An Attempt to Prevent Operational Incidents by Applying the SECI Model

Takeshi Okada
School of Knowledge Science, Japan Advanced Institute of Science and Technology
1-1 Asahidai, Nomi, Ishikawa 923-1292, Japan
t-okada@jaist.ac.jp

ABSTRACT

The purpose of this paper is to clarify the fact that, with some changes and innovations, the SECI model can function effectively as a means of reducing operational risk and preventing recurrence using groupware. When applying the SECI model to operational risk management, there are two basic problems. First, there is the possibility that the organization will not grasp the true cause and background of a problem if a real "*ba*" (*ba* is a Japanese word with no exact translation. It refers to a shared place or context for human interaction) is established for Socialization (where people develop an understanding of the basic situation of an incident) and Externalization (where they report the incident). Second, a lot of thought must be given to Combination. To resolve these problems, this paper proposes that real *ba* be changed to virtual *ba* based on groupware. This creates a non-judgmental atmosphere where information on incidents is regarded as an asset, and wisdom is accumulated. Operational risk is covered by Basel II (International Convergence of Capital Measurement and Capital Standards), and is attracting a great deal of attention, particularly among financial institutions. At present, there are no examples of using the SECI model, together with groupware, to prevent recurrence of operational incidents at financial institutions. This paper describes a new attempt to apply the SECI model.

Keywords: SECI model, *ba*, risk management, operational incident, groupware

1. INTRODUCTION

The Basel Committee on Banking Supervision gives the following definition: "Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk." [1] However, the view that "At present, there is no agreed upon universal definition of operational risk." [2] is considered to be valid, even today. Here, operational risk shall be tentatively defined as risk relating to business (clerical) processes.

Publicizing and sharing information about operational incidents is thought to be an effective way of reducing operational risk. However, there may be information or sensitive matters that persons involved in an incident do not want publicized. If the goal is reduction of risk and prevention of recurrence, not punishment, then what is the most appropriate method of public disclosure?

The SECI model [3] is often mentioned when talking about matters such as knowledge creation, development of good products and sophisticated business models. However, the model goes beyond this and has excellent potential as a model for reducing operational risk and preventing recurrence. To achieve this, however, will require some changes and innovations in the model.

2. OPERATIONAL RISK MANAGEMENT

2.1. The Operational Risk Management Situation

Operational risk is covered by Basel II (International Convergence of Capital Measurement and Capital Standards), and is attracting a great deal of attention, particularly among financial institutions. The following is a good description of the operational risk management situation at Japanese financial institutions: "All financial institutions in Japan are working to respond to the upcoming implementation of Basel II. The approach which each financial institution actually selects for operational risk management depends on many factors, including the size of the financial institution, its progressiveness, and the nature and complexity of its work." [4].

If, for example, we look at the disclosure documents of Japanese financial institutions concerning departments with jurisdiction over operational risk, there are two basic patterns: institutions where a permanent department has jurisdiction (i.e. a work supervision department or compliance department) and institutions where a cross-departmental organization such as a risk management committee has jurisdiction. In recent years, an increasing number of institutions have introduced a division of labor -- having one department dedicated to risk called the risk management department which is placed in charge of operational risk, market risk and

liquidity risk etc., and a compliance department which specifically handles legal risk. In this way, different approaches are being taken at the discretion of each company. There are also various techniques for evaluating and measuring operational risk including the Capital Asset Pricing Model, Monte Carlo Simulation, Control Self Assessment and Key Risk Indicators, but nothing has emerged which might be called the standard evaluation/analysis model for operational risk.

In Europe and the U.S., "full-scale efforts to manage operational risk have only appeared in the last 4-5 years" [5]. The situation can be described as follows: "Special mechanisms and processes have been developed to manage operational risk in recent years. However, these special mechanisms and processes are still under development, and the world's most progressive banks are working to implement more sound risk management by combining multiple qualitative and quantitative techniques as their system for measuring and evaluating operational risk" [4]. Also: "There were evident differences between the visited banks with regard to the scope of what is recognized as risk (i.e. whether the scope includes such matters as indirect losses and near misses) and with regard to matters such as measurement techniques and methods of capital allocation, but each bank was searching for a system optimal for their own situation, based on the their bank's own risk management policy" [5]. Thus, it is clear that a standard for operational risk management does not exist at the present.

On the other hand, the history of operational risk can be summarized as follows. This type of risk has previously existed, but even the term "operational risk" itself is comparatively new. The term first began to appear in Japanese journals in the latter half of the 1990s. Since 2000, the number of articles has increased, but one factor underlying this is thought to be the fact that operational risk has been clearly described in the 1999 Financial Services Agency Inspection Manual [6].

A big event in Europe was the "Framework for Internal Control Systems in Banking Organizations" [7] issued by the BIS Basel Committee in 1998, and a big event in the U.S. was "COSO I" [8] of the Treadway Commission. In the U.S., the provisions have become more radical, with the 2002 Sarbanes-Oxley Act stipulating that managers have a duty to report on the effectiveness of internal controls and providing strict penalties for violators, and with "COSO II" [9] integrating internal controls and risk management in 2004. In Japan, however, the term "operational risk" was not generally known until just a dozen or so years ago, and the associated phenomena were regarded simply as business process mistakes. The idea is to not regard business process mistakes as simple clerical mistakes, which will happen when they happen; rather such mistakes should be recognized as an important risk factor for corporations, and in the new Basel II framework, efforts are being made to manage this risk. That is the current situation of operational risk management among financial institutions.

2. 2. Two Categories of Operational Risk Management

In managing operational risk, it is important to predict the number of incidents or monetary losses which are likely to occur in the future based on incidents which have already occurred. It is also important to determine the cause of incidents, and formulate a plan for preventing them. If the number of incidents and monetary losses are calculated accurately, efforts must naturally be made to mitigate them if they are large. In recent years, the field of operational risk management has tended to focus on evaluation and measurement techniques, but this paper shall discuss how to reduce incident occurrence based on the SECI model.

3. THE SECI MODEL

3. 1. Overview of the SECI Model

The SECI model is a basic theory of knowledge management advocated by the Japanese scholar Ikujiro Nonaka. The theory concerns the process of knowledge creation, where conversions and transitions of knowledge occur between tacit and explicit knowledge, and those changes occur continuously in a spiral fashion. The model was developed by analyzing successful Japanese companies, and then formalizing the theory based on those results.

In the SECI model, knowledge creation is explained in terms of the following four processes. Socialization is the process that changes individual tacit knowledge into organizational tacit knowledge. Externalization is the process that changes tacit knowledge into explicit knowledge. Combination is the process where new knowledge is created by combining explicit knowledge. Internalization is the process that changes new explicit knowledge into tacit knowledge again at the body and behavior level. The concept of *ba* is expressed in the SECI model as the place where these processes progress -- i.e. “a place where individuals in an organization or community gather, a place where information is exchanged.” [10]. There are different kinds of *ba* corresponding respectively to each process: Originating

Ba, Dialoguing *Ba*, Systemizing *Ba*, and Exercising *Ba*.

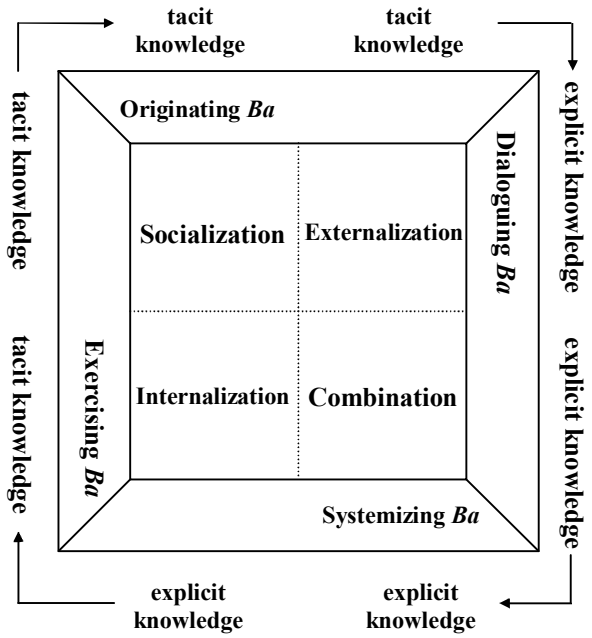

Figure 1. Knowledge spiral of the SECI Model

3. 2. Places where the SECI Model is Applied

The SECI Model is applied where a company produces things like products, technologies and services, and releases them to the market. For example, in Socialization, individuals find out the needs of customers and other information about them. In Externalization, the information possessed by an individual is expressed in language. In this way, it becomes possible to share individual knowledge as group knowledge. In Combination, various kinds of knowledge are combined and systematized, and the needs of customers become realized in the form of products. In Internalization, previous group knowledge penetrates once again to the bodily level as individual knowledge. Furthermore, feedback is provided from customers regarding products which have been released to the market and this connects with Socialization at the beginning. This process continues, repeating in a spiral fashion.

4. APPLICATION OF THE SECI MODEL TO OPERATIONAL RISK MANAGEMENT

4. 1. Effectiveness of the SECI Model for Operational Risk Management

It is encouraging that knowledge creation and other processes described by the SECI model have a forward-looking, positive image of the future. However, the SECI model is also applicable as a risk management model for operational incident prevention, failure response and recurrence prevention. This point is not often mentioned in connection with the SECI model -- perhaps because it gives a backward-looking impression, or an impression of a dark past.

Applying the SECI model to both knowledge creation (which has a positive image) and operational risk management (which has a somewhat negative image), improves corporate fitness and establishes a foundation for improvement. These two approaches are complementary. The favorable reputation of Japanese products was not achieved in a short time. In these times, when we frequently hear of “quality collapse”, the establishment of good business processes and a good reputation are just as important as producing a hit product. Even if a company builds a good reputation, it can quickly collapse due to incidents like leakage of personal data. Operational risk management is the lifeline of a company. Efforts must be made to prevent recurrence by applying the SECI model.

4. 2. Problems when Applying the SECI Model to Operational Risk Management

When applying the SECI model to operational risk management, there are two basic problems. First, there is the possibility that the organization will not grasp the true cause and background of a problem if a real “*Ba*” (*ba* is a Japanese word with no exact translation. It refers to a shared place or context for human interaction) is established for Socialization (where people develop an understanding of the basic situation of an incident) and Externalization (where they report the incident). People do not want to talk about failure. Second, a lot of thought must be given to Combination. Failure does not like to be exposed to the light of day. The purpose is not to blame the person involved in the incident.

To share incident information and prevent people from thinking “it's somebody else's problem”, it is necessary to use various approaches, such as: creating an atmosphere where people will not be blamed, fostering awareness that a knowledge base of information on incidents is an asset, explaining the background which affects people's feelings (i.e. the fact that the system is based on the SECI model), using facilitors, and identifying appropriate *ba*.

5. REAL *BA* OF THE SECI MODEL IN INCIDENT INVESTIGATION

5. 1. The Function of *Ba*

It is hard for a person involved in an incident to have positive feelings about it. The person is often overwhelmed with feelings such as denial, panic, anger, hostility, guilt, evasion and finger-pointing immediately after an incident occurs. Therefore, when interviewed about the cause and background of the incident, the person tends to have feelings like "You made me remember something I didn't want to" or "You're just pouring salt in the wound." Real *ba*, such as face-to-face or telephone comunication, makes the interviewee stubborn or aggressive, and this makes it hard for the interviewer to determine the true cause and background. This problem becomes even worse if an incident is publicly disclosed, and the person will find it even harder to tell the truth. The real *ba* of the SECI model does not work well here.

5. 2. Examples of the Reactions of an Involved Person to the Incident Investigation Process

The following is a classification of the feelings that hinder sharing in the real *ba* of the SECI model. Actual responses are given to illustrate each type.

－Denial :

When asked to submit an incident report, the person replies: "Maybe this was not an incident."

－Panic:

The person leaves a memo on his or her superior's desk: "I cannot come to the office because I made such an awful mistake."

－Anger (at the occurrence of the incident itself):

During the cause and background interview: "If I'm this busy, it's no suprise if a few mistakes happen!"

In response to the first report by telephone: "I've been doing this work for six years. This is the first time I've made a mistake like that in six years!"

－Hostility (at a specific person):

During the cause and background interview: "What's your authority to grill me about all these details?"

In response to the incident assessment report: "What are the grounds for this assessment? This report is a verbal assault!"

－Guilt:

During the cause and background interview; "I'm the cause. It's all my fault."

－Evasion/Finger-pointing:

"I think the incident which happened in that department is a more serious problem than this incident."

6. ESTABLISHING *BA* BY USING GROUPWARE

6. 1. From Real *Ba* to Virtual *Ba*

Originating *Ba* for Socialization and Dialoguing *Ba* for Externalization are basically real *ba* in the SECI model. But, as mentioned above, real places often become a hindrance when the SECI model is applied to risk management.

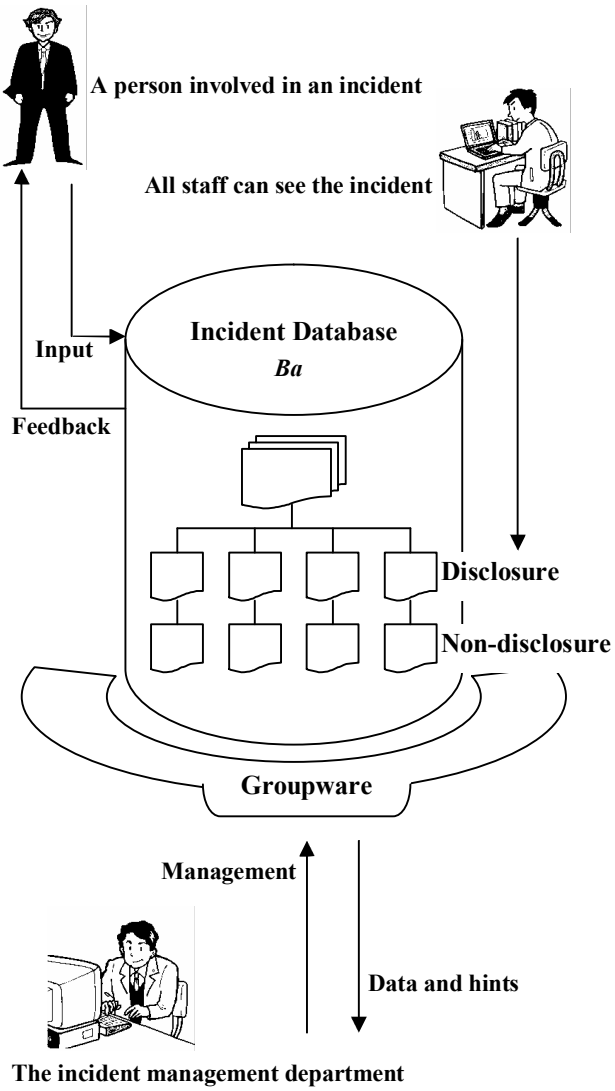

Figure 2. Incident Database

Therefore, the main thrust of this paper is an attempt to change the Originating *Ba* for Socialization and the Dialoguing *Ba* for Externalization from real *ba* to virtual *ba* by using groupware. This makes it possible to share and externalize the true cause and background when an incident occurs.

6. 2. Key Points for Incident Database Design

The following points are crucial to make it easy for people to express themselves.

- The database should provide chat-style information fields in addition to necessary fields such as the cause and the background. This will improve knowledge, and ensure an atmosphere where people are not blamed, and where the archive of incident cases is regarded as an asset.
- The database should have a "subsequent discussion" field to provide information such as "It was a terrible mistake but our reputation among customers was improved by taking honest action".
- Names of individuals should not be released in case of public disclosure.

Also, the following points are essential to make it easy for people to participate

- The database should have a field which anyone can add to with ideas on how to prevent recurrence.
- The database should employ content-related techniques, such as using interesting headlines.

6.3. Management of the Incident Database

The processing flow of this DB after an incident occurs is as follows.

Step 1. A person involved in an incident inputs a status report to the DB.

Step 2. The incident management department publicizes the incident on the DB (unless the information is not subject to disclosure).

Step 3. All staff can see the incident. Any reader who has an idea for preventing recurrence inputs this to the DB.

Step 4. The person involved in the incident can receive feedback on measures to prevent recurrence through the DB.

Step 5. If necessary, the person involved in the incident inputs material such as "subsequent discussion" or status after the incident.

Step 6. The incident management department obtains data and hints for preventing recurrence of operational incidents from the DB.

7. EFFORTS RELATING TO INCIDENTS

7. 1. Overview of actual incidents

Here, as an actual example, I shall discuss proofreading errors in printed material, which tend to be thought of as business process (clerical) mistakes. At the insurance company where I work, there were over 10 cases last year where printed materials were released outside the company with misprints. These are products offered by financial institutions -- such as banks, securities companies and insurance companies -- and they are not material objects, but rather intangibles like agreements and contracts. In almost all cases, these are expressed in the form of printed material. If, for example, even a single character in printed material constitutes a fatal error, this may result in a need to dispose of the entire inventory and reprint it, and monetary losses can become tens of millions of yen. Also, there are cases where significant damage can be inflicted on a company's reputation or customer trust. The Inspection Manual of the Japanese Financial Services Agency clearly states: "Are managers aware of the importance of reducing operational risk, and are they taking proper measures by ensuring that the persons in charge of each department know the importance of reducing operational risk, and the measures for reducing it?" [6]

As a phenomenon, errors of this type are just a matter of mistyping a character, but from the standpoint of risk management, there is a large risk which cannot be categorized as a simple clerical mistake. Work processes like this, which seem at first glance to be clerical mistakes but actually involve a large risk, must be implemented by considering how they should be improved.

7. 2. "Socialization" in Responding to Incidents

The urgent circumstances of an incident are the Originating *Ba* for the involved or relevant persons, and give the flavor of the Socialization process. In contrast with the creation of products, technology and services, this Socialization has a bitter flavor which is hard to put into words. That bitterness serves as the basis for the involved person to grasp the essence of the incident by understanding the overall view of the situation through adequate experience of the bitterness in an atmosphere where the person is not asked questions in an interview or attacked by other persons, and simply inputs the objective facts into the database.

Of course, there is no need to stick with virtual *ba* in the case of an emergency, but it is important to have a

consensus where, basically, response progresses in a straightforward fashion in the virtual *ba*.

The very existence of the incident DB is thought to be effective for the Socialization process.

7. 3. "Externalization" in Responding to Incidents

The involved person may respond emotionally in the incident investigation process. In many cases, resistance appears and impedes progress of the incident investigation -- i.e. denial “Maybe this was not an incident”, or anger “If I'm this busy, it's no suprise if a few mistakes happen!” or “I've been doing this work for six years. This is the first time I've made a mistake like that in six years!”, or guilt “I'm the cause. It's all my fault.”

The emotions of an involved person who caused an incident are delicate, and the person is likely to be nervous about interviews with people, particularly those in the risk management department. The interview can fall into a situation where it is difficult to find out about the incident situation, history, cause and expected impacts etc.

In terms of incident DB management, this is the Step1 process where the person involved in the incident inputs a situation report to the DB. If the information is input to the DB, it is expected that the person involved will not have the emotional feeling of resistance toward the interviewer, and will reflect on the incident by his or herself, with a certain degree of coolness and calmness.

7. 4. "Combination" in Responding to Incidents

In the Combination process, communication was conducted between the relevant departments (including the department to which the involved person belongs) and specialists outside the company. However, printed material is prepared in many departments, and communication with all departments was impossible. Also, there are "hidden specialists" and "idea men" inside the company. There is also a possibility that the wisdom of such people has not been fully exploited.

In terms of incident DB management, the processes here are Step2 where the incident management department publicizes the pertinent incident on the DB (unless it is not subject to disclosure) and Step3 where all staff can see the incident and any reader who has an idea for preventing recurrence inputs this to the DB. If the DB was being used, a better resolution method may have been discovered.

There are various conceivable approaches for reducing proofreading errors in printed material, including cognitive science based approaches of reducing human error, management and quality control based approaches such as adopting "six sigma", IT solutions involving use of proofreading tools, and BPR solutions involving assessment of the proofreading process. The efforts described here fall under the heading of BPR solutions.

More specifically, this involved providing continuous proofreading training, clear indication of a standard proofreading process, monitoring of proofreading work, and on-site inspection of outside contractors.

At ordinary companies which are not printing companies, proofreading of printed material is often done by persons who have not acquired basic knowledge or received the proper training. However, most publicly announced proofreading training is for specialists, and does not really suit the work of persons in charge of printed material at ordinary companies. Thus, a curriculum was developed jointly with a publishing/printing technical school. The school offers a two-day intensive course every six months, and a commuter course held once a week for two months, and it was decided that the commuter course would accept students from other ordinary companies. The course is designed to combine theoretical learning with practical exercises, and printed material used in actual work is used for exercise materials, incorporating misprints, and otherwise making the training close to the actual proofreading work conducted by persons in charge of printed material at ordinary companies.

Next, a standard proofreading process was clearly indicated. The basic process of proofreading work is: manuscript checking (checking the manuscript against the camera-ready master), red mark checking (checking the galley proof against the corrected camera-ready master), and proofreading of the master alone (without checking against the manuscript). In addition, it was decided to conduct 8 checking steps, with a minimum of two people, by combining the creators of the materials and the persons in charge.

Furthermore, in order to monitor that printed matter is being created through a standard proofreading process, use of a "Proofreading Work Monitoring Sheet" was initiated. From the user perspective, this plays the role of a check sheet for determining whether proofreading work is being done properly, and is designed for recording the number of misprints, problems with content and whether there were any items requiring checking in each process. The cooperation of the

printing company was also enlisted, and a system was adopted wherein the entire printed material proofreading process can be seen from a neutral standpoint by the part of the organization outside the department of the involved person.

The understanding of the persons in charge of printed material creation and proofreading was also promoted by creating a "Proofreading Work Monitoring Sheet Entry Manual". This Manual describes not only the method of filling out the sheet, but also things like the importance of proofreading, explanation of basic terminology, and Q&A.

From a third party viewpoint, work done by outside contractors is no different from our company's own work, and our company is responsible for managing the work quality. For that reason, we conducted an on-site inspection of outside contractors.

A "Site Inspection Check Sheet" was created, and checking was done to determine whether quality assurance equivalent to that at our own company was being done at outside contractors.

7. 5. "Internalization" in Responding to Incidents

In taking the response described above, "Internalization" should have occurred, and the results were as follows.

The number of misprints (i.e. the number of printed materials released outside the company with uncorrected misprints) which occurred in the year prior to the initiation of efforts (2004, January to December) was 11. On the other hand, the number of misprints which occurred after initiating efforts (2005, January to September) was 3, and converting to years, this would be 4 (this excludes printed material whose proofreading work was done only by persons who have not undergone the proofreading training). The number of misprints was reduced to a little less than 1/3, so even these efforts appear to have had an effect to a certain degree

8. CONCLUSION

At present, no standards exist for operational risk management, and various approaches are being tried at the discretion of each company. An incident database is currently being designed at my workplace.

So far, there have been no examples of applying the SECI model, based on groupware, to preventing the recurrence of operational incidents at financial institutions. This paper is a new attempt at applying the SECI model.

An incident database is a variation of a knowledge database. Therefore, this DB cannot work just by introducing a system based on methodology. People must have lively communication in the *ba*. “Barbara Seidel, CIO of the temp company Russell Reynolds Associates, puts it this way: “First, the knowledge management system must be designed so that anyone can derive significant benefit from it immediately. Efforts must be made to appeal to the "five senses" of employees in determining what specific advantages the system should provide.” .” [11] This interview expresses well the importance of motivating DB users. I expect this incident DB to be useful for preventing operational incidents through lively communication between people.

REFERENCES

[1] Basel Committee on Banking Supervision, “International Convergence of Capital Measurement and Capital Standards”, Bank for International Settlements, 2004

[2] Basel Committee on Banking Supervision, “Operational Risk Management”, Bank for International Settlements, 1998

[3] I.Nonaka, H.Takeuchi, “The Knowledge-Creating Company”, Oxford University Press, 1995

[4] Integrated Risk Management Study Group “‘Togoteki Risuku Kanri Kenkyukai (Dai 4 bu)' Hokokusho ~ Fukusu Shuho wo Kumiawaseta Operational Risk Kanri no Jissen~ ('Integrated Risk Management Study Group (Dept. 4)' Report -- Practical Operational Risk Management Combining Multiple Techniques)”, Center for Financial Industry Information Systems, 2005 (In Japanese)

[5] Center for Financial Industry Information Systems, Investigation Department, “Operational Risk Kanri ni kansuru Kaigai Chosa Hokoku (Report on Overseas Survey of Operational Risk Management)”, Financial Information Systems, #277, Center for Financial Industry Information Systems, 2005 (In Japanese)

[6] Financial Services Agency (Japan), “Hoken Kensa Manual (Hokengaisha ni kakawaru Kensa Manual) (Insurance Inspection Manual (Inspection Manual for Insurance Companies))”, 2004 (In Japanese)

[7] Basel Committee on Banking Supervision, “Framework for Internal Control Systems in Banking Organisations”, Bank for International Settlements, 1998

[8] The Committee of Sponsoring Organization of the Treadway Commission, “Internal Control – Integrated Framework”, 1992.
[9] The Committee of Sponsoring Organization of the Treadway Commission, “Enterprise Risk Management – Integrated Framework”, 2004
[10] I.Nonaka, N.Konno, “Chishiki-keiei no susume (Recommendations for Knowledge Management)”, Chikuma syobou, 1999 (In Japanese)
[11] “Jissen. Knowledge management seikou riron (Practical Implementation: Knowledge Management Success Theory)”, CIO, Vol.52, IDG Japan, 2004 (In Japanese)