AN ANALYSIS OF SOFTWARE SUPPORTABLE TASKS IN INFORMATION SECURITY MANAGEMENT SYSTEM LIFE CYCLE PROCESSES

Ahmad Iqbal Hakim Suhaimi, Yuichi Goto, and Jingde Cheng
Department of Information and Computer Science, Saitama University,
Saitama, 338-8570, Japan
{iqbal,gotoh,cheng}@aise.ics.saitama-u.ac.jp

ABSTRACT
Secure management of information is becoming critical for any organization because information is one of the most valuable assets in organization’s business operations. Today, many organizations adopt information security management systems (ISMSs) to help them manage their information securely. However, ISMS is a complex management system which requires involvement of wide range of participants to perform a quite number of tasks as well as a number of documents. Furthermore, ISMS needed to be periodically reviewed and maintained to achieve continuous improvement. Consequently, it is difficult to do all tasks in ISMS without any support tools. However, there is no study to identify which tasks related with ISMS can be supported by software tools. Indeed, no one makes clear what tasks and participants exist in ISMS life cycle processes. This paper presents the first analysis to identify software supportable tasks in ISMS life cycle processes. The paper enumerates all participants, documents, and tasks, and shows relationship among them, and identifies all software supportable tasks. The analysis and its result becomes a basis to construct an engineering environment for supporting organizations to implement and maintain their ISMSs.


INTRODUCTION
In the present day, information becomes one of the most valuable assets and extremely important in an organization’s business operations (Brykczynski, 2003). Unsecured management of information may lead to the loss of business, the business’s reputation, and also put the organizations’ future existence in a dangerous state. Therefore, secure management of information is becoming critical for any organization. To this end, many organizations have adopted information security
management systems (ISMSs) to help them manage their information securely as a mean to protect their business operations.

However, it is not easy for organizations to have effective ISMSs because the complexity, inadequacy in standards, and continuity of ISMS. ISMS is a complex management system that requires involvement of wide range of participants to perform a number of tasks as well as a number of documents. Organizations have to perform a huge number of tasks in appropriate sequence consistently. Various participants with different kind of responsibilities towards security have to perform the tasks at different time and places. One of the biggest obstacles for organizations starting to establish ISMSs is writing various ISMS related documents and managing the documents systematically. Organizations have to plan, create, approve, publish, manage, periodically review and revise a number of various ISMS documents. Many organizations have refer to ISMS international standards (ISO, 2005a; ISO, 2005b; ISO, 2009a; ISO, 2009b; ISO, 2010; ISO, 2011) to guide them implement their ISMSs. However, the standards are inadequate to cover every aspect in ISMSs because the standards do not cover all managerial aspects or activities that are need for information security management in the business of organizations (Anttila, 2012). The standards also do not pay enough attention to the cultural differences among organizations (Siponen, 2009). In addition, organizations have to periodical review and maintain their ISMSs in order to achieve continuous improvement because information that are managed by organizations and their threats are changing day by day. Consequently, implementing and maintaining ISMSs can be quite difficult and burdensome activities without any support tools.

However, there is no study to identify which tasks related with ISMS can be supported by software tools. Furthermore, there is no clear and detail definition of ISMS life cycle processes. Although, there has been studies (Kritzinger, 2008; Leitner, 2009) conducted related with ISMS, their scope are partially limited and concentrated only on one or several specific area in information security. Existing works (Monesion, 2011) related to ISMS can be said mainly focused on implementation of security controls in ISMS. Moreover, scope of existing works (Bialas, 2005; Dey, 2011; Lyubimov, 2011) are limited to PDCA model at high level only, not in detail. They do not cover all tasks in ISMS life cycle process in detail and do not consider participants who are important to perform the tasks. PDCA oversimplifies the entire process and do not mentions people who are important to perform particular processes as well as products of the processes (LC Consulting, 2012). Until now, there is no definition of a life cycle processes that takes into consideration every participants, products, and processes in ISMSs.
This paper presents the first analysis to identify software supportable tasks in ISMS life cycle processes. The paper enumerates all participants, documents, and tasks, and shows relationship among them, and identifies all software supportable tasks.

INFORMATION SECURITY MANAGEMENT SYSTEM

Overview

ISMS is a part of overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security (ISO, 2005a). In other words, an ISMS is a systematic management system encompasses management of humans, processes, and technologies in order to establish, implement, operate, monitor, review, maintain, and optimize information security to preserve confidentiality, integrity, and availability of information. It includes all of the policies, procedures, plans, practices, responsibilities, and resources that are used to protect and preserve information.

The purpose of ISMSs is to help organizations to continuously manage risks in order to protect their information securely. By establishing ISMSs, organizations can determine the necessary security level, make up plans, and distribute its assets based on its own risk assessment.

ISO/IEC 27000 Series

ISO/IEC 27000 series standards is a series of international standards published by Joint Technical Committee 1 (ISO/IEC JTC1) Sub Committee 27 (SC27) that provides best practices recommendations on information security management and controls within the context of an overall ISMS.

The series is applicable to any domain, and can be applied to any organization regardless of their size, structure, or business goal. Some of well-known and widely referred standards within the series are as follow.

- ISO/IEC 27000 Information security management systems – Overview and vocabulary (ISO, 2009a)
- ISO/IEC 27001 Information security management systems – Requirements (ISO, 2005a)
- ISO/IEC 27003 Information security management system implementation guidance (ISO, 2010)

In the series, the most important standard is ISO/IEC 27001. It defines a set of requirements that must be met if organizations want their ISMSs to be formally certified (ISO, 2005a). As the standard is known to be the de facto standard for information security management, the standard is internationally accepted and referred for ISMS certification. In conjunction with ISO/IEC 27001, the next important standard is ISO/IEC 27002 that provides guidelines and general principles for implementing, maintaining, and improving information security management in an organization (ISO, 2005b). ISO/IEC 27002 offers a set of best practices that covers 13 different areas collectively containing 39 security categories and 133 controls.

ISMS certification is a system in which a third party accredited certification body assesses whether an ISMS conforms to ISO/IEC 27001 and certifies that it meets requirements of the standard. Certification in compliance with ISO/IEC 27001 has been rapidly increased in recent years, with 4,276 organizations from over 50 countries having done so to date (Japan Information Processing Development Corporation, 2013). A further increase is expected with publication of other standards in ISO/IEC 27000 series standards.

**PDCA Model**

![PDCA Model](image)

Figure 1 PDCA Model

ISMS implementation is based on a process approach which adopts continuously improvement cycle process, the Plan-Do-Check-Act (PDCA) model (ISO, 2005a) as shown in Figure 1. PDCA is a cycle of activities designed to drive continuous improvement. PDCA in ISMS aims to ensure that security controls of an organization are implemented, reinforced, and improved over time. In Plan phase, organizations establish policies and assess risks of their information assets, as well as identify all controls that are needed to mitigate the risks. In Do phase, organizations implement and operate the policies, controls, and procedures. In Check phase, organizations assess and measure process performance against the policies and report the result to management for review. In Act phase, organizations take corrective and preventive
actions, based on the result of internal ISMS audit and management review, and carry out the feedback to Plan phase and start the cycle all over again.

However, it is difficult to have an effective ISMS based on the PDCA alone because it does not cover participants and products which are important managerial aspects in ISMS. PDCA oversimplifies the entire process in ISMS, and do not mentions people who are important to perform particular processes as well as products of the processes in ISMS (LC Consulting, 2012). Human element is important in ISMS because the way of interaction between people and processes determines how well the processes are performed and products are created and managed.

PARTICIPANTS, DOCUMENTS, AND TASKS IN ISMS LIFE CYCLE PROCESSES

ISMS Life Cycle Processes

We defined ISMS life cycle processes which is a life cycle process that covers all phases, every processes and tasks, every level of participants, and every kind of documents as well as relationships among them in ISMS. Until now, there is no studies to make clear what tasks, participants, and documents exist in ISMS life cycle processes. There is no definition a life cycle processes that take into consideration about participants, products, and processes as well as relationship among them for ISMS.

Participants and Their Responsibilities

ISMS requires special focus and participation from all levels of participants with full commitments in establishing such a system and implementing it within the organization because security is everyone’s responsibility (Ashenden, 2008; Dey, 2011; OECD, 2002). The involvement of participants in ISMSs are based on different responsibilities. Therefore, allocating specific individuals or groups with appropriate responsibilities is crucial in order for organizations to ensure their ISMSs go well as they have planned. For that purpose, it is important to clarify participants and their responsibilities in ISMS.

Based on ISMS international standards (ISO, 2005a; ISO, 2005b; ISO, 2009a; ISO, 2009b; ISO, 2010; ISO, 2011) and some literatures (Forte, 2009; Japan Information Processing Development Corporation, 2004; Posthumus, 2004; von Solms, 2006; Stoll, 2013), we elaborated about more than 10 kinds of participants and their responsibilities with respect to ISMS. Table 1 shows examples of participants and their responsibilities in ISMS.
<table>
<thead>
<tr>
<th>Participants</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>Provide the organizational vision and guiding principles, strategic decisions, and coordinate the whole ISMS. Ensure that information security goals are identified, meet the organizational requirements, and are integrated in processes. Formulate, review, and approve policies. Provide the resources needed for information security.</td>
</tr>
<tr>
<td>Information Security Committee</td>
<td>Ensure the completion of risk assessment, establish the plan for the ISMS documents, and determine the contents of the documents. Prepare policies statements, ensuring their compliance with the principles and axioms approved by the management. Review the security policy statements to ensure the efficiency and effectiveness of the controls and recommend improvements.</td>
</tr>
<tr>
<td>Chief Information Security Officer (CISO)</td>
<td>Develops policies and standards and ensures that they are documented, periodically reviewed, and available to all the concerned people documented. Defines the identification and classification methods of the information assets. Establishes and reviews risk assessment methodology and select appropriate controls for risk mitigation. Monitors and reports the compliance of policies to management.</td>
</tr>
<tr>
<td>Project Management Office</td>
<td>Create ISMS implementation schedule and manage the progress. Establish and manage contacts with external parties. Establish ISMS meeting, prepare materials and documents for the meeting, and manage records of the meeting.</td>
</tr>
<tr>
<td>Information Security Managers</td>
<td>Define information security procedures and guidelines. Collect and analyze on information security metrics and incidents. Ensure that suitable controls are in place in accordance with the policies, and are properly applied and used by all workers. Provide the direction, resources, support, and review necessary to ensure that information assets are appropriately protected.</td>
</tr>
<tr>
<td>Security training team</td>
<td>Implement training and awareness programs in the organization. Measure the effectiveness of the program.</td>
</tr>
<tr>
<td>Information Asset Owners</td>
<td>Assess the value of information assets. Classify information assets. Perform a risk assessment on the information assets.</td>
</tr>
</tbody>
</table>
Establish appropriate controls to safeguard the information assets.

<table>
<thead>
<tr>
<th>Internal Auditors</th>
<th>Conduct systematic and periodic checks to verify the effective implementation of the ISMS.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Report any opportunities for improvement of nonconformity to the management.</td>
</tr>
<tr>
<td>Employees</td>
<td>Comply with policies where relevant to their jobs.</td>
</tr>
<tr>
<td></td>
<td>Maintain the security of all information entrusted to them.</td>
</tr>
<tr>
<td></td>
<td>Report security breaches and taking necessary corrective actions.</td>
</tr>
<tr>
<td>Certification body</td>
<td>Conducts documents and on-site review for ISMS certification.</td>
</tr>
<tr>
<td></td>
<td>Registers organizations' ISMS certification.</td>
</tr>
</tbody>
</table>

It is essential for any organizations to have a security organizational structure to make their information security governance plan is well managed (von Solms, 2004). A security organizational structure is a framework to coordinate appropriate participants and their responsibilities with respect to security management into organizations structure. The allocation of participants in the organizational structure should be based on their responsibilities. It presents the relationship between participants in an organization. The relationship between participants may differ from one organization to another according to the company's size. However, from the view point of information security management, a general security organizational structure for ISMS can be demonstrated as shown in Figure 2. Based on participants’ responsibilities, security organizational structure can be categorized into 4 groups: management, audit committee, security committee, and departments. Management generally made up of senior managers and lead by a senior manager with general responsibility, ideally the Chief Executive Officer (CEO). Audit committee is made up of internal auditors. Security committee is generally composed of representatives from various departments, and lead by a Chief Information Security Officer (CISO).
ISMS Documents

In the context of ISMS, documents are products of tasks in ISMS life cycle processes. The documents set out how the ISMS should work and which records the evidence that it has worked and achieved its goals.

ISMS documents need to be controlled by a documented procedure. The procedure should define the management actions to approve, review, revise, and ensure the documents are available across the entire organization. Reviewing and updating the documents is part of the continuous improvement of ISMS.

Although the amount of documents within ISMS may vary from one organization to another depending on the company's size and the nature of its activities, the mandatory documents required in ISMS standards are the same among any organizations. Based on ISO/IEC 27001 (ISO, 2005a) and some literatures (Japan Information Processing Development Corporation, 2004; Farn, 2007), we extracted at least about 20 documents required in ISMS. The documents as well as their explanation are given in Table 2. The table only presents mandatory documents required in ISMS standards. Any additional and supplemental documents may be used or referred during the processes where necessary.
<table>
<thead>
<tr>
<th>Document name</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Records of key management decisions</td>
<td>Records of key management decisions regarding the ISMS.</td>
</tr>
<tr>
<td>ISMS scope</td>
<td>Definitions of all areas that are covered by the ISMS.</td>
</tr>
<tr>
<td>ISMS policy</td>
<td>Definitions the objective-setting management framework for the ISMS, giving it an overall sense of direction/purpose and defining key principles.</td>
</tr>
<tr>
<td>Information security policies</td>
<td>Specification of particular information security control objectives or requirements.</td>
</tr>
<tr>
<td>Information security procedures</td>
<td>Description of information security processes and activities.</td>
</tr>
<tr>
<td>Controls documentation</td>
<td>Documents such as technical security standards, security architectures, and etc.</td>
</tr>
<tr>
<td>Risk assessment methods</td>
<td>Policies, procedures, and/or standards describing how information security risks are assessed.</td>
</tr>
<tr>
<td>Risk assessment reports</td>
<td>Results of information security risk assessment.</td>
</tr>
<tr>
<td>Risk Treatment Plan (RTP)</td>
<td>Description on how the security control objectives are to be achieved.</td>
</tr>
<tr>
<td>ISMS operating procedures</td>
<td>Descriptions of the management processes and activities to plan, operate, and control the ISMS</td>
</tr>
<tr>
<td>Information security metrics</td>
<td>Description on how to measure the effectiveness of security controls.</td>
</tr>
<tr>
<td>Statement of Applicability (SoA)</td>
<td>A statement of selected control objectives and controls that are applicable to the organizations' ISMS.</td>
</tr>
<tr>
<td>Document control procedure</td>
<td>Explanation on how ISMS related documents are approved for use, reviewed, revised, and approved.</td>
</tr>
<tr>
<td>Records control procedure</td>
<td>Explanation on how records proving conformity to ISMS requirements and the effective operation of the ISMS.</td>
</tr>
<tr>
<td>Security awareness, training, and education records</td>
<td>Description of the involvement of all personnel having ISMS responsibilities in appropriate activities.</td>
</tr>
<tr>
<td>Internal ISMS audit plans and procedures</td>
<td>Description of the auditors’ responsibilities for ISMS audit, criteria, scope, and methods of the audit.</td>
</tr>
<tr>
<td>ISMS audit reports</td>
<td>Explanation of agreement on action plans and follow-up/verification/closure reports.</td>
</tr>
<tr>
<td>Management review plans/reports</td>
<td>Statement that prove management in fact review the ISMS on a regular basis.</td>
</tr>
<tr>
<td>Corrective action procedure</td>
<td>Description of requirements for nonconformities are identified, the causes are analyzed and evaluated, corrective actions are carried out, and the results are reviewed.</td>
</tr>
<tr>
<td>Preventive action procedure</td>
<td>Description of requirements for potential nonconformities and their causes are identified and evaluated, preventive action are carried out, and the result are reviewed.</td>
</tr>
</tbody>
</table>

ISMS documents can be classified into 4 classes: policies, standards, procedures, and records.

- **Policies**: A series of documents that describe in formal, brief, and high-level statements that embraces an organizations’ goals and objectives.
- **Standards**: A series of documents that express recommendations on what mandatory actions or rules designed to support and conform to policies.
- **Procedures**: A series of supplemental documents that consist of step by step instructions to implement standards.
- **Records**: Records provide the evidences that the procedures are implemented and their objectives are met.

The relationship among the documents are defined in hierarchy structure. Policies must be developed as top documents of the structure, followed by standards, procedures, and records in sequence. Standards are developed based on policies, procedures are developed based on standards, and records are developed as evidences of implemented procedures. Figure 3 shows the hierarchy structure of ISMS documents and classification of the documents for each class.
Phases, Processes, and Tasks

Based on ISMS international standards (ISO, 2005a; ISO, 2005b; ISO, 2009a; ISO, 2009b; ISO, 2010; ISO, 2011), and some literatures on ISMS implementation (Dey, 2007; Japan Information Processing Development Corporation, 2004), we elaborated phases, processes, and tasks in ISMS.

First, based on the PDCA model, we elaborated ISMS life cycle processes into 7 phases: preparation, establishment, implementation and operation, monitor and review, improvement and optimization, certification, and abolishment. In the preparation phase, organizations obtain important ISMS international standards (ISO/IEC 27001 and ISO/IEC 27002) as well as make a proposal to start off the ISMS with management approval. In establishment phase, organizations define scope of their ISMS, develop policies, identify risks, perform risk assessment and treatment, select appropriate security controls to mitigate risks, and prepare a Statement of Applicability. In implementation and operation phase, organizations establish a Risk Treatment Plan, conduct training and awareness program, manage operations and resources, and implement security incident detection and to deal with any security incident. In monitor and review phase, organizations perform regular review of their ISMS, conduct an ISMS internal audit, and continues with management review. In improvement and optimization phase, organizations implement any the identified improvement, take corrective actions and preventive actions, and communicate taken action to interested parties. In certification phase, organizations undergo document and on-site review by accredited certification body that they have applied. In
abolishment phase, organizations properly dispose ISMS documents with approval from top management. The sequence of the phases is demonstrated in Figure 4.

![Figure 4 A sequence of phases in ISMS.](image)

For each phase, there are a number of processes that organizations have to perform. Figure 5 shows the processes and its sequence.

![Figure 5 A Sequence of processes in ISMS.](image)
Each process in ISMS consists of a set of various tasks. We, then, defined a set of tasks that are required for completion of all processes. Table 3, 4, 5, 6, 7, 8, and 9 show the processes and tasks in for each phases in ISMS life cycle processes. The sequence of tasks flows from top to bottom for each process.

### TABLE 3. PROCESSES AND TASKS IN PREPARATION PHASE.

<table>
<thead>
<tr>
<th>Process</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make proposal</td>
<td>Create ISMS project proposal document.</td>
</tr>
<tr>
<td></td>
<td>Present the proposal to management team.</td>
</tr>
<tr>
<td>Organize an ISMS committee</td>
<td>Select committee members.</td>
</tr>
<tr>
<td></td>
<td>Define responsibilities of each member.</td>
</tr>
<tr>
<td>Plan</td>
<td>Draft out all tasks.</td>
</tr>
<tr>
<td></td>
<td>Plan a schedule for ISMS implementation.</td>
</tr>
<tr>
<td></td>
<td>Estimate costs needed for ISMS implementation.</td>
</tr>
<tr>
<td>Obtain management approval</td>
<td>Clarify the organization's priorities to develop ISMS.</td>
</tr>
<tr>
<td></td>
<td>Obtain management approval to initiate ISMS.</td>
</tr>
</tbody>
</table>

### TABLE 4. PROCESSES AND TASKS IN ESTABLISHMENT PHASE.

<table>
<thead>
<tr>
<th>Process</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define ISMS scope</td>
<td>Define organizational scope and boundaries.</td>
</tr>
<tr>
<td></td>
<td>Integrate every scopes and boundaries.</td>
</tr>
<tr>
<td>Develop ISMS policy</td>
<td>Develop ISMS policy.</td>
</tr>
<tr>
<td></td>
<td>Develop information security policies.</td>
</tr>
<tr>
<td></td>
<td>Obtain approval from management.</td>
</tr>
<tr>
<td>Define a risk assessment approach</td>
<td>Select an appropriate analysis method.</td>
</tr>
<tr>
<td></td>
<td>Document the assessment procedures.</td>
</tr>
<tr>
<td></td>
<td>Define a policy and set a goal for risk treatment.</td>
</tr>
<tr>
<td></td>
<td>Identify an acceptable risk level.</td>
</tr>
<tr>
<td>Identify risk</td>
<td>Sort out and group information assets.</td>
</tr>
<tr>
<td></td>
<td>Identify legal and business requirements.</td>
</tr>
<tr>
<td></td>
<td>Value assets.</td>
</tr>
<tr>
<td></td>
<td>Identify threats and their sources.</td>
</tr>
<tr>
<td></td>
<td>Identify vulnerabilities.</td>
</tr>
<tr>
<td></td>
<td>Asses the likelihood of occurrence.</td>
</tr>
<tr>
<td>Perform risk assessment</td>
<td>Estimate the level of risks.</td>
</tr>
<tr>
<td></td>
<td>Calculate risk value.</td>
</tr>
<tr>
<td>Process</td>
<td>Task</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Establish a RTP</td>
<td>Clarify activities to reduce unacceptable risks.</td>
</tr>
<tr>
<td></td>
<td>Specify the relation between the risks and controls.</td>
</tr>
<tr>
<td></td>
<td>Make a plan to carry out chosen controls.</td>
</tr>
<tr>
<td>Implement security controls</td>
<td>Document procedures for operating controls.</td>
</tr>
<tr>
<td></td>
<td>Implement controls to meet objectives.</td>
</tr>
<tr>
<td></td>
<td>Define how to measure effectiveness of the controls.</td>
</tr>
<tr>
<td>Conduct training and awareness program</td>
<td>Define the competences required of personal involved in training and awareness program.</td>
</tr>
<tr>
<td></td>
<td>Evaluate the effectiveness of the program.</td>
</tr>
<tr>
<td></td>
<td>Record the education and training, skills, experience, and qualifications.</td>
</tr>
<tr>
<td>Manage Operations</td>
<td>Prepare procedure manuals to manage the operation.</td>
</tr>
<tr>
<td></td>
<td>Manage operations based on the procedure manuals.</td>
</tr>
<tr>
<td>Manage Resources</td>
<td>Prepare procedure manuals to manage the resources.</td>
</tr>
<tr>
<td></td>
<td>Manage resources based on the procedure manuals.</td>
</tr>
<tr>
<td>Implement security incident detection and response</td>
<td>Define settings for the person responsible for action.</td>
</tr>
<tr>
<td></td>
<td>Define a report system for stakeholders.</td>
</tr>
<tr>
<td></td>
<td>Prepare procedure manuals for taking action in a security incident.</td>
</tr>
</tbody>
</table>

**TABLE 5. PROCESSES AND TASKS IN IMPLEMENTATION AND OPERATION PHASE.**
Prepare reports on security incidents.

### TABLE 6. PROCESSES AND TASKS IN MONITOR AND REVIEW PHASE.

<table>
<thead>
<tr>
<th>Process</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute monitoring procedures</td>
<td>Execute monitoring procedures and other controls.</td>
</tr>
<tr>
<td>Perform regular review of ISMS</td>
<td>Measure effectiveness of controls.</td>
</tr>
<tr>
<td></td>
<td>Review risk assessment at planned intervals.</td>
</tr>
<tr>
<td></td>
<td>Review residual risks and acceptable risks.</td>
</tr>
<tr>
<td></td>
<td>Identify acceptable risks.</td>
</tr>
<tr>
<td>Conduct an internal ISMS audit</td>
<td>Establish an internal ISMS audit procedure.</td>
</tr>
<tr>
<td></td>
<td>Document the procedure.</td>
</tr>
<tr>
<td></td>
<td>Plan internal ISMS audit projects and activities.</td>
</tr>
<tr>
<td></td>
<td>Carry out regular internal ISMS audit.</td>
</tr>
<tr>
<td></td>
<td>Maintain audit programme records.</td>
</tr>
<tr>
<td></td>
<td>Report audit results to management.</td>
</tr>
<tr>
<td>Perform management review of ISMS</td>
<td>Carry out management review of ISMS.</td>
</tr>
<tr>
<td></td>
<td>Examine the performance of ISMS.</td>
</tr>
<tr>
<td></td>
<td>Assess whether or not the ISMS should be improved.</td>
</tr>
<tr>
<td></td>
<td>Keep a record of ISMS management review.</td>
</tr>
<tr>
<td>Identify improvements for the ISMS</td>
<td>Examine management review inputs.</td>
</tr>
<tr>
<td></td>
<td>Generate decisions and actions.</td>
</tr>
<tr>
<td></td>
<td>Update security plans.</td>
</tr>
<tr>
<td></td>
<td>Record actions and events.</td>
</tr>
</tbody>
</table>

### TABLE 7. PROCESSES AND TASKS IN IMPROVEMENT AND OPTIMIZATION PHASE.

<table>
<thead>
<tr>
<th>Process</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improve ISMS</td>
<td>Implement the identified improvements.</td>
</tr>
<tr>
<td>Take corrective actions</td>
<td>Establish and document a corrective procedure.</td>
</tr>
<tr>
<td></td>
<td>Implement and maintain the procedure.</td>
</tr>
<tr>
<td>Take preventive actions</td>
<td>Establish and document a preventive action procedure.</td>
</tr>
<tr>
<td></td>
<td>Implement and maintain the procedure.</td>
</tr>
<tr>
<td>Apply lesson</td>
<td>Apply the security lessons that have been learned.</td>
</tr>
<tr>
<td>Communicate taken action</td>
<td>Communicate the improvements to interested parties.</td>
</tr>
<tr>
<td></td>
<td>Ensure improvements achieve intended results.</td>
</tr>
</tbody>
</table>
### TABLE 8. PROCESSES AND TASKS IN CERTIFICATION PHASE.

<table>
<thead>
<tr>
<th>Process</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decide for certification</td>
<td>Decide to obtain 27001 certification.</td>
</tr>
<tr>
<td></td>
<td>Allocate resources.</td>
</tr>
<tr>
<td>Apply for certification</td>
<td>Identify and choose a certification body.</td>
</tr>
<tr>
<td></td>
<td>Submit application to the certification body.</td>
</tr>
<tr>
<td></td>
<td>Establish a contract with selected certifier.</td>
</tr>
<tr>
<td>Undergo documents review</td>
<td>Prepare ISMS documents.</td>
</tr>
<tr>
<td></td>
<td>Submit ISMS documents to the certification body.</td>
</tr>
<tr>
<td></td>
<td>Certifier evaluates the documented ISMS against the requirements of ISO 27001.</td>
</tr>
<tr>
<td></td>
<td>Certifier reports any failures.</td>
</tr>
<tr>
<td></td>
<td>Certifier advises the organisation.</td>
</tr>
<tr>
<td>Undergo on-site review</td>
<td>Certifier examine evidence that the ISMS conforms to the documented ISMS.</td>
</tr>
<tr>
<td></td>
<td>Certifier checks whether the selected controls satisfy the findings of the risk assessment.</td>
</tr>
<tr>
<td></td>
<td>Organizations undertake corrective action for any non-conformity identified.</td>
</tr>
<tr>
<td>Obtain ISMS certification</td>
<td>Obtain and register certification.</td>
</tr>
<tr>
<td></td>
<td>Inform to all employees and interested parties</td>
</tr>
<tr>
<td>Maintain ISMS certification</td>
<td>Manage 27001 certificate.</td>
</tr>
<tr>
<td></td>
<td>Manage certification related documents.</td>
</tr>
<tr>
<td></td>
<td>Renew certification.</td>
</tr>
</tbody>
</table>

### TABLE 9. PROCESSES AND TASKS IN ABOLISHMENT PHASE.

<table>
<thead>
<tr>
<th>Process</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan abolishment schedule</td>
<td>Draft out all tasks.</td>
</tr>
<tr>
<td></td>
<td>Plan ISMS abolishment schedule.</td>
</tr>
<tr>
<td></td>
<td>Estimate needed costs.</td>
</tr>
<tr>
<td></td>
<td>Establish and document abolishment procedures.</td>
</tr>
<tr>
<td>Obtain approval</td>
<td>Obtain approval from management to abolish ISMS.</td>
</tr>
<tr>
<td>Dispose documents</td>
<td>Dispose ISMS documents.</td>
</tr>
<tr>
<td></td>
<td>Apply cancellation of ISMS certification.</td>
</tr>
<tr>
<td>Inform to related parties</td>
<td>Communicate to entire internal organization.</td>
</tr>
<tr>
<td></td>
<td>Communicate to external parties.</td>
</tr>
</tbody>
</table>
RELATIONSHIP AMONG PARTICIPANTS, DOCUMENTS, AND PROCESSES IN ISMS

This section presents relationship among participants, documents, processes, and tasks in ISMS. The relationship among them are focused on processes as shown in Figure 5. A process consists of a set of tasks. The process is performed by participant according to their responsibilities. Document is used as input of the tasks as well as output generated by the tasks.

According to responsibilities of participants in ISMS, we clarified the relationship between participants and processes. Table 10 shows the relationship in RACI matrix (Costello, 2012) that indicates which participants are responsible (R), accountable (A), consulted (C), and/or informed (I) for particular processes in ISMS.

Responsible – individual or group who performs a process.
Accountable – individual or group who approves the process.
Consulted – individual or group who gives feedback regarding to the process.
Informed – individual or group who needs to know the status of the process.

TABLE 10. RELATIONSHIP BETWEEN PROCESSES AND PARTICIPANTS.
<table>
<thead>
<tr>
<th>Task</th>
<th>A</th>
<th>C</th>
<th>R</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain ISMS standards</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Make proposal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organize committee</td>
<td>A/R</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Plan</td>
<td>R</td>
<td>A</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Obtain approval</td>
<td>A</td>
<td>I</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>Define ISMS scope</td>
<td>A/R</td>
<td>I</td>
<td>C</td>
<td>I</td>
</tr>
<tr>
<td>Develop ISMS policy</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>Define a risk assessment approach</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>Identify risks</td>
<td>A</td>
<td>I</td>
<td>C</td>
<td>R</td>
</tr>
<tr>
<td>Assess risks</td>
<td>A</td>
<td>I</td>
<td>C</td>
<td>R</td>
</tr>
<tr>
<td>Perform risk treatment</td>
<td>A</td>
<td>I</td>
<td>C</td>
<td>R</td>
</tr>
<tr>
<td>Select control objectives and control</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td>C</td>
</tr>
<tr>
<td>Approve residual risks</td>
<td>A/R</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Obtain management authorization</td>
<td>A</td>
<td>I</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>Prepare a SoA</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>Establish a RTP</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>Implement controls</td>
<td>A</td>
<td>I</td>
<td>C</td>
<td>R</td>
</tr>
<tr>
<td>Conduct training and awareness program</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>I</td>
</tr>
<tr>
<td>Manage operations</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Manage resources</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>Implement security incident detection and response</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>Execute monitoring procedures</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>Perform regular review of ISMS</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>I</td>
</tr>
<tr>
<td>Conduct an internal audit</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>I</td>
</tr>
<tr>
<td>Perform management review</td>
<td>A/R</td>
<td>C</td>
<td>C</td>
<td>I</td>
</tr>
<tr>
<td>Identify ISMS improvements</td>
<td>A</td>
<td>R</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improve ISMS effectiveness</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td>C</td>
</tr>
<tr>
<td>Take corrective actions</td>
<td>A</td>
<td>I</td>
<td>R</td>
<td>C</td>
</tr>
<tr>
<td>Take preventive actions</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Apply lesson</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td>C</td>
</tr>
<tr>
<td>Communicate taken action</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Decide for certification</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>Apply for certification</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td>C</td>
</tr>
<tr>
<td>Undergo documents review</td>
<td>A</td>
<td>I</td>
<td>I</td>
<td>C</td>
</tr>
<tr>
<td>Undergo on-site review</td>
<td>A</td>
<td>I</td>
<td>I</td>
<td>C</td>
</tr>
</tbody>
</table>
Then, we clarified the relationship between documents and processes in ISMS according to inputs and outputs of each process in ISMS. In ISMS, the inputs can be referred as any digital or printed material that provide relevant information the processes and outputs indicate documents that are generated from or updated in the processes.

The relationships among participants, processes, and documents for preparation, establishment, implementation and operation, monitor and review, certification, improvement and optimization, and abolishment phases in ISMS life cycle processes are demonstrated in Figure 6, 7, 8, 9, 10, 11, and 12 respectively.

Figure 6 Relationship among participants, processes, and documents in preparation phase.
Figure 7 Relationship among participants, processes, and documents in establishment phase

Figure 8 Relationship among participants, processes, and documents in implementation and operation phase
Figure 9 Relationship among participants, processes, and documents in monitor and review phase

Figure 10 Relationship among participants, processes, and documents in improvement and optimization phase
From above, it is clearly shown that ISMS is a complex management system that requires involvement of wide range of participants with different responsibilities to perform a number of processes as well as management of a number of documents with complex relationships among them. Because the relationships among participants, documents, processes, and tasks in ISMS are centered at processes, it is important that organizations perform the processes efficiently. The efficiency of processes are determined by the performance of overall tasks of the process. Therefore, it is important to provide support to the tasks in ISMS life cycle processes.
ANALYSIS OF SOFTWARE SUPPORTABLE TASKS

A task in ISMS life cycle processes that can be supported with software tools is such task that can be taken over and performed by software tools in order to eliminate or reduce any difficulties encountered by organizations during preparation, establishment, implementation and operation, monitor and review, improvement and optimization, certification, and abolishment of ISMSs.

We have identified the software supportable tasks based on following criteria:

- Memorization - Tasks that can be memorized so that the tasks can be repeated. In other words, tasks that can be described in a sound and complete algorithm so that the same tasks can be perform repeatedly by various participants according to same method at different time and places.
- Documentation - Tasks that require participants to develop, review, and revise ISMS documents. Furthermore, the tasks should have clear inputs to be used and referred to produce another new documents as well as revise old documents.
- Calculation - Tasks that require participants to accumulate a large number of data and perform complex calculation to identify useful information.
- Visualization - Tasks that can be visualized such that participants can monitor every progress and completion status of the tasks.

Any of tasks in ISMS life cycle processes that satisfy one of the feature above is considered can be supported by software tools. According to the feature, we have identified software supportable tasks in ISMS life cycle processes. Table 11 shows the identification of software supportable tasks based on each feature.

<table>
<thead>
<tr>
<th>Task</th>
<th>Memorization</th>
<th>Documentation</th>
<th>Calculation</th>
<th>Visualization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create ISMS project proposal document.</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Present the proposal to management team.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select committee members.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define responsibilities of each member.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Draft out all tasks.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan a schedule for ISMS implementation.</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Complete</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Estimate costs needed for ISMS implementation.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clarify the organization's priorities to develop ISMS.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obtain management approval to initiate ISMS.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define organizational scopes and boundaries.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrate all scopes and boundaries.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop ISMS policy.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop information security policies.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obtain approval from management.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select an appropriate risk assessment method.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document the assessment procedures.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define a policy and set a goal for risk treatment</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify an acceptable risk level.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sort out and group information assets.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify legal and business requirements.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Value assets.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify threats and their sources.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify vulnerabilities.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assess the likelihood of occurrence.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Estimate the level of risk.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calculate risk value.</td>
<td>✔ ✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enumerate risk treatment options.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduce risk, retain, avoid, and transfer risks.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify applicable objectives and controls.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select control objectives and controls to mitigate risks.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add additional controls where necessary.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document the acceptance of residual risks.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obtain management approval of the proposed residual risks.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approve residual risks.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approve proposed residual risks and ISMS implementation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obtain management authorization for implementing ISMS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approve ISMS implementation and operation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List up all control objectives and controls.</td>
<td>✔ ✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear out goal to perform selected controls.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Justify unselected controls.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clarify activities to reduce unacceptable risks.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specify the relation between risks and controls.</td>
<td>✔ ✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Make a risk treatment plan to carry out chosen controls.</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document procedures for operating controls.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implement controls to meet objectives.</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define how to measure effectiveness of the controls.</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define the competences required of personal involved in training and awareness program.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluate the effectiveness of the program.</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Records the education and training, skills, experience, and qualifications.</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prepare procedure manuals to manage the operation.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage operations based on the procedure manuals.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prepare procedure manuals to manage the resources.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage resources based on the procedure manuals.</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define settings for the person responsible for action.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define a report system for stakeholders.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prepare procedures for taking action in a security incident.</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prepare a report on security incidents.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute monitoring procedures and other controls.</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Measure effectives of controls.</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review risks assessments at planned intervals.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review residual risks and acceptable risks.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify acceptable risks.</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish an internal ISMS audit procedure.</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document the audit procedure.</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan internal ISMS audit projects and activities.</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carry out regular internal ISMS audit.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintain audit program records.</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report audit results to management.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carry out management review of ISMS.</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Examine the performance of ISMS.</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assess whether or not the ISMS should be improved.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keep a record of ISMS management review.</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Examine management review inputs.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generate decisions and actions.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update security plans.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Record actions and events.</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implement the identified improvements.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish and document a corrective procedure.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Complete</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implement and maintain the procedure.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish and document a preventive action procedure.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implement and maintain the procedure.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply the security lessons that have been learned.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communicate the improvements to interested parties.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure improvements achieve intended results.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decide to obtain 27001 certification.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allocates resources for certification.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify and choose a certification body.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Submit application to the certification body.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish contract with selected certifier.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prepare ISMS documents.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Submit ISMS documents to certification body.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certifier evaluates the documented ISMS.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certifier reports any failures.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certifier advises the organization.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certifier examine evidence that the ISMS conforms to the documented ISMS.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certifier checks whether the selected controls satisfy the findings of the risk assessment.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization undertake corrective action for any non-conformity identified.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obtain and register certification.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inform to all employees and interested parties.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage 27001 certificate.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage certification related documents.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Renew certification.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Draft out all tasks for ISMS abolishment.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Estimate needed time for each task.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan ISMS abolishment schedule.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Estimate needed cost.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish abolishment procedures</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obtain approval from management to abolish ISMS.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dispose ISMS related documents.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply cancelation of ISMS certification.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communicate to entire internal organization.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communicate to external parties.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
From the identification, 77 from 111 tasks in ISMS life cycle processes can be supported by software tools. The software supportable tasks can be summarized as follows:

- Documentation of ISMS policy, information security policies, and procedures.
- Memorization of risk assessment method, assets classification, threats and vulnerabilities identification, and controls selection tasks.
- Calculation to estimate risk level.
- Documentation of security controls objectives and controls, SoA, and RTP.
- Visualization of implemented controls, operations, and available resources.
- Documentation of procedures to manage operation and resource.
- Documentation of procedures to take action in security incident.
- Documentation of reports and logs of security incidents.
- Documentation of monitoring procedures.
- Calculation to measure effectiveness of controls.
- Documentation of audit procedure and records.
- Documentation of records of management review.
- Documentation of corrective and preventive procedures and records.
- Visualization of ISMS certification status.

Almost more than half of tasks in ISMS life cycle processes can be supported with software tools and most of them are tasks which are related with documentation. For that reason, Well-established and systematically managed, as well as periodical reviewed ISMS documents can enable organizations to implement effective ISMSs. Instead of completely relying on participants to perform all tasks in ISMS life cycle processes and leaving everything to them, the identified tasks can be performed more effectively by support from software tools.

CONCLUDING REMARKS

We have presented an analysis of participants, documents, phases, processes, tasks and their relationship in order to identify all software supportable tasks in ISMS life cycle processes. Our analysis showed that there are 10 kinds of participants, 20 documents, 7 phases, 41 processes, and 111 tasks. We also have identified 77 software supportable tasks in ISMS life cycle processes.

The analysis and its result becomes a basis to construct an engineering environment we are developing (Suhaimi, 2012) for supporting organizations to implement and maintain their ISMSs.
As future works, we will analyze the characteristics of software tools to support tasks in ISMS life cycle processes. A comprehensive framework and requirements of the software tools also will be analyzed in the near future. At current, we are developing an engineering environment that integrates various software tools to provide organizations with comprehensive facilities to support them implement and maintain ISMSs.

**REFERENCES**


