Feasibility of Automated Information Security Compliance Auditing

Longley D., Branagan M., Caelli W.J. and Kwok LF

1 Introduction

According to AS/NZS ISO/IEC 27001:2006 [11], management of an organization should provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the organization's information security management system. The objective of this research project was to explore the feasibility of designing an intelligent documentation system to assist information security managers in meeting this commitment. In particular, this documentation system would assist in the associated tasks of risk assessment and information security compliance auditing.

The proposed documentation system, comprising both supporting software and a database model of the organizational information security environment, together with formalized compliance requirements, may be used both for automated and ongoing compliance testing as well as risk assessment. The risk assessment aspect of the documentation system has been described in previous papers [3, 14]. This paper will deal with a feasibility study of automated compliance auditing. Such automated compliance auditing would enable security managers to readily benchmark their current systems against the appropriate information security standards.

This study was undertaken to specifically explore the feasibility of automated compliance auditing against an international information security standard. The standard originally selected for the study was AS/NZS ISO/IEC 17799:2001) [9]

Dennis Longley and William J Caelli
International Information Security Consultants Pty Ltd, 21 Castle Hill Drive South, Gaven, Queensland 4211 Australia e-mail: d.longley@iisec.com.au,w.caelli@iisec.com.au

Mark A. Branagan
Information Security Institute Queensland University of Technology, GPO Box 2434, Brisbane, Qld, Aust 4001 e-mail: m.branagan@isi.qut.edu.au

Lam-for Kwok
Department of Computer Science, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon, HKSAR, PRC e-mail: cslfkwok@cityu.edu.hk

but during the course of the project this standard was replaced by AS/NZS ISO/IEC 17799:2006 [10]. However, since the objective of the study was to explore the feasibility of automated information security compliance auditing in general, the decision was taken to complete the detailed work on the previous standard.

Bellamy et al [4] warn against the concept of automatic compliance systems *"because ultimately one or more persons must take personal and legal responsibility for compliance."* Nevertheless the use of automation to significantly reduce the manual effort, currently required by information security personnel, and thus the cost of compliance auditing is a worthwhile venture. It is postulated that automated compliance auditing would significantly reduce the auditing effort currently faced by security personnel. This would enable audits to be routinely performed: as part of a continuing security improvement process, when reporting on the security implications of proposed developments, etc. The provision of audit reports for governance purposes would be a natural byproduct of this process.

The implementation of automated compliance testing is not a cost free process. However, by minimizing duplication of effort and removing the need to have experienced security staff undertake many of the required auditing tasks the overall cost is reduced. With the proposed system, the significant effort of converting a text based standard to a series of logical statements is undertaken by some central body, e.g. an appropriate standards authority or the head office of a large organization. The auditing data collection / collation effort is then simplified to the point where it can be handled by junior technical or administrative staff.

A major component of this research project lay in the experimental conversion of a text based standard into a series of logical statements to be used for automated compliance testing. An idealized view of the proposed system is illustrated in Fig. 1. The compliance auditing software processes the standards requirements and organizational system documentation to produce audit data, subsequently evaluated by an experienced auditor to produce a final report for senior management. The audit data output itself would also provide useful information to security managers.

The study did not assume that standardized system documentation would be readily available to security managers or that current organizational documentation could be readily reformulated. It is however postulated that an interface to the system documentation and data can be developed to facilitate the task of querying

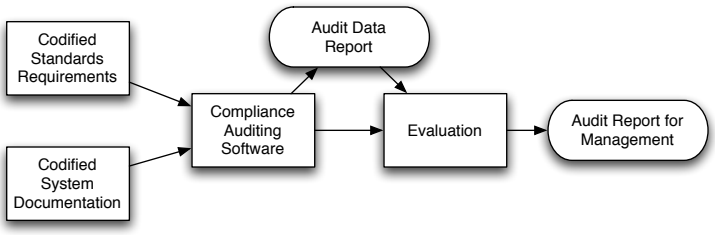

Fig. 1 Automated Compliance Auditing Standards Requirements

organizational security relevant information. This study encompassed: conversion of the ISO/IEC 17799:2001 document into a series of codified compliance requirements (CCR), development of an interface to facilitate querying of organizational security relevant data, and development of prototype compliance auditing software.

The results of this research study demonstrated an automated compliance audit for a small system against the requirements of AS/NZS ISO/IEC 17799:2001 providing useful experience in establishing an automated compliance auditing regime.

2 Governance and Compliance Auditing Background

The U.S. government has been active in information security governance for several decades. Creation and dissemination of standards and guidelines commenced in the early 1970s under the auspices of the National Bureau of Standards (NBS), the predecessor of the National Institute of Standards and Technology (NIST). In 1992, the OECD Guidelines for the Security of Information Systems [15] defined nine principles to address concerns for the dangers of weak information security. The UK Governments Department of Trade and Industry (DTI) published a Code of Practice for Information Security Management [18], amended and re-published by the British Standards Institute as BS 7799 in 1995[5]. This standard was revised in 1999 evolving into ISO/IEC 17799 in 2000 [8]. BS 7799-2, an Information Security Management Specification, was published in 2002 [6]. Currently ISO/IEC 17799:2006 and ISO 27001:2006 [11, 10] represent the latest versions of these standards.

The massive expansion of government and corporate ICT systems in the last decade, coupled with growing concerns about corporate governance practice, have increased the demands made upon management to demonstrate the effectiveness of their information security systems and procedures. Hence legislation has been enacted related to corporate financial governance (the USA's Sarbanes-Oxley Act [17]), maintenance of healthcare information systems (HIPAA [16]), and confidentiality of personal information held by companies (California's SB1386 [2]). These and other similar pieces of legislation require an enterprises management to demonstrate the scope and effectiveness of their information security systems and procedures.

These governance demands have placed a heavy load on corporate management and an estimated cost of $27.9 billion for compliance testing in the U.S alone in 2007 has been quoted [1]. This level of governance implies that management should move beyond a mere demonstration of the "health" of the current ICT system to the adoption of enterprise architectures incorporating information security.

3 An overview of Automated Compliance Auditing

Financial auditing has a centuries old tradition and a financial auditor undertakes two tasks:

- Examination of the organizations financial records against audit requirements to produce a set of audit data indicating any areas of apparent incompatibilities etc.
- Production of a report on the financial situation of the audited organization based upon a detailed evaluation of that audit data.

The first process is normally delegated to junior accounting staff and their task is simplified by the standardization of normal financial documents. This standardization allows them to cope readily with financial records from a variety of sources. The information security manager is usually in a less enviable position since the limited history of information security auditing has not produced detailed guidance on security documentation. Hence, currently, compliance auditing frequently involves significant cross correlation of conventional organizational documentation never designed for that purpose. Consider for example, AS/NZS ISO/IEC 17799:2001 Para 7.1 which includes the statement:

> Critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference.

In the late 1980s a mainframe computer centre manager would probably know from memory the details of any computing systems processing sensitive data, their locations and the physical security of those locations. Current, complex distributed information processing presents an entirely different scenario. The information security auditor must now cross-correlate sensitive information assets with processing systems, identify each component of the distributed system, determine its location and cross correlate its location with any security barriers and entry controls. For present systems, even if this information is documented, there may be no guarantee that system changes are accurately reflected in this documentation.

In these circumstances the compliance auditor is faced with, at best, the difficult task of gleaning the requisite system data from a variety of document sources, and at worst with a major data collection task involving interviews and physical inspections. This data collection task may need to be repeated for each audit. The prime benefit of automated compliance auditing is that it encourages the standardization of the requisite documentation, reducing the effort involved in multiple data collection activities and of cross correlating this data with standards requirements.

3.1 Security Documentation for Auditing

Previous work on security documentation has been reported [3, 14, 13, 12, 7]. Given the problems of reformulating the total set of existing relevant organizational documentation to a form suitable for information security auditing, a proposed alternative approach is illustrated in Fig. 2. Here a database providing a template for an information security model (ISM) of the organization, is developed, e.g. by the standards authority, to facilitate querying for standards compliance checking.

The information security model firstly represents each item relevant to information security in an organization, i.e. IT systems and components, locations, services, documentation etc., as an entity with attributes and inter-relationships. These entities are organized hierarchically in a tree structure. Each database entry thus represents a node of the tree structure and stores the attributes of that entity, e.g. the date of a document, the security sensitivity of an information asset, etc. The inter-relationships between entities are themselves considered as system entities, and their components are similarly stored in database entries.

This template database thus contains entries for entities such as *information processing system* and *buildings*, and relationships between those entities (e.g. *located_in*). This template database reduces duplication of security documentation design effort amongst security managers by providing an operational framework.

When populated the Standardized ISM Database contains: cross-references to the organization's documentation set, information on requisite entities from the documentation, and additional data on entities required for compliance auditing and not available from the current organizational documentation.

The task of implementing and updating the standardized model database is discussed in more detail below (See 5.3). The manual effort required to establish and update the model database depends, to some extent, on the form and content of existing organizational documentation. If the existing documentation can be queried electronically, incorporating the data into the database will involve minimal effort. If the documentation is not in electronic form then populating the database initially will be more labour intensive, as in a manual audit. This initial effort will nevertheless be repaid by the reduction in effort required for subsequent compliance auditing and risk analysis data collection. Further, the end result will be a comprehensive information security database for the security manager. In any event, the use of the template database implies that much of the work can be delegated to junior staff.

The Standardized ISM Database serves as a standards requirements interface to the organizations IT documentation, systems and environment and significantly reduces the task of formulating codified standards requirements to be used in automated compliance auditing. In particular, when a standards requirement makes a reference to a model entity, e.g. a security policy document, that database entry is available to the designer of the codified compliance requirement (See Fig. 3).

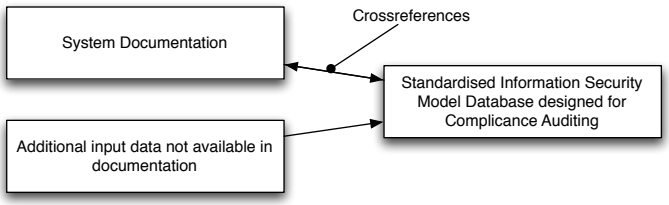

Fig. 2 A Documentation Database for Compliance Auditing

The security manager populates the database by adding organizationally specific information to entries in the template. For example, ISO 17799:2001 specifies the requirement for a management approved security policy document with various subsections. Entities for that document and its subsections would be included as named entities in the database template. The manager would then enter certain attributes of these entities, such as cross-references to the corresponding organizational security policy and its subsections, date and confirmation of management approval, etc. as specified by the compliance requirements.

The security manager is also required to add *children* entities to nodes of the template tree such as, rooms, information processing systems, networks etc. and to add relationship entities indicating, for example, the *location of information processing systems*, *interconnections of networks*, etc. Relationships inherently required by the content of various standards paragraphs are defined in the template database.

When the database has been populated it can be queried via the codified compliance requirements to produce an audit data report (Fig.5). The database is moreover a valuable documentation resource and the model data can also be used for risk assessment studies as described in a previous paper [14].

3.2 Codified Compliance Requirements

A number of the sections of AS/NZS ISO/IEC 17799:2001 [9] are purely informative from the viewpoint of the standard itself, e.g. Sections 1 and 2. In addition, the subsequent sections sometimes contain informative subsections that may be included in the local internal security manual.

The remaining standards paragraphs specify requirements and need to be transformed from simple text format to a series of logical statements for automated compliance auditing. These codified compliance requirements (CCRs) are formulated at a central authority, e.g. by the standards body, and supplied to the security manager with the template ISM database.

Using the ISM database as an interface to organizational information security documentation implies that standards compliance requirements may be specified in

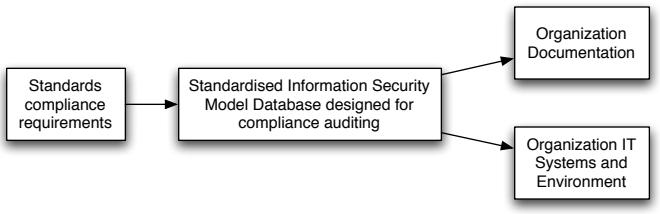

Fig. 3 Standardised ISM Database

terms of ISM database entities, their attributes and interrelationships. Each of these entities may be specified in turn as the address of the corresponding database entry.

The degree of complexity associated with the various sections of information security standards varies widely. Some merely refer to the contents of certain documents, whilst others involve attributes and inter-relationships of users, systems, assets, documentation etc. Experience in developing the CCRs for the various chapters of 17799:2001 indicated the value of a relatively simple basic form of codified requirement, as a building block for the various compliance requirements (Fig. 4).

The codified compliance requirement format developed in this study comprises the following components, compliance reference and brief description, starting entities, relationship between target entities and starting entity, criteria to be met by the target entities, output entities, and audit data.

The starting entity refers to an entry in the ISM Database (See Sect 3.2), and is included as an address in the CCR. This illustrates the advantage of the standardized model in that the designer of the CCR can directly access the entity of concern, once accessed the data included for that entry is queried for compliance checking.

3.3 Information Security Model Database

The ISM database was developed originally for risk assessment [3] and risk assessments may utilize the data entered for compliance auditing and vice versa. The ISM data are stored in a tree structure. There are no constraints on this structure and the ISM software does not assume any particular model or contain any security information; it merely manipulates the entities as required. The parent nodes of the tree hierarchy used in the compliance auditing study were:

- System: Platforms (information processing systems), hardware, networks, software, assets, users and security components
- Environment: Location (sites, buildings, rooms...) and services (power supplies...)
- Security: (not used for compliance testing but retained for risk assessment studies)

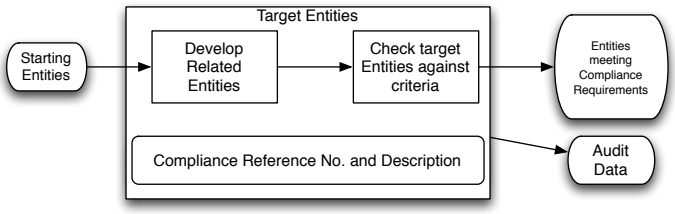

Fig. 4 Codified Compliance Requirement (CCR) Requirements

- Procedures: (documentation, organization, CCRs)
- Relationships

The software displays the tree as a conventional directory tree and entities can be accessed with the conventional GUI for accessing files in a directory structure. The details of each entity: name, description, attributes and relationships, are displayed as the entity is selected Entities can be added or modified manually, but for this study entities were input in the form of an XML file.

Entities may be assigned attributes defined in tag-value format. The value may be a text string, any defined object or another entity. Relationships between entities are themselves treated as entities and are used to define linkages between entities.

3.4 Compliance Software

Development of the compliance software was facilitated by the availability of routines used in the risk assessment studies. Nevertheless there was a considerable degree of experimentation and trouble shooting initially, due to the lack of experience in the interpretation of the standards, design of CCRs and the model template, etc.

A number of valuable lessons were learnt in this development process:

- complex CCRs should be developed as combinations of basic standard forms;
- the correctness of CCRs should be assured before compliance testing;
- the audit data output should be designed to provide maximum information to the auditor rather than as a final report to management.

3.5 Auditing

The immediate output from the automated compliance auditing process is a set of audit data (Fig. 5) representing the detailed results arising from the application of the CCRs to the populated ISM database. The audit data contain details of the standards section, conformance/non conformance to the compliance requirements, names of the starting and target entities and, if required, attributes of those entities.

AUDIT RESULT Seq No. 1.1 Section 17799. Sect 3.1.1

RESULT ConditionResult: initialEntity = Security Policy Document

resultEntity = Security Policy Document targetEntity = Security Policy Document

Decision = true

Candidate attr list

URL doc/policy

Fig. 5 Audit Report

The compliance software creates audit data reports on the information contained in the ISM database but the auditor needs to evaluate this data. For example:

- Do the organizational document subsections cross-referenced in the database actually contain the information specified in the textual standards?
- Is the ISM database content complete and accurate, e.g. is there a sensitive information processing system located in an insecure environment that is not entered in the ISM database?

The automated compliance auditing will have supplied the auditor with a cross-reference to the requisite document subsection, and ideally this will take the form of a URL to that subsection, allowing the auditor to randomly sample the specified document subsections.

The auditor should also seek assurance that the ISM database truly reflects the state of organizational information security by requesting that it be certified by organizational management. For example, the ISM database contents may be recorded as an XML document and signed off by organizational management.

Management in turn will need to seek assurances on the validity of the database contents prior to providing such certification. Such assurances may result from internal audits, facilitated by the format of the ISM database. For example, security managers may run partial audits related to sections of the standards, e.g. physical and environmental security, after known system changes or on a regular basis with a frequency related to the volatility in a particular sector and compare audit results with their local knowledge. Such proposed procedures for updating and checking the ISM database are described in more detail below (See 5.4).

The audit data produced by the compliance software contains a great deal of detail which is useful to the auditor and security manager, as described above, but is superfluous from a governance viewpoint. It is therefore suggested that the audit data be evaluated, and processed into a final audit report, for submission to management (see Fig.1).

4 Designing Codified Compliance Requirements

This study was designed to explore, inter alia, the problem of converting a text based standard to a series of logical statements for automated compliance auditing. In this process it became clear that considerable care was required to ensure that this translation conformed to the intentions of the standards authors. Whilst conventional security auditors have the task of interpreting the individual sections of the standards in the context of their local system, the CCR designer must undertake this interpretation in a much wider context. It is therefore important that some higher authority examines the subsequent set of codified requirements to ensure that they truly reflect the intentions of the standards authority. Codification of legal documents in this regard provides a useful precedent.

The CCRs were developed in this study to indicate the feasibility of such an approach. They were based upon best endeavor interpretation and were not intended as an authorized version for general usage. One of the major concerns in this interpretation process was that of deciding the level of compliance checking. Consider for example: 17799:2001 Section 8.1.4 *Segregation of duties* referring to the danger of fraud if personnel have excessive access privileges.

Bracketing the potential compliance levels one might consider the upper and lower levels of compliance to be:

- **Least Stringent:** insert a paragraph in the local security manual to the effect that managers were to apply segregation of duties principles when allocating access privileges
- **Highly Stringent:** checking the access privileges of every individual member of staff to ensure adequate segregation of duties.

In some cases it may prove impossible to agree upon a single codified compliance for all organizations. In this case categories of organizations could be defined, and CCRs developed for each category. In summary, the CCR designer requires guidance on the interpretation of the text based standard, and the subsequent codified compliance requirements should be subjected to approval from a higher authority.

4.1 Basic Compliance Requirements

A codified compliance requirement (CCR) is essentially an IF-THEN statement. Nevertheless, considerable experimentation with the format of CCRs occurred in the course of this project. The lesson learnt from this experimentation was that a simple basic format, capable of parameterization and combination, presented the best solution. The basic format selected is illustrated in Fig. 4. The parameterization comprised the routines used to relate target entities to individual starting entities and apply criteria for the target entities.

A target entity will satisfy one or more of the following conditions in relation to the starting entity:

- any immediate child of the starting entity, from the viewpoint of sub trees in the model database;
- any descendent of the starting entity;
- any entity linked to the starting entity in a specified model database relationship;
- any entity linked recursively to the starting entity in a specified model database relationship;
- any entity contained in the starting entity when the latter is a specified relationship.

In some cases a simple Boolean AND was used to combine conditions. It was found that all the compliance requirements of 17799:2001 could be formulated using this approach. The criteria used for 17799:2001 requirements were that the target entity must be an entity:

- with the same model database address as a CCR specified entity;
- with the same name as a CCR specified entity;
- which is a child of a CCR specified entity;
- with a CCR specified attribute, or set of attributes;
- with a CCR specified attribute value.

This basic CCR was adequate for one of the most common compliance requirements, i.e. for those sections of the standard recommending that specified subsections be included in a given document.

4.2 Serial Compliance Requirements

A serial combination of CCRs was commonly used to report upon situations related to operational documentation concerning a given set of entities, e.g. documentation for processing systems, information assets etc. For example, 17799:2001 section 8.1.1 Documented Operating Procedures states, *The operating procedures identified by the security policy should be documented and maintained*. Audit of this requirement essentially involves a multi stage operation: select all the information processing systems; retrieve the operating procedure documentation for each information processing system; and check that each operating procedure document contains the subsections specified in Section 8.1.1.

Whilst the number of stages could be reduced by the use of AND conditions the multistage CCR was used to ensure comprehensive reporting in the audit data, e.g. it was important to report if there were no operating procedures for a particular information processing system.

5 Implementation

There are three parties in the proposed scheme:

- the body responsible for the design of the ISM database template and codified compliance requirements (CCR). It is expected that the software comprising the ISM template, CCRs and compliance checking software would be supplied to security managers;
- security managers responsible for populating the ISM database and maintaining and certifying the database contents for audit purposes;
- compliance auditors responsible for checking and evaluating the audit data.

The first task in the process leading to the automated compliance system lies in the definition of the ISM template database providing an indication of the assumed IT environment for the audit. The CCRs utilizing the template database must then be produced and tested.

Organizations will then be supplied with software comprising the ISM template database, compliance checking software and CCRs. The security managers will then populate the ISM database with details of the organizational IT environment, and accept responsibility for checking and maintaining this database for use in audits.

The information security auditors will run the compliance checking software with the CCRs to produce the audit data and make checks on the validity of this data, before evaluating it and producing an audit report for management. Each of these processes is described in more detail in the following sections.

5.1 Defining the Information Security Model Template

In this study the information security model template was defined and the database was populated with model data to test the codified compliance requirement (CCR) design. There were two major aspects of the template model developed for compliance auditing: documentation entities and system entities. A high proportion of the 17799:2001 sections refer to implied organizational documentation and experience of codifying those requirements suggested that the requisite documentation entities fell into four categories: security policy; internal security manual; operational security documentation; and reports, contracts, logs, reviews etc.

The requirements for the security policy document are described in 17799:2001 Section 3.1.1 and enhanced in subsequent sections e.g. Section 8.3.1: *"a formal policy requiring compliance with software licences and prohibiting the use of unauthorized software."*

The internal security manual informs all organizational parties of the security requirements and is, in effect, an edited version of the standards document translated for the local environment. The corresponding operational security documentation entities represent the documents recommended within the security manual for the various system entities, e.g. the documented operating procedures for each information processing system as described in 17799:2001 Section 8.1.1

The first three categories of documentation have a one-to-one relationship with the standards and hence represent entities defined by the CCR designer, having addresses in the database known to the designer. The fourth category of documentation entities *reports, contracts, logs, reviews etc.* represent multiple documents produced by the organization and are listed under headings specified by the CCR designer.

The model system entities were added as they were mentioned within the various sections of the standards. These system entities included: platforms (i.e. information processing systems), hardware, software, networks, users, information assets, security, locations and services, and the various subheadings were added as they arose in the standard.

The relationships were also defined as the need was indicated by the standards, e.g. systems were *located_in* in sites/buildings, and were *supplied* by power supplies, cabling was *installed_in* locations, gateways were *connected_ to* networks and so on.

5.2 Designing the Codified Compliance Requirements

The conversion of textual standards statements into CCRs is not a mechanical process. Standards authors assume that the requirements will be interpreted by auditors in the context of a local IT environment. The ISM database template serves to give some context for the design of the CCRs and this template must therefore be defined as the first task in the translation process. The translation of some standards requirements, e.g. those dealing with documentation, was reasonably straightforward. For others the design of the CCRs was not so clear. Many standards requirements related to system entities necessitated careful analysis of the standards text and significant assumptions related to the organizational context when designing CCRs. It is likely that for some standards statements a number of organizational contexts may need to be postulated and CCRs specified for each.

Following the requirements translation the design of the CCRs may be undertaken in a four stage process:

- commence with a classification of the various sections of the translated standard into CCR categories,
- design CCRs for each of these categories;
- translate the standards textual statements into these CCRs categories;
- produce the CCRs.

The experience of CCR design described above (See 3.2) may well assist in the procedure. In this study the CCR design proceeded quite rapidly once the foundations on CCR formats and template design had been established. It is recommended that software be developed to aid CCR designers in the production of CCR XML documents. Checking the CCR format before it is processed by the compliance checking software significantly reduced the complexity of that software, and facilitated trouble shooting in the CCR design.

5.3 Implementing and Maintaining the ISM Database

There are perhaps three potential classes of organizational information security documentation:

- Case 1: comprehensive, in electronic form and containing all the information required by the standard;
- Case 2 : reasonably comprehensive, in electronic form but not sufficiently complete in terms of the standards requirements;
- Case 3: not comprehensive and only partially or not in electronic form.

In the first case the codified compliance requirements could be formulated to allow for direct access to the organizational information, and the ISM database would not be required. Tools used to explore and report upon networks would probably produce this form of documentation, but other aspects of the documentation, e.g.

personnel, physical and environmental security would also need to be in this format.

In the second case effort required to bring the documentation to the level of Case 1 would probably be greater than that of implementing the ISM database. It should, in any case, be possible to arrange for much of the electronic documentation to be queried so to produce the data for direct entry into the ISM database.

In the third case there would be a significant amount of effort expended in extracting the requisite input data for the ISM database. However, this would be a once-off task, the alternative approach of conventional manual auditing would involve this amount of effort for every audit. In any event much of this work related to the population of ISM database is a of routine nature and may be delegated to junior staff.

5.4 Conducting Audits

The objective of automated compliance auditing is to transform the audit process from a major manual task, which may be viewed as a bureaucratic burden by information security managers, to a routine activity, conducted periodically to provide feedback on the organizational information security stance.

Audits for governance purposes will follow the process illustrated in Fig. 1. The auditor will evaluate the audit data from the viewpoint of ensuring its correctness, completeness and significance. The audit data is a reflection of the contents in the ISM database and the auditor will seek some re-assurance that it reflects the true organizational situation hence the auditor may conduct additional investigations to:

- ensure that cross-references lead to documents that do indeed have the requisite contents;
- check that the documentation has a valid certification and that there is evidence of periodic internal audits verifying the ISM database contents;
- check that some random samples of the database contents are consistent with the results of interviews and physical inspections.

Once the audit data has been subject to verification as described above the auditor will then consider the significance of the audit data in relation to the management intentions on information security and produce a final report for senior management.

6 Conclusion

The objective of information security standards is to raise the level of information security in an organization to an optimum state. If the auditing process is a periodic and highly onerous task undertaken merely to satisfy governance requirements, there is a danger that it can simply serve to increase the burden on the information

security manager without materially improving the actual level of information security in the enterprise. Automated compliance auditing as described here provides the information security officer with a valuable resource in terms of the ISM database which can be used both for compliance auditing and associated risk assessment [14]. The compliance audits can moreover be undertaken more routinely, allowing the security manager take a more proactive role in terms of continuous improvement and quick reaction to system changes.

References

1. C. Abrams, J. vonKänel, S. Müller, B. Pfitzmann, and S. Ruschka-Taylor. Optimized enterprise risk management. *IBM Systems Journal*, 46 (2):219–234, 2007.
2. California Security Breach Information Act. SB 1386, 2003.
3. Alison Anderson, Dennis Longley, and Lam For Kwok. Security modelling for organisations. In *CCS '94: Proceedings of the 2nd ACM Conference on Computer and communications security*, pages 241–250, New York, NY, USA, 1994. ACM.
4. R.K.E Bellamy, T. Erickson, B. Fuller, W.A. Kellogg, R. Rosenbaum, J.C. Thomas, and T. Vetting Wolf. Seeing is believing: Designing visualizations for managing risk and compliance. *IBM Systems Journal*, 46 (2):205 –218, 2007.
5. British Standards Institute. BS 7799, Code of Practice for Information Security Management, 1995.
6. British Standards Institute. BS 7799-2, Information Security Management Specification, 2002.
7. W.J. Caelli, G. Gaskell, LF Kwok, and D. Longley. A model to support information security governance. *Journal of Information Risk Management and Audit*, 16(1):7–24, 2006.
8. International Standards Organisation. ISO/IEC 17799:2000, Information technology—Code of practice for information security management, 2000.
9. Joint Australian and New Zealand Standard. AS/NZS ISO/IEC 17799:2001 Information technology—Code of practice for information security management, 2001.
10. Joint Australian and New Zealand Standard. AS/NZS ISO/IEC 17799:2006 Information technology — Security techniques— Code of practice for information security management, 2006.
11. Joint Australian and New Zealand Standard. AS/NZS ISO/IEC 27001:2006 Information technology — Security techniques — Information security management systems- Requirements, 2006.
12. L-F Kwok and D. Longley. Information security management and modelling. *Information Management and Computer Security*, 7(2):3–4, 1999.
13. Lam For Kwok and Dennis Longley. A security officer's workbench. *Computers & Security*, 15(8):695–705, 1996.
14. Lam-for Kwok and Dennis Longley. Security modelling for risk analysis. *Security and Protection in Information Processing Systems*, pages 29–45, 2004.
15. Organisation for Economic Co-operation and Development, Directorate for Science Technology and Industry. Guidelines for the security of information systems, 1992.
16. Health Insurance Portability and Accountability Act of 1996. Public law 104-191, united states senate and house of representatives in congress, 1996.
17. Sarbanes-Oxley Act of 2002. Public law 107-204 (116 statute 745), united states senate and house of representatives in congress, 2002.
18. U.K. Department of Trade and Industry. Code of practice for information security management, 1992.