of Business and Management*, 5, 23.

Nosworthy, J. (2000) Implementing information security in the 21st Century – do you have the balancing factors?, *Computers & Security*, 19, 4, 337 – 347.

Novell Connection, (2009) About the National Library of South Africa; retrieved September 12, 2013 from https://www.novell.com/connectionmagazine/2009/04/national-library-of-south-africa.html.

Oates, B. J. (2006) Researching information systems and computing, SAGE Publications, London.

Petty, N. J., Thomson, O. P. and Stew, G. (2012) Ready for a paradigm shift? Part 2: Introducing qualitative research methodologies and methods, *Manual Therapy*, 17, 378 – 384.

PNC, (2007) Proposal to provide an open source software support, Change management and training services to Presidential National Commission' – by Impi Linux (Pty) Ltd.

Rakers, J. (2010) Managing professional and personal sensitive information, *SIGUCCS*, October 24 – 27, Norfolk, Virginia, USA.

Ross, S. J. (2008) Enforcing information security: architecture and Responsibilities, *Network Security*, 7 – 10.

Ruighaver, A. B., Maynard, S. B. and Chang, S. (2007) Organisational security culture: Extending the end-user perspective, *Computers & Security*, 26, 56 – 62.

Runeson, P. and Host, M. (2009) Guidelines for conducting and reporting case study research in software engineering, *Empirical Software Engineering*, 14, 131 – 164.

Sasse, M. A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Flechais, I. and Kearney, P. (2007) Human vulnerabilities in security systems, human factors working group, *Cyber security KTN* human factors white paper.

Schneier, B. (2000) Secrets & lies, Digital security in a networked world, New York, John Wiley.

Tashakkori, A. and Creswell, J. W. (2007) Editorial: the new era of mixed methods, *Journal of Mixed Methods Research*, 1, 1, 1 – 8.

Tate, R. A. (2003) A comparison of selected empirical methods for assessing the structure of responses to test items, *Applied Psychological Measurement*, 27, 159 – 203.

Thompson, B. (1992) A partial test distribution for cosines among factors across samples, In B. Thompson (ed.) *Advances in Social Science methodology*, 2, 81 – 97.

Von Solms, B. (2000) Information security – the third wave*?*, *Computers & Security*, 19, 7, 615 – 620.

Von Solms, R. and van Niekerk, J. (2013) From information security to cyber security, *Computers & Security*, 38, 97 – 102.

Wiid, J. and Diggines, C. (2013) Marketing research, 2nd edn. Juta & Company Ltd., Cape Town, South Africa.

Worthington, R. L. and Whittaker, T. A. (2006) Scale Development Research: A Content Analysis and Recommendations for Best Practices, *The Counseling Psychologist*, 34, 6, 806 – 838.

Yin, R. K. (2003) Case study research, design and methods, Applied social research methods series, 3rd edn., SAGE Publications, Inc.

Yin, R. K. (2009) Case study research design and methods, SAGE Publications Inc., Thousand Oaks, CA.