# A Conceptual Model for Cultivating an Information Security Culture

Emad Sherif[1], Steven Furnell[1,2,3], Nathan Clarke[1,3]
[1] *Computer Centre for Security, Communications and Network Research, University of Plymouth, UK*
[2] *Centre for Research in Information and Cyber Security, Nelson Mandela Metropolitan University South Africa*
[3] *Security Research Institute, Edith Cowan University, Western Australia*

## Abstract

*In terms of information security, work within organisations should be guided by a culture of security, with the purpose of protecting the organisation's assets and affecting individual's behaviours towards better security behaviour. The way in which individuals behave with security controls that are implemented to protect an organisation's assets is crucial in protecting such assets. Should the behaviour of individuals not be security compliant, it could have an impact on an organisation's productivity and confidentiality of data. In this paper, key literature relating to security culture in the period of 1999 to 2014 is reviewed. The purpose is to identify frameworks and factors that have been postulated to cultivate a culture of security within organisations in order to develop a tool that assist organisations to cultivate such culture. Our contribution is being able to develop a conceptual model that can assist organisations in cultivating a security culture. The proposed model that comprises three sub-models of creating, maintaining and improving a security culture has been developed based on the outcome of the literature analysis that has identified senior management support, security behaviour, compliance, and awareness as crucial factors along with other variables that have an impact on the continuous process improvement of such a culture.*

## 1. Introduction

In today's business world, information is considered among the most valuable assets an organisation has [1]–[3]. This information must be protected, making sure integrity, confidentiality, and availability are met [2]. The traditional approach that organisations follow in order to protect their assets is implementing technical solutions with regards to information security, such as firewalls, intrusion detection and prevention, and access control systems [2]. Although, such an approach tends to improve the level of information security within organisations, internal threat is overlooked. Despite the nature of such a threat, cultivating a culture of information security that is in line with the organisation's vision and goals can help in improving the level of information security within the organisation [4], [5].

This study is considered as a continuous work to the previous study that aimed at identifying variables that influence cultivating a security culture, whereas this study seeks to develop a preliminary model that can be used to develop a toolkit that assists organisations in measuring, assessing, cultivating a culture of security, and thus to guide the individuals' behaviour towards the protection of an organisation's assets. The aim is to provide an approach that can assist in cultivating a culture of security within an organisation, as well as, assessing and maintaining such a culture. The outcome of such assessment could be used to guide individuals' behaviour towards security compliant behaviour. Such a tool can also provide guidance to organisations on how to develop and maintain a culture of security. Therefore, this paper aims to develop a conceptual model that can be used to develop a tool that can assist organisations in cultivating a culture of information security. This paper will describe information security culture briefly, since it is expected that the reader has background knowledge of the topic. The variables that influence the cultivation of information security culture will be presented within information security compliance section as variables that influence employees' compliance. Finally, the theoretical scenario design of the conceptual model will be presented in the form of three sub-models; creating, maintaining, and improving an information security culture.

## 2. Literature review

Key literature relating to information security culture in the period of 1999 to 2014 has been reviewed. And then, a deeper analysis was conducted to identify frameworks, models and factors that have been postulated to cultivate a culture of security within organisations in order to develop the proposed model. Suitable publications including peer reviewed journals and conferences were identified (e.g. top information security journals, IEEE, etc.). Therefore, a comprehensive literature review has

been conducted to identify key literature relating to information security culture. And then, the outcome of the literature summary and findings analysis led to the identification of the variables that influence information security compliance, and thus, they influence information security culture. As such, a comprehensive literature review has been conducted to identify key literature relating to cultivating or creating a culture of information security. As a result of the analysis, the outcome indicated that in order to cultivate an information security culture, a continuous process improvement of the existed culture needs to be followed, and thus, three categories have been identifies based on the analysis of the summary of relevant findings referring to creating, maintaining, and improving an information security culture sub-models. Therefore, using this approach later in the theoretical scenario design section has been adopted based on the key literature analysis along with the influential variables that have been identified in the first stage of the review. In addition, information security culture and compliance are described as follows:

## 2.1. Information Security Culture

According to [6], "security can only be effective if staff know, understand, and accept the necessary precautions". This highlights the need to foster a culture in which users are aware of the security issues that pertain to them, and have the required knowledge and skills to act appropriately [7]. However, according to [3], "no security policies, standards, guidelines or procedures can foresee all of the circumstances in which they are to be interpreted". Therefore, if stakeholders are not grounded in a culture of security, there is potential for improper actions [3]. And thus, to summarise; the concept of security culture is similar to the concept of culture with focus on being free from danger or threat in terms of human and improper actions, however, security culture have evolved as a logical response to security threats, and are espoused by the management of the organisation.

Furthermore, according to [8], information security culture is often explained using a variety of theories and established principles from other research areas. This is because information security culture is a new and emerging area of research, thus making use of other theories as a basis for research appears logical. Also, according to [9], experts have previously proposed conceptual frameworks for information security management that include information security cultural development based on management initiatives of policy, awareness, training, and education. Attitudes towards the ethics of computer use were affected by various reasons and differences were found among individuals within the same company from the same social background [10].

## 2.2. Information Security Culture

According to [11], information security policy is a written statement that defines the requirements for the organisational security management. It is the employees' responsibility and obligations, sanctions and countermeasures for non-compliance. There are two forms of control that leads to information security compliance behaviour, where informal controls have a stronger effect over formal controls; "Formal controls are important in shaping employee behaviour. This form of control operates through the regularised rules and corresponding sanctions established by the organization. Information security policies are supposed to clearly define unacceptable or illegal conduct, thereby increasing the perceived threat of punishment.", however, "Informal controls reflect the effect of social morality on individual's behaviour. Employees are involving in an organisation and they cannot get rid of group norms and relationships. Individual's form ties with the organisation and the pressure from others can both influence his/her action" [11]. Also, [11] have discussed that perceived certainty of sanctions will be negatively related to employees' information security policy violation intention, as well as, the empirical results of their study suggest the importance of deterrence, social bond and social pressure factors in preventing information security policy violation (influencing compliance/security behaviour).

Furthermore, [10] have concluded that the knowledge retained within the people working for an organisation are the real assets, balancing the fine line between the end user's demands and the security risks posed is where organisations should focus their efforts. Therefore, key literature analysis of twenty five studies was analysed. The process used to identify the candidate variables was to extract all common candidate variables in the key literature relating to information security compliance with regards to information security culture. For each key source, all candidate variables were extracted, and then top common variables were selected, then counted against number of times cited in which they were identified respectively as security behavior, top management, security awareness, policy, and compliance. Despite the fact that it is very difficult to examine every candidate variable that have an impact on information security compliance, the goal of counting variables is to identify top common variables as candidates. Most of the literature studied information security compliance and culture broadly. There is no consensus on what these variables are. And thus, these variables that are postulated to influence security compliance which in turn

influence security culture are described as outlined below.

### 2.2.1. Top Management.

According to [4], the corporate information security policy should describe the vision and goals of senior management in relation to information security. Also, [12] concluded that management of the organisation needs to appreciate where their problems lie, and what each awareness or education option could do to help. However, [13] has argued that the challenges for Information Security from an organisational perspective; develops an argument that builds on research from the management and behaviour. Also, [14] developed a framework of information security practices that could contribute to information security management by identifying behaviours related to different modes of information security practice.

Table 1.Summary of the sub-variables regarding management

| Source | Sub-variable |
|---|---|
| [4] [12] [8] | Senior management support |
| [15] [13] | Security management |
| [2] | Educate management |

Table 1 highlights the need for top level management support, as well as the importance of the role of security managers in supporting information security compliance. [4] suggested that "senior management must be made aware that the protection of information should be their responsibility". Also, [12] suggested that "security culture will be achievable if the concept is supported by top level of the organisation". And such, when considering a culture change in order to change the culture within an organisation into a culture that is more in line with information security, [8] concluded that "identifying the key roles of management in the culture change process is crucial". However, in terms of security management, [15] argued that "information security officer roles are becoming more strategic". And thus, "they need to be aware of and engaged in and supportive of security issues, strategies, and policies" [15]. And such, [13] has concluded that "Good communication with users and senior managers will improve the identity of the Security Manger". Therefore, in order to identify the true outcome and effectiveness of the security process, knowledge and ability of security managers are needed. Finally, according to [2], "management insights regarding information security issues can be used when defining the scope". Thus, educating management about information security is needed.

### 2.2.2. Information Security Policy

According to [9], in response to the organisational security risk that insiders might contribute in, many organisations have developed an interest in cultivating intuitive employees' compliance with information security policy. However and with regards to information security policy violations, [11] concluded that the empirical results of their study suggest the importance of deterrence, social bond and social pressure factors in preventing security policy violation.

Table 2.Summary of the sub-variables regarding information security policy

| Source | Sub-variable |
|---|---|
| [4] | Vision & Goals |
| [16] | Communication methods |
| [17] | Level of acceptance |
| [11] | Policy violation behaviours |

Table 2 highlights the need for having visions and goals along with considering effective methods of communications in order to control policy violations behaviour. According to [4], "The corporate security policy should describe the vision and goals of senior management in relation to information security". However, [16] have suggested that "Encouraging others to communicate and exchange their ideas and beliefs in support of embedding the security policy more widely is important". Such a method offers individuals the chance to get involved in the decision-making process, as well as, it helps to establish trust and support. Moreover, [17] suggested that "the success of security policies and controls will depend on the level of acceptance and compliance". Therefore, recognising the current levels of security acceptance within organisations is crucial. Finally, with regards to the issue of policy violation that might influence an individual's behaviour towards violating security polices within organisations, [11] have concluded that policy violation behaviours can be explained through considering both formal and informal control factors.

### 2.2.3. Information Security Awareness

According to [16], many organisations do not naturally think to check whether awareness is getting through. Furthermore, [9] suggested that "awareness processes must be assessed regularly". As such, [4] argued that assessing employees' awareness help in determining the best approach for the effectiveness and implementation of the information security policy. However, [2] suggested that an information security culture should be based on management-set and endorsed policies, procedures and regulations.

Table 3.Summary of the sub-variables regarding information security awareness

| Source | Sub-variable |
|---|---|
| [12] | Education |
| [9] | External support |
| [16] | Promotion method |
| [2] | Awareness campaigns |
| [10] | Cultural awareness |

Table 3 highlights the need for questioning the effectiveness of the selected promotion methods and awareness campaigns, as well as, fostering a cultural awareness along with the proper support could lead to compliant security behaviour. Information security education is an important process that needs to be managed properly within organisations. According to [12], "All employees need to understand how security relates to them". And such, the selection and implementation process of promotion methods needs to be assed. Also, [16] have suggested that "Significantly questioning the value and effectiveness of the promotion methods". However, [9] concluded that "there is need for external support in order to develop the necessary proactivity to promote and support information security culture internally". Finally, according to [2], "Awareness campaigns should be used both to increase awareness and to make information security a natural part of the organization". And such, "Focus should be on fostering a cultural awareness and understanding surrounding the incredibly diverse range of inf. security issues" [10].

### 2.2.4. Information Security Acceptance

According to [7], cultivating security culture starts by recognising the current levels of security acceptance. As such, "the fact that achieving security acceptance is a multi-stage process can represent a challenge in its own right". Therefore, "The gap between grudging and wholehearted acceptance is filled by a security culture" [3]. Moreover, [3] argued that informed security risk acceptance is an aspect of information security culture.

Table 4. Summary of the sub-variables regarding information security acceptance

| Source | Sub-variable |
|---|---|
| [4] | Security Obedience |
| [7] | Levels of acceptance |
| [14] | Monitoring |
| [17] | Compliance behaviour |

Table 4 highlights that information security acceptance comprises user compliant behaviour, recognising current levels of security acceptance, and monitoring users' security behaviour can have a positive impact on information security compliance. Security obedience is considered as a sub-variable of information security acceptance and defined as "user behaviour complying with the vision of senior management as defined in the corporate information security policy" [4]. However, in terms of cultural change, it is the management responsibility to begin cultivating a culture that is more in line with information security, "having firstly established a solid starting point by recognising the current levels of security acceptance" [7]. Moreover, monitoring individual's behaviour can have a positive impact on information security acceptance. According to [14], "The behaviour of users' needs to be directed and monitored to ensure compliance with security requirements". Finally, [17] presented a model suggesting "using a tool to understand the compliance behaviour of an employee rather than a fully-fledged mechanism that can measure behaviour directly".

### 2.2.5. Information Security Behaviour

According to [18], by changing the organisation to one that is more in line with information security, the behaviour of the individual will adapt to incorporate security. Also, [14] developed a framework of information security practices that could contribute to information security management by identifying behaviours related to different modes of information security practice. However, [19] developed an integrated framework with which to approach the behavioural study of threats and attacks on information and computer systems in organisations. Moreover, [20] argued that security culture and job satisfaction lead to increased compliant security behaviour.

Table 5. Summary of the sub-variables regarding information security behaviour

| Source | Sub-variable |
|---|---|
| [18] | Culture change |
| [13] | Organisational & Human behaviour |
| [21] | Top Management Commitment |
| [14] | Awareness & Education |
| [22] | Personality tests |
| [20] | Security compliance intention/ behaviour |
| [11] | Security violation behaviour |

Table 5 highlights that information security behaviour comprises the following sub-variables: culture change, behaviours, and security awareness & compliance. According to [13], organisational behaviour can be described as "What people do in an organisation and how their behaviour affects the performance". And thus, cultural change can have a positive impact towards changing individuals' behaviour into a behaviour that's more in line with security, according to [18] "culture change can be implemented at three levels: Individuals, group, and

the formal organisation". However, [21] have suggested top management commitment can have a positive impact on information security behaviour. Moreover, according to [14], levels of security training along with security awareness programs in place can have a positive impact towards changing individual's behaviour into security compliant behaviour. Also, [20] suggested that "Job satisfaction and perceived organizational support have a positive effect". Furthermore, according to [22], "Personality test results may possess a predictive value for security behaviour". Finally, according to [11] "Social pressure & Stating penalties for policy violation increases security behaviour".

## 3. Theoretical design

Twenty five studies relating to the top five variables were retrieved for the last ten years. In addition, key literature relating to the cultivation of an information security culture in the period of 1999 to 2014 were studied and discussed in the scenario design section.

### 3.1. Vision

An ideal tool will be designed or developed based on a base line that comprises pre-rules such as does the organisation has an information security policy in place. In addition, such tool must have dimensions (Variables) that influence or affect the implementation or the life cycle process stages of the tool. Accordingly, it must be applicable to every member of staff within an organisation in terms of behaviour, knowledge, attitudes, etc. Such tool will produce contents tailored to individuals or groups based on an organisation's needs assessment with regards to information security.

### 3.2. Dimensions

The literature review analysis has concluded that there are various variables that influence the cultivation of an information security culture. However, five main candidate variables have been identified in which they are postulated to play a crucial rule in the successful development of a security culture tools based on the proposed conceptual model. In addition, there has been a mixture of theoretical and practical research types in the relevant literature. Thus, and in order to list all candidate variables along with their sub-variables, Table 6 illustrates the related research sources along with the nature of the approaches that were used to construct such variables.

Table 6. Summary of the candidate variables and sub-variables in security compliance research

| Source | Variable | Sub-variables | Method |
|---|---|---|---|
| [18] | Security behaviour | Culture change | Theoretical |
| [13] | | Human cooperative behaviour | Theoretical |
| [21] | | Top management commitment | Survey & Questionnaire |
| [14] | | Security awareness & education | Semi-structured interviews |
| [22] | | Personality tests | Focus group |
| [20] | | Compliance behaviour | Survey |
| [4] | Top Management | Senior management support | Theoretical |
| [12] | | | Theoretical |
| [8] | | | Theoretical |
| [15] | | Security management | Theoretical |
| [13] | | | Theoretical |
| [2]) | | Educate management | Interviews |
| [12] | Security awareness & Education | Education | Theoretical |
| [9] | | External support | Focus groups |
| [16] | | Promotion method effectiveness | Theoretical |
| [2] | | Awareness campaigns | Interviews |
| [10] | | Cultural awareness | Theoretical |
| [4] | Security policy | Vision & Goals | Theoretical |
| [16] | | Communication methods | Theoretical |
| [17] | | Level of acceptance | Focus groups |
| [11] | | Policy violation behaviours | Questionnaire |
| [4] | Security acceptance | Security Obedience | Theoretical |
| [7] | | Levels of acceptance | Theoretical |
| [14] | | Monitoring | Semi-structured interviews |
| [17] | | Compliance behaviour | Focus groups |

### 3.3. Scenario design

According to [20], employees' behaviour can be influenced by cultivating a culture of security that enhances security-aware decision making and information security compliance. Such culture comprises the values, beliefs, and assumptions shared by an organisation's employees, which could have an impact on the organisation's security. And thus, a cultural change is needed in order to modify the current beliefs of an organisation's employees [2], however, such change might create some resistance amongst employees. In this scenario the most influential factor is the working environment, which is why such change has to start with the top management. However and according to [2], information security culture should be created then maintained and improved.

#### 3.3.1. Creating an ISC

According to [3], "although information security culture cannot be created, it can be intentionally shaped and directed". As such, according to [23], "Creating a security culture means to change the current culture to a more security-conscious one", however, in order to change the culture, an assessment of the current culture is required, an thus, working areas that need to be focused on during change can be identified. Therefore, creating a secuirty culture means to embed security into the behvaiour of individuals. We used a hypothetical scenario in which items have been adopted from various peer-reviewed sources during the literature review. The identified relevant findings are as follows:

Security decision: "Creating security aware cultures is dependent on improving how individuals make security decisions." [1].

Security Obedience & Knowledge: "Employees should be informed about the security vision of senior management and their roles and responsibilities.", however, "Information Security Obedience as 'de facto user behaviour complying with the vision of senior management as defined in the Corporate Information Security Policy" [5].

Espoused values vs Employees' beliefs & values: "Creating a security culture by instilling the aspects of information security to every employee as a natural way of performing his or her daily job." [24].

Management Support & Vision: "Information secuirty culture is the interaction among many attitudes and beliefs that give a culture life." [3].

#### 3.3.2. Maintaining and Improving an ISC

According to [2], security culture should be maintained and improved in a continues cycle. We used a hypothetical scenario in which items have been adopted from various peer-reviewed sources during the literature review. The identified relevant findings are as follows:

Management commitment & Staff roles: "Identifying the key roles of management and employees is crucial in improving the IT security culture in an organization's operational environment" [23].

Awareness & Monitoring: "Improving our self-awareness as security practitioners and key to doing this is in understanding the process of how we really make decisions. Awareness and monitoring is a key to avoiding groupthink." [1], however, if an organisation is not able to run an effective security awareness program, outsourcing awareness can be considered.

Awareness campaigns and methods: "Developing security culture is not viable without practical examples. Different awareness methods are needed, but each must also be tailored" [25].

Education & Training: "All employees need basic training in information security concepts and procedures" [5].

Security behaviour & Audit: "This data indicates that some cultural values may impact on an individual's security-related behaviour and ultimately influence information security culture in a positive way." [14]. However, "The personnel's knowledge and education should be audited within a year after the initial information security education, as well as, the management and maintenance of the information security culture should be developed based on the results from the audit" [2].

Such model can be adopted and followed in order to maintain and improve an information security culture in a systemised way of working. "These phases are designed to be continuously used as a never-ending cycle to ensure that the organization's information security is kept up to date and improved" [2].

## 4. Findings

According to [2], information security culture should be created then maintained and improved. We therefore are proposing the information culture cultivation tool (see Figure 1) which comprises three models (Create, Maintain, and Improve), where every model has a set of stages that form its life-cycle, along with the five main influential variables (Dimensions) that have an impact upon the process of establish a culture of information security within organisation. Figure 1 illustrated the proposed model, where it comprises three sub-models of creating and maintaining & improving an ISC, along with the main five variables (Dimensions) that have an impact on the processes of creating and maintaining such a culture. Such processes should be developed in different stages as outlined below.

Firstly, creating a culture of information security sub-model comprises three stages where they are exposed to three variables (Management support, Security policy, and security behaviour):

Stage 1: Starts with the assessment of the current state of culture within an organisation while supported by senior management.

Stage 2: Describes the crucial involvement of information security management, setting up an organisation's vision & goals, then defining espoused values (management demands) regarding information security that in line with the vision & goals that have been identified in the previous stage.

Stage 3: Starts with the creating of an information security policy that's in line with the vision & goals that have been identified in the first stage, then educating the management on regular basis while planning cultural change & feedback process throughout the organisation based on the cultural

assessment from the first stage and espoused values that have been identified in the second stage.
Secondly, maintaining a culture of information security sub-model comprises five stages where they are exposed to three variables (Management support, Security policy, and security behaviour):
Stage 4: Starts with establishing an effective information security awareness & education programs where methods need to be studied and selected carefully prior to the implementation of such programs.
Stage 5: Describes the management commitment and involvement is crucial in the process.
Stage 6: Refers to the importance of individuals' behaviour in the process and how it can be affected or transform it into security compliance behaviour with the intention to comply with the security policy where this stage can involve behaviour observation.
Stage 7: Describes that conducting personality tests along with measuring levels of acceptance within an organisation can play an important role in the process.
Stage 8: Refers to the existence of so-called policy violation behaviour that could have a negative impact on the process.
Thirdly, improving a culture of information security model comprises five stages where they are exposed to three variables (Management support, Security awareness & acceptance):
Stage 9: Starts with measuring the current level of security acceptance within an organisation along with using different methods of security awareness promotion can have a positive effect on the process.
Stage 10: Describes that security education & knowledge transfer can enhance security obedience, and thus they have a positive impact on the process.
Stage 11: Starts with asking the organisation whether an external support (Outsourcing) is needed in terms of raising security awareness & education, then, moving to auditing and monitoring individual's behaviour to ensure compliance with security requirement
Stage 12: Describes the importance of reaching the compliance behaviour level within an organisation, along with the effectiveness of the security promotion methods is crucial in this stage.
Stage 13: Describes that evaluating the effectiveness of the awareness campaigns is crucial, as well as, the important role that senior managers, security managers, and staff play in the process is crucial.

Furthermore, it is worth mentioning that 'create ISC' process or changing the current culture to a more security conscious culture happened in the beginning, whilst 'maintain & improve ISC' are ongoing processes. Finally, as illustrated, the three sub-models and their stages are exposed to and influenced by the identified variables (Management support, Security policy, Security behaviour, Security awareness & acceptance).

## 5. Discussion

The proposed model (see Figure 1) can be used to develop a tool that should offer a testing element in order to assist organisations in finding out the current levels of individuals in terms of information security such as security training, skills, and acceptance [14], [26]. However, [18] have argued that "Investigating employee behaviour with regard to information security would be similar to conducting performance appraisals". Therefore, such tests or assessments reports should be used in evaluating an organisation's employees and included within an organisation's staff appraisals. Furthermore, with regards to training and the crucial part that it plays. On the other hand, during the literature review, we have identified two tools that have been developed with regards to information security culture as follows: QinetiQ has developed a security tool that provides ability to measure security behaviour, however, variables that influence information security culture have not been considered [27]. CPNI has developed a tool called "SeCuRE 2", a survey and analysis tool to help organisations understand what their current security culture is, and what they want it to be [28]. However, we argue that there is always need for QinetiQ to analyse the data which in turn might lead to privacy issues, as well as, the fact being dependent on QinetiQ. We also argue that how can we evaluate such tools

## 6. Conclusion

We conclude that properly security trained employees are considered as one of the most valuable organisation's assets. Similarly, creating or developing a culture of information security will improve levels of security compliance and acceptance. And thus, the proposed conceptual model is considered as a valuable contribution towards information security area of research. Furthermore, according to [25], "the development of new tools is needed. These tools must help companies during the creation of a new type of security culture". As such, "This review of the security culture research area illustrates the lack of empirical measurement in the security culture area" [24]. Therefore, the proposed model in this study is considered as a basis for developing a tool that assists organisations in cultivating a culture of information security, where it can be developed, tested, evaluated in future research. In addition, due to lack of relevant practical work in the literature, i.e. rather than simply discussing theories, we suggest exposing some of theories to a more practical context in our future work.

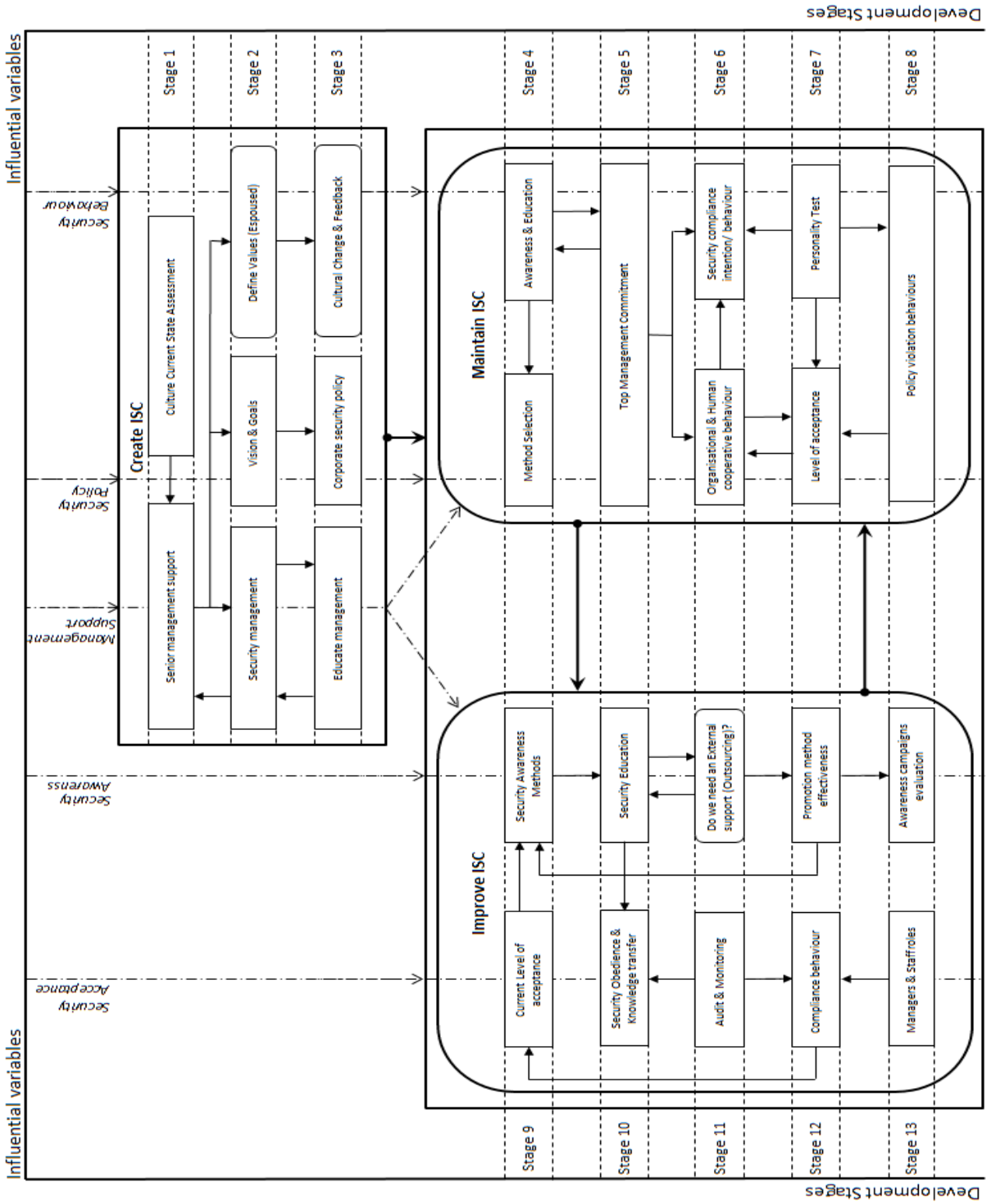


Figure 1. A Conceptual Model for Cultivating an Information Security Culture

## 6. References

[1] Chris Garrett, "Developing security awareness culture improving security decision making," 2004.

[2] A. Fagerström, "Creating, Maintaining and Managing an Information Security Culture.," 2013.

[3] S. J. Ross and R. Masters, Creating a Culture of Security. 2011.

[4] K.-L. Thomson and R. von Solms, "Information security obedience: a definition," Comput. Secur., vol. 24, no. 1, pp. 69–75, Feb. 2005.

[5] K. Thomson, R. Von Solms, and L. Louw, "Cultivating an organizational information security culture," Comput. Fraud Secur., pp. 49–50, 2006.

[6] K. Roer, "How to build and maintain security culture," 2014.

[7] S. Furnell and K. L. Thomson, "From culture to disobedience: Recognising the varying user acceptance of IT security," Comput. Fraud Secur., vol. 2009, no. 2, pp. 5–10, Feb. 2009.

[8] L. Ngo, W. Zhou, and M. Warren, "Understanding Transition towards Information Security Culture Change," pp. 67–73, 2005.

[9] S. Dojkovski, S. Lichtenstein, and M. J. Warren, "Fostering Information Security Culture in Small And Medium Size Enterprises: An Interpretive Study In Australia," pp. 1560–1571, 2007.

[10] J. O'Brien, S. Islam, S. Bao, F. Weng, W. Xiong, and A. Ma, "Information Security Culture Literature Review," no. Lacey 2009, 2013.

[11] L. Cheng, Y. Li, W. Li, E. Holm, and Q. Zhai, "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory," Comput. Secur., vol. 39, pp. 447–459, Nov. 2013.

[12] S. Furnell and N. Clarke, "Organisational Security Culture : Embedding Security Awareness, Education and Training," no. Dti, 2005.

[13] D. Ashenden, "Information Security management: A human challenge?," Inf. Secur. Tech. Rep., vol. 13, no. 4, pp. 195–201, Nov. 2008.

[14] K. Alfawaz, Salahuddin and Nelson, Karen and Mohannak, "Information security culture : A Behaviour Compliance Conceptual Framework," 2010.

[15] M. E. Johnson and E. Goetz, "Embedding Information Security into the Organization," IEEE Secur. Priv. Mag., vol. 5, no. 3, pp. 16–24, May 2007.

[16] C. Chipperfield and S. Furnell, "From security policy to practice: Sending the right messages," Comput. Fraud Secur., vol. 2010, no. 3, pp. 13–19, Mar. 2010.

[17] S. Furnell and A. Rajendran, "Understanding the influences on information security behaviour," Comput. Fraud Secur., vol. 2012, no. 3, pp. 12–15, Mar. 2012.

[18] C. Vroom and R. von Solms, "Towards information security behavioural compliance," Comput. Secur., vol. 23, no. 3, pp. 191–198, May 2004.

[19] I. J. Martinez-Moyano, S. H. Conrad, and D. F. Andersen, "Modeling behavioral considerations related to information security," Comput. Secur., vol. 30, no. 6–7, pp. 397–409, Sep. 2011.

[20] G. Greene and J. D. Arcy, "Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance," pp. 1–8, 2010.

[21] A. Da Veiga and J. H. P. Eloff, "A framework and assessment instrument for information security culture," Comput. Security, vol. 29, no. 2, pp. 196–207, Mar. 2010.

[22] T. Gabriel and S. Furnell, "Selecting security champions," Comput. Fraud Secur., vol. 2011, no. 8, pp. 8–12, Aug. 2011.

[23] L. Ngo, "IT Security Culture Transition Process," 2008.

[24] M. a. Alnatheer, "A Conceptual Model to Understand Information Security Culture," Int. J. Soc. Sci. Humanit., vol. 4, no. 2, pp. 104–107, 2014.

[25] L. Malandrin and T. C. M. B. Carvalho, "Maintaining Information Security in the New Technological Scenario," vol. 5, no. 3, 2013.

[26] S. Furnell and K. L. Thomson, "Recognising and addressing 'security fatigue,'" Comput. Fraud Secur., vol. 2009, no. 11, pp. 7–11, Nov. 2009.

[27] QinetiQ, "Security Culture Tool," 2013. [Online]. Available: http://assets-production.govstore.service.gov.uk/G4/QinetiQ_Ltd-0150/51f978b312a2fcb9e8000aa2/QD1/QQ_HumanFactors Service Description 4.0.pdf. [Accessed: 26-Feb-2015].

[28] CPNI, "SeCuRE: Security Culture Review and Evaluation Tool," Crown, 2014. [Online]. Available: http://www.cpni.gov.uk/Documents/Publications/2014/2014-02-20-secure_tool_guide_for_organisations.pdf. [Accessed: 21-Feb-2015].