PAPER

An Information Security Management Database System (ISMDS) for Engineering Environment Supporting Organizations with ISMSs

Ahmad Iqbal Hakim SUHAIMI^{†a)}, Student Member, Yuichi GOTO[†], and Jingde CHENG[†], Nonmembers

SUMMARY Information Security Management Systems (ISMSs) play important roles in helping organizations to manage their information securely. However, establishing, managing, and maintaining ISMSs is not an easy task for most organizations because an ISMS has many participants and tasks, and requires many kinds of documents. Therefore, organizations with ISMSs demand tools that can support them to perform all tasks in ISMS lifecycle processes consistently and continuously. To realize such support tools, a database system that manages ISO/IEC 27000 series, which are international standards for ISMSs, and ISMS documents, which are the products of tasks in ISMS lifecycle processes, is indispensable. The database system should manage data of the standards and documents for all available versions and translations, relationship among the standards and documents, authorization to access the standards and documents, and metadata of the standards and documents. No such database system has existed until now. This paper presents an information security management database system (ISMDS) that manages ISO/IEC 27000 series and ISMS documents. ISMDS is a meta-database system that manages several databases of standards and documents. ISMDS is used by participants in ISMS as well as tools supporting the participants to perform tasks in ISMS lifecycle processes. The users or tools can retrieve data from all versions and translations of the standards and documents. The paper also presents some use cases to show the effectiveness of ISMDS.

key words: Information Security Management System, ISO/IEC 27000 series, database system, data model, XML

1. Introduction

Many organizations, which are commercial enterprises, government agencies, or non-profit organizations who do business or provide services have adopted Information Security Management Systems (ISMSs) as an approach to manage their information assets securely [1]. An ISMS is a systematic management system encompasses the 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 [2].

However, establishing and maintaining ISMSs is not easy for most organizations because an ISMS is a complex management system that requires involvement of many participants to perform a lot of tasks and manage extensive amount of documents [3]. Furthermore, because threats and vulnerabilities are found day by day, organizations have

to improve their ISMSs to deal with these evolving risks. Participants in the organizations have to perform the tasks in ISMS repeatedly to achieve continuous improvement of ISMS. Moreover, because various participants perform various tasks in ISMS at different times and places, the participants tend to perform the tasks based on improper method depending on situations or different approaches according to their own experiences. Thus, it is difficult for an organization to ensure the continuity and consistency in their ISMSs. Thus, organizations with ISMSs demand tools that can support them to perform all tasks in ISMS lifecycle processes consistently and continuously.

Therefore, we proposed an engineering environment for supporting organizations with ISMSs [4]. An engineering environment is an environment that includes various software tools to support its users to perform various tasks. An engineering environment for supporting organizations with ISMSs is an environment that integrates various tools and provides comprehensive facilities to all level of participants starting from top management to end employees in an organization such that they use the tools and facilities to perform all tasks in ISMS life cycle processes consistently and continuously.

In order to realize such support tools, a database system that manages common data shared by all participants in ISMSs and the tools is indispensable. The database system plays an important role as the core component of the environment [4]. At present, the common data are ISO/IEC 27000 series, which are international standards for ISMSs, and ISMS documents, which are the products of tasks in ISMS lifecycle processes.

To enable effective utilization of the standards and documents in the environment, the database system should manage data of the standards and documents for all available versions and translations, relationship among the standards and documents, authorization to access the standards and documents, and metadata of the standards and documents according to the following reasons. First, various versions and translations of the standards are used in the environment. Secondly, the standards and documents are related to each other. Thirdly, access to certain ISMS documents that contain confidential information should be restricted for particular participants. Lastly, the standards and documents have a set of metadata.

No such database system has existed until now. AI-

Manuscript received September 19, 2013.

Manuscript revised January 22, 2014.

[†]The authors are with the Department of Information and Computer Sciences, Saitama University, Saitama-shi, 338–8570 Japan.

a) E-mail: iqbal@aise.ics.saitama-u.ac.jp

DOI: 10.1587/transinf.E97.D.1516

though organizations can use electronic document management systems to manage various documents or records, such systems are often primarily used for storing and archiving [5], [6]. However, in the environment that we are developing to support organizations with ISMSSs, all documents (e.g., ISO/IEC 27000 series, ISMS documents, and so on) should not only be managed, but also used effectively by various support tools of the environment. The data of ISO/IEC 27000 series and ISMS documents is not only used from users, but also from tools supporting the users' tasks in ISMS. Therefore, it is important to manage such documents as structured data appropriately. From the viewpoint of an engineering environment supporting organizations with ISMSSs, current electronic document management systems are inadequate for providing data for support tools of the environment. While electronic document management systems focus on document-centric approach, support tools of the environment require both document-centric and data-centric for effective utilization of the documents. An information security engineering database system has been proposed to manage data of ISO/IEC security standards [7]. However, the database system is only constructed to manage ISO/IEC 15408, and did not mention how to manage ISO/IEC 27000 series and ISMS documents. Thus, there is no database system for managing ISO/IEC 27000 series and ISMS documents.

This paper presents the development of the Information Security Management Database System (ISMDS), a central database system of an engineering environment to support organizations with ISMSSs that manages ISO/IEC 27000 series and ISMS documents to be used from participants in ISMS and tools for supporting tasks in ISMS lifecycle processes. The paper also presents some use cases to show the effectiveness of ISMDS. At first, the paper shows requirements analysis of database system for managing the standards and documents. The paper then, presents appropriate data model for the standards and documents based on their characteristics, presents a design of a database system to manage data of the standards and documents, and shows its implementation. Finally, the paper shows some use cases of the database system and new effective usages of the standards and documents by using the database system.

2. Information Security Management Systems

2.1 ISMS

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 [2]. It is a complex management system that requires involvement of over 10 kinds of participants with various responsibilities to perform more than hundreds of tasks through the whole life cycle processes [3]. A task in ISMS is a set of actions need to be done from preparation to abolishment through the life cycle processes of ISMS by accounted participants. The implementation of ISMS is based on con-

tinuous improvement cycle process, the Plan-Do-Check-Act (PDCA) model [2]. PDCA is a cycle of activities designed to drive continuous improvement. In ISMS, PDCA aims to ensure that security controls of an organization are implemented, reinforced, and improved over time.

ISMS requires special focus and involvement from all levels of participants with full commitments in establishing and maintaining such a system within an organization. Various information need to be shared and exchanged by all participants in all tasks through the life cycle processes of ISMS within the organization in order to ensure the tasks are performed based on common information. However, at the same time, access to confidential information also should be restricted to only those who have rights to it according to their responsibilities in ISMS.

2.2 ISO/IEC 27000 Series

ISO/IEC 27000 series is a series of international standards 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 follows:

- ISO/IEC 27000 Information security management systems - Overview and vocabulary [8].
- ISO/IEC 27001 Information security management systems - Requirements [2].
- ISO/IEC 27002 Code of practice for information security management [9].
- ISO/IEC 27003 Information security management system implementation guidance [10].
- ISO/IEC 27004 Information security management - Measurement [11].
- ISO/IEC 27005 Information security risk management [12].

ISMSS can be certified in compliance with ISO/IEC 27001 by third party accredited certification bodies. ISMS certifications have been rapidly increased in recent years, with 4,431 organizations from over 50 countries having done so to date [13]. A further increase is expected with publication of other standards in ISO/IEC 27000 series.

Standards in ISO/IEC 27000 series are available in various versions and translations. Over time, the standards are newly published, revised, withdrawn, and translated. In order to be added into the ISO/IEC 27000 series, other standards are also renumbered or renamed. For example, ISO/IEC 17799 standard was renumbered under the ISO 27000 series as ISO/IEC 27002. Some standards can be also dropped from the series. The standards are also translated to various languages to be used globally.

Standards in ISO/IEC 27000 series are closely related to each other. The relationship is defined in each standard's "normative references". "Normative references" of

Fig. 1 Relationship among ISMS documents.

each standard gives a list of referenced standards cited in the standard that are indispensable for the application of the standard. For instance, ISO/IEC 27001 normatively refers to ISO/IEC 27002.

2.3 ISMS Documents

ISMS documents are products of tasks in ISMSs. The documents are inputs used in tasks and outputs generated by the tasks. The documents are essential in ISMSs because they set out how the ISMSs should work and which records the evidence that it has worked and achieved its goals.

At least, 20 kinds of documents have to be created and managed in ISMS [2]. The mandatory documents are summarized as follows: 1) Records of key management decisions, 2) ISMS scope, 3) ISMS policy, 4) Information security policies, 5) Information security procedures, 6) Controls documentation, 7) Risk assessment methods, 8) Risk assessment reports, 9) Risk Treatment Plan, 10) Statement of Applicability, 11) ISMS operating procedures, 12) Information security metrics, 13) Document control procedure, 14) Records control procedure, 15) Security awareness, training, and education records, 16) Internal ISMS audit plans and procedures, 17) ISMS audit reports, 18) Management review plans/reports, 19) Corrective action procedure, and 20) Preventive action procedure.

The documents are also closely related to each other. The relationship is demonstrated in Fig. 1. Each node indicates each document in the above ISMS documents, and an arc indicates the necessary document(s) need to be referred to create certain document(s). From the figure, ISMS documents need to be created according to other document(s) in an appropriate sequence. In other words, except the first document, an ISMS document only can be created if the previous document(s) exists. Thus, when a revision was made to a certain document, other documents that were created based on the document also need to be revised.

2.4 Usages of ISO/IEC 27000 Series and ISMS Documents

In an engineering environment for supporting organizations with ISMSs, ISO/IEC 27000 series and ISMS documents are used for various purposes to support participants performing tasks in ISMS life cycle processes. The use of ISO/IEC 27000 series is important in the environment to ensure all tasks are performed satisfying a certain level of quality. Various participants also refer to the standards as guidelines or best practices to perform tasks in ISMS. Moreover, the standards are also used by tools to support the participants performing their tasks. ISMS documents are used to ensure that organizations' ISMSs are continuously improved in alignment with the PDCA cycle. Therefore, effective utilization of the standards and documents is very important in the environment.

However, it is difficult to use the standards and documents effectively to provide continuous and consistent support for all participants in an organization with ISMS. It is not easy to extract the necessary information from various versions and translations of the standards and documents. In addition, the number of standards in ISO/IEC 27000 series will increase with the publications of new versions and translations of the standards. The number of ISMS documents will increase as organizations continuously improve their ISMSs according to the PDCA cycle. At the same time, previous versions of the standards and documents also need to be managed and controlled. Furthermore, participants who can access certain documents that contain confidential information also need to be managed according to their responsibilities in ISMS.

Thus, in order to enable effective utilization in the environment, it is important to manage the standards and documents systematically by database system.

3. Requirements Analysis of Database System for Managing ISO/IEC 27000 Series and ISMS Documents

In order to manage ISO/IEC 27000 series and ISMS documents by database system, various characteristics of the standards and documents have to be taken into a careful consideration. A database system to manage ISO/IEC 27000 series and ISMS documents should satisfy following requirements according to their characteristics.

R1: *The database system should correspond with semi-structured structure of the standards and documents and able to extract needed parts from the standards and documents.* The structures of the standards and documents are semi-structured and different among each other. Each of the standard is a large document that consists of a number of chapters, and moreover the composition, contents, and descriptions of these chapters are different each other's. ISMS documents are different in various perspectives because the purpose of each document is different. Even for the same

Fig. 2 Relationship among ISO/IEC 27000 series and ISMS documents.

kind of documents, formats, styles, compositions, and descriptions of the documents differ greatly from one organization to another. One of the factors is there are no concrete criteria for constructing the documents properly. The formats, styles, and descriptions of documents greatly depend on each organization who writes the documents. In the environment, specific contents of the standards and documents needed to be extracted easily according to the structure of the standards and documents.

R2: *The database system should maintain the relationship among the standards and the documents.* ISO/IEC 27000 series and ISMS documents are related to each other. Standards are related to each other in the series because usage of certain standards requires reference to other standards normatively. Each of ISMS document is related to each other and has to be created and managed sequentially in order. Moreover, the documents are also related to ISO/IEC 27000 series because the documents are basically created based on the standards. The relationship among the standards and documents is shown in Fig. 2.

R3: *The database system should correspond with changes occurred on the standards and documents.* Over time, standards in ISO/IEC 27000 series are revised, re-named, renumbered, translated, and disposed. The number of versions and translations of standards within the series is expected to continue to increase with publications in various languages and revisions of the standards. During such events, the structure and descriptions of the standards may be changed and need to be addressed. Furthermore, the standards are used in various ways in the environment. The standards also may be used in different new ways that have not

been identified yet with the development of various support tools of the environment. Basically, the standards are used as terminological reference, requirements check, best practices reference, and guideline Ref. [14]. Usage of a certain standard can be changed depending on the tasks in ISMS. As an example, for a certain task in ISMS, the standards are used as terminological reference, however in other tasks, the standards also can be used in a different way such as best practices reference.

R4: *The database system should manage every available versions and translations of the standards and documents.* In the environment, every available versions and translations of the standards are used in all tasks in ISMSs [4]. Existing versions are not disposed and be kept managed even though there are new ones being added for various purpose. For instant, an ISMS document that was created or certified by a certain version of the standard may re-use the standard again to revise the document. By comparing differences among various versions, users can easily identify changes in the new version and use the information to revise ISMS documents that were created or certified according to the old version of the standards. By retrieving various translations crossly, users also can translate their ISMS documents into suitable languages so that they can pursue ISMS certification according to their country or region. All versions of ISMS documents also need to be managed in order to ensure that the organizations' ISMSs are improved periodically according to the PDCA cycle.

R5: *The database system should manage metadata of the standards and documents.* It is important to manage metadata for identification of the standards and documents. In the environment, various versions and translations of the standards and documents are used in tasks in ISMS. Therefore, it is important to easily identify and distinguish current versions of standards from old ones. Moreover, ISO/IEC 270001 requires all ISMS documents to be controlled where the documents must be approved, have a current version and status, have an issue date, owner, record the change history, and be withdrawn when obsolete. Such information should be managed separately from the standards or the documents as their metadata.

R6: *The database system should manage progress of ISMS documents.* It is important to manage progress of ISMS documents in order to support various participants prepare and manage extensive amount of documents. ISMS documents are used as inputs and outputs of various tasks in ISMS continuously according to the PDCA cycle. Some of the documents require a lot of time for completion. In fact, the documents have to go through various phases until the final publication. Moreover, a wide range of participants within organizations involves during the process. For that purpose, it is important to record the current completion progress of the documents, and identify which phase of tasks used the documents and participants who accessed the documents at a specific time. It is also important to keep records of how many times the documents are used in particular tasks and how many cycle the documents have com-

pleted.

R7: *The database system should restricted access to confidential documents.* Although common data should be shared by all users, certain ISMS documents are confidential and should be restricted to specific users only. Standards in ISO/IEC 27000 series are global standards used worldwide, and therefore the standards can be shared by all users. However, in the environment, ISMS documents can be divided into 2 categories: predefined templates of ISMS documents and ISMS documents that are created by organizations. Some of ISMS documents that are created by organizations cannot be shared by all users because the documents may contain confidential information of organizations who own the documents. Disclosure of such documents to external parties can be undesirable for the organizations. Such documents should only be shared within the organizations. Thus, it is also important to limit the access to certain information to specific users.

From above, the standards and documents have various characteristics. Moreover, these characteristics are dependent upon one another and influence one another. Therefore, it is important to define appropriate data model that can deal with all of the characteristics above in order to manage the standards and documents by database system.

4. Data Model for ISO/IEC 27000 Series and ISMS Documents

Various characteristics of ISO/IEC 27000 series and ISMS documents have to be considered when defining a data model for the standards and documents.

First, based on the characteristics, we identified the following data that should be managed in order to manage ISO/IEC 27000 series and ISMS documents by database system.

- ISO/IEC 27000 series: All content of standards in ISO/IEC 27000 series.
- ISMS documents: All content of ISMS documents.
- Authorization: Access authority to the standards and documents.
- Participants: Information of participants and their responsibilities in ISMS.
- Users: Information of all users in an organization.
- Standards' metadata: Information of the versions, translations, and relationship of the standards.
- Documents' metadata: Information of versions, relationship, and progress of the documents.

Then, we defined a data model for ISO/IEC 27000 series and ISMS documents. Conceptually, data model for the standards and documents is a database model based on a combination of XML data model and relational model to manage various versions and translations of the standards and documents. The identified data can be divided into dynamic and static data. Dynamic data, which are contents of ISO/IEC 27000 series and ISMS documents should be represented in XML data model. Static data, which are autho-

Fig. 3 An overview of data model for ISO/IEC 27000 series and ISMS documents.

riziation, participants, users, standard's metadata, and documents' metadata should be represented in relational data model as usual. Therefore, data model to manage the standards and documents should be a hybrid. Figure 3 shows an overview of the data model to manage ISO/IEC 27000 series and ISMS documents. Each box indicates a set of data, and a line indicates the relationship among the data set. Box with dotted line indicates a group of XML data model.

XML data model is flexible to represent data of ISO/IEC 27000 series because the standards are semi-structured and the structures are different each other. Although structures of standards in the series are vary each other, there are several similarities exist in the pattern among the standards because they are belonging to the same series. Similar parts of all standards can and should be managed in a same way. In order to manage such standards, we have identified the patterns for the standards. International standards such as ISO/IEC 27000 series can be divided into common and uncommon parts [15]. Common parts of standards are the sections that are same and appear on all standards. Uncommon parts are the remaining sections of the standards, which are generally the main contents of the standards and different from standards to standards. We have extracted common parts from ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, and ISO/IEC 27005. The common parts are as follows:

- Number/number: Name/number of the standard.
- Version: Current version of the standard.
- Language: The language of the standard.
- Published date: The standard published date.
- Reference number: The official number used to refer to the standard.
- Introduction: Introduction of the standard.
- Scope: Scope or objective of the standard.
- Terms: Terms and definitions defined in the standard.
- References: Normative reference to other standards in ISO/IEC 27000 series.
- Annex: Annexes provided in the standard.
- Bibliography: Bibliography listed in the standard.

For the common part, same XML data model can be used for its representation. For uncommon part, an XML data model

should be defined for each part according to its structure.

XML data model is flexible to represent data of ISMS documents because the documents are semi-structured and the structures are different each other. Structures of ISMS documents are different for the same kind of documents among organizations. ISO/IEC 27000 series only state what to be written or included in each document, but not how to construct the document. Therefore, for the same kind of documents, not only the formats, styles, and descriptions are varied according to each organization, the presence or absence of mandatory contents of the document is also different for each organization. Similar to standards in ISO/IEC 27000 series, although organizations can add new or remove unwanted predefined items from each ISMS document, there are common items that should be defined in every document. We extracted common parts from 20 ISMS documents. The common parts are as follows:

- Name: The document name.
- Author: The name of the person who creates the document.
- Created date: Date when the document is created.
- Version: Version of the document.
- Revised date: The revision date of the document.
- Approver: The name of person who approves the document.
- Approved date: The date when the document is approved.
- Status: Current status of the document (drafted, reviewed, revised, approved, published, withdrawn).
- Referred standard: Standard's official reference number.
- Input of tasks: The tasks in ISMS which use the document as input.
- Output of tasks: The tasks in ISMS which use the document as output.

Similarly, same XML data model can be used for the representation for the common part and a XML data model should be defined for each uncommon part according to its structure.

Relational model is used manage metadata of the standards and documents. In order to manage various metadata related to the standards and documents, our basic idea is that the management of the metadata should be separated from the standards and documents. Because the structure of the metadata is fixed, it can be represented in a fixed table schema. Therefore, we adopt relational data model to represent the metadata.

Relational model is also used to manage the relationship among the standards and documents. Despite the fact that the structures of the standards and documents are different each other, the relationship among them are fixed. The structure of the standards or documents also may change upon revision, but the relationship among them still the same. Therefore, we took full advantage of this unchanged relationship and adopt relational model to represent the relationship. The relationship among the standards and the

documents is based on their actual relationship as shown in Fig. 2.

The use of XML data model and relational data model to manage data of ISO/IEC 27000 series and ISMS documents can correspond with some issues in ISMS. Predefined XML data model for common part of ISO/IEC 27000 series and ISMS documents can at least reduce the inconsistency issues in managing the standards and documents. Predefined relational data model for managing relationship among the standards and documents can ensure the relationship among the standards and documents are well-maintained.

We, then, adopted Extensible Markup Language (XML) [16] to implement the data model for various reasons. First, it has been widely accepted that semi-structured data are best expressed in XML [17]. Therefore, XML is an appropriate to represent the structure of the standards as well as the documents. Secondly, the adoption of XML is suitable to correspond with the differences in structure among standards in the series. For the common part, we defined XML Schemas [18] to describe structure for common parts for all standards [19]. For uncommon part of the standards, the XML tags are defined according to each standard or each document. From above, a standard consists of several XML documents of common parts and uncommon parts. Thirdly, the adoption of XML is also appropriate to correspond with the differences in structure of the same kind of documents among organizations. XML is flexible to represent the differences in formats, styles, and descriptions of documents for each organization. For the common parts of the documents, we defined XML tags for all documents [19]. For uncommon part, the XML tags are defined according to each document. From above, ISMS document can be as one XML document for each document. Finally, XML is both human and machine readable format. From the viewpoint of usage of the standards and documents in the environment, we have emphasized several times that the standards and documents need to be used by both participants and support tools of the environment. The representation of the data in XML allows the standards and documents to be more readable to both humans and machines. Furthermore, XML tags can allow specific information to be retrieved out easily for the standards and documents.

We have proposed our basic idea to manage a standard for each version and for each translation separately in order to manage various and translations of the standards systematically. An XML document is specified to manage a standard for one standard, one version, and one translation. Therefore, the document is considered as a different document if either one of the 3 elements above is changed. Although the structures of the standards are same for different translations, the structures may be different in different versions. For example, structure of ISO/IEC 27002:2005 is different from its previous version, ISO/IEC 17799:2000. Moreover, it is important to distinguish between the latest version and old versions of the standards. Therefore, the standards for each version and for each translation should be managed separately. Thus, existing standards should not

be altered or interfered with when a new version or a new translation of a standard is published.

We, then, adopted XML database to manage the XML documents. XML database is adopted to correspond with the usages of the standards. The usages of the standards in ISMSs are vary depending on tasks in ISMS. Moreover, the most important point is, in the environment, the usages are not fixed at the moment of the database to manage the standards was designed. In the future, the standards also may be used in different new ways that have not been identified yet. Therefore, design of the database for standards must also correspond with the new usages. In general, design of a database is determined by the usages of the data because the data need to be structured in the way that it will be used frequently. Therefore, it is difficult to manage the standards and documents with traditional relational database because that requires fixed-structure table schemas [20]. It is not practical for altering the design of the database every time when there are new usages of the standards are identified. For that purpose, we adopt XML database as our basic consideration to manage the standards and documents such that the new usages can be at least corresponded on data retrieval without altering the design of the database. Thus, in order to manage various versions and translations of the standards, one database is allocated to manage the standards for each version and translation. In other words, one XML database manages XML documents for each version and each translation of a standard in ISO/IEC 27000 series.

However, it is difficult to completely deal with the access restriction for ISMS documents at data modeling level. There are ISMS documents that are restricted and cannot be shared. Such documents should be managed separately. Our proposed approach is that the documents should be managed in separate databases. ISMS documents that can be shared should be managed by one database that can be accessed from every user. ISMS documents that cannot be shared should be managed by separate databases for each organization such that only the organization can retrieve the documents.

It is also difficult to precisely represent the relationship of databases for standards and documents at data modelling level. Although it is possible to define the relationship among documents in ISMS document for each database, it is difficult to represent relationship among the standards and documents as well as relationship among standards in the series at data modelling level because the documents are managed in separated databases for each organization, and the standards are managed in separated databases for each version and for each translation. Our proposed approach is that the relationship is managed as relational data on another database separately.

In order to manage ISO/IEC 27000 series and ISMS documents by database system, there are several characteristics that can be corresponded at data modeling level. However, there are also several characteristics that are difficult to deal at data modeling level. The solutions for such characteristics are considered when designing the database system.

5. Information Security Management Database System

5.1 ISMDS

ISMDS is a central database system for an engineering environment supporting organizations with ISMSs. The database system is the core component of the environment. It manages data of ISO/IEC 27000 series and ISMS documents shared by all participants in an organization with ISMS as well as various tools supporting the participants integrated in the environment

5.2 Design

Based on the data model for ISO/IEC 27000 series and ISMS documents, obviously ISMDS should be a meta-database system that manages several databases of the standards for various versions and translations as well as various databases of the documents. In the environment, support should be provided consistently and continuously through all tasks in ISMS according to various versions and translations of ISO/IEC 27000 series. Therefore, when a new version or translation of standards needs to be added to the environment, altering activity to the databases that manage existing versions or translations should be avoided as possible. One of the biggest reasons is because altering existing databases requires termination of connection from support tools to the databases, and consequently will interrupt or disable the consistent and continuous support from the tools.

In order to manage the standards and documents, ISMDS should consist of 6 type of databases: *Criteria DB*, *Criteria Meta DB*, *Personal DB*, *Personal Meta DB*, *Case DB*, and *User DB*. *Criteria DB* is an XML database that should manage data for each version and each translation of a standard in ISO/IEC 27000 series. Therefore, there are multiple *Criteria DBs* to manage every standard. *Criteria Meta DB* is a relational database that should manage metadata of all standards and relationship among the standards. *Personal DB* is an XML database that should manage data of ISMS documents for each organization. Therefore, there are multiple *Personal DBs* to manage the documents according to the number of organizations. *Personal Meta DB* is a relational database that should manage metadata of ISMS documents, relationship among the documents, and relationship between the documents and ISO/IEC 27000 series. A *Case DB* is an XML database that should manage data of pre-defined, templates, and samples of published ISMS documents. A *User DB* is a relational database that should manage information of users, participants and their responsibilities, and authorization to access other databases.

Databases in ISMDS are related to each other. The relationship among databases in ISMDS means restriction of data in a database to refer to data in other databases by support tools. The structure of the database system and the relationship among databases is demonstrated in Fig. 4. The re-

Fig. 4 Structure of Information Security Management Database System.

relationship is defined based on referencing relations between data stored in each database. A *Criteria meta DB* manages metadata of all standards stored in *Criteria DBs*, and therefore the database is related to all *Criteria DBs*. Data of standards stored in *Criteria DBs* are referred from *Personal DBs*, and therefore, *Criteria meta DBs* are related to *Personal DBs*. Data of ISMS documents stored in *Personal DBs* refer to data stored in a *Case DB*, data of all standards stored in *Criteria DBs*, user's information stored in a *User DB*, and metadata of the documents in a *Personal Meta DB*. However, data stored in each *Personal DB* should not be shared among organizations, and therefore there are no relationships among *Personal DBs*. Thus, *Personal DBs* are related to *Criteria DBs*, a *Case DB*, a *User DB*, and a *Personal Meta DB*.

The relationship among the standards and the relationship among the documents are managed at different level. The relationship among standards is represented as relationship among *Criteria DBs* that manage the standards. However, the relationship among ISMS documents is managed in a *Personal DB*. The relationship among the documents means the input and output relationship.

From the viewpoint of management, there should be multiple separate databases for the standards and documents. However, accessing and retrieving data from more than one database can be burdensome tasks for users. Thus, from the viewpoint of usage, the separated databases should appear as a single database to the users. The users should not have to access multiple databases to retrieve various standards. Moreover, when there are new databases added to manage new versions and translations of standards in the database system, users should be able to retrieve every versions and translations including the new ones as usual.

5.3 Current Implementation

We have implemented ISMDS by using IBM DB2 Express-C Database Management System [21]. At current, IBM DB2 Express-C is the most suitable database management system for our purpose to implement and manage databases of ISO/IEC 27000 series and ISMS documents. IBM DB2 Express-C is a free hybrid type database management system that can provide management of both relational and XML data model effectively [22]. It provides a function called “pureXML” which supports storing XML documents natively, validating documents against schemas, and querying documents [23]. IBM DB2 Information Integrator [24] provides facilities to make multiple databases appear as if they were a single database.

Because it is difficult to manage relationship among database as managing relationship among tables in a database, at present we manage the relationship among the databases as a metadata in other database. The data is managed in a table in *Criteria Meta DB*. The table indicates which databases are directly related to each other based on relationship among databases in Fig. 4.

We use both SQL and XQuery query languages [25] to retrieve data of the standards and documents in the database system. SQL is used for querying the metadata of the standards and documents that are represented in relational data model, and XQuery is used for querying the data of the standards as well as the documents that are represented in XML data model. DB2 also allows the combination of the usage of SQL and XQuery [22]. In order to retrieve data of various standards from multiple databases, first we generate an SQL query to retrieve a list of databases from *Criteria Meta DB*. The list provides information of standards and information of databases that manages the standards that a currently managed in the database system. Then, based on the list, we generate a set of XQuery to retrieve data of standards from each database.

At present, we have constructed a total of 8 databases to manage ISO/IEC 27000 series' metadata, ISO/IEC 27000: 2009 English, ISO/IEC 27000:2012 English, ISO/IEC 27001:2005 English, ISO/IEC 27001:2005 Japanese, ISO/IEC 27002:2005 English, ISO/IEC 27002:2005 Japanese, and ISO/IEC 27003:2010 English versions. Based on XML Schema of ISO/IEC 27000 series, we generated XML documents of the standards and stored them in the databases above. However, we did not store data of ISMS documents because the data should be stored and managed by each user of the database system.

In addition, we also have developed web-based tools for users to easily utilize the database system. The users can easily retrieve all data that the database system manages without knowledge of any database query languages.

6. Use Cases

Managing ISO/IEC 27000 series and ISMS documents by a

Welcome to Information Security Management Database System

Advanced Information Systems Engineering Laboratory
Saitama University
Copyright (C) AISE Laboratory, Saitama University, All rights reserved.

Information security management dictionary based on ISO/IEC 27000 series standards

Search terms and definitions from ISO/IEC series standards

1. Please insert term
2. Please select target
 - ☒ Retrieve from all ISO/IEC 27000 series standards
 - ☐ Retrieve from target standard(s)
 - ☐ ISO/IEC 27000:2009
 - ☐ ISO/IEC 27001:2005
 - ☐ ISO/IEC 27002:2005
 - ☐ ISO/IEC 27003:2010
3. Please select language(s)
 - ☒ English ☐ Japanese ☐ Chinese
4. Please click search button

Fig. 5 A user interface for terms and definitions retrieval.

central database system can allow systematic management and effective utilization of the standards and documents. From the viewpoint of management, various versions and translations of the standards and documents can be easily managed without altering existing versions or translations. From the viewpoint of usage, one of biggest advantages is that various versions and translations of the standards and documents can be retrieved easily from multiple databases. The data can be easily retrieved and the standards can be shared by various users. Moreover, it can be accessed from anywhere at any time.

Next, we presented 3 use cases of ISMDS to show the validity of the data model we have proposed. The objective of the first use case is to show that the data of ISO/IEC 27000 series for various versions and translations can be retrieved easily in an instant from multiple databases in ISMDS. The objective of the second and third use cases is to show that the specific part of the standards can be retrieved easily according to the structure of the standards.

First use case shows data retrieval from multiple databases that manage various versions and translations of ISO/IEC 27000 series. Figure 5 shows a user interface of ISMDS to retrieve definitions of terms from ISO/IEC 27000 series. Firstly, the users input keyword of term to the text box. Next, the users have an option to choose the retrieval target from all standards in ISO/IEC 27000 series or from target standard(s) by selecting the radio button. Finally, the users choose target language(s) by checking the box, and click the “Search” button. Figure 6 shows a result of definitions related with “incident” in English version defined in various standards in ISO/IEC 27000 series. From the result, the users can easily retrieve data from various standards in an instant from multiple databases. Moreover, the users are not required to generate query languages to retrieve the data.

Second use case shows a comparison of definitions of terms for different versions of 2 standards in ISO/IEC 27000

Search result

Keyword: incident Target: all standards Language: English

Term	Definition	Reference
Information security incident	single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security	ISO/IEC 27000:2009(E)
information security incident management	processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents	ISO/IEC 27000:2009(E)
information security incident	a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security	ISO/IEC 27001:2005(E)
information security incident	an information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security	ISO/IEC 27002:2005(E)

Fig. 6 Retrieval result.

Comparison of definitions of terms between different versions of ISO/IEC 27000

Please select 2 versions of target standard

2009
2012

Please select a language of target standard

English

Please insert term

risk analysis

Fig. 7 A user interface for comparison of versions of terms.

Term: risk analysis

ISO/IEC 27000:2009	ISO/IEC 27000:2012
systematic use of information to identify sources and to estimate risk	process to comprehend the nature of risk and to determine the level of risk

Fig. 8 Versions comparison result.

series. Figure 7 shows a user interface of ISMDS to compare definitions of terms for 2 different versions of ISO/IEC 27000. Firstly, the users choose 2 versions to be compared by selecting the target version from the drop down menu. Then, the users choose a target language. Finally, the users input keyword of term to the text box, and click the “Compare” button. Figure 8 shows a result of comparison between definitions of “risk analysis” defined in 2009 and 2012 version of ISO/IEC 27000 in English. From the result, the definition of “risk analysis” has been changed in 2012 version of the standard. Comparing definitions of terms of different versions of the same standard can allow the users easily examine the difference between definitions of specific terms. The users can use such information to make corrections to their ISMS documents according to the latest terminologies

Fig. 9 A user interface for comparison of translations.

Standard: ISO/IEC 27002:2005	
Target: Security control	
Keyword: security policy document	
English	Japanese
Control : An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.	管理策: 情報セキュリティ基本方針文書は、経営陣によって承認され、全従業員及び関連する外部関係者に公表し、通知することが望ましい。

Fig. 10 Translations comparison result.

defined in ISMS standards in order to periodically review and revise the documents.

Third use case shows a comparison of translation of specific part for different languages of standards in ISO/IEC 27000 series. Figure 9 shows a user interface of ISMDS to compare translations between 2 different languages of ISO/IEC 27002. Firstly, the users select 2 languages as target languages for comparison. Then, the users select a version of the target languages. Next, the users specify target content to be compared. Finally, the users input the keywords of target content to the text box and click the “Compare” button. Figure 10 shows a result of comparison between a security control of ISO/IEC 27002:2005 in clause “5.1.1 Information security policy document” in English and Japanese. Comparing translations of a specific part of a standard can allow the users to examine the meanings of target parts without having to rely heavily on translators or other translations support tools. The users can use such information to easily translate their ISMS documents into another language so that they can apply ISMS certification according to their country or region.

Managing the standards and documents by a database system not only allows the data to be easily retrieved by the users, but also can be accessed and crossly retrieved from various support tools in engineering environment supporting organizations with ISMSSs. The support tools can provide users with more effective usages of the standards and documents. Some of the effective usages by using the sup-

port tools are as follows:

- The users can check relationship among standards in ISO/IEC 27000 series, relationship among ISMS documents, and relationship between the standards and documents.
- The users can create templates of ISMS documents based on data of ISO/IEC 27000 series and data of pre-defined or certified ISMS documents.
- The users can revise current version of ISMS documents according to the newest version of ISO/IEC 27000 series standards.
- The users can verify whether their ISMS documents meet the requirements defined in the standards and make correction where appropriate in order to acquire ISMS certification.

7. Evaluation

This section shows our evaluation of ISMDS. The evaluation of ISMDS evaluates the total number of security controls generated by ISMDS according to ISO/IEC 27000 series and number of processes can be reduced by using ISMDS in order to select security controls for risks mitigation.

As we have stated earlier that risks are always evolving, it is important that assessments are kept up to date and that any new risks are addressed as soon as they arise. Therefore, organizations have to rapidly establish appropriate controls to mitigate the new known risks. However, controls establishment involves a lot of processes and requires a lot of time. After new risks have been identified, organizations have to assess the risks to identify applicable risk treatments options. Then, the organizations are required to examine 11 security categories, 39 security objectives, and 133 security controls from over 100 pages of ISO/IEC 27002:2005 to identify and select appropriate controls for mitigation of the known risks.

By using ISMDS, users can rapidly select appropriate security controls in order to mitigate risks. In ISO/IEC 27002:2005, security objectives state what is to be achieved for mitigation of risks and each security objective includes one or more controls that can be implemented to achieve the above control objective. Based on the security objectives, ISMDS suggests applicable controls for users to choose. In detail, based on the risks as keywords, ISMDS finds associate security objectives from 11 categories defined in ISO/IEC 27002:2005 that contains the keywords. Because ISMDS manages the standard in XML data, full-text search can be performed on specific part of the data to extract needed keyword. Moreover, because the XML data are managed according to the hierarchical structure of the standard, parent nodes which are security objectives can enumerate all child nodes which are security controls that belong to the security objectives.

A process flow for controls selection with and without using ISMDS is shown in Fig. 11. From the figure, ISMDS can reduce a lot of effort and time to select appropriate se-

Fig. 11 Flow of controls selection.

curity controls.

For example, users want to define security controls for managing risks related with “network”. The keyword in this situation is “network”. ISMDS uses the word “network” as target keyword to perform full-text search in specific part in 39 control objectives that include the keyword. Based on security objectives, ISMDS extracts related security controls from 133 controls and suggests following controls to the users: 1) 10.4.1 Controls against malicious code, 2) 10.4.2 Controls against mobile code, 3) 10.6.1 Network controls, 4) 10.6.2 Security of network services, 5) 11.4.1 Policy on use of network services, 6) 11.4.2 User authentication for external connections, 7) 11.4.3 Equipment identification in networks, 8) 11.4.4 Remote diagnostic and configuration port protection, 9) 11.4.5 Segregation in networks, 10) 11.4.6 Network connection control, and 11) 11.4.7 Network routing control. Over 133 security controls, ISMDS enumerated 11 controls that are associated with “networks” according to the controls objectives. From the given controls identification number and control name, the users only have to examine the 11 controls and select appropriate controls to mitigate the risks related to “network” where relevant. Thus, the users are not required to examine through 11 security categories, 39 security objectives, and 133 security controls which require the users to spend a lot of time and effort.

The validity of security controls enumerated by ISMDS are extracted from ISO/IEC 27002:2005, and therefore, the controls are at least satisfying a certain level of quality shared globally by most organizations and are well accepted

in international communities. Furthermore, all controls are ensured up to date according to the latest versions because ISMDS manages all available versions of the standard. The accuracy of security controls enumerated by ISMDS satisfying the users’ needs or not depends on keyword. Therefore, the users should make proper considerations and choose the keyword appropriately.

From above, ISMDS is capable to help users to rapidly select security controls for risks mitigation which can be a good help in supporting the users to continuously improve their ISMS. In addition, by reducing unnecessary tasks in controls selection, ISMDS also can help organizations to enhance the consistency of task in ISMS life cycle processes.

8. Concluding Remarks

We have presented our development of ISMDS, a central database system as a basis to provide comprehensive facilities to support organizations with ISMSs, presented some use cases to show the effectiveness of ISMDS, and explored new effective usages of ISO/IEC 27000 series and ISMS documents by using the database system.

ISMDS can provide organizations with ISMSs with many benefits. Organizations can systematically manage ISO/IEC 27000 series and ISMS documents and use them effectively. Various tools integrated in engineering environment for supporting organizations with ISMSs can retrieve data of the standards and documents to support participants performing tasks in ISMSs.

As future works, other standards in ISO/IEC 27000 series and samples of published ISMS documents (e.g., templates of security policies) will be managed in ISMDS and support tools will be developed to collaborate with ISMDS in order to provide the effective usage of ISO/IEC 27000 series and ISMS documents. Our ultimate goal of development of ISMDS is to provide an infrastructure for the environment we are developing to enforce users to perform their tasks in ISMS based on ISO/IEC 27000 series with help from support tools.

Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of presentation of the paper.

References

- [1] J.S. Broderick, “ISMS, Security Standards and Security Regulations,” Int. J. Information Security Technical Report, vol.11, no.1, pp.26–31, Jan. 2002.
- [2] International Organization for Standardization, “ISO/IEC 27001: Information Technology - Security Techniques - Information Security Management Systems - Requirements,” 2005.
- [3] A.I.H. Suhaimi, Y. Goto, and J. Cheng, “An analysis of software supportable tasks in information security management system life cycle processes,” Proc. 2013 International Conference on Information and Social Science, Nagoya, Japan.

- [4] A.I.H. Suhaimi, Y. Goto, and J. Cheng, "An engineering environment for supporting information security management systems," Proc. 2012 International Conference on Security Technology, Jeju Island, Korea, Communications in Computer and Information Science, vol.339, pp.30–37, Springer-Verlag, 2012.
- [5] Jr. H.R. Sprague, "Electronic document management: Challenges and opportunities for information systems managers," MIS Quarterly, vol.19, no.1, pp.29–49, 2005.
- [6] S. Owen, "Electronic document management systems: A case study," http://www.vpit.ualberta.ca/edrms/pdf/edms_case_study.pdf/, accessed Sept. 10. 2013.
- [7] D. Horie, S. Morimoto, N. Azimah, Y. Goto, and J. Cheng, "ISEDS: An information security engineering database system based on ISO standards," Proc. 3rd International Conference on Availability, Reliability and Security, pp.1219–1225, Barcelona, Spain, March 2008.
- [8] International Organization for Standardization, "ISO/IEC 27000: Information technology - Security Techniques - Information Security Management Systems - Overview and vocabulary," 2009.
- [9] International Organization for Standardization, "ISO/IEC 27002: Information Technology - Security Techniques - Code of Practice for Information Security Management," 2005.
- [10] International Organization for Standardization, "ISO/IEC 27003: Information Technology - Security techniques - Information Security Management Implementation Guidance," 2005.
- [11] International Organization for Standardization, "ISO/IEC 27004: Information Technology - Security Techniques - Information Security Management - Measurement," 2009.
- [12] International Organization for Standardization, "ISO/IEC 27005: Information Technology - Security Techniques - Information security risk management," 2011.
- [13] Japan Information Processing Development Corporation, "List of ISMS certified organizations," <http://www.isms.jpdec.or.jp/english/1st/ind/org-list.html>, accessed Jan. 15. 2014.
- [14] A.M. Fal', "Standardization in information security management," Int. J. Cybernetics and Systems Analysis, vol.46, no.3, pp.512–525, May 2010.
- [15] A.I.H. Suhaimi, T. Manji, Y. Goto, and J. Cheng, "A systematic management method of ISO information security standards for information security engineering environments," Proc. International Conference on Informatics Engineering and Information Science 2011, Kuala Lumpur, Malaysia, Part I, Communications in Computer and Information Science, vol.251, pp.370–384, 2011.
- [16] World Wide Web Consortium, "Extensible Markup Language (XML) 1.0 (Fifth Edition)," <http://www.w3.org/TR/REC-xml/>, accessed June 14. 2013.
- [17] D. Suciu, "Semistructured data and XML," The Springer International Series in Engineering and Computer Science, vol.579, pp.9–30, Springer-Verlag, 2000.
- [18] World Wide Web Consortium, "XML Schema Part 0: Primer Second Edition," <http://www.w3.org/TR/xmlschema-0/>, accessed June 14. 2013.
- [19] Advanced Information Systems Engineering Laboratory, Department of Information and Computer Sciences, Saitama University, "XML Schema For ISO/IEC 27000 Series Standards and ISMS Documents," <http://www.aise.ics.saitama-u.ac.jp/isec/schema.pdf>, accessed June 26. 2013.
- [20] G. Kappel, E. Kapsammer, and W. Retschitzegger, "XML and relational database systems - A comparison of concepts," Proc. 2nd International Conference on Internet Computing, pp.199–205, Las Vegas, USA, June 2001.
- [21] IBM, "DB2 Express C 9," <http://www-01.ibm.com/software/data/db2/express-c/>, accessed June 1. 2013.
- [22] K. Beyer, et al., "DB2 Goes Hybrid: Integrating native XML and XQuery with relational data and SQL," IBM Systems Journal, vol.45, no.2, pp.271–298, 2006.
- [23] IBM, "DB2 pureXML - Intelligent XML Database Management," <http://www-01.ibm.com/software/data/db2/linux-unix-windows/>

[xml/](http://www-01.ibm.com/software/data/integration/), accessed June 1. 2013.

- [24] IBM, "Information Integration," <http://www-01.ibm.com/software/data/integration/>, accessed June 14. 2013.

- [25] World Wide Web Consortium, "XQuery 1.0: An XML Query Language (Second Edition)," <http://www.w3.org/TR/xquery/>, accessed June 14. 2013.

in information security management system.

Ahmad Iqbal Hakim Suhaimi is a Ph.D. student of computer science at Graduate School of Science and Engineering, Saitama University in Japan. He received the degree of Bachelor of Engineering in computer science and the degree of Master of Engineering in computer science from Saitama University in 2009 and 2011, respectively. His current research interests include information security engineering environment, database system, information security related international standards and its applications

in information security management system.

Yuichi Goto is an assistant professor of computer science at Graduate School of Science and Engineering, Saitama University in Japan. He received the degree of Bachelor of Engineering in computer science, the degree of Master of Engineering in computer science, and the degree of Doctor of Engineering in computer science from Saitama University in 2001, 2003, and 2005, respectively. His current research interests include relevant reasoning and its applications, automated theorem finding, anticipatory reasoning-reacting systems, and Web services engineering. He is a member of ACM, IEEE-CS, IPSJ, and JSAI.

in information security management system.

Jingde Cheng is a professor of computer science at Graduate School of Science and Engineering, Saitama University in Japan. He received the Bachelor of Engineering degree in computer science from Tsinghua University in China in 1982, and the Master of Engineering degree and the Doctor of Engineering degree, both in computer science from Kyushu University in Japan, in 1986 and 1989 respectively. Before he joined Saitama University in 1999, he was a research associate (1989-1991), an associate professor (1991-1996), and a professor (1996-1999) at Kyushu University. His current research interests include relevant and ampliative reasoning, relevant logic and its applications, epistemic programming paradigm for scientific discovery, autonomous evolution of knowledge-based systems, anticipatory reasoning-reacting systems, persistent computing, and information security engineering environment. He is a senior member of ACM, and a member of IEEE-CS, IEEE-SMC, IEEE, and IPSJ.