A Conceptual Information Security Culture Framework for Higher Learning Institutions

Charles Mawutor Ocloo, Adéle Da Veiga, Jan Kroeze

A Conceptual Information Security Culture Framework for Higher Learning Institutions

Charles Mawutor Ocloo[1[0000-0002-4869-8546]], Adéle da Veiga[2[0000-0001-9777-8721]] and Jan Kroeze[3[0000-0001-7118-4853]]

School of Computing, College of Science, Engineering and Technology, UNISA, South Africa
mcocloo@gmail.com; kroezjh@unisa.ac.za; dveiga@unisa.ac.za

Abstract. Education institutions within and outside Ghana continue to experience mass information leakages at an alarming rate even with the huge investment made in information technology infrastructure to secure their information assets. The lack of organisational commitment to enhance the non-technical aspects of information security – thus, information security culture (ISC) – largely accounts for the consistent rise of security breaches in institutions like the educational institutions. Securing information assets goes beyond technical controls and encompasses people, technology, policy, and operations. The aim of this paper is to identify a comprehensive list of the factors of ISC and construct a conceptual ISC framework (InfoSeCulF) that can be used to provide guidance for the cultivation of a strong ISC in higher learning institutions to secure information assets. A scoping literature review was conducted to determine what constitutes a comprehensive list of factors for cultivating ISC in higher learning institutions. The study proposes a comprehensive list of factors and provides a conceptual framework (InfoSeCulF) which serves as guide for cultivating a strong ISC in institutions.

Keywords: Information security culture · Dimensions · Factors · Framework · Organisation Culture

1 Introduction

The increasing reliance of individuals and institutions on information and technologies has established the need for institutions to secure their information assets. The huge investments being made in technology to protect information assets are not yielding the desired result, and the lack of organisational commitment to enhance the non-technical aspects of information security (thus, information security culture) largely accounts for the consistent rise of security breaches in institutions [1]. Securing information assets "goes beyond technical controls and encompasses people, technology, policy, and operations" [2: 380]. Hence, focusing only on technical controls as the solution to the challenges of information security is not effective. Organisations must give equal attention to the human aspects of information security [2–5] to promote a strong information security culture (ISC) to achieve a holistic approach to tackling information security challenges.

For this study, the factors of ISC refer to components of information security culture such as information security policy and awareness that influence the creation of artefacts and shape assumptions, beliefs, values, attitudes and knowledge. Thus, factors influence ISC on the levels of Schein's definition of organisational culture which are

assumptions and beliefs (for example, our members are our "human firewall"), espoused values, norms and knowledge (for example, members' security compliance increases the organisation's security) and artifacts (for example, an information security policy handbook). The shared information security values and beliefs of members of an organisation influence their behaviour. For the purpose of this study, organisational members of higher learning institutions refer to both staff and students of such institutions.

2 Research aim and question

This paper aims at identifying a comprehensive list of factors of ISC to construct a conceptual information security culture framework (InfoSeCulF) that can provide guidance to effectively cultivate a strong ISC in higher learning institutions to secure information assets. The study seeks to answer the research question:

- What constitutes a comprehensive list of factors for cultivating an information security culture in higher learning institutions?

Sections 1 and 2 provide the introduction and the aim of this study. The paper discusses what constitutes an ISC in section 3, and the challenges of cultivating ISC in higher learning institutions in section 4. Section 5 is a proposal of a list of factors required for cultivating a strong ISC in higher learning institutions. The InfoSeCulF is proposed in section 6 and further discussed in section 7. Limitations and future research work are discussed in section 8, and section 9 presents the conclusion.

3 Background

3.1 Understanding information security culture

This study adopts a comprehensive definition of information security culture proposed by [6] to provide an understanding of what constitutes information security culture. Da Veiga, Astakhova, Botha and Herselman [6: 19] define information security culture as:

> "Information security culture is contextualised to the behaviour of humans in an organisational context to protect information processed by the organisation through compliance with the information security policy and procedures and an understanding of how to implement requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives.
>
> The behaviour over time becomes part of the way things are done, i.e., second nature, as a result of employee assumptions, values and beliefs, their knowledge and attitude towards and perception of the protection of information assets. The information security culture is directed by the vision of senior management together with management support in line with the information security policy and influenced through internal and external factors, supported by an adequate ICT environment, visible in the artefacts of the organisation and behaviour exhibited by employees, thereby creating an environment of trust with stakeholders and establishing integrity."

The above definition was chosen because it is centred on [7] concepts of

organisational culture adapted by [8] to the context of ISC and considers the impact of time on cultivating ISC. The definition provides a comprehensive view of ISC, focusing on six areas namely, knowledge, values and attitudes, behaviour, time, and assumptions, beliefs and perception.

The definition indicates that ISC refers to the security behaviour of members towards protecting the information assets of an organisation. The focus of ISC is on how human actions or inactions (behaviour) in relation to the management, access, sharing and communicating of information affects the security of organisational information assets. All human behaviour aspects are governed by norms [9]. This definition suggests that ISC is relative to an organisational setting, which informs the nature of ISC that ought to be promoted to secure the organisational information assets. The definition also lays emphasis on the essential role of senior management in establishing a strong ISC in organisations [10–12].

The definition indicates that the collective security behaviour of members (thus, ISC) evolves with time. Warrick [13] states that culture, whether purposely developed or left to chance, will certainly evolve with time. Therefore, strategies adopted in dealing with ISC challenges must be relevant to the challenges experienced at a particular period. Per this definition, ISC is greatly influenced by the underlying security assumptions, beliefs, knowledge and attitude promoted in an organisation, as affirmed by [14]. Hence, ISC seeks to address human behaviour so that information security becomes a second nature to employees [15] by defining constructs that create artefacts, shape assumptions, beliefs, values, attitudes and knowledge with respect to time. This implies that ISC in an organisation exists at the levels of security knowledge, assumptions, values, beliefs, attitudes, and artefacts of an organisation; the factors of ISC impact these levels of ISC.

3.2 Organisational Culture and Information Security Culture

A number of research studies [4, 8, 16, 17] have established the connection between organisational culture and ISC. Da Veiga and Martins [17: 72] indicate that "an information security culture (ISC) is a critical component of an organisation's information security programme. It must be embedded in the organisation, changed and influenced to direct employee, contractor and third-party behaviour, in order to reduce risk to the organisation's information assets". Making ISC part of the organisational culture [16] implies embedding ISC in an organisation to positively influence the information security behaviour of members. Organisational culture represents the dominant culture and ISC a subculture [17]. This is implying that ISC should not be functionally isolated from its operational environment (dominated by organisational culture) but must be cultivated within an organisational context.

Schlienger and Teufel [18: 405] indicate that "organizational culture is consequently expressed in the collective values, norms and knowledge of organizations" which impact the behaviour of members. Similarly, ISC is the collective information security knowledge, assumptions, values and artefacts within an organisation [8]. Hence, literature confirms there is a relationship between organisational culture and ISC [8, 17] with organisational culture as the superset and ISC as the subset, and both cultures having common cultural attributes and manifestations.

4 Cultivating information security culture in universities

The discussion on identifying the challenges of cultivating ISC in higher learning institutions was not limited to the Ghanaian context but considers the global situation due to the limited number of literature available on this subject at the time of this study. This offered an appreciation of the information security challenges confronting institutions of higher learning from a global perspective.

Higher learning institutions manage varied information technology resources which include people, IT systems, data or information, software and hardware [19] for the purpose of teaching, learning and research. The vast amount of student, staff, research and financial information owned by higher learning institutions makes them a breeding ground for cybercriminal activities. Kwaa-Aidoo and Agbeko [19] indicate that a successful attack launched on a university's information system will cause economic, operational, reputational, and legal damage.

Higher learning institutions continue to experience mass information leakages at an alarming rate even with the huge investment made in information technology infrastructure to secure their information assets, and the situation keeps worsening as ICT advances [20, 21]. As a result, the education sector has been tagged as a hotbed for data breaches [22].

There are several contributing factors to this trend, with the neglect of the human elements of information security as the ultimate factor [21]. "Unlike business enterprises that have substantial resources to invest into information security, educational institutions are more constrained" [19: 93], making it difficult for them to make adequate investments in establishing ISC.

Kwaa-Aidoo and Agbeko [19] state that the dynamic interactions that occur between students and IT resources in higher learning institutions in Ghana present the most demanding problems associated with establishing ISC. The promotion of Bring Your Own Device (BYOD) in higher learning institutions poses new security risks to institutional information on personal devices of staff [19].

Higher learning institutions in Ghana suffer security incidents such as online fraud, phishing, identity theft, password theft, unauthorized access, malware attacks and change of information on systems, with malware as the most common incident [19]. Hence, [19] states the need for regular information security training programmes for stakeholders of these institutions to mitigate such security risks.

The security investments made in higher learning institutions are highly focused on technical security controls, with little or no attention given to addressing the human elements of information security [21]. Hina, Panneer Selvam and Lowry [23: 1] indicate that "behavioural influence is still a challenge in the information security domain" which needs to be tackled. "An organization's investment in just technology does not eliminate the many security challenges" [1: 269]; equal investment in human factors is also required. The over-reliance on technical controls to secure information assets significantly contributes to the high number of data breaches recorded in higher learning institutions [20, 21, 23]. Hina and Dominic [21: 5] posit that "[t]echnological solutions and behavioral controls together bring a security culture within the organizations".

Moreover, the staff and students of higher learning institutions lack sufficient levels of information security awareness, leading to noncompliance of information security

policies [20] which impacts ISC negatively. The lack of awareness in higher learning institutions has a significant correlation with security attacks like social engineering [24]. Therefore, higher educational institutions must invest in information security training for its workforce [20]. The lax attitude of staff, the culture of openness and availability of information, and the lack of a thorough security policy and plan in higher learning institutions make their IT systems vulnerable to data breaches [21, 25].

The IT security unit of higher learning institutions often develop and implement all information security strategies and procedures without involving end users and top management [21], though employees' and management's involvement is key to reducing employees' violations of security measures [26]. This causes a big communication gap which promotes noncompliance to information security policies and procedures [21]. Apart from the lack of complete and effective security policies and plan, an overwhelming majority of staff of higher learning institutions do not know and understand the content of the information security policies and procedures of their institution [21]. Another cause of the high rate of security breaches is the lack of effective monitoring measures [21].

Although higher learning institutions have invested hugely in implementing technical controls they still experience a consistent attitude of noncompliance with security policies which contributes to the mass leakage of information, reputational damage and possible lawsuits [20]. It is obvious that the information security challenges faced by higher learning institutions are mostly caused by the human elements, and, hence, can be well addressed by implementing a strong ISC. Glaspie and Karwowski [1: 270] state that "a positive information security culture can increase security policy compliance, strengthen the overall information security posture, and reduce financial loss caused by security breaches". It is eminent for higher education institutions to offer due attention to tackle the human issues of information security to implement a strong ISC to reduce the mass leakage of information.

5 Scoping Literature Review

This study adopted a scoping literature review and meta-analysis to identify the factors for cultivating and assessing ISC to propose an appropriate ISC framework that can be used for cultivating ISC in higher learning institutions in Ghana. While a scoping literature review is "an ideal tool to determine the scope or coverage of a body of literature on a given topic and give clear indication of the volume of literature and studies available as well as an overview (broad or detailed) of its focus" [27: 2], meta-analysis employs the use of statistical methods to summarise the results of the literature collected [28]. According to [27], one of the main purposes of conducting a scoping literature review is to identing key factors of a concept, making this method of review suitable for this study.

The scoping literature review was conducted by searching the content of five electronic databases namely ACM, AIS, Emerald, IEEE, Scopus, and Web of Science. The search for articles was conducted by combining keywords related to ISC into search phrases using Boolean operators. The keywords used to conduct the literature search are information security, culture, assessment, measurement, dimension, factors, framework, and maturity model. The terms dimension and factor are used interchangeably by different authors and are both included in frameworks and questionnaires. Hence, both terms were used as keywords to conduct the literature

search to enable the researcher to identify a complete list of ISC factors.

The search was aimed at identifying English papers published from the year 2010 to 2019, where factors for cultivating or assessing ISC were identified. The list was limited to conceptual, and literature works that identified ISC factors or developed ISC framework or designed ISC questionnaire. However, conceptual and literature works with hypotheses that were only stated but not tested were excluded.

Existing frameworks and questionnaires were included because they are designed to comprise and measure factors. Therefore, frameworks and questionnaire were included in selecting the studies for this review as a comprehensive approach to identify all possible factors for assessing and cultivating ISC. This offers the advantage of capturing a holistic view of issues relating to ISC.

5.1 Results of scoping literature review

Per the search conducted, 20 out of 177 initial works identified satisfied the eligibility criteria. Among these 20 works, 8 of them identified factors of ISC, 10 assessed ISC and 2 were works that did both. However, this review focuses on the factors of ISC. Hence, the researchers identified a total of 10 (thus, 8+2) papers that provide content on the factors of ISC.

5.2 Factors for cultivating information security culture

Table 1 provides an overview of related studies. It presents a summary of the ten studies identified during the literature search, indicating the factors proposed by each study and the research approaches by each.

The factors listed in Table 1 with similar description but captioned differently by different studies were recaptioned under the same name. For example, the factors captioned as information security policy, security policies, policy and procedures, and procedural countermeasures were all recaptioned as “Information Security Policy”.

The total count of each factor used in the studies identified for this literature analysis were examined. The factors of studies 4 and 7 were counted as one since study 4 is an update of study 7. The result indicates that factors such as Top management support, Information security awareness, Information security policy and Information security training and education were consistently used, with Top management support as the most cited factor among the studies considered. Though Table 1 indicates the list of main factors proposed by the various studies considered, the subfactors of these main factors were further examined to establish some similarities that exist between these main factors to produce the final list of twenty-five main factors, namely Strategy, Technology, Organisation/Organisational Culture, People, Environment, Top management support, Information security awareness, Information security policy, Information security training and education, Information security risk and assessment, Information security compliance, Information security ownership, Deterrence and incentives, Technology protection and operations, Change management, National and ethical culture, Government initiatives, IT vendors, Information security knowledge, Budget, Information security knowledge sharing, Monitoring, Program Organisation, Trust, and Privacy.

These twenty-five factors of ISC identified are a synthesis of all the various aspects of ISC considered by the ten studies examined, to achieve a more comprehensive list

of factors. This provides the foundation for developing a framework that provides a solution to a broad range of ISC issues to promote the cultivation of a strong ISC in organisations.

5.3 Literature Gaps Identified

The studies considered for this review as captured in Table 1 were either generic in context or conducted for a different context other than higher learning institutions. This indicate the need to conduct a study to develop a framework that fits the context of higher learning institutions since ISC must be contextualised.

Some of these studies [1], [29]–[32] only considered critical or few factors of ISC, indicating that the frameworks or list of ISC factors these studies proposed are not exhaustive and can be expanded to include other factors in different contexts. The results of the review conducted by [30] point out the fact that most of the frameworks considered are fragmented and present a limited view of ISC challenges which is still the case of this review as well. AlHogail and Mirza [30] emphasise the need to conduct more research that take a holistic view of ISC related issues to enable the development of comprehensive frameworks.

This brings to the fore the need to conduct further research that consolidates these fragmented frameworks or lists of ISC factors to present a holistic view of ISC challenges in specific contexts like the higher learning environment.

Although [29, 30], applied the STOPE view to develop an ISC framework, using the STOPE components as factors of this framework with no subfactors or underlining factors will make the implementation of this framework and the assessment of these factors difficult due to fact that the STOPE components capture a broad classification of the factors of ISC. There is a need to connect the STOPE components to factors of ISC for a better appreciation and implementation of the proposed framework.

Considering the impact of human behaviour on ISC and the technology aspects of information security on ISC, [1] notes the limited number of research studies on this subjects, hence advocates for more studies in these issues.

Per the literature analysis conducted, though management was listed as a factor for cultivating ISC by majority of the studies conducted, [1] again advocates the need to conduct research to assess the impact of role of management and other organisational members on ISC.

The literature analysis reveals the following gaps:

1. The need for more research that takes a holistic view (thus, a good appreciation) of ISC related issues to develop a comprehensive framework.
2. There are limited studies that discuss the impact of human behaviour on ISC and how the technology aspects of information security impact the human factors of ISC.
3. The need to conduct further studies for a good appreciation of the roles of management, employees, and other users in organisations and how that influence the cultivation of ISC.
4. The need to consider the tasks that originate due to the relationships between factors of ISC to develop an assessment instrument to assess the ISC level of organisations.
5. The frameworks proposed from the studies considered were either generic in context or focussed on different contexts other than higher learning institutions.

Table 1. Factors of information security culture

Study	Authour(s)	Factors	Approaches
1	Glaspie and Karwowski [1]	5 Factors: Information security policy; deterrence and incentives; attitudes and involvement; training and awareness; management support	Literature Review
2	Masrek, Harun and Zaini [33]	6 Factors: Management support; Policy and procedures; Compliance; Awareness; Budget; Technology	Literature Review
3	Nasir, Arshah, and Ab Hamid [34]	7 Factors: Procedural Countermeasures; Risk Management; Security Education, Training and Awareness (SETA; Policy enforcement Commitment (TMC); Monitoring (MON); Information Security Knowledge (ISK); Information Security Knowledge Sharing (ISKS)	Literature Review
4&7	AlHogail and Mirza [29], [30]	5 Factors: Strategy; Technology; Organisation; People; Environment	Literature Review Survey Validation
5	AlKalbani, Deng and Kam [31]	3 Factors: Management Commitment; Accountability; Information Security Awareness	Literature Review Quantitative Validation
6	Alnathee [35]	8 Factors: Top management support; Information security policy; Information awareness; Information security training and education; Information security risk and assessment; Information security compliance; Ethical conduct policies; Organisational culture	Literature Review
8	Alnatheer, Chan, and Nelson [32]	5 Factors: Security awareness; Information security ownership; Top management involvement; Policy enforcement; Security training	Literature Review Qualitative Quantitative Validation
9	Da Veiga and Eloff [14]	7 Factors: Leadership and governance; Security management and operations; Security policies; Security program management; User security management; Technology protection and operations; change	Literature Review Quantitative Validation
10	Dojkovski, Lichtenstein, and Warren [36]	8 Factors: National and ethical culture; Government initiatives; IT vendors; leadership/corporate governance; Organisational culture; Managerial; Individual and organisational learning; Organisational security awareness	Literature Review Qualitative Focus group discussion Validation

6 A Conceptual Information Security Culture Framework

The final list of factors obtained during the literature review has been used in this study to propose a comprehensive ISC framework (InfoSeCulF) for higher learning institutions grounded on the following:

1. STOPE view developed by [37]
2. Schein's concept of organisational culture [7]

The STOPE view used as the first or primary building block to provide the five development components of the InfoSeCulF. The theory of organisational culture which indicates the levels of culture was used as the second building block.

6.1 The STOPE View

The STOPE view, originally developed by [38], has been applied in conducting various research studies [29], [30], [37], [39]–[43]. This model has been used in various domains of information systems to support the development, integration, and evaluation of IT problems [30].

The STOPE development model is made up of five components namely, Strategy, Technology, Organisation, People and Environment. Security challenges are concerned with organisation, technology, people and environment which can be resolved by adopting appropriate strategies [38]. This presents a holistic view of ISC related issues. Per ISC's focus on context, these components of STOPE, though common to organisations, shows the uniqueness of each organisation, hence, the STOPE view focuses on context. These features make the STOPE view suitable for managing ISC-related issues, hence, it makes this model suitable for implementing ISC that fits within a context.

Each ISC factor (thus, underlining factor of ISC) of the InfoSeCulF, classified under a component of the STOPE view is influenced, developed, and implemented from the standpoint of the STOPE component that it is aligned with. The following paragraphs discuss the STOPE components.

The strategy component defines the development objectives and provides the directions (plan) for achieving these objectives within a time frame [40]. This component consists of ISC factors that serve as plans of action, policies, or best practices adopted to guide employees towards protecting information assets [29]. The strategy component of the InfoSeCulF consist of factors such as Top Management Support, Information Security Policy, Budget, Monitoring, Change and Program Organisation.

The technology component of the STOPE view caters for non-technical issues associated with the use of technology, such as vulnerability caused by how technology is designed, implemented or managed [38]. Although ISC focuses on the non-technical aspect of information security, technology impacts the nature of ISC cultivated in organisations, hence, ISC must consider the non-technical issues associated with technology-related measures that an institution adopts to help build the right values, assumptions and knowledge compatible with technological measures adopted, since technological components of information security affect how employees interact with information assets which translate into security culture [14, 30]. ISC factors such as Technology Protection and Operations, Information Security Risk and Assessment, and IT Vendors constitute the technology component of the InfoSeCulF.

The organisation component of the STOPE view is centred on the structure and culture of an organisation. This component is "the collection of information security related beliefs, values, assumptions, symbols, norms and knowledge that uniquely represent the organization" [29: 569]. Researchers [4, 16, 17] put it firmly that an ISC framework should be developed within an organisational context as it is strongly influenced by the culture and structure of an organisation. This component of the InfoSeCulF, made up of the organisational culture factor, aims at managing the security related cultural attributes to make ISC a part of the dominant organisational culture.

The people component of the STOPE view focuses on transforming the security behaviour of users with direct access to an organisation's information asset. Security behaviour originates from users' interactions with information assets, hence, ISC must manage human factors to improve the security behaviour of users [2, 30]. The factors that constitute the people component are Trust, Information Security Awareness, Information Security Training and Education, Information Security Compliance, Deterrence and Incentives, Information Security Ownership, Privacy, Information Security Knowledge, Information Security Knowledge Sharing and Monitoring.

The environment component of the STOPE model is "the identifiable external elements surrounding the organization that affect its structure and operations and in turn the security of the information assets and the information security culture" [30: 246]. For this reason, the effects of these external elements must be managed when implementing ISC. The factors that constitute the environment component of the InfoSeCulF are National and Ethical Culture and Government Initiatives.

6.2 The Relationship of STOPE Components

The InfoSeCulF adopts the relationship that exist between the STOPE components proposed by [30] in the context of ISC. This relationship which exists because of the interactions between the STOPE components signifies the existing interactions between the subfactors of the InfoSeCulF. This addresses the fourth literature gap stated under section 5.3 for this study.

AlHogail and Mirza [30] argue that the environment component influences ISC, but not vice versa, hence, other components have no relationship to the environment component.

However, [30: 248] states that the relationship between the STOPE components "shows the relationship between factors through the information security culture (ISC)", and not between the factors and ISC. More so, the relationships between the STOPE components signify the underlying interactions between the subcomponents (factors) of the InfoSeCulF. Therefore, the researchers are of the view that there exist relationships between other components of the STOPE model and the environment component, making all the relationships bidirectional.

6.3 Schein's Concept of Organisational Culture

A good understanding of culture is to see it as existing at three different levels (artifacts, espoused values and basic assumptions) spanning from the level of very tangible manifestation that one can see and feel to those that are invincible (thus, deeply embedded), unconscious basic assumptions [7, 44]. Schein [44] posits that behaviour is the result of learned, shared, tacit assumptions that inform people's understanding of

reality, resulting in the way people do things (culture).

Van Niekerk and Von Solms [8] argue that in the context of ISC, knowledge underpins and supports all three levels of organisation culture proposed by [44]. In the context of organisational culture, knowledge is ignored because it is assumed that the average employee has the requisite knowledge to perform core work functions. However, in the context of information security, it cannot be assumed that employees have the required security related knowledge to perform core work functions in accordance with security rules or standards, hence knowledge cannot be ignored [8]. For this reason, [8] introduces the fourth level (knowledge) of culture in the context of ISC.

Information security culture is made up of four levels. The artifact level refers to the visible products or phenomena that is observed when one encounters a group with an unfamiliar culture [7, 44]. Espoused values reflect consciously held beliefs that are carefully stated and practiced [7, 13]. Schein [7] refers to basic assumptions as the degree of agreement that originate from the repeated success of implementing certain beliefs and values, and the knowledge level refers to the information security related knowledge of employees [8]. Schein's concept of organisational culture [7] as adapted by [8] provides a good appreciation of what constitute an ISC and thus, provides a good premise for the development of the InfoSeCulF.

These four levels of ISC which collectively reflects the nature of ISC cultivated in an organisation are influenced by the factors of ISC, such as security awareness and security compliance. Hence, this research considers ISC existing at these four levels which collectively influence the security behaviour of members of an organisation.

7 The InfoSeCulF

The InfoSeCulF adopts the four components of the STOPE view as the ISC development component and the four levels of organisational culture (namely, knowledge, assumptions, beliefs and values, and artefacts). Figure 1 depicts the design of the InfoSeCulF developed for the cultivation of ISC. Each factor of the InfoSeCulF has been mapped to an ISC development component as a subcomponent. The STOPE components represent a holistic view of the categories of ISC issues that must be addressed by the factors of the InfoSeCulF to promote a strong ISC. Therefore, each factor of the InfoSeCulF must be developed and implemented to address the category of ISC that the issue is mapped to. The twenty-one factors of the InfoSeCulF influence the cultivation of ISC which reflects at the levels of ISC which are knowledge, assumptions, espoused values, and artifacts.

These factors of the InfoSeCulF can address the ISC challenges of higher learning institutions. For example, the top management commitment factor is key to addressing the challenge of establishing a strong ISC in higher learning institutions due to the lack of management commitment. Again, the information security policy factor – if comprehensively developed with the involvement of all stakeholders – will significantly promote security ownership and impact the security behaviour of members. This implies that this list of factors fits the context of higher learning institutions, hence, it answers the research question for this study. The design of the InfoSeCulF at this stage is a generic framework which is not specific to the context of Ghana and can be applied in institutions within or outside the educational sector, hence, further research is needed to validate the InfoSeCulF to tailor it to the context of Ghana.

The following bullet points provide information on the factors of the InfoSeCulF.

- Organisational culture: This factor refers to the collective security related assumptions, values, beliefs, and knowledge of an organisation. Its aim is to ensure that these security related attributes of higher learning institutions are in sync with information security measures to motivate organisational members to comply with security guidance to promote ISC.
- Top management commitment: This refers to senior management's appreciation of security functions and involvement in activities to protect the information assets of its organisation. This factor is key to implementing ISC [35].
- Information security policy: This consists of required guidelines or rules established by an organisation (higher learning institution) to guide all information security matters to influence a positive security behaviour to protect information assets [1, 35].
- Information security training and education: This factor refers to the provision of training and education to enable organisational members to acquire the requisite knowledge and skill of dealing with matters of information security.
- Information Security Risk and Assessment: This factor identifies and analyses the information security risk an institution is exposed to and assesses possible threats and their effects on the institution, and actions required to avoid or mitigate the risk [45].
- Deterrence and Incentives: This factor refers to the mechanism for holding members of an organisation accountable to adhering to its information security policy and procedures via the use of punitive measures and rewards. This is very important as it provides a strategy to compel and motivate organisational members to adhere to security policies.
- Technology Protection and Operations: This factor addresses soft issues that arise due to the management of assets and security incidents, development of technical systems, business continuity and management, and other security-related technical operations to protect organisational information assets [14].
- Change Management: This factor manages the security changes that occur in the way of doing things as a result of the implementation of new information security reforms to ensure a more reliable and stable working environment [29].
- National and Ethical Culture: This factor manages the impact of national culture on cultivating ISC [46] and ethical values and beliefs which define what is right or wrong in the context of information security.
- Government Initiatives: This factor manages information security interventions made by governments (such as national information security regulations, policies, guidelines, information security benchmarking and security awareness promotion programmes), all in a bid to promote information security to protect the national digital space and information assets.
- IT Vendors: This factor defines and manages security-related processes and procedures in relation to pre- and post-validation of IT systems supplied by vendors to an organisation to avoid or reduce the risk of compromising their information assets.
- Budget: This refers to information security budget practice (ISC activities) and investment (ISC action taken to gain benefits for attaining ISC goals) made by institutions to attain a reliable and an effective information security culture [33].
- Program Organisation: This factor addresses the programming or systemising of series of ISC activities in order to achieve the collective goals of protecting information assets for the implementation of a successful ISC programme.

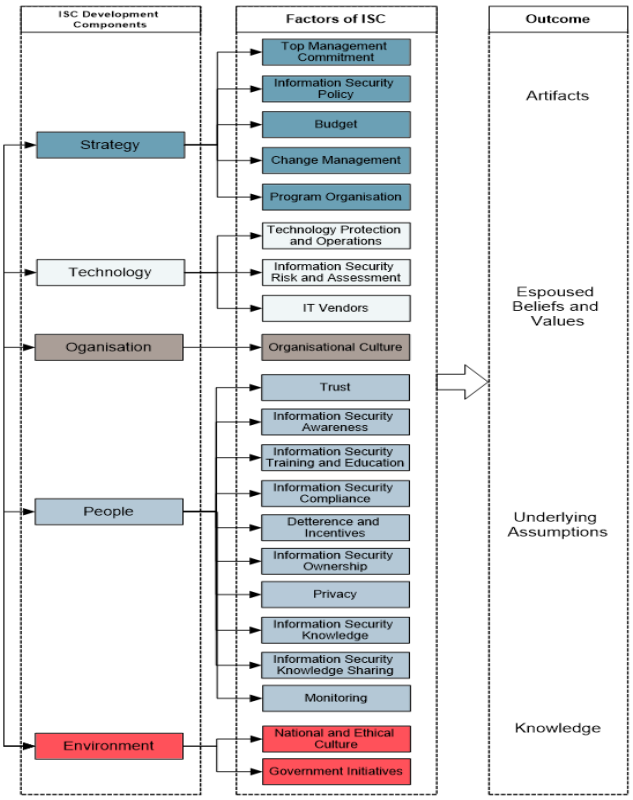

Fig. 1. Proposed information security culture framework (InfoSeCulF)

- Information Security Knowledge Sharing: This factor ensures the availability of security knowledge in the organisation by having members externalise the information security knowledge they have acquired by sharing and [internalise] [by] learning security practices from each other [34].
- Monitoring: Monitoring refers to hidden activities employed to check and ensure the security compliance and behaviour of organisational members and, to some extent, assess the belief and trust of members of an organisation [34].
- Trust: This factor deals with building mutual trust between all parties to promote the joint or team operation in the performance of information security tasks in an organisation [47].
- Privacy: This factor manages the appropriate collection and use of personal information stored on a computing system to avoid compromising information assets.
- Information Security Awareness: Rahman, Lubis and Ridho define information security awareness as “a state of consciousness where [a] user [is] ideally committed to the rules, recognize the potentiality, understand the importance of responsibilities and act accordingly” [48: 361].
- Information Security Compliance : This factor refers to “human information system behaviors with regard to information security policies” [49: 1], indicating the extent at

which the information security behaviour of organisational members is in adherence with the information security policy of an organisation.

- Information Security Knowledge: This factor deals with providing the requisite information security related knowledge to organisational members to influence the cultivation of a stable information security culture at the other three levels of culture, thus, assumptions, values and artefacts [8].
- Information Security Ownership: This deals with instilling a sense of ownership in organisational members that impact their information security behaviour by ensuring that members have a good appreciation of their roles and responsibilities in championing the ISC course of their organisation.

This framework makes a contribution to research by consolidating the different factors of ISC proposed by other researchers to provide a more comprehensive ISC framework that covers a broader scope of issues associated with cultivating ISC. The InfoSeCulF also provides the knowledge on how the underlining factors of ISC such as information security policy, information security awareness and compliance are classified under the main (broader) categories of issues associated with ISC (thus, the STOPE components). This indicates the role played or security related issues tackled by each factor of ISC, providing an effective way to assess and implement an ISC programme.

8 Limitations and future research

This study is limited in the sense that the proposed InfoSeCulF is a conceptual framework, though its factors provide a solution to the challenges associated with cultivating ISC in higher learning institutions, hence, in future work, the researchers intend to conduct a study to evaluate the InfoSeCulF using expert reviewers (information security professionals in higher learning institutions) to validate its comprehensiveness and usefulness and to customise it further to the context of higher learning institutions in Ghana.

9 Conclusion

A scoping literature review was conducted to determine what constitutes a comprehensive list of factors for cultivating ISC in higher learning institutions. The factors identified through the scoping review exercise were explored to propose the InfoSeCulF. The proposed framework (InfoSeCulF) is an integration of the STOPE model with the factors of ISC, where the five components of the STOPE model developed by [38] have been applied in the context of ISC as key components of implementing a successful information security culture. Hence, the InfoSeCulF can be regarded as an extended STOPE model, which can be used for establishing a strong ISC in institutions, especially higher learning institutions.

The InfoSeCulF is a holistic and theoretically sound framework that can assist management and information security professionals in cultivating an effective ISC in higher learning institutions. The development of this framework is motivated by available ISC frameworks, the STOPE view developed by [38] and the theory of organisational culture [7, 8].

References

[1] H. W. Glaspie and W. Karwowski, “Human factors in information security culture: A literature review,” *Adv. Intell. Syst. Comput.*, vol. 593, pp. 267–280, 2018.

[2] A. Caballero, *Information Security Essentials for IT Managers: Protecting Mission-Critical Systems*. Waltham, MA: Morgan Kaufman Publishers, 2013.

[3] A. N. Singh, M. P. Gupta, and A. Ojha, “Identifying factors of ‘organizational information security management,’” *J. Enterp. Inf. Manag.*, vol. 27, no. 5, pp. 644–667, 2014.

[4] M. Tang, M. Li, and T. Zhang, “The impacts of organizational culture on information security culture : a case study,” *Inf. Technol. Manag.*, vol. 17, no. 2, pp. 179–186, 2016.

[5] A. Alhogail, A. Mirza, and S. H. Bakry, “A comprehensive human factor framework for information security in organizations,” *J. Theor. Appl. Inf. Technol.*, vol. 78, no. 2, pp. 201–211, 2015.

[6] A. Da Veiga, L. V. Astakhova, A. Botha, and M. Herselman, “Defining organisational information security culture – Perspectives from academia and industry,” *Comput. Secur.*, pp. 1–52, 2020.

[7] E. H. Schein, *Organizational culture and leadership*, Third. San Francisco,: Jossey-Bass, 2004.

[8] J. F. Van Niekerk and R. Von Solms, “Information security culture: A management perspective,” *Comput. Secur.*, vol. 29, no. 4, pp. 476–486, 2010.

[9] J. E. Anderson and D. Dunning, “Behavioral Norms: Variants and Their Identification,” *Soc. Personal. Psychol. Compass*, vol. 8, no. 12, pp. 721–738, 2014.

[10] M. Mokwetli and T. Zuva, “Adoption of the ICT Security Culture in SMME’s in the Gauteng Province, South Africa,” in *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, 2018.

[11] M. I. Merhi and P. Ahluwalia, “Top management can lower resistance toward information security compliance,” *2015 Int. Conf. Inf. Syst. Explor. Inf. Front. ICIS 2015*, pp. 1–11, 2015.

[12] H. Glaspie, “Assessment of Information Security Culture in Higher Education,” p. 155, 2018.

[13] D. D. Warrick, “What leaders need to know about organizational culture,” *Bus. Horiz.*, vol. 60, no. 3, pp. 395–404, 2017.

[14] A. Da Veiga and J. H. P. Eloff, “A framework and assessment instrument for information security culture,” *Comput. Secur.*, vol. 29, no. 2, pp. 196–207, Mar. 2010.

[15] I. Okere, J. Van Niekerk, and M. Carroll, “Assessing information security culture: A critical analysis of current approaches,” in *The proceedings of IEEE conference on Information Security for South Africa*, 2012, no. August, pp. 136–143.

[16] A. AlHogail and A. Mirza, “Information Security Culture: A Definition and A Literature Review,” in *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, 2014.

[17] A. Da Veiga and N. Martins, “Defining and identifying dominant information security cultures and subcultures,” *Comput. Secur.*, vol. 70, pp. 72–94, 2017.

[18] T. Schlienger and S. Teufel, “Analyzing Information Security Culture : Increased Trust by an Appropriate Information Security Culture iimt (international institute of management in telecommunications),” in *Proceedings of 14th International Workshop on Database and Expert Systems Applications*, 2003, pp. 405–409.

[19] E. K. Kwaa-Aidoo and M. Agbeko, “An Analysis of Information System Security of a Ghanaian University,” *Int. J. Inf. Secur. Sci.*, vol. 7, no. 2, pp. 90–99, 2016.

[20] M. Rajab and A. Eydgahi, “Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education,” *Comput. Secur.*, vol. 80, pp. 211–223, 2019.

[21] S. Hina and D. D. Dominic, “Compliance : A Perspective in Higher Education Institutions,” *Proc. 5th Int. Conf. Res. Innov. Inf. Syst.*, pp. 1–6, 2017.

[22] L. Dignan, “Ransomware incidents surge, education a hotbed for data breaches, according to Verizon.,” 2017. [Online]. Available: http://www.zdnet.com/article/ransomware-incidents-surge-education-a-hot-bed-for-data-breaches-according-to-verizon/. [Accessed: 18-Aug-2017].
[23] S. Hina, D. D. D. Panneer Selvam, and P. B. Lowry, “Institutional governance and protection motivation: Theoretical insights into shaping employees’ security compliance behavior in higher education institutions in the developing world,” *Comput. Secur.*, vol. 87, pp. 1–15, 2019.
[24] E. Metalidou, “Human factor and information security in higher education,” 2014.
[25] J. Saltzman, “Designing Information Systems Security Policy in Higher Education in Higher Education,” 2004.
[26] K. A. Alshare, P. L. Lane, and M. R. Lane, “Information security policy compliance : a higher education case study,” vol. 26, no. 1, pp. 91–108, 2018.
[27] Z. Munn, M. D. J. Peters, C. Stern, C. Tufanaru, A. McArthur, and E. Aromataris, “Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach,” *BMC Med. Res. Methodol.*, vol. 18, no. 1, 2018.
[28] F. O’Kelly, K. DeCotiis, I. Aditya, L. H. Braga, and M. A. Koyle, “Assessing the methodological and reporting quality of clinical systematic reviews and meta-analyses in paediatric urology: can practices on contemporary highest levels of evidence be built?,” *J. Pediatr. Urol.*, vol. 16, no. 2, pp. 207–217, 2020.
[29] A. AlHogail, “Design and validation of information security culture framework,” *Comput. Human Behav.*, vol. 49, pp. 567–575, 2015.
[30] A. AlHogail and A. Mirza, “A Proposal of an Organizational Information Security Culture Framework,” in *Proceedings of 2014 International Conference on Information, Communication Technology and System, ICTS 2014*, 2014, pp. 243–249.
[31] A. AlKalbani, H. Deng, and B. Kam, “Organisational Security Culture and Information Security Compliance for E-Government Development: The Moderating Effect of Social Pressure,” *19th Pacific Asia Conf. Inf. Syst. PACIS 2015 Proceedings. 65.*, Jan. 2015.
[32] M. Alnatheer, T. Chan, and K. Nelson, “Understanding And Measuring Information Security Culture,” in *PACIS 2012 Proceedings*, 2012.
[33] M. N. Masrek, Q. N. Harun, and M. K. Zaini, “Information Security Culture for Malaysian Public Organization: A Conceptual Framework,” in *4th International Conference on Education and Social Sciences 6-8 (INTCESS 2017)*, 2017, pp. 156–166.
[34] A. Nasir, R. A. Arshah, and M. . R. Ab Hamid, “Information security policy compliance behavior based on comprehensive dimensions of information security culture: A conceptual framework,” in *ACM International Conference Proceeding Series*, 2017, vol. Part F1282, pp. 56–60.
[35] M. A. Alnatheer, “Information security culture critical success factors,” in *Proceedings - 12th International Conference on Information Technology: New Generations, ITNG 2015*, 2015, pp. 731–735.
[36] S. Dojkovski, S. Lichtenstein, and M. Warren, “Enabling Information Security Culture: Influences and Challenges for Australian SMEs,” in *ACIS 2010 Proceedings*, 2010.
[37] S. H. Bakry, “Development of e-government: A STOPE view,” *Int. J. Netw. Manag.*, vol. 14, no. 5, pp. 339–350, 2004.
[38] S. H. Bakry, “Development of security policies for private networks,” *Int. J. Netw. Manag.*, vol. 13, no. 3, pp. 203–210, 2003.
[39] N. Adhiarna, Y. M. Hwang, M. J. Park, and J. J. Rho, “An integrated framework for RFID adoption and diffusion with a stage-scale-scope cubicle model: A case of Indonesia,” *Int. J. Inf. Manage.*, vol. 33, no. 2, pp. 378–389, 2013.
[40] S. H. Bakry and F. H. Bakry, “A strategic view for the development of E-business,” *Int. J. Netw. Manag.*, vol. 11, no. 2, pp. 103–112, 2001.

[41] H. Bin-Abbas and S. H. Bakry, “Assessment of IT governance in organizations: A simple integrated approach,” *Comput. Human Behav.*, vol. 32, pp. 261–267, 2014.
[42] M. S. Saleh and A. Alfantookh, “A new comprehensive framework for enterprise information security risk management,” *Appl. Comput. Informatics*, vol. 9, no. 2, pp. 107–118, 2011.
[43] J. Esteves and R. C. Joseph, “A comprehensive framework for the assessment of eGovernment projects,” *Gov. Inf. Q.*, vol. 25, no. 1, pp. 118–132, 2008.
[44] E. H. Schein, *The Corporate Culture Survival Guide*, vol. 17, no. 4. San Francisco, CA: Jossey-Bass, 2009.
[45] H. Naseer, G. Shanks, A. Ahmad, and S. Maynard, “Towards an analytics-driven information security risk management: A contingent resource based perspective,” in *Proceedings of the 25th European Conference on Information Systems, ECIS 2017*, 2017, vol. 2017, pp. 2645–2655.
[46] S. Govender, E. Kritzinger, and M. Loock, “The influence of national culture on information security culture,” in *2016 IST-Africa Week Conference*, 2016, pp. 1–9.
[47] A. Da Veiga, L. V. Astakhova, A. Botha, and M. Herselman, “Defining organisational information security culture – Perspectives from academia and industry,” *Comput. Secur.*, p. 101713, 2020.
[48] A. Rahman, M. Lubis, and A. Ridho, “Information Security Awareness at the Knowledge-Based Institution : Its Antecedents and Measures,” *Procedia - Procedia Comput. Sci.*, vol. 72, pp. 361–373, 2015.
[49] T. B. Lembcke, S. Trang, P. Plics, K. Masuch, S. Hengstler, and M. Pamuk, “Fostering information security compliance: Comparing the predictive power of social learning theory and deterrence theory,” *25th Am. Conf. Inf. Syst. AMCIS 2019*, no. Bandura 1977, pp. 1–10, 2019.