JOURNAL OF GOVERNANCE AND REGULATION

Postal Address:

Postal Box 136
Sumy 40000
Ukraine

Tel: +380-542-698125
Fax: +380-542-698125
e-mail: info@virtusinterpress.org
www.virtusinterpress.org

Journal of Governance and Regulation is published four times a year, in September-November, December-February, March-May and June-August, by Publishing House "Virtus Interpress", Gagarina Str. 9, office 311, Sumy, 40000, Ukraine.

Information for subscribers: New orders requests should be addressed to the Editor by e-mail. See the section "Subscription details".

Back issues: Single issues are available from the Editor. Details, including prices, are available upon request.

Advertising: For details, please, contact the Editor of the journal.

Journal of Governance and Regulation

ISSN 2220-9352 (printed version)

ISSN 2306-6784 (online version)

FACTORIAL INVARIANCE OF AN INFORMATION SECURITY CULTURE ASSESSMENT INSTRUMENT FOR MULTINATIONAL ORGANISATIONS WITH OPERATIONS ACROSS DATA PROTECTION JURISDICTIONS

Nico Martins,* Adéle da Veiga**

Abstract

An information security culture is influenced by various factors, one being regulatory requirements. The United Kingdom (UK) has been regulated through the UK Data Protection Act since 1995, whereas South Africa (SA) only promulgated the Protection of Personal Information Act (PoPI) in 2013. Both laws stipulate requirements from an information security perspective with regard to the processing of personal information, however in the UK this has been regulated for a longer period. Consequently, it is to be expected that the information security culture for organisations in the UK will be significantly different from that of SA. This raises the question as to whether the same information security culture assessment (ISCA) instrument could be used in an organisation with offices in both jurisdictions, and whether it might be necessary to customise it according the particular country's enforcement of information security and privacy-related conditions. This is reviewed, firstly from a theoretical perspective, and secondly a factorial invariance analysis was conducted in a multinational organisation with offices in both the UK and SA, using data from an ISCA questionnaire, to determine possible factorial invariances in terms of the ISCA.

Keywords: Information Security, Information Security Culture, Factorial Invariance, Structural Equation Modelling, Data Protection, Privacy, Maturity, South Africa, United Kingdom

* *Department of Industrial and Organisational Psychology, University of South Africa*
** *College of Science, Engineering and Technology, School of Computing, University of South Africa*

1. Introduction

An information security culture assessment (ISCA) instrument can be used to assess the level of the information security culture in an organisation. This assessment gives management an indication of their employees' perception of the protection of information, and shows whether their resultant behaviour is conducive to such protection (Da Veiga and Martins 2015b). A strong information security culture is a critical component in protecting information. However, the type of information processed and the associated risks tend to be different for each organisation. The selected information security controls would therefore need to be adjusted accordingly (Pfleeger, Pfleeger and Margulies 2015). This will result in different information security policies, procedures and requirements to be adhered to by employees. The "way things are done" in organisations to protect information would similarly vary from one organisation to another. This would result in different information security cultures between different organisations in much the same way as the general organisational culture of one organisation would tend to be different from that of another organisation (Brown 2015).

One factor that could potentially influence the information security culture would be the regulatory requirements pertaining to data protection and information security (Da Veiga and Martins 2015a). In a global economy, regulatory requirements tend to differ between jurisdictions, and therefore the data protection and information security requirements would also tend to differ. This could lead to different information security policies, controls and/or processes to be implemented by employees across jurisdictions. Over time, different information security cultures would therefore become evident across jurisdictions. For example, the definition of personal information in the Protection of Personal Information (PoPI) Act includes "juristic persons" (PoPI 2013). Therefore, the eight conditions of data processing in PoPI would also apply to company information (e.g. to company registration numbers) and not only to personal information of natural living individuals (e.g. the person's name, surname, national identification number, etc.). This means that the same information security controls and procedures would have to be implemented when processing the juristic information of third parties or suppliers, as when processing personal information of customers or

employees. In future, employees of South African organisations will have to abide by stronger information security controls, such as the secure transfer of emails, and restricted access to certain files. Currently, the laws of some countries do not include this requirement. In time this will impact on the way things are done in an organisations when dealing with information security issues, and this could potentially influence the prevailing information security culture.

Multinational or international organisations could face the challenges posed by having operations in jurisdictions, some with stringent data protection laws, and others with minimal or no data protection laws. This creates a challenge when transborder data flows occur between these jurisdictions. Some organisations, such as Accenture and the Siemens Group (Wikipedia 2015), have opted for Corporate Binding Rules (BRCs) originally developed by the Article 29 Party (Article 29 of 2015). BRCs provide a framework for the international transfer of personal information within the same group of companies. They stipulate the minimum data protection and information security controls to be adhered to, across multiple jurisdictions, by the respective operations of the organisation. Organisations with BRCs approved by the data protection authority of an EU member state, may process the personal information of their employees or customers between their operations even though they may reside in different countries (Swire and Berman 2007).

In the absence of BRCs, organisations typically develop global or group data protection and information security policies stipulating the requirements to be complied with by their various operations. However, it becomes a challenge when the organisation operates across jurisdictions with varying privacy requirements. This could make it difficult to enforce such policies across countries (Swire and Berman 2007).

When assessing an information security culture, the assessment instrument selected must be reliable and consistent, even when applied within the same organisation but across different countries and regulatory jurisdictions. Multinational organisations should compare the results of their operations in different countries to determine if similar or different interventions are needed. The purpose of this study is to determine whether multinational organisations can apply ISCA with confidence across their operations, especially in countries where the maturity levels of data protection regulation may vary.

1.1. Aim of this paper

This paper deals with the following three main research objectives:

- To determine whether there are differences in the maturity levels of the UK and SA in terms of data protection, such that it could influence the implementation of ISCA across both countries.
- To confirm the validity of the ISCA questionnaire by means of confirmatory factor analysis (CFA).
- To determine if there is evidence of factorial invariance between the two countries, one operating with data protection laws (UK), and the other without such laws (SA).

The paper is structured as follows: Section 3 provides background information pertaining to data protection regulation in both the UK and SA, with the objective of identifying similarities and differences. This is used to define the data protection maturity level of each country by applying the capability maturity model concept. The research methodology and case study applications are discussed in section 4. This is followed, in section 5, by a discussion of the results of the factor and item analysis and factorial invariance analysis. Section 6 presents the research contribution and proposed future research, followed by the conclusion in section 7.

2. Literature review

The following section provides a high-level overview of data protection in the UK and SA respectively.

2.1 Data protection in the UK

The processing and protection of personal data in the UK and Northern Ireland are governed by the Data Protection Act (DPA) of 1998. This Act came into effect in March 2000, and compliance is regulated by the Information Commissioner's Office (ICO 2015). The DPA brings the processing of personal information on a par with the requirements of the EU Data Protection Directive 95/46/EC (1995), which requires member states to protect the right to privacy. The directive (1995) came into effect in 1998, and has subsequently been amended to transpose it from a directive to a regulation for all EU member states (EC 2014). The first draft of the regulation was published in 2012 by the European Commission. Once this regulation comes into full effect, all EU member states will have to comply with it, including the UK.

The DPA (1998) contains eight data protection principles, of which principle seven relates directly to information security. This principle states: "*Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*." Additionally, this principle requires organisations to "*ensure a level of security appropriate to (a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and (b) the nature of the data to be protected*." The DPA also requires data processors (e.g. third parties)

involved in data processing on behalf of the data controller, to comply with the seventh principle.

In addition to the DPA, the UK also has other laws regulating information processing, such as the Freedom of Information Act (2000), the Privacy and Electronic Communications Regulations Act (2003) and the Computer Misuse Act (1990).

2.2 Data protection in SA

In South Africa, the right to privacy is encapsulated in section 14 of the Constitution of the Republic of South Africa 108 of 1996 which states:

"14. Privacy: Everyone has the right to privacy, which includes the right not to have -

(a) their person or home searched;
(b) their property searched;
(c) their possessions seized; or
(d) the privacy of their communications infringed."

To realise the right to privacy, the Protection of Personal Information (PoPI) Act was ascended by the President in November 2013. This piece of legislation brings SA in line with international privacy legislation and regulates the flow of personal information across the borders of SA. PoPI's objective is to promote the protection of personal information processed by public and private bodies domiciled in SA, and also to introduce conditions for processing personal information. Organisations will have one year to implement the provisions once the commencement date has been announced.

Condition seven (PoPI 2013) relates to information security and stipulates that organisations (the responsible party) must "*secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent*

(a) loss of, damage to or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information."

PoPI further requires the identification of risks to personal information, the establishment of safeguards against such risks and the verification and regular updating of these safeguards. In addition, it also requires security measures for the processing of personal information by third parties and outlines the requirements for the notification of security compromises.

Additionally, SA has other pieces of legislation in place that regulate information processing and relate to the protection of information, for example, the Electronic Communications and Transactions Act of 2002, the Regulation of Interception of Communications and Provision of Communication-related Information Act of 2002, the Promotion of Access to Information Act 2 of 2000, and the National Cyber Security Policy framework which was approved in 2012 (Grobler et al 2012).

2.3 Differences in data protection between the UK and SA

To determine whether the same ISCA instrument could be used within an international organisation with offices in both the UK and SA, the differences, from a data protection perspective, need to be considered. The various aspects discussed below are included for the purpose of illustrating that the maturity level of data protection legislation and its implementation may vary significantly between the two countries. In this paper, the focus is on data privacy, and therefore the Data Protection Act of 1998 (for the UK), and the Protection of Personal Information Act of 2013 (for SA), are used as the respective points of reference from a regulatory perspective.

In the UK data protection regulations have been in place since 1984, whereas in SA the appropriate legislation is yet to be commenced. Section 114 of PoPI specifies that organisations will be required to comply with the regulations within one year of the commencement date, but that the Minister may extend the period for up to three years (PoPI 2013). Many organisations in SA are uncertain about the amount of effort that would be required to become compliant with PoPI, but generally it is believed that it might require a number of years to fully implement (PwC 2011).

The only PoPI provisions to come into effect in 2014, relate to the establishment of the Information Regulator, who has yet to be appointed. In the UK the Information Commissioner's Office (ICO 2015) fulfils this role and, among other things, publishes guidance for individuals and organisations, conducts audits, issues monetary penalties and prosecutes criminal offences. Legal cases (and fines) involving privacy issues, have not affected South African organisations much to date. Zurich Insurance, however, was fined £2,275,000 by the Financial Services Authority (FSA) because their South African operations displaced an unencrypted backup tape in 2008 with the personal details of some 46 000 customers (Condon 2010). Other examples of fines and legal cases are somewhat ad hoc and limited in the absence of the commencement of PoPI and the appointment of an Information Regulator. In the UK, cases of litigation related to privacy issues rose by 22% in 2013 (Turvill 2013), while the ICO had fined organisations a total £6.7 million between 2010 and 2014 for violations under the DPA. £4.5 million of the fines were related to the public sector (Curtis 2014).

The information security culture is not only influenced by regulatory requirements. Many other factors could also influence a culture, such as the organisation's leadership and its information and

communication systems and policies (Ogbanna 1992). National culture often plays a significant role when employees from different cultures have different perceptions of privacy (Hoffstede 1980). Some view Europe as a continent with a bureaucratic approach to privacy legislation, with more than half of the world's data privacy laws having been implemented in Europe (Greenfield 2014), whereas countries such as North America follow a more permissive approach (Bygrave 2010). This is evident in the EU data protection law (EC 2014), which will apply to all EU member states in future, whereas the US follows a sectorial-based approach to privacy.

According to Bygrave (2010), expectations of privacy vary from one culture to another, as does the manner in which various cultures protect their privacy from an information security perspective. One could therefore assume that there would be some differences in the national cultures of the UK and SA respectively, with regard to privacy and information security. One reason is that individual and country expectations of privacy often vary. European citizens view privacy as highly important (Hallinan et al, 2012) and typically have broad privacy expectations and rights (Herath 2011). South African consumers are becoming more aware of their right to privacy and specifically with regard to intrusion from a marketing perspective (Jordaan 2007). A study by Jordaan (2007) indicates that in SA, older consumers are more concerned about privacy protection than their younger counterparts, middle- and high-income groups more so than lower income groups, and females more than males.

2.4 The data protection maturity of the UK versus SA

To better understand the differences in data protection measures between the UK and SA, the researchers aimed to explore the maturity of the two countries with regard to data protection. The capability maturity model (CMM) scale (Cobit 2007) was selected for this purpose. Many organisations make use of a CMM to rate their IT and information security capabilities. The CMM aids organisations in performing benchmarking exercises, both internal to the organisation and externally, in an attempt to compare themselves against other organisations. The Cobit maturity scale (Cobit 2007) is based on the original Software Engineering Institute's CMM, and was adapted for IT management with a specific rating scale for each of the 34 processes outlined in Cobit. The Cobit maturity assessment is conducted on a five-point scale, namely:

0 – non-existent (no management processes)

1 – initial/ad hoc (processes are ad hoc and disorganised)

2 – repeatable but intuitive (processes follow a regular pattern)

3 – defined processes (processes are monitored and measured)

4 – managed and measurable (good practices are followed)

5 – optimised

For the purpose of this research, several criteria were defined that can be rated using the five-point scale of the CMM. This will help to determine whether the same questionnaire could be used by an organisation with operations in both countries, to assess the prevailing information security culture. Table 1 outlines the five criteria identified in line with the discussions above. Although other criteria could also be applied, the selected criteria were deemed adequate to illustrate that the UK is more mature than South Africa in the implementation and regulation of data privacy conditions, including information security.

The CMM ratings indicate that the UK is probably on a maturity level 4, with data protection (privacy and security) being managed and measured consistently, both within organisations and from a government perspective. The maturity level in SA may be rated at an initial/ad hoc level, i.e. level 1. This rating is due to the fact that the Act has yet to be formally commenced, and many organisations are yet to implement the conditions of the Act.

From a theoretical perspective the CMM ratings illustrate that the level of data protection maturity in the UK significantly exceeds that of SA, which relates to the first of our research questions. Consequently, one would expect that the information security principles or conditions implemented in organisations in the two countries respectively, as well as the ability to enforce these principles and conditions, would be at different levels, and that the relative information security cultures would be affected accordingly.

To further investigate whether the ISCA could be used as a valid and reliable assessment instrument in an organisation with offices both in the UK and in SA, it was necessary to conduct a factorial invariance analysis.

Table 1. UK and SA data protection criteria and CMM ratings

Maturity indicators	UK	CMM rating UK	SA	CMM rating SA
Regulation in place	**Data Protection Act of 1998** First published in 1998, i.e. 17 years ago, but reprinted in 2005 to incorporate certain important corrections. Other related regulations are also in place, as well as the EU Data Directive.	4	**Protection of Personal Information Act 4 of 2013** The President of SA assented to the Act in 2013, i.e. 2 years ago. Other pieces of legislation are also in place.	1
Commence-ment date	March 2000, thus the Act commenced 15 years ago.	5	The Act has not commenced as yet. Only certain sections pertaining to the establishment of a Regulator commenced in 2014.	1
Time frame in place	15 years	4	Not implemented in terms of compliance from a public and privacy body perspective	0
Regulator in place	Yes, in the form of the Information Commissioner's Office (ICO) http://www.ico.org.uk	4	No, still in the process of being defined.	0
Court cases	Court cases rose by 22% in 2013. £6.7 million from 2010 up to the end of 2014 for violations under the UK Data Protection Act.	4	No court cases under the Protection of Personal Information Act and no fines.	0

3. Research methodology

Firstly, a confirmatory factor analysis was conducted to confirm the validity of ISCA across the two countries, thus confirming the reliability of the analysis. Secondly, a base structural equation model was compiled consisting of the data from the two countries, i.e. SA and UK. Sufficient responses were obtained. This was followed by an analysis to determine the goodness-of-fit indices across the two countries and the nested model comparisons.

3.1 Sample

A global financial institution was selected for the research and a case study similar to that which was used in previous research to validate ISCA, was applied (Da Veiga and Martins 2015a). The selected organisation employed 8 220 employees in 2013, and had operations across 12 countries. In total, 2 159 employees participated in the 2013 ISCA survey. A total of 968 employees from the UK participated, representing 44.9% of the responses from across all 12 countries. Some 866 employees from SA participated, representing 40.1% of all the responses. Since the number of responses received from the other countries was insufficient for multivariate comparisons, they were excluded from further analysis.

The organisation used for the case study appointed a group information security officer (ISO) who, in collaboration with several country security officers (CSOs), manages information security and data protection in the organisation. The organisation has implemented a group information security policy which was duly approved by an executive committee. The objective of the policy is to define the acceptable behaviour of employees using the information processing facilities of the organisation, and to inform them of their obligation to protect the confidentiality, integrity and availability of the organisation's information. In addition, the organisation also has a group data protection policy in place, and privacy notices to customers visiting their website. Operations in both the UK and SA are obligated to conform to these policies.

3.2 The measuring instrument

The ISCA questionnaire, which was validated in a previous research (Da Veiga and Martins, 2015a) with good reliability rating of between 0.764 and 0.877, was again used in this research. The ISCA questionnaire comprises nine dimensions measuring information security perceptions on a five-point Likert scale.

3.3 Research procedure

The Group ISO of the multinational organisation referred to above, granted approval to conduct the ISCA across all 12 of countries where the organisation operates. The questionnaire was sent out electronically to employees to complete. The Group ISO was responsible for informing employees of the survey and to communicate various details relating to

the survey, as well as to send all employees the survey link for the electronic HTML survey. The survey was conducted anonymously to preserve the confidentiality of the respondents. Employees were given a three-week period to complete the survey and responses were tracked on a weekly basis. After the three-week period the survey was closed and the statistical analysis commenced in order to give feedback and recommendations to the organisation.

4. Results

4.1 Factor and reliability analysis

To confirm the dimensionality of the data, principal axis factoring (PAF) with IBM SPSS Statistics 22 (2011) was used to examine patterns of correlations among the questions to measure the perceptions of the respondents from the two countries regarding information security.

Pearson's product-moment correlation coefficient was used to investigate the factorability of the correlation matrix. Preliminary distribution analyses indicated that the assumptions of normality, linearity and homoscedasticy were not violated. The correlation matrix demonstrated a number of coefficients that had a score of 0.3 and above. The Kaiser-Meyer-Olkin value was 0.968, which was well above the recommended minimum value of 0.6. The Bartlett's test of sphericity reached statistical significance, $p<.001$. Thus, the correlation matrix was deemed factorable (Bartlett, 1954; Hair, Black, Babin, Anderson and Tatham, 2010).

Seventy two items (questions) were initially subjected to PAF and 7 of the variables (dimensions) demonstrated very little contribution to the solution, with communalities of less than 0.3 (see Table 2).

Table 2. ISCA items omitted

Question number	Communality
20	0.272
25	0.221
37	0.095
41	0.270
51	0.145
63	0.269
68	0.272

The variables in Table 2 were excluded from the analysis one by one to determine the overall contribution of each variable to the final result. This resulted in a 7-factor solution with two variables (Q47 and Q52) having loadings of less than 0.3. Accordingly, it was decided to exclude Q47 and Q52 from the analysis. The remaining 45 variables resulted in a 7-factor solution, explaining 51.427% (Table 3) of the variation in the data. Due to the large sample, it was decided to allow factor loadings of 0.3 and higher since increasing this cut-off value to 0.4 would have resulted in many more questions being excluded from the solution.

Promax rotation, a rotation method that allows for correlation among the latent factors, was performed. Excluding factor loadings of less than 0.3 resulted in a reasonably simple structure (Hair et al, 2010; Thurstone, 1947), with the 7 factors each showing a number of strong loadings (Table 4).

Table 3. Total variance explained by exploratory factor analysis

Factor	Initial eigen values			Extraction sums of squared loadings		
	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %
1	16.313	36.251	36.251	15.848	35.218	35.218
2	3.739	8.310	44.561	3.297	7.327	42.545
3	1.696	3.769	48.330	1.202	2.671	45.216
4	1.366	3.036	51.366	.846	1.880	47.096
5	1.154	2.564	53.929	.785	1.744	48.840
6	1.076	2.392	56.321	.629	1.398	50.238
7	1.002	2.227	58.548	.535	1.189	51.427
8	.908	2.017	60.565			
9	.826	1.835	62.400			
10	.794	1.765	64.165			
11	.764	1.697	65.862			

The researchers conducted a second-phase factor analysis with the objective of establishing whether the items (questions) in factors 1 and 2 could be further divided into sub-dimensions. Table 5 illustrates that two new dimensions could be created by regrouping the items.

Table 5 illustrates that two new dimensions could be created by regrouping the items.

Table 4. First factor analysis results

Factors	Number of items (statements)	Cronbach's alpha
Factor 1 (see below)	21	0.940
Factor 2 (see below)	11	0.891
Factor 3: Effectiveness	5	0.849
Factor 4: Perception	2	0.626
Factor 5: Assets	2	0.920
Factor 6: Directives	2	0.890
Factor 7: Consequences	2	0.548

Cronbach's alpha was calculated to determine the reliability of each. Table 5 portrays the nine new factors (dimensions) of ISCA. In column three, the corresponding Cronbach's alpha is listed, which is above the lower limit of 0.70. This value may be decreased to 0.60 for exploratory research purposes (Hair, Black, Babin, Anderson and Tatham 2006).

Table 5. Second phase factor analysis

Factors	Number of statements/items	Cronbach's alpha
Factor 1a: Commitment	11	0.909
Factor 1b: Importance	7	0.863
Factor 2a: Responsibility	4	0.779
Factor 2b: Necessity	7	0.847

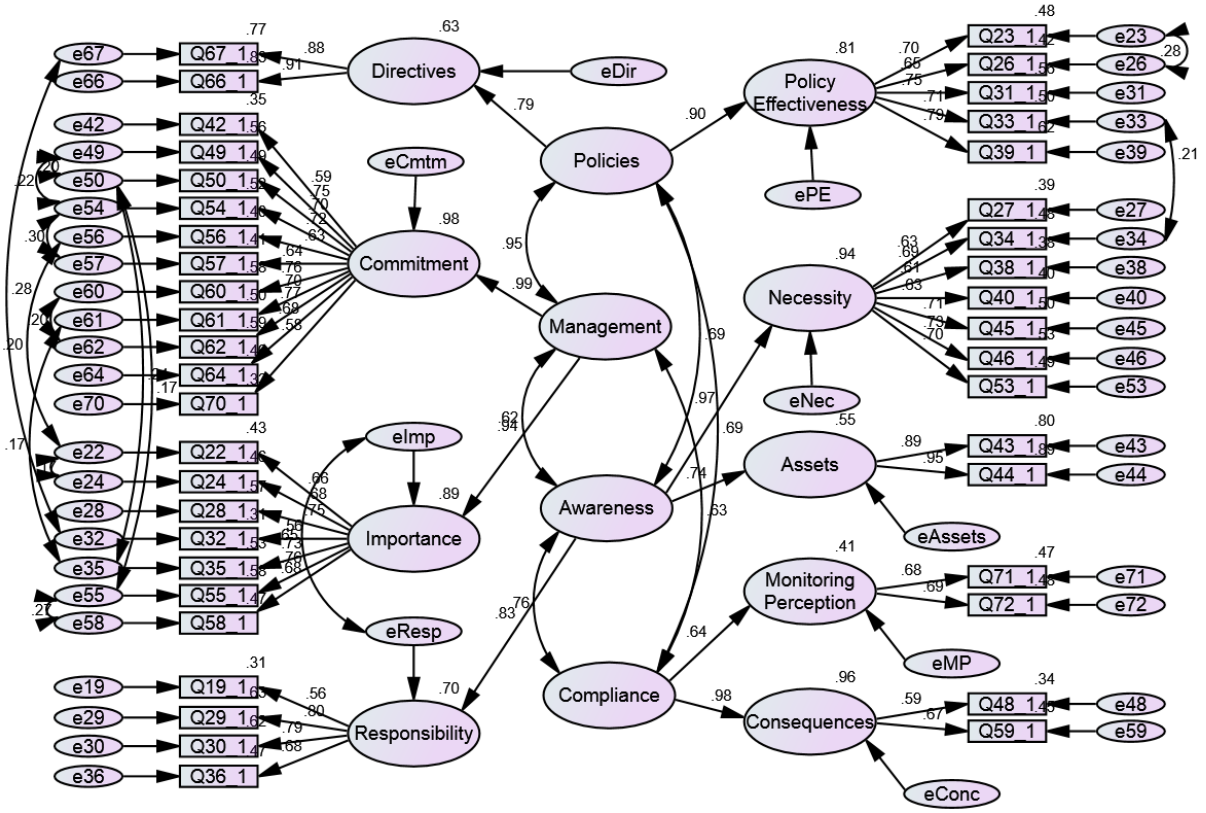
4.2. Overall structural equation modelling

A confirmatory factor analysis (CFA) was conducted next to develop and define the measurement model used for the ISCA questionnaire and dimension's (Hair et al, 2010) on the first-order latent construct level. The assessment was performed using the AMOS (Analysis of Moment Structures) computer program.

To determine whether the measurement model, i.e. ISCA, was equivalent for the UK and SA, the pattern of factor loadings for each observed measure was tested for its equivalence across the two countries. The next step in the process was to test certain hypotheses relating to group invariance. Applying the guidelines provided by Jöreskog and explained by Byrne (2004), the testing of hypotheses relating to group invariance begins with scrutinising the measurement model. In particular, the pattern of factor loadings for each observed measure is tested for its equivalence across the two countries. Once it is known which observed measures are group invariant, these parameters are constrained to be equal, while subsequent tests of the structural parameters are conducted. As each new set of parameters is tested, those known to be group invariant are constrained to be equal across groups (the two countries). According to Bentler and Wu (2002), it is strongly recommended that this orderly sequence of analytic steps be followed. As a prerequisite for invariance, it is also customary to consider a baseline model, which is then estimated separately for each group. The baseline model used to compare with the regression weight equality constraints model is the model obtained as a result of CFA across countries (Martins, 2014).

The error variance of the first-order Commitment construct, however, was .011 ($p<.01$) for SA and -.005 ($p>.05$) for the UK. This negative variance caused a problem and it was therefore decided to constrain the variance for both countries to .01 in the base model. This additional constraint did not cause any change in fit statistics. The regression weights for the 2 countries were constrained to be equal in the model (measurement weights). The final baseline measurement model developed is portrayed in Figure 1 below.

Figure 1. Baseline measurement ISCA model



The next step was to determine the measurement model's validity. Accordingly, acceptable levels of goodness-of-fit (GOF) needed to be established. The GOF illustrates how well the specified model reproduces the observed covariance matrix among the indicator items (Hair et al, 2010). SEM uses several fit indices to determine model fit. Structural equitation modelling fit indices have no single statistical test of significance to identify the best model (Schumacker and Lomax, 1996) therefore more than one model should be considered (Hu and Bentler, 1999). Hair et al (2010) classify GOF measures into three general groups, namely (1) absolute measures, (2) incremental measures, and (3) parsimony fit measures. The authors further suggest using three to four fit indices to provide adequate evidence of model fit, with at least one incremental index and one absolute index in addition to the chi-square and the associated degrees of freedom. The researchers thus used five indices in addition to the chi-square. The results of the GOF analysis and the accompanying criteria are portrayed in Table 6.

Except for the chi-square index, all the other GOF indices were at a level recommended by various authors (Hair et al, 2010; Hu and Bentler, 1999; Schumacker and Lomax). The model thus indicates an overall good fit and can be accepted as a valid model for measuring ICSA, hereby answering research question 2.

Table 6. *Goodness-of-fit indices and criteria for the overall measurement model*

Indices **Absolute fit indices criteria**	Acceptable level	Value	Interpretation
Chi square (CMIN)	Tabled CMIN value (Hair et al 2010)	4057.386	Not a good model fit based on the CMIN value. However, the size of the sample (average n = 1 834) reduced the meaningfulness of this GOF index (Schumacker and Lomax, 1996). Many researchers disregard the CMIN index for samples >200. Accordingly, it is suggested that other GOF indices which may be used to determine the GOF, be considered as well (Schumacker and Lomax, 1996; Hair et al, 2010).
Ratio of CMIN to its degrees of freedom (df)		792	
P-value		0.000	
Goodness-of-fit index (GFI)	0 (no fit) to 1 (perfect fit) (Hair et al, 2010, Hu and Bentler, 1999)	0.941	A good model fit.
Root mean square error of approximation (RMSEA)	< .05 (Hu and Bentler 1999)	0.44	A good model fit.
Incremental fit indices			
Incremental fit index (IFI) - Bollen's IFI	> .90	0.934	A good model fit.
Tucker Lewis index (TLI)	0 (no fit) to 1 (perfect fit) (Hair et al. 1995, 2010)	0.928	A good model fit.
Comparative fit index (CFI)	> .90 (Hair et al, 2010, Hu and Bentler 1999)	0.934	A good model fit.

4.3 Multigroup invariance

To determine if the measurement model was equivalent for the 2 countries, the pattern of factor loadings for each of the observed measures was tested. The baseline ISCA model obtained from the CFA across the 2 countries was used to compare the regression weight equality constraints model. The regression weights for the 2 countries were constrained to be equal in the model (measurement weights). The testing of the baseline model provides a model that might be identically specified for each of the 2 countries.

If the revised model was specified in the same way for each country, this would not necessarily mean that the measurement items and underlying theoretical structure could be applied to both countries, but rather that it should be tested statistically to confirm it.

The GOF indices for the two countries are depicted in Table 7. When the discussed guidelines are considered for the two countries, the results show that the GOF for the UK and SA both indicated good measurement fit. The GFIs for the two countries are lower than the overall GFI, but very close to the proposed 0.90 value. Further analysis of the results of the variances indicated that the variance for all the dimensions of the overall data was significant.

Table 7. GOF indices overall and across the two countries

Indices	Overall	SA	UK
Absolute fit indices			
Chi square (CMIN)	4057.386	2214.380	2567.929
Chi-square/degrees of freedom (df)	792	793	793
P-value	0.000	0.000	0.000
GFI index	0.941	0.888	0.887
Root mean square error of approximation (RMSEA)	0.44	.046	.048
Incremental fit indices			
Incremental fit index (IFI) - Bollen's IFI	0.934	.931	.921
Tucker Lewis index (TLI)	0.928	.925	.914
Comparative fit index (CFI)	0.934	.931	.921

The covariance results indicated that both countries displayed significant relationships between the dimensions, in line with the base model. The two countries were further compared with the objective of identifying the invariance between the countries for the regression weights. The chi-square change from the unconstrained model across the two countries to the measurement weights model is not significant, $\chi 2$ (33) = 44.565, p = .086 (ns) (See Table 8). Thus, the null hypothesis of equal measurement (regression) weights across the two countries could not be rejected. Multigroup invariance can be assumed. The researchers therefore conclude that the constructs for the two countries were formed in the same way.

Table 8. Nested model comparisons

Model	DF	CMIN	P	NFI Delta-1	IFI Delta-2	RFI rho-1	TLI rho2
Measurement weights	33	44.565	.086	.001	.001	-.001	-.001

5. Discussion

This research illustrated that the UK and SA have different maturity ratings with regard to data protection from a regulatory point of view. The UK has data protection laws covering information security principles that have been in place for more than 15 years. SA has a data protection law that is yet to commence and many organisations anticipate that it will take them more than a year to comply with the provisions of the law. From a theoretical perspective one might conclude that the same ISCA instrument cannot be deployed in an organisation with operations in both these countries, as information security principles/conditions are not regulated in the same manner in these countries. To confirm this argument a case study was conducted to derive data that could be used to conduct statistical analysis and establish whether the ISCA could be deployed in this scenario.

The results of the CFA confirmed the validity and reliability of the ISCA across the UK and SA when applied in the context of a national organisation. The data were used to proceed with invariance testing between the two countries. The results of the analysis indicate that multigroup invariance could be assumed. It can thus be stated that the constructs for the UK and SA as measured by the ISCA were formed in the same manner. It is concluded that the ISCA questionnaire can be applied with confidence to measure the information security dimensions (constructs) across the two countries, thus answering research question 3.

This research scope and discussion are limited to the data of the UK and SA as the responses from the other countries that participated in the ISCA were not sufficient to include in the analysis. Another scope limitation is the fact that only a view of data protection and information security was considered, without taking into account the effect of other factors that could influence an information security culture between these two countries, for example, the type of industry, the size of the organisation or the type of information being processed by the organisation.

Additional research could focus on defining an acceptable information security culture level for countries with or without data protection regulation. Such an investigation would need to consider the type of information processed and the risks and business model of the organisation. For future research it is suggested that larger samples from other countries are used through follow-up surveys to retest the multigroup invariance.

6. Conclusion

This research investigated whether an information security culture questionnaire, i.e. ISCA, could be applied by a national organisation at its operations across jurisdictions with limited as well as mature data protection regulations. The data protection in the UK and SA was compared using illustrative criteria

to enable the researchers to rate the data protection maturity of each country. The CMM ratings indicate that the UK is probably on a maturity level of 4, with data protection (privacy and security) being managed and measured consistently, both within organisations and from a government perspective. The maturity level in SA is rated at 1, being at an initial/ad hoc level, with PoPI yet to be commenced and many organisations still having to implement its conditions.

CFA was conducted using a case study where the ISCA was deployed in the UK and SA for an international organisation. The analysis indicates that the ISCA questionnaire can be used with confidence to measure the information security culture in an international organisation with operations across a jurisdiction like the UK with mature data protection regulations, and a jurisdiction like SA where data protection regulation is about to commence. It appears that the international organisation's culture, i.e. the way data protection is being managed internationally by the organisation's group security policy group, the data protection policy and privacy notices to customers visiting their website (operations in the UK and SA have to conform to these policies) does influence its information security culture.

Future research will investigate whether a larger sample of organisations can be included in an ISCA analysis to further test the validity and reliability of ISCA across other countries. Other factors that could potentially influence the information security culture, such as policies and national culture could also be investigated.

References

1 Article 29 Party. Available from: http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm. [Accessed 20.04.15].

2 Bartlett, M.S. (1954), "A note on the multiplying factors for various chi square approximations", Journal of the Royal Statistical Society, Vol.16 No. B, pp. 296–298.

3 Bentler, P.M. and Wu E.J.C. (2002), EQS 6 for Windows guide, Multivariate Software, Encino, CA.

4 Brown, D. (2015), Experiential approach to organizational development, Pearson Education Limited, Essex.

5 Byrne, N. (2004), "Testing for multi group invariance using AMOS graphics: a road less travelled", Structural Equation Modelling, Vol.11 No.2, pp. 272–300.

6 Bygrave, L. (2010), "Privacy and data protection in an international perspective", Scandinavian Studies in Law, Vol 56, pp. 165- 200.

7 Church, A.H. and Waclawski, J. (2001), Designing and using organizational surveys: A seven-step process, Jossey-Bass, San Francisco.

8 Cobit 4.1. (2007), ISBN 1-933284-72-2, IT Governance Institute.

9 Computer Misuse Act of 1990. Available from: http://www.legislation.gov.uk/ukpga/1990/18 [accessed 05.05.15].

10 Condon, R. (2010), "Zurich Insurance breach payment: data breach fine highest on record", Computer Weekly.com. Available from: http://searchsecurity.techtarget.co.uk/news/article/0,289142,sid180_gci1519296,00.html [accessed 25.04.15].

11 Constitution of the Republic of South Africa, (1996), Available from: http://www.gov.za/documents/constitution/constitution-republic-south-africa-1996-1 [accessed 24.04.15].

12 Curtis, J. (2014), "ICO warns of surge in UK healthcare data breaches", ITPRO. Available from: http://www.itpro.co.uk/data-protection/23669/ico-warns-of-surge-in-uk-healthcare-data-breaches#ixzz3ZFQKAkDN [accessed 05.05.15].

13 Da Veiga, A. and Martins, N. (2015a), "Improving the information security culture through monitoring and implementation actions illustrated through a case study", Computers and Security, Vol 49 No 2015, pp. 162-176.

14 Da Veiga, A. and Martins, N. (2015b), "Information security culture and information protection culture: A validated assessment instrument", Computer Law and Security Review, Vol. 31 No. 2015, pp. 243-256.

15 Data Protection Act (PDA). (1998), Available from: http://www.legislation.gov.uk/ukpga/1998/29/contents [accessed 05.05.15].

16 Electronic Communications Act (ECTA). (2005), Available from: http://www.acts.co.za/electronic-communications-act-2005/index.html [accessed 05.05.15].

17 EU Data Directive 95/48/EC. (1995), Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML [accessed 05.05.15].

18 European Commission (EC). (2014), Reform of data protection legislation. Available from: http://ec.europa.eu/justice/dataprotection/ [accessed 05.05.15].

19 Freedom of Information Act. (2000), Available from: http://www.legislation.gov.uk/ukpga/2000/36/contents [accessed 05.05.15].

20 Gatignon, H. (2010), Statistical analysis of management data, 2nd edition. Springer, New York.

21 Greenfield, G. (2014), "Scheherazade and the 101 data privacy laws: Origins, significance and global trajectories", Journal of Law, Information and Science, Vol. 23 No. 1, pp. 1–48.

22 Grobler, M., Jansen van Vuuren, J. and Leenen, L. (2012), "Implementation of a Cyber Security Policy in South Africa: Reflection on Progress and the Way Forward", edited by MD Hercheui et al. (Eds.): HCC10, IFIP AICT 386, pp. 215.

23 Hair, J.F. Jr, Black, W.C., Babin, B.J. and Anderson, R.E. (2010), Multivariate data analysis: A global perspective, 7th edition, Pearson, New York.

24 Hair, J.F. Jr, Black, W.C., Babin, B.J., Anderson, R.E. and Tatham, R.L. (2006), Multivariate data analysis, 6th edition, Prentice Hall, Englewood Cliffs, NJ.

25 Hallinan, D., Friedewald, M. and McCarthy, P. (2012), "Citizen's perceptions of data protection and privacy in Europe", Computer Law and Security, Vol. 28 No. 3, pp. 63–272.

26 Herath, K.M. (2011), "Building a privacy program: A practitioner's guide", International Association of Privacy Professionals, Portsmouth.

27 Herold, R. (2011), Managing an information security and privacy awareness and training program, Taylor and Francis Group, Boca Raton.

28 Hoffstede, G. (1980), Culture's consequences: international differences in work-related values, Sage, Beverley Hills.

29 Hu, L.T. and Bentler, P.M. (1999), "Cut off criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives", Structural Equation Modelling, Vol 6, pp. 1–31.

30 IBM SPSS Statistics. (2011), (Version 21.0 for Microsoft Windows platform) [Computer Software]. Chicago, IL: SPSS Inc.

31 Information Commissioner's Office (ICO). (2015), Available from: https://ico.org.uk/ [accessed 14.04.15].

32 Jordaan, Y. (2007), "Information privacy concerns of different South African socio-demographic groups", Southern African Business Review, Vol. 11 No. 2, pp. 19-38.

33 Martins, N. (2014), "Factorial invariance of the South African culture instrument", Problems And Perspectives In Management, Vol. 12 No. 4, pp. 242-252.

34 Ogbanna, E. (1992), "Managing organisational culture: Fantasy or reality?", Human Resource Management Journal, Vol. 3 No. 2, pp. 42-54.

35 Pfleeger, C.P., Pfleeger, S.L. and Margulies, J. (2015), Security in computing (5th ed.). Prentice Hall, Massachusetts.

36 PricewaterhouseCoopers (PwC). (2011), The Protection of Personal Information Bill: The journey to implementation. Available from: http://www.pwc.co.za/en_ZA/za/assets/pdf/popi-white-paper-2011.pdf [accessed 05.05.15]

37 Privacy and Electronic Communications Regulations. (2003), Available from: http://www.legislation.gov.uk/uksi/2003/2426/contents/made [accessed 05.05.15].

38 Promotion of Access to Information Act (PAIA). (2002), Available from: http://www.acts.co.za/promotion-of-access-to-information-act-2000/index.html [accessed 24.04.15].

39 Protection of Personal Information Act (PoPI). (2013), Available from: http://www.acts.co.za/protection-of-personal-information-act-2013/index.html [accessed 05.05.15].

40 Regulation of Interception of Communications and Provision of Communication and Related Information Act (RICA). (2002), Available from: http://www.acts.co.za/regulation-of-interception-of-communications-and-provision-of-communication-related-information-act-2002/index.html [accessed 05.05.15].

41 Schumacker, R.E. and Lomax RG. (2010), A beginner's guide to structural equation modeling, 3rd ed., Taylor and Francis Group, New York.

42 Swire, P.P. and Berman, S. (2007), Information privacy, official reference for the certified information privacy professional. IAPP, Portsmouth.

43 Thurstone, L.L. (1947), Multiple factor analysis. Chicago University.

44 Turvill, W. (2013), Surge in number of privacy cases heard in UK courts. Pressgazette. Available from: http://www.pressgazette.co.uk/surge-number-privacy-cases-heard-uk-courts [accessed 25.04.15].

45 Wikipedia, Binding Corporate Rules. (2015), Available from: http://en.wikipedia.org/wiki/Binding_corporate_rules [accessed 25.04.15].

46 Zurich, Zurich American Insurance Company. Data security: A growing liability threat fact sheet. (2009), Available from: http://www.zurichna.com/NR/rdonlyres/23D619DB-AC59-42FF-9589-C0D6B160BE11/0/DOCold2DataSecurity082609.pdf [accessed 20.04.15].