Secure Software Development Practice Adoption Model: A Delphi Study

Sri Lakshmi Kanniah and Mohd Naz'ri bin Mahrin Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, MALAYSIA. lksri2@live.utm.my

Abstract— Developing secure software is a major concern in public service organizations as highly-sensitive and confidential data are transacted through online applications. A great number of departments around the public sectors depend on online services to ensure effective services delivery. The insecure software can lead to loss of revenue and damage to business reputation. Implementation of secure development practices throughout the software development lifecycle is influenced by many various factors such as organizational and people factor. Although numerous methods, models and standards in regards to secure software development has been established, implementation of the whole model is quite challenging as it involves cost, skill and time. On that account, this paper presents the results of the Delphi study conducted at the Malaysian Public Service Organization (MPS) with the aim to identify the factors which affect the implementation of secure software development practices. Identified factors are mapped to the security practices in order to establish a relationship between the factors and security practices. In the efforts to achieve this objective, 10 experts who were involved in software development from Malaysian Public Service Organization participated in the study.

Index Terms—Delphi; Secure Software Development; Software Development; Software Security.

I. INTRODUCTION

The rapid growths of internet and e-commerce have instilled revolutionary changes in peoples' lifestyle and living standards. An apparent example of this phenomenon can be witnessed through the fact that almost all business organizations convert the way they run their daily operations and marketing activities from manual to the use of websites. In the same way, the government has been trying to deliver their services effectively and efficiently to meet the needs of citizens, employees, and businesses through electronic means. In accordance with that, E-Government (EG) was initiated to provide online government services delivery to the public users and prompted many government organizations to execute its implementation. Similarly, the Malaysian Public Sector targeted zero face-to-face services delivery with 90% of government services made available online by 2015 [1]. As more services go online, security became the biggest challenge thus increasing the importance of safeguarding the web application from internal and external threats.

This paper reports on the results of an exploratory study conducted at the Malaysian Public Service Organization (MPS) to identify the factors influencing the implementation of secure software development practices. Before addressing the security vulnerability issues that are present in their software, it is important to understand the factors that can influence the organization to implement secure development practices. Several researches have been conducted on secure software development issues [2-4]; however, none of them focused primarily on public service organizations.

II. RELATED WORK

Research in security covers a varied range of approaches and processes that deal with security during software development. Several actions have been suggested in order to incorporate security in the software development life cycle (SDLC) by using different software models. Several modifications have been made to traditional lifecycle by inserting security activities into traditional lifecycle for the purpose of creating security enhanced methodologies and processes [5].

Researchers at University College London have developed 'Appropriate and Effective Guidance in Information Security' (AEGIS), a research model that has integrated security and usability using a spiral model, based on UML. This model defines a UML meta-model of the definition and the rational over the system's assets [6]. AEGIS guides developers to deal with security and usability requirements in system design. The UML meta-model defined by authors identifies assets, the context of operation and supporting the modeling of security requirements. All security decisions in AEGIS are derived from knowledge of assets of the system. Core security activities for system design sessions in AEGIS are: Identification of assets and security requirements, analysis of risk and secure design, and identification of the risks, vulnerabilities, and threats to the system. The output from these activities is documented in a design document which consists of the system architecture with all specified countermeasures. In AEGIS, security expertise is absent in the development process. Moreover, decision making in the selection of security countermeasures is done by stakeholders. The author's rationale behind this is that decision-makers are "better suited to deal with the enforcement of the social requirements of security" while developers are "necessary for the technical implementation of security.

Secure Software Development Model (SSDM) which was developed at the Nigerian University of Agriculture [7] integrates security activities into engineering process, which are: Security training, threat modeling, security specification, review of security specification, and penetration testing. Furthermore, SSDM has separated security specification from functional specification.

The security process 'Comprehensive, Lightweight Application Security Process' - CLASP [8] introduces a lightweight process for SSD. CLASP provides structured practices for deriving security requirements of software systems [9]. CLASP outlines seven key best practices, such as Security awareness, application evaluations, derivation of security requirements, implementation of secure development practices, developing vulnerability remediation measures, defining and monitoring metrics, and publishing operational guidelines. CLASP also specifies a set of activities that should be incorporated in the development lifecycle. CLASP provides roles and security to structure and supports the activities in the resources methodology.

The Microsoft's Security Development Lifecycle (SDL) has incorporated security activities into each development phase of SDLC [10]. Its purpose is to reduce the number of vulnerabilities in software [10]. SDL consists of a set of activities that overcome security issues. The activities in SDL are grouped in phases, which can be mapped to general software development phases.

Seven 'touchpoints' exhibit how software developers can implement them in the development stages. The aim of 'touchpoints' is to increase effectiveness through: code review, architectural risk analysis, penetration testing, riskbased security tests, abuse cases, security requirements, and security operations [9].

Conclusively, the aforementioned models focus on what is needed to build secure software. However, there is a lack of research on identifying the factors required for successful implementation of the SSD process.

III. METHODOLOGY

A Delphi survey technique was conducted with eight (8) experts to determine the SSD implementation factor, assessment indicators for each and the relationship between factors and practices. This information facilitates the development team in identifying SSD practices for each software development project based on the achievement of factors.

A. Delphi Method

The Delphi method was found to be advantageous: (1) to explore or expose underlying assumptions or information leading to different judgments and to seek out information which may generate a consensus on the part of the respondent group [5]. [6] identified two major areas for application of the Delphi technique are the traditional forecasting and more recently concept/framework development where studies typically involve a two-step process being: (1) identifying and elaborating а set of concepts and (2)classification/taxonomy development. Α more comprehensive view of experts in software development was required to identify the factors and assessment criteria. Expert input is also needed in identifying the dependence of secure software development practices on the factors. This can be achieved by mapping each practice with factors influencing the practice. Views from experts could vary according to their level of knowledge and experiences. Thus, the Delphi method was found to be appropriate in exploring these similarities and differences in opinions from experts. The Delphi method is also suitable to facilitate extensive and effective communication and collaboration by multiple experts in determining the factors, indicators, and practices which are

dependent on the factors.

Besides this, the Delphi method encourages sincere opinions from experts without imposing any pressure or conflict that commonly occurs during face-to-face meetings. This improves the validity of the results obtained from this study [7]. Furthermore, the Delphi method is also capable of providing reliable consensus on views among experts, without possible biases during the process [8].

The Delphi method was executed in three phases. Phase 1 and Phase 2 was completed in a single round. However, Phase 3 was completed in two rounds to achieve satisfactory consensus among experts. The objectives of each phase are shown in Table 1.

B. Experts Selection

A fundamental aspect of the Delphi Technique is the selection of the expert panel. [9] indicates that this selection will potentially determine the success of a Delphi study. The initial targeted sample size of experts was 10. To obtain the target sample size of experts in this method, purposive sampling was used with a combination of expert sampling and snowball sampling. Expert sampling and snowball sampling are non-probability sampling techniques, whereby with expert sampling, experts were chosen based on a set of predefined criteria in the area of knowledge and expertise aligned with the objectives of the Delphi method, as well as their ability and willingness to contribute to the study [10]. Since the population of experts with experience in software development and/or software security in the Malaysian Public Sector is unknown, and it was difficult to locate the required experts in the population, snowballing sampling was used to penetrate the unknown population. Therefore, the selection of experts was made on a referral basis. A total of 10 experts participated in this Delphi study consisting of two consultants and eight senior ICT practitioners in the public sector who are involved in software development.

Table 1 Three phases of the Delphi study

Phase	Objective
Phase 1	To determine factors that influence implementation of
(1 Round)	Secure Software Development practices in the public
	sector and to suggest new factors, if any
Phase 2	To determine assessment indicators for each factor that
(1 Round)	influence implementation of Secure Software
	Development practices in the public sector and to
	suggest new indicators, if any
Phase 3	To determine Secure Software Development practices
(2 rounds)	which are dependent on each factor

C. Questionnaire Development for Delphi Study

The questionnaires for the Delphi phases were designed with the appropriate assessment items to achieve the method's objectives. The questionnaires for all three phases were piloted prior to actual the Delphi study to detect and correct inflexibility in terms of questionnaire design, measurement, and analysis. This also increases the validity and reliability of the results from the Delphi study.

IV. RESULTS

A. Phase 1 Delphi Study: To determine factors that influence implementation of Secure Software Development practices in the public sector and to suggest new factors

Phase 1 Delphi study aimed to determine factors that influence the implementation of Secure Software Development practices in the public sector. Experts were asked to state their level of agreement for each of the factor. For this purpose, a structured questionnaire was completed by each of the selected experts. Factors listed in the questionnaire was derived through Systematic Literature Review [11] and interviews with practitioners from public service organizations. An influential factor was determined using a five-point Likert scale: Strongly Agree (5), Agree (4), Neutral (3), Disagree (2) and Strongly Disagree (1). Suggestions by experts on potential factors were analyzed qualitatively using the Grounded Theory. Using the Grounded Theory technique, suggested factors were analyzed to ensure the factors were new factors and different from those listed as constructs in the questionnaire. Meanwhile, the Quantitative analysis was conducted using SPSS Statistics 20 to determine the mode for the probability of occurrences identified by experts. The modes were used as a measure of consensus among the experts. The consensus is achieved if at least 75% of the total experts agreed on a mode, or the majority of the experts have stated the given mode. If multiple modes were calculated, this shows consensus is not achieved among the experts with regards to an agreement on the factors. The modes for the influential factors after Phase 1 Delphi Study is shown in Table 2. The results clearly indicate that all the experts agree that the stated factors influence secure software development practice implementation. Since consensus was achieved in the First Round, there was no need for a second round.

Table 2 Mode for Level of Agreement on Influential Factors for Secure Software Development Practice Adoption

	Factors	Mode of
		Agreement
А	Institutional Context	
1.	Change Management	5
2	Policy Enforcement	5
3	Security Training and Awareness	5
4	Reward and Incentives	4
5	Organization's objectives and culture	5
В	People and Action	
6	Developer	5
7	Top Management	4
8	Security Experts	5
9	Project Manager	4
С	Project Content	
10	Automated tool support	5
11	Cost	4
12	Project Team	5
13	Security Audit Team	5
14	Segregation of role	4
15	Team size	5
16	Team Collaboration	5
17	Development Time	5
D	System Development Processes	
18	Security Documentation	4
	-	
19	Software development methodology	5

 Table 3

 Mean for Level of Agreement on Assessment Indicators

ORGANIZATIONAL CONTEXT Change CM1. Existence of Change Management 4.4 Management Team 4.7 CM2. Change management strategies are 4.7 well communicated with stakcholders. 4.7 Policy PE1. SSD practices and procedures are 4.7 compliance with security policy PE2.SSD practices and procedures are 4.2 compliance with security policy PE3.SSD policy is communicated well 4.1 TAI.Adequate SSD security training is 4.6 about new security policies 7A4.Developers are educated or trained Awareness TA4.Developers are of my information 4.5 reversity polics TA5.Top management and developers are 4.3 aware of the risk of not following the SSD policy TA6.Developers are familiar with the SSD 4.2 reversity colleges TA7.Developers are aware of the reverad 4.1 for reporting security policy violation RE 4.4 occl.Existence of a participative decision 0.3 madic culture OC2.Existence of a support and 4.4 collaboration culture OC2.Exist	Factor	Assessment Indicators	Mean
Change Management (CM) CM1. Existence of Change Management Team 4.4 (CM) CM2. Change management strategies are well communicated with stakeholders. 4.7 Policy PEI. SSD practices and procedures are continually monitored to ensure compliance with security policy 4.7 PE2.SSD violations are reported to the proper authority 4.6 Training and Awareness TA1.Adequate SSD security training is given to all developers 4.6 TA3.Developers are reducated or trained about new security policies 4.6 TA4.Developers aware of my information security roles and responsibilities 4.7 TA5.Top management and developers are aware of the risk of not following the SSD policy 4.2 TA7.Developers are aware of the procedures and culture 4.1 Organization (RD) CCLExistence of a learning and development culture OC3.Existence of a participative decision making culture 4.0 OC2.Existence of a support and collaborito culture OC3.Existence of orleance for conflicts and risk culture 4.3 Developer D.2.Existence of a support and collaborito culture OC3.Existence of tolerance for conflicts and risk culture 4.4 D2.Existence of sDayer sharing culture OC3.Existence of communication skills 4.4 D2.Existence of sDayen the overall goals of the SSD 4.2 D2.Existence of commu		ORGANIZATIONAL CONTEXT	
Management (CM) Team 4.7 Olicy PEI. SSD practices and procedures are continually monitored to ensure compliance with security policy 4.7 POICY PEI. SSD practices and procedures are continually monitored to ensure continually monitored to ensure continually monitored to the proper authority 4.2 Security TA1.Adequate SSD security training is given to all developers 4.6 Awareness TA2.SDD policy is communicated well 4.1 (TA) TA3.Developers are ducated or trained about new security policies 4.6 TA4.Developers aware of my information security roles and responsibilities 4.5 TA5.Top management and developers are aware of the risk of not following the SSD policy 4.2 TA6.Developers are aware of the procedures for reporting security policy violation 4.0 Reward and Incentives RI1.Existence of a learning and s objectives and culture 4.4 OC2.Existence of a participative decision (OC) OC3.Existence of a support and collaboration culture 4.3 Developer D1.Existence of rommunication skills 4.4 D2.Existence of SD experience 4.3 D3.Existence of SD support resources is recognized by management skills 4.4 D2.Existence of SD support	Change	CM1. Existence of Change Management	4.4
(CM) CM2. Change management strategies are well communicated with stakeholders. 4.7 Policy PEI. SSD practices and procedures are continually monitored to ensure compliance with security policy 4.7 (PE) PEI.SSD practices and procedures are externally audited 4.2 proper authority PEI.SSD practices and procedures are to compliance with security painting is given to all developers 4.6 (TA) TA3.Adequate SSD security training is given to all developers are ducated or trained about new security policies 4.6 (TA) TA3.Developers are ducated or trained about new security policies 4.7 TA5.Top management and developers are aware of the risk of not following the SSD policy TA6.Developers are familiar with the SSD 4.2 policy TA7.Developers are of the procedures of the reward policy violation 4.1 Reward and lineentives RI1.Existence of a participative decision queveloperating security policy violation 4.3 s objectives GO2.Existence of a participative decision queveloperating skills 4.4 ocollaboration culture OC2.Existence of a support and queveloperating skills 4.4 (D) D1.Existence of a management skills 4.4 Docy DO2.Existence of a support and queveloperating skills 4.4 (D)	Management	Team	
well communicated with stakeholders. Policy Peli. SSD practices and procedures are combinanely monitored to ensure combinance with security policy PE2.SSD practices and procedures are externally audited PE3.SSD violations are reported to the 4.5 proper authority Training and Awareness Awareness Awareness (TA) TA3.Developers are educated or trained about new security policies TA4.Developers and reponsibilities TA5.Top management and developers are aware of the risk of not following the SSD policy TA6.Developers are familiar with the SSD 4.2 policy TA7.Developers aware of the procedures for reporting security policy violation Reward and RI1.Existence of a participative decision ds.10 GC1 organization' OC2.Existence of a participative decision driks and risk culture OC3.Existence of communication skills OC4.Existence of communication skills OP Diezexistence of controlling skills A1 Developer D1.Existence of communication skills A4 CO2.Existence of a partricipative decision driks and risk culture	(CM)	CM2. Change management strategies are	4.7
Policy PE1. SSD practices and procedures are compliance with security policy 4.7 PE1.SSD practices and procedures are externally audited 4.2 PE3.SSD violations are reported to the proper authority 4.5 Security TA1.Adequate SSD security training is given to all developers TA4.Developers are educated or trained about new security policies 4.6 TA4.Developers are educated or trained about new security policies 4.5 TA4.Developers are advacated or trained about new security policies 4.3 TA5.Top management and developers are aware of the risk of not following the SSD policy 4.2 TA7.Developers are familiar with the SSD 4.2 policy TA7.Developers are aware of the procedures for reporting security policy violation 4.0 Reward and lncentives R1.Existence of reward policy 4.0 OC1.Existence of a participative decision making culture 0.2.Existence of a support and collaboration culture 4.4 OC2.Existence of consuminication skills 4.4 4.4 Developer D1.Existence of controlling skills 4.4 D2.Existence of folerance for conflicts and risk culture 4.3 D2.Existence of SD experience 4.4 D2.Existence		well communicated with stakeholders.	
Enforcement continually monitored to ensure (PE) continually audited PE2.SSD practices and procedures are externally audited 4.2 PE3.SSD violations are reported to the proper authority TA1.Adequate SSD security training is 4.6 Training and given to all developers TA2.SSD policy is communicated well 4.1 (TA) TA3.Developers are educated or trained about new security policies 4.5 TA4.Developers aware of my information security roles and responsibilities 4.5 TA5.Top management and developers are aware of the risk of not following the SSD policy TA6.Developers are familiar with the SSD policy TA6.Developers are aware of the procedures for reporting security policy violation 4.0 Incentives RI1.Developers are aware of the reward policy 4.0 Incentives OC1.Existence of a participative decision development culture 4.3 organization' OC2.Existence of a support and collaboration culture 4.4 OC3.Existence of communication skills 4.4 Developer D1.Existence of ronagement skills 4.4 D2.Existence of communication skills 4.4 D2.Existence of conoronling skills 4.4	Policy	PE1. SSD practices and procedures are	4.7
(PE) compliance with security policy PE3.SSD practices and procedures are externally audited PE3.SSD violations are reported to the proper authority Security TA1.Adequate SSD security training is given to all developers are educated or trained about new security policies 4.6 (TA) TA3.Developers are educated or trained about new security policies 4.5 TA4.ADevelopers aware of my information security roles and responsibilities 4.3 TA5.Top management and developers are aware of the risk of not following the SSD policy 4.6 TA6.Developers aware of the procedures 4.1 Reward and ln.Existence of reward policy 4.0 R12.Developers are aware of the reward 4.1 Policy TA7.Developers are aware of the reward 4.1 OC1.Existence of a learning and s objectives development culture 4.3 OC2.Existence of a payner sharing culture 4.3 OC3.Existence of romunication skills 4.4 (DC) D2.Existence of a power sharing culture 4.3 OC2.Existence of controlling skills 4.4 Developer D1.Existence of controlling skills 4.4 (D) D2.Existence of sD1 experience 4.4 D6.Existence of SD1 experience 4.4	Enforcement	continually monitored to ensure	
PE2.SSD practices and procedures are externally audited 4.2 PE3.SSD violations are reported to the proper authority 4.5 Security TA1.Adequate SSD security training is d.6 (TA) TA2.SSD policy is communicated well d.1 TA2.SSD policy is communicated well to the about new security policies 4.4 TA4.Developers are educated or trained about new security policies 4.5 TA5.Top management and developers are aware of the risk of not following the SSD policy 4.7 TA6.Developers are familiar with the SSD policy 4.2 TA7.Developers are familiar with the SSD policy 4.4 rA6.Developers are familiar with the SSD policy 4.0 Reward and R11.Existence of reward policy violation 4.1 Reward and R11.Existence of a participative decision development culture 4.3 organization' OC1.Existence of a participative decision disculture 4.4 OC3.Existence of a power sharing culture 0.3 4.4 OC4.Existence of communication skills 4.4 4.4 Developer D1.Existence of communication skills 4.4 D2.Existence of SD experience 4.4 4.4 D2.Existence of SD experience 4.4 D2.Existence of SD experie	(PE)	compliance with security policy	1.0
PE3.SSD violations are reported to the proper authority Security TA1.Adequate SSD security training is Awareness TA2.SSD policy is communicated well (TA) TA3.Developers are educated or trained about new security policies TA4.Developers aware of my information security roles and responsibilities TA5.Top management and developers are aware of the risk of not following the SSD policy TA6.Developers aware of the procedures for reporting security policy violation Reward and R1.Existence of reward policy TA7.Developers are aware of the procedures for reporting security policy violation Reward and R1.Existence of a learning and s objectiv OC2.Existence of a learning and 4.4 collaboration culture OC3.Existence of a support and collaboration culture OC3.Existence of a support and collaboration culture OC3.Existence of planning skills 4.4 DE.Existence of SDD experience 4.3 Di Existence of SDD experience TM1.The degree to which functional Management Management (TM) SDD explores to full as a support resources to the SDD intexistence of SDD experience 4.4 Di Existence of controlling skills 4.4 Di Existence of controlling skills 4.5 Management Management M3.The degree to which functional Management is enthusiastic about the possibilities of SSD TM4.The degree to which functional Management support the overall goals of the SSD Security Experts (SE) SE1.Existence of controlling skills 4.6 Project M1.Existence of controlling skills 4.6 PM1.Existence of controlling skills 4.7 PM4.Existence of controlling skills 4.7		PE2.SSD practices and procedures are	4.2
Proper authority Proper authority Security TA1.Adequate SSD security training is given to all developers 4.6 Mwareness TA2.SSD policy is communicated well 4.1 (TA) TA3.Developers are educated or trained about new security policies 4.6 TA4.ADevelopers aware of my information security roles and responsibilities 4.5 TA5.Top management and developers are aware of the risk of not following the SSD policy 4.2 TA7.Developers aware of the procedures 4.1 Reward and R11.Existence of reward policy 4.0 R1.Developers are aware of the reward 4.1 policy TA7.Developers are aware of the reward 4.1 R1.Developers are aware of the reward 4.1 policy TA7.Developers are aware of the reward 4.1 policy CO1.Existence of a participative decision 4.3 (CC) OC2.Existence of a participative decision 4.3 (OC) OC2.Existence of communication skills 4.4 collaboration culture OC4.Existence of controlling skills 4.4 D D1.Existence of SD experience 4.4 D D2.E		EXECUTION AUDITED	15
Description Description Project analysis 4.6 Training and Awareness TA1. Adequate SSD security training is given to all developers 4.1 (TA) TA3.Sevelopers are educated or trained about new security policies 4.1 (TA) TA3.Developers are educated or trained about new security policies 4.5 TA4.Developers are educated or trained aware of the risk of not following the SSD policy 4.3 TA6.Developers are familiar with the SSD 4.2 policy TA7.Developers are familiar with the SSD 4.2 repolicy TA7.Developers are familiar with the SSD 4.2 repolicy TA7.Developers are aware of the procedures 4.1 (RI) policy 4.0 Organization' CC1.Existence of a learning and s objectives 4.4 and culture OC2.Existence of a power sharing culture 4.3 (OC) D1.Existence of communication skills 4.4 (D) D2.Existence of communication skills 4.4 (D) D2.Existence of Communication skills 4.4 (D) D2.Existence of communication skills 4.4 (D)		proper authority	4.5
Security TA1.Acculate SDD security training its 4.3 Awareness TA2.SSD policy is communicated well 4.1 (TA) TA3.Developers are educated or trained about new security policies 4.5 TA4.Developers aware of my information security roles and responsibilities 4.5 TA5.Top management and developers are aware of the risk of not following the SSD policy 4.3 TA6.Developers aware of the procedures for reporting security policy violation 4.1 Reward and RI1.Existence of reward policy 4.0 RI2.Developers aware of the reward sobjectives 4.1 and collaboration culture OC1.Existence of a learning and development culture 4.4 OC2.Existence of a participative decision making culture 4.3 OC3.Existence of tolerance for conflicts and risk culture 4.4 OC4.Existence of communication skills 4.4 D2.Existence of controlling skills 4.4 D3.Existence of controlling skills 4.4 D4.Existence of controlling skills 4.4 D5.Existence of controlling skills 4.4 D4.Existence of controlling skills 4.4 D4.Existence of controlling skills 4.4 D5 D5.Existence of sDD experinece <td< td=""><td>Security</td><td>TA1 Adequate SSD security training is</td><td>16</td></td<>	Security	TA1 Adequate SSD security training is	16
TAwareness TA2.SSD policy is communicated well 4.1 (TA) TA3.Developers are educated or trained about new security policies 4.6 TA4.Developers are educated or trained about new security policies 4.5 TA4.Developers aware of my information security roles and responsibilities 4.5 TA5.Top management and developers are aware of the risk of not following the SSD policy 4.3 TA6.Developers are familiar with the SSD 4.2 policy TA7.Developers are of the procedures for reporting security policy violation 4.1 (RI) policy 4.0 Organization' CO1.Existence of a learning and s objectives 4.4 and culture OC2.Existence of a support and collaboration culture 4.4 OC3.Existence of communication skills 4.4 (OC) D1.Existence of communication skills 4.4 (D) D2.Existence of controlling skills 4.4 (D) D2.Existence of controlling skills 4.4 (D) D2.Existence of technical skills 4.3 (D) D2.Existence of controlling skills 4.4 (D) D2.Existence of technical skills 4.3 D3.Existence of controlling skills 4.4	Training and	given to all developers	4.0
(TA) TA3.Developers are educated or trained about new security policies 4.6 TA4.Developers are educated or trained about new security policies 4.5 TA4.Developers are and responsibilities 4.5 TA5.Top management and developers are aware of the risk of not following the SSD policy 4.3 TA6.Developers are familiar with the SSD policy 4.2 TA6.Developers are aware of the procedures 4.1 for reporting security policy violation 4.0 Reward and RI1.Existence of reward policy 4.0 Incentives R12.Developers are aware of the reward 4.1 (RI) policy 4.0 Organization' s objective development culture 4.1 4.4 c01.Existence of a participative decision 4.3 (OC) making culture 4.3 OC2.Existence of a power sharing culture 4.3 OC4.Existence of communication skills 4.4 c0laboration culture 4.3 Developer D1.Existence of communication skills 4.4 Developer D1.Existence of communication skills 4.4 D2.Existence of SD experience 4.4 D4.Existence of controlling skills 4.6 </td <td>Awareness</td> <td>TA2 SSD policy is communicated well</td> <td>41</td>	Awareness	TA2 SSD policy is communicated well	41
(III) The intervent of the security policies 1.0 about new security policies TA4.Developers aware of my information security roles and responsibilities 4.5 TA5.Top management and developers are aware of the risk of not following the SSD policy TA6.Developers are familiar with the SSD 4.2 TA6.Developers are familiar with the SSD policy TA7.Developers are familiar with the SSD 4.2 TA7.Developers are aware of the procedures for reporting security policy violation 4.1 Reward and Incentives RI1.Existence of reward policy 4.0 Reward and culture OC1.Existence of a learning and development culture 4.4 organization' OC1.Existence of a participative decision 4.3 4.4 collaboration culture OC2.Existence of a support and collaboration culture 4.4 OC5.Existence of tolerance for conflicts and risk culture 4.3 Developer D1.Existence of communication skills 4.4 D2.Existence of controlling skills 4.4 D3.Existence of controlling skills 4.4 D4.Existence of controlling skills 4.4 D5.Existence of controlling skills 4.4 D4.Existence of controlling skills 4.4 D4.Existence of subrohic functional managers willingly assign resources to	(TA)	TA3 Developers are educated or trained	4.6
TA4. Developers aware of my information security roles and responsibilities 4.5 TA5. Top management and developers are aware of the risk of not following the SSD policy 4.3 TA6. Developers are familiar with the SSD 4.2 policy TA7. Developers aware of the procedures for reporting security policy violation 4.1 Reward and Incentives R11. Existence of reward policy 4.0 Riz. Developers are aware of the reward 4.1 (RI) policy 4.4 organization' OC1. Existence of a learning and s objectives 4.4 (OC) making culture 0C2. Existence of a support and culture 4.4 OC3. Existence of tolerance for conflicts and risk culture 4.3 OC4. Existence of tolerance for conflicts and risk culture 4.4 Developer D1. Existence of romanication skills 4.4 D1. Existence of rommunication skills 4.4 D2. Existence of controlling skills 4.4 D4. Existence of controlling skills 4.4 D5. Existence of controlling skills 4.4 D6. Existence of controlling skills 4.4 D5. Existence of sSD experience 4.4 D6. Existence of sufficient security experts <	(111)	about new security policies	1.0
security roles and responsibilities TA5. Top management and developers are aware of the risk of not following the SSD policy TA6. Developers are familiar with the SSD policy TA7. Developers are of the procedures for reporting security policy violation Reward and R11. Existence of reward policy Norganization' s objectives development culture and culture OC2. Existence of a learning and s objectives development culture OC3. Existence of a support and collaboration culture OC4. Existence of a support and collaboration culture OC4. Existence of a participative decision development culture OC4. Existence of a participative decision (OC) Developer D1. Existence of tolerance for conflicts and risk culture D2. Existence of tolerance for conflicts and risk culture D1. Existence of tolerance for conflicts and risk culture D2. Existence of communication skills 4.4 D4. Existence of technical skills 4.5 D5. Existence of controlling skills 4.2 Top TM1. The degree to which functional managers willingly assign resources to the (TM) SSD implementation as they are needed TM2. The degree to which executive managers of SDD support resources is recognized by management TM3. The degree to which all levels of management support the overall goals of the SSD SE6. Existence of communication skills 4.7 SE3. Existence of sD furticing skills 4.7 SE3. Existence of planning skills 4.6 D5. Existence of sD experience 4.1 Management support the overall goals of the SSD TM4. The degree to which all levels of management support the overall goals of the SSD SE6. Existence of controlling skills 4.6 Project PM1. Existence of controlling skills 4.6 (PM) PM3. Existence of controlling skills 4.7 PM4. Existence of controlling skills 4.7 PM4. Existence of controlling skills 4.7 PM4. Existence of technical skills 4.7 PM4. Existence of technical skills 4.7 PM4. Existence of SSD experience 4.2 PM6. Existence of controlling skills 4.7		TA4.Developers aware of my information	4.5
TA5.Top management and developers are aware of the risk of not following the SSD policy 4.3 TA6.Developers are familiar with the SSD policy TA6.Developers are familiar with the SSD 4.2 TA7.Developers aware of the procedures for reporting security policy violation 4.1 Reward and R11.Existence of reward policy 4.0 Incentives R2.Developers are aware of the reward 4.1 (RI) policy 4.0 Organization' OC1.Existence of a learning and 4.4 4.3 s objectives development culture 4.3 (OC) making culture OC3.Existence of a support and collaboration culture 4.4 OC4.Existence of a power sharing culture 4.3 OC5.Existence of communication skills 4.4 (D) D2.Existence of communication skills 4.4 (D) D2.Existence of communication skills 4.4 (D) D2.Existence of controlling skills 4.6 D5.Existence of controlling skills 4.6 D5.Existence of controlling skills 4.2 (D) D2.Existence of controlling skills 4.2 (D) D2.Existence of sDD experience 4.4 D6.Existence of sDD support resources		security roles and responsibilities	
aware of the risk of not following the SSD policy TA6. Developers are familiar with the SSD policy TA7. Developers aware of the procedures for reporting security policy violation 4.1 Reward and Incentives RI1. Existence of reward policy 4.0 Reward and Incentives RI1. Existence of reward policy 4.0 Organization' OC1. Existence of a learning and sobjectives 4.4 GV2. Existence of a participative decision 4.3 (OC) making culture 0C2. Existence of a support and culture 4.4 OC3. Existence of a power sharing culture 0C4. Existence of communication skills 4.4 (DC) D2. Existence of communication skills 4.4 (D) D2. Existence of SDD experience 4.4 (D) D2. Existence of support esources to the SSD implementation as they are needed 4.2 Top TM1.The degree to which functional management 4.2 (TM) SSD implementation as they are needed 4.1 TM2.The degree to which executive management senthusiastic about the possibilities of SSD 4.5 SE2. Existence of communication skills 4.6 SE3. Existence of SD experience 4.8 SE4. Existence of support resources is recognized by managem		TA5.Top management and developers are	4.3
policy TA6.Developers are familiar with the SSD policy TA7.Developers aware of the procedures for reporting security policy violation 4.2 Reward and Reward and RI1.Existence of reward policy Incentives ad culture RI2.Developers are aware of the reward (R) policy 4.0 Organization' s objectives and culture OC2.Existence of a learning and evelopment culture OC3.Existence of a participative decision making culture OC4.Existence of a support and collaboration culture OC4.Existence of a power sharing culture OC4.Existence of tolerance for conflicts and risk culture 4.4 Developer D1.Existence of communication skills D2.Existence of tolerance for conflicts and risk culture 4.4 Developer D1.Existence of tolerance for conflicts and risk culture 4.4 D2.Existence of SSD experience Management 4.4 D4.Existence of SSD experience Management 4.4 TM2.The degree to which functional managers willingly assign resources to the SSD implementation as they are needed TM2.The degree to which all levels of management support the overall goals of the SSD 4.1 Security Experts (SE) SE1.Existence of sufficient security experts SE2.Existence of planning skills 4.5 SE4.Existence of SDD experience 4.8 SE4.Existence of planning skills 4.7 SE3.Existence of communication skills 4.7 SE4.Existence of communication skills 4.7 SE4.Existence of communic		aware of the risk of not following the SSD	
TA6.Developers are familiar with the SSD 4.2 policy TA7.Developers aware of the procedures for reporting security policy violation 4.1 Reward and RI1.Existence of reward policy 4.0 Incentives RI2.Developers are aware of the reward 4.1 (RI) policy 4.0 Organization' OC1.Existence of a learning and development culture 4.4 and culture OC2.Existence of a support and collaboration culture 4.3 (OC) making culture 0C3.Existence of tolerance for conflicts and risk culture 4.6 Developer D1.Existence of tolerance for conflicts and risk culture 4.4 Developer D1.Existence of technical skills 4.4 (D) D2.Existence of sD3D experience 4.4 D4.Existence of controlling skills 4.4 D4.Existence of controlling skills 4.2 Top TM1.The degree to which functional managers willingly assign resources to the management is enthusiastic about the possibilities of SSD 4.1 (TM) SSD implementation as they are needed TM2.The degree to which executive experts (SE) 4.5 Security SE1.Existence of sufficient security experts 4.9 4.5 SE2.Existence of sufficient		policy	
policy TA7.Developers aware of the procedures for reporting security policy violation 4.1 Reward and Incentives RII.Existence of reward policy RI2.Developers are aware of the reward (RI) 4.0 Organization' S objectives OC1.Existence of a learning and evelopment culture OC2.Existence of a participative decision making culture OC3.Existence of a support and collaboration culture OC4.Existence of a power sharing culture OC5.Existence of tolerance for conflicts and risk culture 4.3 Developer D1.Existence of IT management skills 4.4 (D) D2.Existence of IT management skills 4.4 (D) D2.Existence of sSD experience 4.4 D4.Existence of controlling skills 4.4 D4.Existence of controlling skills 4.2 Top TM1.The degree to which functional managers willingly assign resources to the SSD implementation as they are needed 4.1 (TM) SSD support resources is recognized by management TM3.The degree to which all levels of the SSD 4.5 Security SE1.Existence of sufficient security experts 4.9 SE2.Existence of planning skills 4.6 SE3.Existence of sufficient security experts 4.9 Existence of sufficient security experts 4.9 SE3.Existence of controlling skills 4.7 SE3.Exi		TA6.Developers are familiar with the SSD	4.2
TA7. Developers aware of the procedures for reporting security policy violation 4.1 Reward and Incentives RII. Existence of reward policy 4.0 Nether Mark Policy 4.0 Organization' OC1. Existence of a learning and s objectives 4.1 Norganization' OC1. Existence of a participative decision making culture 4.3 (OC) OC3. Existence of a power sharing culture OC4. Existence of a power sharing culture 4.4 OC5. Existence of tolerance for conflicts and risk culture 4.6 Developer D1. Existence of communication skills 4.4 (D) D2. Existence of planning skills 4.4 (D) D1. Existence of technical skills 4.4 (D) D1. Existence of sDD experience 4.4 (D) D2. Existence of controlling skills 4.2 Top TM1. The degree to which functional Management 4.2 Management TM2. The degree to which the need for Inog-term SSD support resources is reccognized by management 4.1 TM3. The degree to which all levels of management is enthusiastic about the possibilities of SSD 4.5 SE1. Existence of sufficient security experts 4.9 Experts (SE) SE2. Existence of suff		policy	
for reporting security policy violation Reward and Incentives RII. Existence of reward policy 4.0 Incentives RIZ.Developers are aware of the reward 4.1 (RI) policy 0 Organization' OC1.Existence of a learning and development culture 4.4 s objectives Maing culture 0 OC2.Existence of a participative decision 4.3 (OC) making culture 0 OC3.Existence of a support and collaboration culture 4.4 OC4.Existence of of conflicts and risk culture 4.6 Developer D1.Existence of IT management skills 4.3 D3.Existence of SSD experience 4.4 D6.Existence of controlling skills 4.2 Top TM1.The degree to which functional managers willingly assign resources to the SSD implementation as they are needed 4.1 Iong-term SSD support resources is recognized by management 4.5 TM2.The degree to which all levels of management is enthusiastic about the possibilities of SSD 4.5 Security SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence o		TA7.Developers aware of the procedures	4.1
Reward and Incentives RII.Existence of reward policy 4.0 Incentives RI2.Developers are aware of the reward 4.1 (RI) policy 0 Organization' OC1.Existence of a learning and development culture 4.4 objectives OC2.Existence of a participative decision 4.3 (OC) making culture 0 4.4 OC3.Existence of a power sharing culture 4.4 OC4.Existence of a power sharing culture 4.3 OC5.Existence of tolerance for conflicts and risk culture 4.6 Developer D1.Existence of communication skills 4.4 (D) D2.Existence of planning skills 4.3 D3.Existence of controlling skills 4.4 D4.Existence of controlling skills 4.2 Top TM1.The degree to which functional managers willingly assign resources to the SSD implementation as they are needed 4.1 (TM) SSD implementation as they are needed 4.1 TM2.The degree to which the need for hong-term SSD support resources is recognized by management 4.5 SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence of communication skills 4.7 <td></td> <td>for reporting security policy violation</td> <td></td>		for reporting security policy violation	
Incentives RI2.Developers are aware of the reward 4.1 (RI) policy 0 Organization' OC1.Existence of a learning and development culture 4.4 and culture OC2.Existence of a participative decision 4.3 (OC) making culture OC3.Existence of a support and collaboration culture 4.4 OC4.Existence of a power sharing culture OC4.Existence of conflicts 4.6 and risk culture OC5.Existence of communication skills 4.4 (D) D2.Existence of communication skills 4.4 (D) D2.Existence of support and participative decision 4.3 Developer D1.Existence of communication skills 4.4 (D) D2.Existence of SDD experience 4.4 D4.Existence of support and gase willingly assign resources to the managers willingly assign resources to the TM2.The degree to which functional 4.2 Top TM1.The degree to which the need for long-term SSD support resources is recognized by management 4.1 Management SSD SE1.Existence of sufficient security experts 4.9 SE1.Existence of sufficient security experts 4.9 5.0 SE2.Existence of communication skills 4.7 <td< td=""><td>Reward and</td><td>RI1.Existence of reward policy</td><td>4.0</td></td<>	Reward and	RI1.Existence of reward policy	4.0
(R) poincy Organization' OC1.Existence of a learning and 4.4 s objectives development culture and culture OC2.Existence of a participative decision 4.3 (OC) making culture OC3.Existence of a support and collaboration culture 4.4 OC4.Existence of a power sharing culture 4.3 OC5.Existence of tolerance for conflicts and risk culture 4.6 Developer D1.Existence of communication skills 4.4 (D) D2.Existence of IT management skills 4.3 D3.Existence of sSD experience 4.4 D6.Existence of controlling skills 4.4 D6.Existence of SSD support resources to the SSD implementation as they are needed TM2.The degree to which functional managers willingly assign resources is recognized by management 4.1 IM3.The degree to which executive management is enthusiastic about the possibilities of SSD 4.5 Security SE1.Existence of communication skills 4.6 SE2.Existence of communication skills 4.6 SE3.Existence of communication skills 4.7 SE4.Existence of planning skills 4.6 SE2.Existence of communication skills 4.7 SE3.Existence of sSD	Incentives	RI2.Developers are aware of the reward	4.1
Organization s objectives and culture (OC) OC1.Existence of a participative decision making culture OC3.Existence of a participative decision (OC) 4.3 (OC) making culture OC3.Existence of a power sharing culture OC4.Existence of a power sharing culture OC4.Existence of tolerance for conflicts and risk culture 4.4 Developer D1.Existence of communication skills D2.Existence of IT management skills D3.Existence of planning skills D4.Existence of controlling skills D5.Existence of controlling skills D5.Existence of controlling skills D6.Existence of controlling skills D6.Existence of controlling skills D7.DE 4.2 Top TM1.The degree to which functional managers willingly assign resources to the SSD implementation as they are needed TM2.The degree to which the need for long-term SSD support resources is recognized by management TM3.The degree to which executive scognized by management 4.1 Security SE1.Existence of sufficient security experts the SSD 4.5 Security SE1.Existence of sufficient security experts SE2.Existence of planning skills 4.7 SE3.Existence of SSD experience 4.8 SE4.Existence of SD experience 4.9 SE5.Existence of SD experience 4.9 Experts (SE) SE2.Existence of communication skills 4.7 SE4.Existence of planning skills 4.6 SE5.Existence of SD experience 4.8 SE7.Existence of communication skills	(RI)	policy	
s objectives development culture and culture OC2.Existence of a participative decision 4.3 (OC) making culture OC3.Existence of a support and 4.4 collaboration culture OC4.Existence of a power sharing culture 4.3 OC5.Existence of tolerance for conflicts 4.6 and risk culture PEOPLE AND ACTION Developer D1.Existence of communication skills 4.4 (D) D2.Existence of planning skills 4.4 D4.Existence of technical skills 4.6 D5.Existence of controlling skills 4.2 Top TM1.The degree to which functional 4.2 managers willingly assign resources to the SSD implementation as they are needed TM2.The degree to which he need for 4.1 long-term SSD support resources is recognized by management TM3.The degree to which executive 4.1 management is enthusiastic about the possibilities of SSD TM4.The degree to which all levels of 4.5 management support the overall goals of the SSD Security SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence of funding skills 4.6 SE5.Existence of SSD experience 4.8 SE7.Existence of communication skills 4.6 SE4.Existence of communication skills 4.7 PM4.Existence of communication skills 4.6 SE7.Existence of communication skills 4.7 PM4.Existence of communication skills 4.6 Project PM1.Existence of communication skills 4.7	Organization	OCI.Existence of a learning and	4.4
and Collaboration of a participative decision 4.3 (OC) making culture OC3.Existence of a support and collaboration culture 4.4 OC3.Existence of a power sharing culture 4.3 OC4.Existence of of oblerance for conflicts and risk culture 4.6 PEOPLE AND ACTION PEOPLE AND ACTION 4.4 (D) D2.Existence of communication skills 4.4 (D) D2.Existence of planning skills 4.4 D4.Existence of sufficient security experime 4.4 D6.Existence of controlling skills 4.2 Top TM1.The degree to which functional managers willingly assign resources to the SSD implementation as they are needed 4.1 (TM) TM2.The degree to which executive management is enthusiastic about the possibilities of SSD 4.5 TM4.The degree to which all levels of the SSD 4.5 Security SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence of romanication skills 4.7 SE3.Existence of planning skills 4.6 SE4.Existence of SDD experience 4.8 SE7.Existence of contr	s objectives	OC2 Existence of a participative design	12
(OC) Infakting currure OC3.Existence of a support and collaboration culture OC4.Existence of a power sharing culture OC5.Existence of tolerance for conflicts and risk culture 4.3 Developer D1.Existence of communication skills 4.4 (D) D2.Existence of planning skills 4.4 D4.Existence of planning skills 4.4 D4.Existence of sSD experience 4.4 D6.Existence of controlling skills 4.4 D6.Existence of controlling skills 4.2 Top TM1.The degree to which functional managers willingly assign resources to the SSD implementation as they are needed 4.1 (TM) SSD implementation as they are needed 4.1 TM3.The degree to which the need for long-term SSD support resources is recognized by management 4.1 TM3.The degree to which all levels of management is enthusiastic about the possibilities of SSD 4.5 Security SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence of rommunication skills 4.7 SE3.Existence of SSD experience 4.8 SE7.Existence of controlling skills 4.6 SE5.Existence of controlling skills 4.6 SE6.Existence of Controlling skills 4.6 SE7.Existence of	(\mathbf{OC})	making culture	4.5
collaboration culture OC4.Existence of a power sharing culture 4.3 OC4.Existence of a power sharing culture 4.3 OC5.Existence of colerance for conflicts and risk culture 4.6 Developer D1.Existence of communication skills 4.4 D2.Existence of planning skills 4.3 D3.Existence of controlling skills 4.4 D4.Existence of controlling skills 4.4 D5.Existence of sSD experience 4.4 D6.Existence of controlling skills 4.2 Top TM1.The degree to which functional 4.2 Management managers willingly assign resources to the SSD implementation as they are needed TM2.The degree to which the need for long-term SSD support resources is recognized by management 4.1 TM3.The degree to which executive management is enthusiastic about the possibilities of SSD 4.5 Security SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence of communication skills 4.7 SE3.Existence of sSD experience 4.8 SE4.Existence of SSD experience 4.8 SE5.Existence of controlling skills 4.6 SE4.Existence of controlling skills 4.6 <td>(00)</td> <td>OC3 Existence of a support and</td> <td>4.4</td>	(00)	OC3 Existence of a support and	4.4
OC4-Existence of a power sharing culture 4.3 OC5-Existence of tolerance for conflicts 4.6 and risk culture PEOPLE AND ACTION Developer D1-Existence of communication skills 4.4 D2-Existence of IT management skills 4.3 D3-Existence of planning skills 4.4 D4-Existence of sSD experience 4.4 D6-Existence of controlling skills 4.2 Top TM1.The degree to which functional 4.2 Management managers willingly assign resources to the SSD implementation as they are needed TM2.The degree to which the need for 4.1 long-term SSD support resources is recognized by management TM3.The degree to which executive management is enthusiastic about the possibilities of SSD 4.5 Security SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence of communication skills 4.7 SE3.Existence of SDD experience 4.8 SE7.Existence of SD experience 4.8 SE7.Existence of controlling skills 4.6 SE7.Existence of Controlling skills 4.6 SE7.Existence of Controlling skills 4.6 SE7.Existence of Controlling sk		collaboration culture	7.7
OC5.Existence of tolerance for conflicts and risk culture 4.6 PEOPLE AND ACTION Developer D1.Existence of communication skills 4.4 (D) D2.Existence of IT management skills 4.3 D4.Existence of planning skills 4.4 D4.Existence of sSD experience 4.4 D5.Existence of controlling skills 4.2 Top TM1.The degree to which functional managers willingly assign resources to the (TM) 4.2 Management SSD implementation as they are needed 4.1 Iong-term SSD support resources is recognized by management 4.1 M3.The degree to which all levels of management is enthusiastic about the possibilities of SSD 4.5 Security SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence of communication skills 4.7 SE3.Existence of SSD experience 4.8 SE7.Existence of SSD experience 4.8 SE7.Existence of communication skills 4.6 SE5.Existence of controlling skills 4.6 SE7.Existence of controlling skills 4.6 SE7.Existence of controlling skills 4.		OC4.Existence of a power sharing culture	4.3
and risk culture PEOPLE AND ACTION Developer D1.Existence of communication skills 4.4 (D) D2.Existence of IT management skills 4.3 D3.Existence of planning skills 4.4 D4.Existence of technical skills 4.6 D5.Existence of SSD experience 4.4 D6.Existence of controlling skills 4.2 Top TM1.The degree to which functional 4.2 Management managers willingly assign resources to the SSD implementation as they are needed TM2.The degree to which the need for long-term SSD support resources is recognized by management 4.1 M3.The degree to which executive management is enthusiastic about the possibilities of SSD 4.5 TM4.The degree to which all levels of the SSD 4.5 Security SE1.Existence of sufficient security experts 4.9 SE2.Existence of IT management skills 4.4 SE4.Existence of SSD experience 4.8 SE4.Existence of communication skills 4.7 SE3.Existence of SSD experience 4.8 SE4.Existence of SSD experience 4.8 SE5.Existenc		OC5.Existence of tolerance for conflicts	4.6
PEOPLE AND ACTIONDeveloper (D)D1.Existence of communication skills4.4(D)D2.Existence of IT management skills4.3D3.Existence of planning skills4.4D4.Existence of technical skills4.6D5.Existence of SSD experience4.4D6.Existence of controlling skills4.2TopTM1.The degree to which functional4.2Managementmanagers willingly assign resources to the SSD implementation as they are needed4.1Iong-term SSD support resources is recognized by management4.1TM3.The degree to which the need for uong-term SSD4.1ManagementTM3.The degree to which all levels of management is enthusiastic about the possibilities of SSD4.5SecuritySE1.Existence of sufficient security experts4.9Experts (SE)SE2.Existence of of IT management skills4.4SE4.Existence of planning skills4.6SecuritySE2.Existence of communication skills4.7SE3.Existence of SSD experience4.8SE7.Existence of controlling skills4.6ProjectPM1.Existence of communication skills4.6PM2.Existence of planning skills4.6PM3.Existence of technical skills4.1PM4.Existence of controlling skills4.7PM4.Existence of controlling skills4.7PM4.Existence of controlling skills4.7PM4.Existence of controlling skills4.7		and risk culture	
Developer (D)D1.Existence of communication skills4.4(D)D2.Existence of IT management skills4.3D3.Existence of planning skills4.4D4.Existence of technical skills4.6D5.Existence of SSD experience4.4D6.Existence of controlling skills4.2TopTM1.The degree to which functional managers willingly assign resources to the SSD implementation as they are needed4.1(TM)SSD implementation as they are needed4.1Iong-termSSD support resources is recognized by management4.1TM3.The degree to which the need for unanagement is enthusiastic about the possibilities of SSD4.5SecuritySE1.Existence of sufficient security experts4.9Experts (SE)SE2.Existence of sufficient security experts4.9Experts (SE)SE2.Existence of resperience4.8SE7.Existence of SSD experience4.8SE7.Existence of SDD support resources4.6ProjectPM1.Existence of controlling skills4.6ProjectPM1.Existence of controlling skills4.6PM3.Existence of IT management skills4.7PM4.Existence of SDD experience4.8SE7.Existence of SDD support resources4.8SE7.Existence of controlling skills4.6PM3.Existence of SDD experience4.8SE7.Existence of controlling skills4.6PM4.Existence of controlling skills4.7PM4.Existence of controlling skills4.7PM4.Existence of SDD experience4.2		PEOPLE AND ACTION	
(D)D2.Existence of IT management skills4.3D3.Existence of planning skills4.4D4.Existence of technical skills4.6D5.Existence of SSD experience4.4D6.Existence of controlling skills4.2TopTM1.The degree to which functional managers willingly assign resources to the SSD implementation as they are needed4.1(TM)SSD implementation as they are needed4.1Iong-termSSD support resources is recognized by management4.1TM3.The degree to which the need for long-term4.1ManagementTM3.The degree to which executive management is enthusiastic about the possibilities of SSD TM4.The degree to which all levels of management support the overall goals of the SSD4.5SecuritySE1.Existence of sufficient security experts4.9Experts (SE)SE2.Existence of rIT management skills4.4SE4.Existence of SDD support resource4.8SE7.Existence of SDD support the overall goals of the SSD4.6SE4.Existence of planning skills4.6SE5.Existence of SDD support skills4.6SE6.Existence of SDD supperience4.8SE7.Existence of controlling skills4.6ProjectPM1.Existence of controlling skills4.6PM2.Existence of rIT management skills4.7PM4.Existence of controlling skills4.7PM4.Existence of sSD experience4.2PM6.Existence of SSD experience4.2PM6.Existence of controlling skills4.7	Developer	D1.Existence of communication skills	4.4
D3.Existence of planning skills4.4D4.Existence of technical skills4.6D5.Existence of SSD experience4.4D6.Existence of controlling skills4.2TopTM1.The degree to which functional managers willingly assign resources to the SSD implementation as they are needed4.1(TM)SSD implementation as they are needed4.1Iong-termSSD support resources is recognized by management4.1TM3.The degree to which the need for long-term4.1TM3.The degree to which executive management is enthusiastic about the possibilities of SSD TM4.The degree to which all levels of management support the overall goals of the SSD4.5SecuritySE1.Existence of sufficient security experts4.9Experts (SE)SE2.Existence of running skills4.6SE5.Existence of SSD experience4.8SE7.Existence of SSD experience4.8SE7.Existence of controlling skills4.6ProjectPM1.Existence of controlling skills4.6PM3.Existence of SSD experience4.8SE7.Existence of SSD experience4.8SE7.Existence of controlling skills4.6PM3.Existence of SSD experience4.2PM4.Existence of sSD experience4.2PM4.Existence of controlling skills4.7PM4.Existence of controlling skills4.7PM4.Existence of controlling skills4.7PM4.Existence of controlling skills4.7PM4.Existence of SSD experience4.2PM6.Existence of SSD experience4.2 <t< td=""><td>(D)</td><td>D2.Existence of IT management skills</td><td>4.3</td></t<>	(D)	D2.Existence of IT management skills	4.3
D4. Existence of technical skills4.6D5. Existence of SSD experience4.4D6. Existence of controlling skills4.2TopTM1. The degree to which functional managers willingly assign resources to the(TM)SSD implementation as they are needed TM2. The degree to which the need for long-term SSD support resources is recognized by managementTM3. The degree to which executive management is enthusiastic about the possibilities of SSD TM4. The degree to which all levels of management support the overall goals of the SSDSecuritySE1. Existence of sufficient security expertsSE3. Existence of rIT management skills4.4SE4. Existence of SSD experience4.8SE5. Existence of sufficient security experts4.9Experts (SE)SE2. Existence of rIT management skills4.6SE6. Existence of SSD experience4.8SE7. Existence of controlling skills4.6ProjectPM1. Existence of communication skills4.6PM3. Existence of SSD experience4.8SE7. Existence of SSD experience4.8SE7. Existence of SSD experience4.8SE7. Existence of controlling skills4.6PM3. Existence of SSD experience4.2PM4. Existence of SSD experience4.2PM4. Existence of SSD experience4.2PM4. Existence of SSD experience4.2PM4. Existence of controlling skills4.7PM4. Existence of SSD experience4.2PM6. Existence of SSD experience4.2PM6. Existence of controlling skills4.7 <td></td> <td>D3.Existence of planning skills</td> <td>4.4</td>		D3.Existence of planning skills	4.4
D5. Existence of SSD experience4.4D6. Existence of controlling skills4.2TopTM1. The degree to which functional managers willingly assign resources to the4.2(TM)SSD implementation as they are needed TM2. The degree to which the need for long-term SSD support resources is recognized by management4.1TM3. The degree to which executive management is enthusiastic about the possibilities of SSD TM4. The degree to which all levels of management support the overall goals of the SSD4.5SecuritySE1. Existence of sufficient security experts SE3. Existence of IT management skills SE6. Existence of SSD experience SE6. Existence of controlling skills4.6SE5. Existence of SSD experience management support the overall skills SE3. Existence of IT management skills SE6. Existence of SSD experience SE6. Existence of controlling skills SE6. Existence of controlling skills SE7. Existence of controlling skills SE7. Existence of Controlling skills SE7. Existence of IT management skills SE7. Existence of SSD experience Manager PM3. Existence of IT management skills SE7. Existence of Controlling skills Manager PM3. Existence of SSD experience M4. Existence of SSD experience M5. Existence of SSD experience M5. Existence of SSD experience M6. Existence of SSD experience M6. Existence of SSD experience M6. Existence of SSD experience M6. Existence of Controlling skills M4. The Existence of Controlling skills M4. The Existence of Controlling skills M4. The SSD SSD SSD SSD SSD SSD SSD SSD SSD SS		D4.Existence of technical skills	4.6
D6.Existence of controlling skills4.2TopTM1.The degree to which functional managers willingly assign resources to the4.2(TM)SSD implementation as they are needed TM2.The degree to which the need for long-term SSD support resources is recognized by management4.1TM3.The degree to which executive management is enthusiastic about the possibilities of SSD TM4.The degree to which all levels of the SSD4.5SecuritySE1.Existence of sufficient security experts SE3.Existence of rIT management skills4.7SE4.Existence of SID SE5.Existence of SSD experience4.8SE5.Existence of SSD experience security4.6SE5.Existence of SID SE6.Existence of controlling skills4.6SE7.Existence of SD experience PM1.Existence of communication skills4.6Project PM1.Existence of rIT management skills PM3.Existence of rIT management skills A.64.7PM4.Existence of SD experience PM3.Existence of SD experience PM3.Existence of rIT management skills A.64.7PM4.Existence of SD experience PM3.Existence of rIT management skills A.74.7PM4.Existence of rechnical skills A.64.7PM4.Existence of rechnical skills A.74.7		D5.Existence of SSD experience	4.4
TopTM1.1he degree to which functional managers willingly assign resources to the SSD implementation as they are needed4.2(TM)SSD implementation as they are neededTM2.The degree to which the need for long-term SSD support resources is recognized by management4.1TM3.The degree to which executive management is enthusiastic about the possibilities of SSD4.1TM4.The degree to which all levels of management support the overall goals of the SSD4.5SecuritySE1.Existence of sufficient security experts SE2.Existence of communication skills SE4.Existence of planning skills4.6SE5.Existence of SSD experience SE6.Existence of controlling skills4.6ProjectPM1.Existence of rumanagement skills 4.64.7PM2.Existence of rumanagement skills SE7.Existence of communication skills 4.64.6ProjectPM1.Existence of communication skills 4.64.7PM4.Existence of SSD experience PM3.Existence of SSD experience 4.84.6PM3.Existence of communication skills 4.64.7PM4.Existence of communication skills 4.74.7PM4.Existence of sSD experience PM3.Existence of sSD experience 4.24.2PM6.Existence of controlling skills4.7		D6.Existence of controlling skills	4.2
Management managers withingly assign resources to the (TM) SSD implementation as they are needed TM2.The degree to which the need for long-term SSD support resources is recognized by management 4.1 TM3.The degree to which executive management is enthusiastic about the possibilities of SSD 4.1 TM4.The degree to which all levels of management support the overall goals of the SSD 4.5 Security SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence of communication skills 4.7 SE3.Existence of planning skills 4.6 SE5.Existence of SSD experience 4.8 SE6.Existence of controlling skills 4.6 Project PM1.Existence of communication skills 4.6 Manager PM2.Existence of IT management skills 4.6 PM3.Existence of communication skills 4.6 PM4.Existence of communication skills 4.6 PM4.Existence of SSD experience 4.2 PM6.Existence of controlling skills 4.7	Тор	TM1. The degree to which functional	4.2
(TM) SSD implementation as they are needed TM2.The degree to which the need for 4.1 long-term SSD support resources is recognized by management TM3.The degree to which executive 4.1 management is enthusiastic about the possibilities of SSD TM4.The degree to which all levels of 4.5 management support the overall goals of 4.5 management support the overall goals of 4.7 Security SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence of communication skills 4.7 SE3.Existence of planning skills 4.6 SE5.Existence of SSD experience 4.8 SE6.Existence of controlling skills 4.6 Project PM1.Existence of rommunication skills 4.6 Manager PM2.Existence of planning skills 4.6 (PM) PM3.Existence of sSD experience 4.8 PM4.Existence of sSD experience 4.2 PM6.Existence of controlling skills 4.7	Management	managers willingly assign resources to the	
IN2.1 the degree to which the need for long-term SSD support resources is recognized by management 4.1 TM3.The degree to which executive management is enthusiastic about the possibilities of SSD 4.1 TM4.The degree to which all levels of the SSD 4.5 Security SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence of communication skills 4.7 SE3.Existence of planning skills 4.6 SE5.Existence of planning skills 5.0 SE6.Existence of controlling skills 4.6 SE7.Existence of communication skills 4.6 Project PM1.Existence of communication skills 4.6 Manager PM2.Existence of IT management skills 4.6 PM3.Existence of controlling skills 4.6 PM4.Existence of communication skills 4.7 PM4.Existence of SSD experience 4.2 PM6.Existence of controlling skills 4.7	(1 M)	TNO The deeper to which the need for	4.1
Inde-term SSD support Tesofices Is recognized by management TM3.The degree to which executive 4.1 management is enthusiastic about the possibilities of SSD 4.5 TM4.The degree to which all levels of 4.5 management support the overall goals of 4.5 the SSD Security SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence of communication skills 4.7 SE3.Existence of planning skills 4.6 SE5.Existence of scherical skills 5.0 SE6.Existence of controlling skills 4.6 Project PM1.Existence of communication skills 4.6 Project PM1.Existence of IT management skills 4.6 Manager PM2.Existence of IT management skills 4.6 (PM) PM3.Existence of planning skills 4.7 PM4.Existence of SSD experience 4.2 PM6.Existence of SSD experience 4.2		INIZ. The degree to which the need for	4.1
TM3.The degree to which executive management is enthusiastic about the possibilities of SSD 4.1 TM4.The degree to which all levels of the SSD 4.5 Security SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence of communication skills 4.7 SE3.Existence of planning skills 4.6 SE5.Existence of technical skills 5.0 SE6.Existence of communication skills 4.6 SE7.Existence of controlling skills 4.6 Project PM1.Existence of rumanagement skills 4.6 Manager PM2.Existence of IT management skills 4.7 PM4.Existence of controlling skills 4.6 PM4.Existence of communication skills 4.7 PM4.Existence of SSD experience 4.8 Amager PM2.Existence of planning skills 4.6 PM4.Existence of communication skills 4.7 PM4.Existence of SSD experience 4.2 PM6.Existence of controlling skills 4.7		recognized by management	
Instance degree to which executive the management is enthusiastic about the possibilities of SSD 4.1 TM4.The degree to which all levels of the SSD 4.5 Security SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence of communication skills 4.7 SE3.Existence of IT management skills 4.6 SE4.Existence of planning skills 4.6 SE5.Existence of SSD experience 4.8 SE7.Existence of communication skills 4.6 Project PM1.Existence of IT management skills 4.6 Manager PM2.Existence of IT management skills 4.6 PM3.Existence of SSD experience 4.8 SP7.Existence of communication skills 4.6 PM4.Existence of SSD experience 4.2 PM6.Existence of SSD experience 4.2		TM3 The degree to which executive	4.1
Image in the instant of the bound interpossibilities of SSD TM4.The degree to which all levels of the SSD Security SE1.Existence of sufficient security experts Security SE1.Existence of sufficient security experts Security SE2.Existence of communication skills SE3.Existence of IT management skills 4.4 SE4.Existence of planning skills 4.6 SE5.Existence of technical skills 5.0 SE6.Existence of SSD experience 4.8 SE7.Existence of communication skills 4.6 Project PM1.Existence of IT management skills 4.6 Manager PM2.Existence of IT management skills 4.7 PM3.Existence of planning skills 4.6 PM4.Existence of SSD experience 4.2 PM6.Existence of SSD experience 4.2		management is enthusiastic about the	4.1
TM4.The degree to which all levels of management support the overall goals of the SSD 4.5 Security SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence of communication skills 4.7 SE3.Existence of IT management skills 4.4 SE4.Existence of planning skills 4.6 SE5.Existence of technical skills 5.0 SE6.Existence of SSD experience 4.8 SE7.Existence of controlling skills 4.6 Project PM1.Existence of communication skills 4.6 Manager PM2.Existence of planning skills 4.6 (PM) PM3.Existence of planning skills 4.7 PM4.Existence of SSD experience 4.2 PM6.Existence of SSD experience 4.2		possibilities of SSD	
management support the overall goals of the SSD Security SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence of communication skills 4.7 SE3.Existence of IT management skills 4.4 SE4.Existence of planning skills 4.6 SE5.Existence of technical skills 5.0 SE6.Existence of SSD experience 4.8 SE7.Existence of controlling skills 4.6 Project PM1.Existence of communication skills 4.6 Manager PM2.Existence of planning skills 4.6 (PM) PM3.Existence of planning skills 4.7 PM4.Existence of SSD experience 4.2 PM6.Existence of SSD experience 4.2		TM4. The degree to which all levels of	4.5
the SSD Security SE1.Existence of sufficient security experts 4.9 Experts (SE) SE2.Existence of communication skills 4.7 SE3.Existence of IT management skills 4.4 SE4.Existence of planning skills 4.6 SE5.Existence of technical skills 5.0 SE6.Existence of SSD experience 4.8 SE7.Existence of controlling skills 4.6 Project PM1.Existence of communication skills 4.6 Manager PM2.Existence of planning skills 4.7 PM4.Existence of technical skills 4.1 PM5.Existence of SSD experience 4.2 PM6.Existence of controlling skills 4.7		management support the overall goals of	
SecuritySE1.Existence of sufficient security experts4.9Experts (SE)SE2.Existence of communication skills4.7SE3.Existence of IT management skills4.4SE4.Existence of planning skills4.6SE5.Existence of technical skills5.0SE6.Existence of SSD experience4.8SE7.Existence of controlling skills4.6ProjectPM1.Existence of communication skills4.6ManagerPM2.Existence of IT management skills4.6(PM)PM3.Existence of planning skills4.7PM4.Existence of planning skills4.1PM5.Existence of SSD experience4.2PM6.Existence of controlling skills4.7		the SSD	
Experts (SE)SE2.Existence of communication skills4.7SE3.Existence of IT management skills4.4SE4.Existence of planning skills4.6SE5.Existence of technical skills5.0SE6.Existence of SSD experience4.8SE7.Existence of controlling skills4.6ProjectPM1.Existence of communication skills4.6ManagerPM2.Existence of IT management skills4.6(PM)PM3.Existence of planning skills4.7PM4.Existence of technical skills4.1PM5.Existence of SSD experience4.2PM6.Existence of controlling skills4.7	Security	SE1.Existence of sufficient security experts	4.9
SE3.Existence of IT management skills4.4SE4.Existence of planning skills4.6SE5.Existence of technical skills5.0SE6.Existence of SSD experience4.8SE7.Existence of controlling skills4.6ProjectPM1.Existence of communication skills4.6ManagerPM2.Existence of IT management skills4.6(PM)PM3.Existence of planning skills4.7PM4.Existence of technical skills4.1PM5.Existence of SSD experience4.2PM6.Existence of controlling skills4.7	Experts (SE)	SE2.Existence of communication skills	4.7
SE4.Existence of planning skills4.6SE5.Existence of technical skills5.0SE6.Existence of SSD experience4.8SE7.Existence of controlling skills4.6ProjectPM1.Existence of communication skills4.6ManagerPM2.Existence of IT management skills4.6(PM)PM3.Existence of planning skills4.7PM4.Existence of technical skills4.1PM5.Existence of SSD experience4.2PM6.Existence of controlling skills4.7		SE3.Existence of IT management skills	4.4
SE5.Existence of technical skills5.0SE6.Existence of SSD experience4.8SE7.Existence of controlling skills4.6ProjectPM1.Existence of communication skills4.6ManagerPM2.Existence of IT management skills4.6(PM)PM3.Existence of planning skills4.7PM4.Existence of technical skills4.1PM5.Existence of SSD experience4.2PM6.Existence of controlling skills4.7		SE4.Existence of planning skills	4.6
SE6.Existence of SSD experience4.8SE7.Existence of controlling skills4.6ProjectPM1.Existence of communication skills4.6ManagerPM2.Existence of IT management skills4.6(PM)PM3.Existence of planning skills4.7PM4.Existence of technical skills4.1PM5.Existence of SSD experience4.2PM6.Existence of controlling skills4.7		SE5.Existence of technical skills	5.0
SE7.Existence of controlling skills4.6ProjectPM1.Existence of communication skills4.6ManagerPM2.Existence of IT management skills4.6(PM)PM3.Existence of planning skills4.7PM4.Existence of technical skills4.1PM5.Existence of SSD experience4.2PM6.Existence of controlling skills4.7		SE6.Existence of SSD experience	4.8
ProjectPM1.Existence of communication skills4.6ManagerPM2.Existence of IT management skills4.6(PM)PM3.Existence of planning skills4.7PM4.Existence of technical skills4.1PM5.Existence of SSD experience4.2PM6.Existence of controlling skills4.7		SE7.Existence of controlling skills	4.6
Manager PM2.Existence of IT management skills 4.6 (PM) PM3.Existence of planning skills 4.7 PM4.Existence of technical skills 4.1 PM5.Existence of SSD experience 4.2 PM6.Existence of controlling skills 4.7	Project	PM1.Existence of communication skills	4.6
(PM) PM3.Existence of planning skills 4.7 PM4.Existence of technical skills 4.1 PM5.Existence of SSD experience 4.2 PM6.Existence of controlling skills 4.7	Manager	PM2.Existence of IT management skills	4.6
PM4.Existence of technical skills4.1PM5.Existence of SSD experience4.2PM6.Existence of controlling skills4.7	(PM)	PM3.Existence of planning skills	4.7
PM5.Existence of SSD experience4.2PM6.Existence of controlling skills4.7		PM4.Existence of technical skills	4.1
PM6.Existence of controlling skills 4.7		PM5.Existence of SSD experience	4.2
		PM6.Existence of controlling skills	4.7

B. Phase 2 Delphi Study: To determine assessment indicators for each factor that influence implementation of Secure Software Development practices in public sector and to suggest new indicators, if any

Phase 2 Delphi study aimed to determine assessment indicators for each factor that influence the implementation of Secure Software Development practices in the public sector. Experts were asked to state their level of agreement for each of the assessment indicator. Similar to Phase 1, a structured questionnaire was completed by each of the selected experts. Assessment indicators included in the survey questionnaire was derived from literature [12-14] and interviews with practitioners from public service organizations. A five-point Likert scale: Strongly Agree (5), Agree (4), Neutral (3), Disagree (2) and Strongly Disagree (1) was used to determine the agreement on each of the assessment indicator. The response from the experts was analyzed using quantitative analysis method. Mean was used as a measure of consensus among the experts. Indicators with a mean of 4.0 and above are accepted and used in the next phase. There was no need for an additional round since consensus was achieved in the First Round. The result of the Phase 2 study (for Organizational Context and People and Action) is shown in Table 3.

Table 4 List of Secure Software Development Practices Adopted from CLASP model

P1	Institute Security Awareness Program
P2	Monitoring Security Metrics
P3	Specify operational environment
P4	Identify global security policy
P5	Identify resources and trust boundaries
P6	Identify user roles and resource capabilities
P7	Document security-relevant requirements
P8	Detail misuse cases. Misuse cases are identical to use cases, except that they are meant to detail common attempted abuses of the system.
P9	Identify the attack surface. The system attack surface is the collection of possible entry points for an attacker.
P10	Apply security principles to design
P11	Research and assess the security posture of technology solutions
P12	Annotate class designs with security properties
P13	Specify database security configuration
P14	Perform security analysis of system requirements and
	design (threat modeling)
P15	Integrate security analysis into source code management
DIC	process
P10 D17	Implement interface contracts
P1/	technologies
P18	Address reported security issues
P19	Perform source-level security review
P20	Identify, implement and perform security tests
P21	Verify security attributes of resources
P22	Perform code signing
P23	Build operational security guide
P24	Manage security issue disclosure process

C. Phase 3 Delphi Study: To determine Secure Software Development practices which are dependent on each factor

The third and final phase of Delphi is aimed to map the Secure Software Development practice with factors that influence the implementation of the practice. The practices were adopted from the CLASP model as shown in Table 4. The data from the phase 3 study was analysed, and the factors were ranked according to the total number of practices that were being influenced by each factor. Figure 1 shows the top 10 factors that influence the implementation of secure software development practices.



Figure 1: Ranking of top 10 factors that influence the implementation of Secure Software Development Practices

The Delphi study was conducted to facilitate the development of Secure Software Development Practice Adoption Model based on the factors achieved by public service organizations. In Phase 3, the practices were mapped to the factors that affect the implementation of each practice. Table 5 depicts the list of practices affected by each factor.

 Table 5

 List of Secure Software Development Practices by Influential Factors

	Factors	List of Affected Practices
А	Institutional Context	
1.	Change Management	P1, P2
2	Policy Enforcement	P1, P2, P3, P7, P16, P21 -
	-	P24
3	Security Training and	P1, P2, P7, P11, P12, P23
	Awareness	
4	Reward and Incentives	P1
5	Organization's objectives	P1, P4, P24
	and culture	
В	People and Action	
6	Developer	P1, P6, P7, P9 – P22
7	Top Management	P1, P4, P7, P8, P16, P17, P22
		– P24
8	Security Experts	P1 – P21, P23 – P24
9	Project Manager	P1 – P10, P13, P16, P17, P20
		– P24
С	Project Content	
10	Automated tool support	P2, P8 – P11, P14, P18 – P19
	Cost	
11	Cost	P1 – P2, P8, P11, P14, P18
11 12	Project Team	P1 – P2, P8, P11, P14, P18 P1, P4-P7, P9, P11-P13,P15
11 12	Project Team	P1 – P2, P8, P11, P14, P18 P1, P4-P7, P9, P11-P13,P15 –P16, P20 – P22, P24
11 12 13	Project Team Security Audit Team	P1 – P2, P8, P11, P14, P18 P1, P4-P7, P9, P11-P13,P15 –P16, P20 – P22, P24 P1, P2, P4-P7, P11, P17-
11 12 13	Project Team Security Audit Team	P1 – P2, P8, P11, P14, P18 P1, P4-P7, P9, P11-P13,P15 –P16, P20 – P22, P24 P1, P2, P4-P7, P11, P17- P21,P24
11 12 13 14	Project Team Security Audit Team Segregation of role	P1 – P2, P8, P11, P14, P18 P1, P4-P7, P9, P11-P13,P15 –P16, P20 – P22, P24 P1, P2, P4-P7, P11, P17- P21,P24 P6
11 12 13 14 15	Project Team Security Audit Team Segregation of role Team size	P1 – P2, P8, P11, P14, P18 P1, P4-P7, P9, P11-P13,P15 –P16, P20 – P22, P24 P1, P2, P4-P7, P11, P17- P21,P24 P6 P10 –P13, P19 –P20, P24
11 12 13 14 15 16	Project Team Security Audit Team Segregation of role Team size Team Collaboration	P1 – P2, P8, P11, P14, P18 P1, P4-P7, P9, P11-P13,P15 –P16, P20 – P22, P24 P1, P2, P4-P7, P11, P17- P21,P24 P6 P10 –P13, P19 –P20, P24 P1-P6, P9,P11,P13,P17,
11 12 13 14 15 16	Project Team Security Audit Team Segregation of role Team size Team Collaboration	P1 – P2, P8, P11, P14, P18 P1, P4-P7, P9, P11-P13,P15 –P16, P20 – P22, P24 P1, P2, P4-P7, P11, P17- P21,P24 P6 P10 –P13, P19 –P20, P24 P1-P6, P9,P11,P13,P17, P18,P20,P22-P23
11 12 13 14 15 16 17	Project Team Security Audit Team Segregation of role Team size Team Collaboration Development Time	P1 – P2, P8, P11, P14, P18 P1, P4-P7, P9, P11-P13,P15 –P16, P20 – P22, P24 P1, P2, P4-P7, P11, P17- P21,P24 P6 P10 –P13, P19 –P20, P24 P1-P6, P9,P11,P13,P17, P18,P20,P22-P23 P1-P2, P8, P11-P14, P18-P20
11 12 13 14 15 16 17 D	Project Team Security Audit Team Segregation of role Team size Team Collaboration Development Time System Development	P1 – P2, P8, P11, P14, P18 P1, P4-P7, P9, P11-P13,P15 –P16, P20 – P22, P24 P1, P2, P4-P7, P11, P17- P21,P24 P6 P10 –P13, P19 –P20, P24 P1-P6, P9,P11,P13,P17, P18,P20,P22-P23 P1-P2, P8, P11-P14, P18-P20
11 12 13 14 15 16 17 D	Cost Project Team Security Audit Team Segregation of role Team size Team Collaboration Development Time System Development Processes	P1 – P2, P8, P11, P14, P18 P1, P4-P7, P9, P11-P13,P15 –P16, P20 – P22, P24 P1, P2, P4-P7, P11, P17- P21,P24 P6 P10 –P13, P19 –P20, P24 P1-P6, P9,P11,P13,P17, P18,P20,P22-P23 P1-P2, P8, P11-P14, P18-P20
11 12 13 14 15 16 17 D 18	CostProject TeamSecurity Audit TeamSegregation of roleTeam sizeTeam CollaborationDevelopment TimeSystem DevelopmentProcessesSecurity Documentation	P1 – P2, P8, P11, P14, P18 P1, P4-P7, P9, P11-P13,P15 –P16, P20 – P22, P24 P1, P2, P4-P7, P11, P17- P21,P24 P6 P10 –P13, P19 –P20, P24 P1-P6, P9,P11,P13,P17, P18,P20,P22-P23 P1-P2, P8, P11-P14, P18-P20 P1-P3, P6-P17, P19,P21-P24
11 12 13 14 15 16 17 D 18 19	Project Team Security Audit Team Segregation of role Team size Team Collaboration Development Time System Development Processes Security Documentation Software development	P1 – P2, P8, P11, P14, P18 P1, P4-P7, P9, P11-P13,P15 –P16, P20 – P22, P24 P1, P2, P4-P7, P11, P17- P21,P24 P6 P10 –P13, P19 –P20, P24 P1-P6, P9,P11,P13,P17, P18,P20,P22-P23 P1-P2, P8, P11-P14, P18-P20 P1-P3, P6-P17, P19,P21-P24 P6,P21,
11 12 13 14 15 16 17 D 18 19	Cost Project Team Security Audit Team Segregation of role Team size Team Collaboration Development Time System Development Processes Security Documentation Software development methodology	P1 – P2, P8, P11, P14, P18 P1, P4-P7, P9, P11-P13,P15 –P16, P20 – P22, P24 P1, P2, P4-P7, P11, P17- P21,P24 P6 P10 –P13, P19 –P20, P24 P1-P6, P9,P11,P13,P17, P18,P20,P22-P23 P1-P2, P8, P11-P14, P18-P20 P1-P3, P6-P17, P19,P21-P24 P6,P21,

V. DISCUSSION

Based on the results shown in Figure 1 and Table 5, Security Experts influences the implementation of secure software development practices the most as it is top of the list. As secure software development involves technical knowledge, the need for having a security expert becomes an important factor followed by Security Documentation, the Project Manager, and Developer. Meanwhile, the less influential factors are Change Management, Rewards, and Incentives, Segregation of Role and System Development Methodology. From the perspective of the secure software development practices, implementation of P1(15 factors) and P2 (12 factors) are influenced by the most number of factors meanwhile P3(5 factors), P8(5 factors) and P15(4 factors) are the least influenced practices. This study determines the factors and practices affected by the factors. The results obtained can be used to assess the achievement of factors and identify the practices that are able to be implemented at any organization. Since CLASP model enables tailoring of its practices, this model can be used to select the most applicable practices by the organization, hence produce an acceptable secured software. Furthermore, the organization will also be able to improve on their weaknesses by taking measures in achieving all the factors required to implement secure software development practices.

VI. CONCLUSION

Security has become a very important quality attribute for all kinds of software and must be considered from the initial stages of the software development process. The insecure software can lead to loss of revenue and damage the business reputation. Public service organizations are facing challenges in implementing secure development practices due to the high cost, lack of skills and development time. This study has taken a novel approach by identifying factors that affecting each secure development practice. These factors are assessed by assessment indicators to identify the achievement level of the factors for any software development project. Based on the achieved factors, the list of practices that can be applied to the software project can be identified. This approach enables software to be developed with some security practices based on the organization's environment and also improve the factors not achieved by the organization. Future work involves evaluating the model by conducting multiple case study in Malaysian Public Service Organization.

ACKNOWLEDGMENT

The authors would like to thank the Universiti Teknologi Malaysia for their support and cooperation including students and other individuals who are either directly or indirectly involved in this project.

REFERENCES

- [1] MAMPU, The Malaysian Public Sector ICT Strategic Plan. 2011.
- [2] Xiao, S., J. Witschey, and E. Murphy-Hill, Social influences on secure development tool adoption: why security tools spread, in Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing. 2014, ACM: Baltimore, Maryland, USA. p. 1095-1106.
- [3] Thuraisingham, B. and K.W. Hamlen. Challenges and Future Directions of Software Technology: Secure Software Development. in Computer Software and Applications Conference (COMPSAC), 2010 IEEE 34th Annual. 2010. IEEE.
- [4] Woon, I.M.Y. and A. Kankanhalli, *Investigation of IS professionals'* intention to practise secure development of applications. International Journal of Human Computer Studies, 2007. 65(1): p. 29-41.
- [5] Turoff, M., *The design of a policy Delphi*. Technological forecasting and social change, 1970. 2(2): p. 149-171.
- [6] Okoli, C. and S.D. Pawlowski, *The Delphi method as a research tool:* an example, design considerations and applications. Information & management, 2004. 42(1): p. 15-29.
- [7] Williams, P.L. and C. Webb, The Delphi technique: a methodological discussion. Journal of advanced nursing, 1994. 19(1): p. 180-186.
- [8] Dalkey, N. and O. Helmer, An experimental application of the Delphi method to the use of experts. Management science, 1963. 9(3): p. 458-467.
- [9] Powell, C., The Delphi technique: myths and realities. Journal of advanced nursing, 2003. 41(4): p. 376-382
- [10] Keeney, S., F. Hasson, and H.P. McKenna, A critical review of the Delphi technique as a research methodology for nursing. International journal of nursing studies, 2001. 38(2): p. 195-200
- [11] Kanniah, S.L. and M.N.r. Mahrin, A Review on Factors Influencing Implementation of Secure Software Development Practices. World Academy of Science, Engineering and Technology, International Journal of Social, Behavioural, Educational, Economic, Business and Industrial Engineering, 2016. 10(8): p. 2860-2867.
- [12] McLeod, L. and S.G. MacDonell, Factors that affect software systems development project outcomes: A survey of research. ACM Computing Surveys (CSUR), 2011. 43(4): p. 24.
- [13] Alnatheer, M., T. Chan, and K. Nelson. Understanding And Measuring Information Security Culture. in PACIS. 2012.
- [14] Hanafizadeh, P. and A.Z. Ravasan, A McKinsey 7S model-based framework for ERP readiness assessment. International Journal of Enterprise Information Systems (IJEIS), 2011. 7(4): p. 23-63.