2006

A quantitative method for ISO 17799 gap analysis

Bilge Karabacak
Franklin University, bilge.karabacak@franklin.edu

Ibrahim Sogukpinar
Gebze Institute of Technology

Recommended Citation

Karabacak, B., & Sogukpinar, I. (2006). A quantitative method for ISO 17799 gap analysis. *Computers & Security, 25* (6), 413-419. https://doi.org/10.1016/j.cose.2006.05.001

available at www.sciencedirect.com

SCIENCE DIRECT®

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A quantitative method for ISO 17799 gap analysis

Bilge Karabacak[a,*], *Ibrahim Sogukpinar*[b]

[a]*National Research Institute of Electronics & Cryptology (UEKAE), P.O. Box 74, 41470 Gebze, Kocaeli, Turkey*
[b]*Gebze Institute of Technology, 41400 Gebze, Kocaeli, Turkey*

ARTICLE INFO

Article history:
Received 7 May 2005
Revised 22 March 2006
Accepted 19 May 2006
Published on line ■

Keywords:
BS 7799
ISO 17799
ISO 27001
Compliance
Information security
Risk analysis
Quantitative risk analysis
Survey

ABSTRACT

ISO/IEC 17799:2005 is one of the leading standards of information security. It is the code of practice including 133 controls in 11 different domains. There are a number of tools and software that are used by organizations to check whether they comply with this standard. The task of checking compliance helps organizations to determine their conformity to the controls listed in the standard and deliver useful outputs to the certification process. In this paper, a quantitative survey method is proposed for evaluating ISO 17799 compliance. Our case study has shown that the survey method gives accurate compliance results in a short time with minimized cost.

1. Introduction

Standards play an essential role for drawing the roadmap of information security. ISO/IEC 17799:2005 is an essential standard for information security (ISO/IEC, 2005). Originally, it was a British Standard named BS 7799, which was revised on a large scale in 1999. After this revision, BS 7799 was adopted as international standard by International Organization for Standardization, which is abbreviated as ISO. The new worldwide standard was named as ISO/IEC 17799:2000. ISO 17799 is revised significantly in 2005.

British Standards Institution launched formal certification scheme for BS 7799 in 1999, which was named as BS 7799-2:1999. In 2005, ISO released its own certification standard, ISO/IEC 27001:2005 (ISO, 2005). ISO/IEC 17799:2005 and ISO/IEC 27001:2005 have strong relationships. ISO/IEC 17799:2005 is the code of practice in which there are 133 controls. ISO/IEC 27001:2005 establishes the framework of Information Security Management System. The controls, which are listed in the former, are used consistently in Information Security Management Systems.

Compliance is the practical process of comparing the applied controls of an organization with those in ISO 17799. It is basically a gap analysis in which the differences between the situation of organization and the standard are discovered. The task of checking conformity level helps companies to determine their situation, thus it delivers useful input to the certification process.

Certification has become a popular issue for organizations. Today, many organizations quote intent for ISO 27001 (or BS 7799) certification. Also, some organizations are on the route to certification. Some of them are already certified. It is

* *Corresponding author.*
E-mail addresses: bilge@uekae.tubitak.gov.tr (B. Karabacak), ispinar@bilmuh.gyte.edu.tr (I. Sogukpinar).
0167-4048/$ – see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2006.05.001

expected to have significant international increase in certification demand.[1] Thus, the importance of compliance process increases day by day.

In this work, we proposed a quantitative survey method for evaluating ISO 17799 compliance. This method is built upon the risk model of ISRAM (Karabacak and Sogukpinar, 2005). The risk model of ISRAM is customized in order to be used in a compliance process. ISRAM is a quantitative survey-based risk analysis tool, which makes use of basic mathematical operations. Its risk model is based on the famous risk formula; risk is equal to multiplication of the probability of threat occurrence and the impact of occurred threat. ISRAM elaborates this basic risk formula, so that the risk formula contains the number of participants, the number of questions, the weight of questions and the weights of answer choices. The survey, thus the risk analysis process, can be successfully finished by following the risk model of ISRAM. The reader is referred to Karabacak and Sogukpinar (2005) for a detailed explanation.

Like ISRAM, the heart of proposed compliance method is a quantitative formula. The formula covers the basic steps of a compliance survey. In this case, it produces the compliance percentage instead of a risk value. Our compliance method assigns quantitative weight values to ISO 17799 controls. These controls are converted into survey questions. It designates answer choices to all of the questions, and weight values are also assigned to all of the answer choices. The weight values of the answers and the questions are represented as variables in our model. In addition to these values, the number of participants and the percentage conversion operators is also represented in our model.

Our compliance method inherits the advantages of ISRAM. The proposed compliance method is cost effective and flexible. The organization may change the values of weight values according to its needs. It does not require any specialized software. Our method's open model gives rise to its ease of use, which is crucial for compliance checks.

The rest of this paper is organized as follows: ISO 17799 compliance and certification methods are introduced in the second section. The proposed method of ISO 17799 compliance is presented in the third section. The fourth section contains some ideas on the verification, comparison and the results of the application. The fifth section is the conclusion.

2. The methods for ISO 17799 compliance

Today, a number of tools are available for performing ISO 17799 compliance. These tools usually make use of questionnaires to determine the compliance level. Most of them are supported by software.

Riskwatch is one of the ISO 17799 gap analysis software in market (Riskwatch, 2005). Riskwatch is used extensively in private and governmental organizations. Some of the clients of Riskwatch are U.S. DoD, the U.S. Dept. of Justice, NSA, AT&T and General Electric. Riskwatch has a modular structure. ISO 17799 knowledge base is one of these modules, by which ISO 17799 gap analysis is performed.

[1] Computer Fraud & Security (2003), BS 7799–Slow uptake by companies, p. 3.

Cobra is just another software tool to make ISO 17799 compliance (C&A Systems Security Limited, 2000). Like Riskwatch, Cobra has an ISO 17799 module. Once a risk analyst runs the module, he is asked a number of questions extracted from the ISO 17799 standard. According to the selected answer choices, Cobra risk model calculates ISO 17799 compliance percent.

CRAMM (CRAMM, 2001) is third software tool, which makes ISO 17799 gap analysis. CRAMM is extensively used in NATO. Like other software based ISO 17799 compliance tools, CRAMM has ISO 17799 module. By using this question module, ISO 17799 gap analysis is performed in the same way.

ISO 17799 Toolkit (The ISO 17799 Toolkit) is a series of documents and items brought together to help companies in the process of ISO 17799 certification. The documents in the toolkit are composed of questions and answer choices related to the information security policy, business impact analysis, disaster recovery planning, dependency analysis and contingency analysis. Contrary to the software tools in market, ISO 17799 Toolkit does not make a compliance check. It directly guides the user to establish an Information Security Management System.

There are novel suggestions for ISO 17799 certification. Incremental information security certification (Solms and Solms, 2001) is such a tool. Incremental security certification divides the ISO 7799 into different levels. Each of the levels contains a subset of the ISO 7799 controls. For example, a company can get a Level 1 certification, if it conforms to those requirements specified for Level 1. The basic idea behind the incremental security certification is the "all-or-nothing" design of certification process (Solms and Solms, 2001). Although most companies are very anxious to get some form of information security certification, the official certification route can be very difficult because of its "all-or-nothing" design. The tools, which are dedicated for ISO 17799 certification are not widely used yet and quite expensive. Incremental security certification is suggested as a simpler alternative method.

Information Security Risk Analysis Method, ISRAM, uses a survey-based formula for quantitative risk analyses (Karabacak and Sogukpinar, 2005). It converts survey questions and answer choices into the numbers and makes necessary calculation to express risk. It makes this effort by using an open risk model. Because ISO 17799 compliance can be performed by making a survey and analyzing the results, ISRAM can be used in ISO 17799 compliance process.

3. Evaluating the ISO 17799 compliance by using quantitative survey

ISO 17799 is not a technical standard. It is related to the business risks and information itself. Thus, by taking the scope into consideration, at least one person from each affected area within the scope should participate in ISO 17799 compliance process. The most suitable approach to reach this goal is to perform a survey, which covers all affected areas within the scope.

3.1. *The model of compliance evaluation*

Our model of ISO 17799 compliance evaluation is deduced from the risk model of ISRAM. ISRAM has a flexible and

open risk calculation formula. All of the survey process can be followed via examining the basic formula. The number and values of survey questions, the number of participants and answer choices can be changed freely.

Our compliance model is shown at formula (1). The number of controls in ISO 17799 limits the number of questions in our customized model. Thus, the number of questions can be at most 133. Depending on the organization type, and its processes within the organization, this number can be less than 133. For example, if there is no software development facility within the organization, the controls related with the software development should be eliminated from the survey. Thus, these controls do not contribute to the compliance value negatively.

ISO 17799 can be thought as a countermeasure list, which is organized into 11 fundamental clauses (Table 1). Once an organization decides to perform a compliance check, it should select relevant clauses and relevant questions within the clauses according to the scope of the compliance process and its business processes within the scope.

$$\text{CompliancePercentage} = \frac{\nabla \sum_{f} \left(\sum_{m} w_m p_m \right)}{f} \quad (1)$$

where f, the number of surveyors for a specified ISO 17799 clause. (The number of the surveyors depends on the clause of ISO 17799.); m, total number of the controls (questions) that are extracted from the specified clause of ISO 17799. (The maximum values of m are shown in Table 1.); w_m, weight of the control (question) 'm'; p_m, weight of the selected answer choice for the control (question) 'm'; ∇, numerical value to percentage conversion. This operation converts the bulk survey result into percentage value, namely '*xx*%'; *CompliancePercentage*, single percentage value for ISO 17799 compliance.

All of the factors for ISO 17799 gap analysis can be seen in formula (1). These factors are the number of participants for each clause, the number of controls and their weight values, the answer choices for each control and their weight values. The result of formula (1) is the ISO 17799 compliance percentage. The inverse delta tool converts bulk survey result into the percentage value. It is a simple direct proportion operation. It calculates the maximum value of the bulk survey result for a specified survey (as if all the controls exist within the company). After the maximum and real survey results are calculated, inverse delta converts this bulk result into percentage value by performing direct proportion.

Table 1 – Clauses and the number of control within the clauses

ISO 17799 clause	The number of controls within the clause
Security policy	2
Organization of information security	11
Asset management	5
Human resources security	9
Physical and environmental security	13
Communications and operations management	32
Access control	25
Information security acquisition, development and maintenance	16
Information security incident management	5
Business continuity management	5
Compliance	10
Total	133

Survey questions should be directed to the relevant staff within the scope. Modular structure of our compliance method makes this possible. The number and profiles of survey participants ~~are determined by~~ the clause of ISO 17799. In our case study, the questions regarding to the clause of security policy is directed to seven participants, who are the CEO, the business manager, and the security officers. The questions regarding to the clause of asset management is directed to 40 participants, who are the system administrators, the security administrators and the system developers. The details of survey process are explained in the following sections.

3.2. *Extracted survey question*

Some of the extracted survey questions are written out in Table 2, which is categorized into 11 clauses as in the ISO 17799 standard. All of the questions cannot be written here, because 133 questions are extracted.

These questions are nothing more than the control statements of the standard, but converted to the survey questions.

3.3. *Survey evaluation module*

Survey evaluation is based on the quantitative measures. To evaluate a survey, it is necessary to convert survey questions and answer choices into the numerical values. This task is done by using Tables 3 and 4, respectively. They are similar to the reference tables of ISRAM method. Tables 3 and 4 are ~~revised~~ by taking the compliance requirements into account.

In our method, the weight values of questions and answer choices are determined by using several standards and best practices like BS 7799-2, COBIT, ISF and NIST guidelines (BSI, 2002; ISACA, 2004; ISF, 2003; NIST, 2001~~a,b~~). But these weight values may be changed according to the security requirements of the organization and this task belongs to the members of the compliance team. For example, inactive sessions may have to be shut down after ~~10 min~~ of inactivity for the military organizations. On the other hand, this control can be omitted by the universities. In this case, military organization should give more weight value to this control. The same scenario is also applied to the weights of answer choices.

In Table 5, some controls, their answer choices and the weight values are given. Some of the questions are simply yes–no questions. Some of them have multiple choices ~~other than the answers of yes or no~~. For multiple-choice questions, only one answer choice is allowed to be selected.

First question in Table 5 is a yes–no question. Second question is a multiple-choice question. If the control is composed of just one factor like the first question, it is regarded as a yes–no question. If the control in ISO 17799 consists of multiple factors like the second question, all possible answer

Table 2 – Some of the extracted questions

Security policy	Is an information security policy document approved by management, and published and communicated to all employees and relevant external parties?
Organization of information security	Are information security activities coordinated by representatives from different parts of the organization with relevant roles and job functions? Are all information security responsibilities defined clearly? Is a management authorization process for new information processing facilities defined and implemented?
Asset management	Are all assets clearly identified and an inventory of all-important assets drawn up and maintained? Are all information and assets associated with information processing facilities owned by a designated part of the organization?
Human resources security	Is there a formal disciplinary process for employees who have committed a security breach? Are responsibilities for performing employment termination or change of employment clearly defined and assigned?
Physical and environmental security	Is physical security of offices, rooms, and facilities designed and applied? Are physical protection and guidelines for working in secure areas designed and applied? Is equipment correctly maintained to ensure its continued availability and integrity?
Communications and operations management	Are operating procedures documented, maintained, and made available to all users who need them? Are changes to information processing facilities and systems controlled?
Access control	Are the allocation and use of privileges restricted and controlled? Is the allocation of passwords controlled through a formal management process? Are users required to follow good security practices in the selection and use of passwords? Are inactive sessions shut down after a defined period of inactivity?
Information security acquisition, development and maintenance	Is data input to applications validated to ensure that these data are correct and appropriate? Is key management in place to support the organization's use of cryptographic techniques? Are there procedures in place to control the installation of software on operational systems?
Information security incident management	Are information security events reported through appropriate management channels as quickly as possible?
Business continuity management	Are business continuity plans tested and updated regularly to ensure that they are up to date and effective?
Compliance	Are data protection and privacy ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses? Are cryptographic controls used in compliance with all relevant agreements, laws, and regulations?

choices are given as in Table 5. Note that, the weights of the two or more of the answer choices can be the same.

Weight values should carefully be determined and agreed prior to each compliance checking process because the compliance percentage is directly related with the weight values of the questions and their answers. Weight values should be selected by a committee (compliance team) whose members should be directly related to the information security.

It is also important that, prior to each compliance check, surveyors should be orientated. It should be stated that, their answers to the questions would directly affect the future information security investments of the company.

The following controls are considered to be essential to an organization from a legislative point of view, depending on applicable legislation (ISO/IEC, 2005):

a. Data protection and privacy of personal information.
b. Protection of organizational records.
c. Intellectual property rights.

The following controls are considered to be common practice for information security (ISO/IEC, 2005):

a. Information security policy document.
b. Allocation of information security responsibilities.

Table 3 – Reference table for the weight values of the controls

Weight of the control (w)	Explanation
3	The control is directly associated with the compliance of ISO 17799. The absence of the control is directly associated with a severe vulnerability and/or the control is directly associated with a critical asset
2	The control is somewhat associated with the compliance of ISO 17799. The absence of the control is directly associated with an important vulnerability and/or the control is directly associated with an important asset
1	The control is a little associated with the compliance of ISO 17799. The absence of the control is directly associated with an insignificant vulnerability and/or the control is indirectly associated with an important asset

c. Information security awareness, education, and training.
d. Correct processing in applications.
e. Technical vulnerability management.
f. Business continuity management.
g. Management of information security incidents and improvements.

Thus, special attention should be given to controls that are related with these factors. The weight values of these questions and their positive answer choices should be maximized.

3.4. *Application of the method*

A number of preliminary technical applications are performed. Firstly, a survey application is programmed by using ASP® web technologies. ~~This survey webpage is arranged to serve whole the organization.~~ A built-in authentication and access-control mechanism is developed, so that authenticated survey users are authorized to see and answer only the questions designated for them.

All of the questions and answer choices and their weight values are imported into web based survey application. Survey evaluation module is at the heart of the process. It ~~is the~~ computerized compliance model depicted in formula (1). It calculates the compliance percentage by taking surveyor answers as input (Fig. 1).

The authentication and access-control mechanism are vital modules for accurate results. This mechanism gives access only to the designated surveyors for each clause of ISO 17799. The application of access-control mechanism for our case study is presented in Table 6.

Table 4 – Possible weight values of the answer choices

Weight of the answer choice (p)	Explanation
4	Most effective answer choice. Affect the compliance enormously
3	Rather effective answer choice. Affect the compliance highly
2	Somewhat effective answer choice. Affect the compliance considerably
1	Least effective answer choice. Affect the compliance slightly
0	No effect on compliance

Table 5 – A subset of questions, answer choices and their weight values

Control questions and corresponding weights	Answer choices and corresponding weight
Are inactive sessions shut down after a defined period of inactivity? (2)	Yes (2) No (0)
Is an information security policy document approved by management, and published and communicated to all employees and relevant external parties? (3)	Yes – all of them (4) Yes but not communicated to external parties (3) Yes but partially communicated (2) Yes but not communicated (1) Yes but not published (0) Yes but not approved (0) No – none of them (0)

4. The results of the application, verification and comparison

A case study is performed to measure the compliance of a governmental organization, which has about 200 staff. All of the staff are participated in the survey. All of the clauses of ISO 17799 are covered within the survey. The details of the survey and the results are shown in Table 6.

In Table 6, the roles of the survey participants for each clause are also shown. Note that, because of the modular structure of our model, partial compliances for each clause can be calculated. This helps to see which clauses show more noncompliance to the standard. For our case study, the company has major problems at the clauses of physical

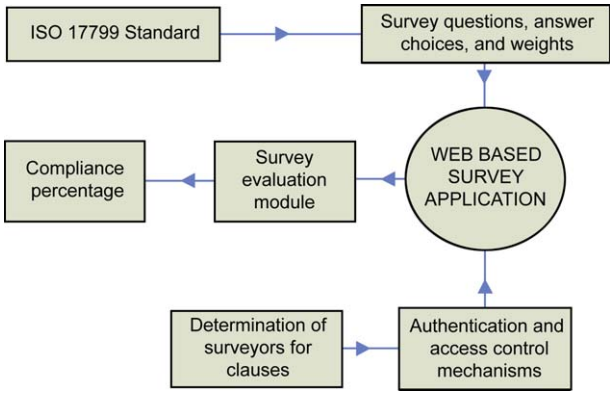

Fig. 1 – Basic flow diagram of the application of quantitative survey process.

Table 6 – The results of the case study

	Total number of answered questions	Total number of participants for these questions	Compliance percentage	The role of surveyors
Security policy	2	7	70	General manager Security officers Managers of the departments
Organization of information security	11	35	50	General manager Managers of the departments Human resources department staff Technical managers
Asset management	5	40	35	System administrators Security administrators System developers Staff
Human resources security	9	9	68	General manager Managers of the departments Human resources manager
Physical and environmental security	13	15	20	Physical security guards Technical managers Staff
Communications and operations management	32	45	54	Security officers System administrators Security administrators System developers System testers Technical managers
Access control	25	87	23	Security officers System administrators Security administrators Physical security guards System developers System testers Technical managers
Information security acquisition, development and maintenance	16	20	67	System developers System testers
Information security incident management	5	8	45	Security administrators Staff
Business continuity management	5	4	22	General manager Technical managers Managers of the departments
Compliance	10	4	85	General manager Managers of the departments Human resources department staff
Total	133	All of the staff	49	

and environmental security, business continuity management and access control. By making necessary treatments at these clauses, the compliance percent can be raised to 70%.

The final percentage value of compliance, 49%, is found by taking the arithmetic average of single percentage values of clauses. Information security should be considered holistically. Thus, equal importance should be given to all of the clauses, if they are applicable for an organization.

~~Software~~ tools in market, which perform ISO 17799 gap analysis, ~~also~~ perform risk analysis. Therefore, these tools

may not be affordable for all organizations. Our compliance method is far cheaper than the software tools like Riskwatch and CRAMM.

It has also advantageous for its ease of use. Most of the software tools require mandatory training sessions prior to starting to use them. Riskwatch and CRAMM are such tools. Cobra is also easy to use like our method.

Both our method and Cobra have flexibility features. The module manager of the Cobra permits to customize the values of the questions and answer choices. For our method, the risk analysis committee performs this task. Riskwatch and CRAMM have capabilities of tailoring the weight values.

As stated in the second section of this paper, ISO 17799 Toolkit does not perform compliance checks. It is very valuable toolkit to help companies for establishing an Information Security Management System. Our method may be used in accordance with the ISO 17799 Toolkit.

Incremental information security certification concepts introduce unique aspects for information security certification. Like, ISO 17799 Toolkit, our compliance method may be used in accordance with this proposed certification scheme.

After case study, it is shown that making compliance analysis by using our method is practical and does not take much time and effort. Our compliance model is flexible enough to make accurate surveys in different circumstances. Some of the irrelevant questions can be omitted. Another flexibility feature is that the weight value of questions and answers can be revised for different surveys in different organizations. Also our method has low-cost. In fact, it does not require any software support. Web based survey application, which is stated in this paper, is an optional component to automate the survey process. All of the compliance process can be realized as paper based by using our method.

5. Conclusion

In this work a quantitative survey method is proposed for ISO 17799 compliance checks. Proposed method has some unique features. Its ease of use and flexibility are important advantages. Technical personnel can easily change the number of questions, answer choices, and adjust new numerical values of them. Compliance analysis does not take much time by using our method. The cost of our model is low compared to the software tools in market.

There are several ISO 17799 compliance analysis software packages in market. Most of them perform surveys like our method. Although this software allows the changes in survey, they do not have the role based access control mechanisms. If the survey is performed by using web application, role based access-control mechanism is utilized. Also, using web technologies eases the tailoring activities.

The success of our method depends on the answers of surveyors. Accurately answered questions lead to accurate compliance results. Several actions play important role to improve accuracy. Firstly, role based access control help intensively on accuracy. Only related surveyors answer the dedicated questions. Secondly, special attention is paid while preparing answer choices and the weight values of questions (controls) and their answers. Thirdly, depending on the type of the organization, and the type of the processes within the organization, several clauses and the several questions in the clauses can be omitted. Fourthly, prior to each compliance check, surveyors should be orientated. All these actions should be performed to improve the accuracy of the surveys before starting any survey process.

Uncited references

McEvoy and Whitcombe, 2002; Tong et al., 2003; United States General Accounting Office (USGAO), 1999.

REFERENCES

British Standards Institution (BSI). Information security management systems – specification with guidance of use; 2002.
C&A Systems Security Limited. COBRA consultant products for Windows, evaluation & user guide; 2000.
Information Security Forum (ISF). The standard of good practice for information security; 2003.
Information Systems Audit and Control Association (ISACA). Certified information systems auditor review manual; 2004.
Karabacak B, Sogukpinar I. Information security risk analysis method. J Comput Secur 2005;24(2):147–59.
McEvoy N, Whitcombe A. Structured risk analysis. In: InfraSec; 2002. p. 88–103 [LNCS 2437].
National Institute of Standards and Technology (NIST). NIST special publication 800-26, security self-assessment guide for information technology systems; 2001.
National Institute of Standards and Technology (NIST). Risk management guide for information technology systems; 2001 [special publication 800-30].
Riskwatch, <http://www.riskwatch.com>; 2005.
Solms B, Solms R. Incremental information security certification. J Comput Secur 2001;20(4):308–10.
The International Organization for Standardization, The International Electrotechnical Commission (ISO/IEC). ISO/IEC 17799:2005: information technology – code of practice for information security management; 2005.
The International Organization for Standardization, The International Electrotechnical Commission (ISO). ISO/IEC 27001: 2005: information technology, security techniques, information security management systems, requirements; 2005.
The ISO 17799 Toolkit, <http://www.iso17799-made-easy.com>; 2005.
Tong CKS, et al. Implementation of ISO 17799 and BS7799 in picture archiving and communications system: local experience in implementation of BS7799 standard. In: International congress series 1256; 2003. p. 311–18.
United Kingdom Central Computer and Telecommunication Agency. CCTA risk analysis and management method, CRAMM user guide, issue 2.0; 2001.
United States General Accounting Office (USGAO). Information security risk assessment, <http://www.gao.gov/cgi-bin/getrpt?GAO/AIMD-00-33>; 1999.