Information Systems Reliability Assurance by Financial Auditing Approach

Takashi SAITO*

Certified Public Accountants（CPAs）have long striven to evaluate the reliability of the information systems of the corporations that they are auditing, in order to express opinions concerning the fairness of financial statements from the standpoint of an independent auditor. Now, "Information Systems Reliability Assurance" services by CPAs are offered as a business in a category separate from that of financial audit. Assurance services on the reliability of information systems provide users with "assurance that an information system has been designed and operated to produce reliable information."

In previously published papers in some proceedings or journals, the author had already studied the concepts of assurance services on the reliability of information systems by CPAs who were not experts on information system development and operation, and clarified the concepts of the internal controls necessary for building reliable information systems. Moreover, through these concepts, the author had made proposals to the person in charge of information system development and operation concerning focus points when managing his or her job responsibility.

However, discussion on the logical basis for these concepts was not sufficient. Therefore, this paper has reconsidered the focus points proposed previously from the viewpoint of a "financial auditing approach."

Keywords: information systems reliability assurance, financial auditing approach, internal controls, audit trail, control environment

会計監査アプローチによる情報システムの信頼性の保証

斎藤　隆*

公認会計士は従来より、会計監査人としての立場から財務諸表の適正性について意見表明するために、被監査企業の情報システムの信頼性を的確に評価することに努めてきた。そして、今、会計監査とは別の業務範疇で、公認会計士による「情報システムの信頼性に関する保証業務」がビジネスとして実際に提供されている。情報システムの信頼性に関する保証業務とは、情報システムのユーザに「情報システムが信頼できる情報を提供するように設計され運用されていることについての保証を提供すること」である。

筆者は既発表論文にて、情報システム開発または運用業務の専門家ではない公認会計士による情報システムの保証業務の概念を検討し、信頼できる情報システムを構築するために必要な内部統制の考え方を明らかにした。そして、その考え方を通じて、情報システム開発または運用担当者へ担当業務を管理する際の着眼点を提言した。

しかしながら、既発表論文ではその論理的根拠の考察が十分ではなかった。それゆえ、本稿は既発表論文にて提言した着眼点を「会計監査アプローチ」という観点から再考したものである。

キーワード：情報システムの信頼性、会計監査アプローチ、内部統制、監査証跡、統制環境

*東京情報大学　総合情報学部　情報ビジネス学科
Tokyo University of Information Sciences, Faculty of Informatics,Department of Business and Information

2011年12月19日受理

1. Introduction

In the United States, from the end of the 1990s, as the scope of work performed by Certified Public Accountants (CPAs) expanded, "the business of providing assurances on the reliability of information systems" by CPAs was the subject of active debate [1]. Some specific products were WebTrust and SysTrust which were developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). WebTrust and SysTrust have been united and are now called Trust Services, which are offered as a business. Assurance services on the reliability of information systems provide users with "assurance that an information system has been designed and is in operation to produce reliable information."

In previously published papers [2] in some proceedings or journals, the author had already studied the concepts of these assurance services on the reliability of information systems by CPAs who were not experts on information system development and operation, and clarified the concepts of the internal controls necessary for building reliable information systems. Moreover, through these concepts, the author had made proposals to the person in charge of information system development and operation ("IS manager") concerning focus points when managing his or her job responsibility.

However, discussion on the logical basis for these concepts was not sufficient. Therefore, this paper has reconsidered the focus points proposed previously from the viewpoint of a "financial auditing approach."

2. WebTrust

2. 1 Overview of WebTrust

WebTrust is one of Web assurance services developed jointly by AICPA and CICA for Business to Consumer ("BtoC") electronic commerce. This Web assurance service is a professional service in which an independent auditor receives a fee from a business that conducts BtoC electronic commerce ("EC businesses") and provides assurances on the reliability of the BtoC electronic commerce conducted by the EC business.

The official name of WebTrust is "AICPA/CICA WebTrust^{SM} Principles and Criteria for Business-to-Consumer Electronic Commerce." Version 1.0 was announced in December 1997.

2. 2 The Business Potential of WebTrust

Why do EC businesses go so far as to pay to obtain assurance on the reliability of the BtoC electronic commerce that they themselves operate ? It is to gain the trust of the customer in the BtoC electronic commerce in question. Even if a customer is aware of the convenience of BtoC electronic commerce, there are two concerns that hold back more active use. One concern is the fact that since BtoC electronic commerce is not face-to-face commerce, obtaining the product ordered and settlement of payment are not certain. Another concern is the fact that since the transaction takes place over the Internet, which does not provide sufficient information security, personal or private information will be put to improper use. Web assurance services are intended to eliminate these types of customer concerns, and the result can be a major contribution to the expansion of business for the EC business. In fact, it is said that the first EC business that introduced WebTrust produced a 50% increase in electronic commerce transactions[1].

It is anticipated that BtoC electronic commerce will grow rapidly in the future, and the need for Web assurance services is also likely to increase in tandem. Amidst these developments, since WebTrust is conducted by CPAs, who have already obtained social recognition of their independence, it has considerable business potential.

2. 3 Framework and Features of Assurance

WebTrust provides Web assurance services within

the framework of financial audit. The American Accounting Association defines auditing in the following manner[2]:

"Auditing is a systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions and events to ascertain the degree of correspondence between those assertions and established criteria and communicating the results to interested users." (emphasis added)

The features of assurance methods of WebTrust are those underlined portions above. "Assertions" are the assertions made by an EC business to the effect that the BtoC electronic commerce that the EC business operates can be trusted. The assertions are the subject of the assurance. "Established criteria" are the WebTrust principles established by the AICPA and CICA (see section 2.4 below); they serve as the measures for the assurance provider. The assurance provider evaluates the "degree of correspondence" between the "assertions" and the "criteria." And if the assertions have agreed with the criteria for a certain period, then the assurance provider "communicates" to the EC business's customers that the concerned BtoC electronic commerce can be trusted through the use of an assurance seal (WebTrust Seal) posted on its Web site in question.

For your reference, in case of financial audit, "assertions" are the financial statements, "established criteria" are the Generally Accepted Accounting Principles, and an independent auditor "communicates" through the Independent Auditor's Report.

2. 4 Assurance Evaluation Points

The three principles listed below are the evaluation points used for assurance under WebTrust.

Principle 1: The EC business discloses its business practices for BtoC electronic commerce transactions and executes transactions in accordance with its disclosed business practices (Business Practices Disclosure).

Principle 2: The EC business maintains effective controls to provide reasonable assurance that customers' transactions using BtoC electronic commerce are completed and billed as agreed (Transaction Integrity).

Principle 3: The EC business maintains effective controls to provide reasonable assurance that private customer information obtained as a result of BtoC electronic commerce is protected from uses not related to the EC business's business (Information Protection).

And there are a total of 32 individual criteria to be used as specific measures for each principle. In addition, some internal controls for three types of industry are illustrated for each of the 32 criteria[3].

2. 5 Overview of Work by the Assurance Provider

An overview of the work performed by the assurance provider is done in four steps as follows. These four steps are the same approach as financial auditing, because of providing Web assurance services within the framework of financial audit, as shown in section 2.3 above.

① Consideration of the propriety of concluding a WebTrust engagement

It is necessary for the assurance provider to identify the features of the subject of the assurance, to evaluate his or her own ability to perform the engagement, and to investigate thoroughly the risks entailed following the provision of assurance in the responsibility as an assurance provider. The most important point is evaluation of the integrity of the EC business.

② Understanding of the EC business's internal controls from a perspective of the three principles (see section 2.4 above) and the procedures of maintaining them by the EC business

For the purpose, a questionnaire more than 10 pages in length has been prepared.

③ Obtaining and evaluating evidence that attests to compliance with the WebTrust principles

This is the most important key step of the four. The reason is discussed in section 5.1 below.

Evaluating compliance means evaluating the effectiveness of internal controls. The effectiveness of internal controls is determined by two points. One point is "design conditions," i.e., whether internal controls exist to achieve the control objectives. Another point is "operational conditions," i.e., whether the internal controls have been complied with. The work of making such evaluations is fundamentally the same as the work involved in evaluating the internal controls of information systems for financial audit[4].

In the case of WebTrust, a minimum of three months of compliance must be established.

④ Expressing of an Unqualified Opinion and Granting Approval for Use of the WebTrust Seal

Unqualified means that the EC business complies with the WebTrust principles without a single exception. Only in this case can assurance be provided and the WebTrust seal, which is the symbol of the assurance, be granted. Customers who access the Web site in question will see that the seal is posted. It is intended to allow customers to feel they can shop with a sense of security.

In order to prevent fraudulent use of the seal, VeriSign[5] has been selected as the WebTrust seal manager, and the seal is issued by VeriSign. As a result, it is necessary for EC businesses to obtain the Class 3 Certificate[6] from VeriSign in advance. When customers click on the WebTrust Seal, the EC business's assertions, the unqualified opinion of the assurance provider, and a link to VeriSign are displayed.

2. 6 Term of Validity of Assurance Certificates

The maximum period of validity of an assurance is 90 days. On the expiration date of the period of validity, VeriSign deletes the WebTrust Seal from the EC business's Web site. Consequently, if the EC business wishes to continue the assurance, it must request that the work of attesting compliance with the WebTrust principles be performed every 90 days. The seal may also be deleted at the instruction of the assurance provider even before the expiration of the period of validity.

2. 7 Assurance Provider Qualifications

The qualifications as an assurance provider are sufficient skill and experience, undergoing training held by AICPA/CICA for providing assurance services, and obtaining a license from the AICPA/CICA.

3. SysTrust

3. 1 Overview of SysTrust

Like WebTrust, SysTrust is a professional service, developed jointly by the AICPA and CICA, for assuring the reliability of information systems. Its official name is "AICPA/CICA SysTrust$^{SM/TM}$ Principles and Criteria for Systems Reliability." Version 1.0 was announced in December 1999.

This service issues an attestation report on whether management, the owner of the information system in question, maintained effective internal controls over its system to enable the system to function reliably.

3. 2 Assurance Evaluation Points

SysTrust defines that the information system typically is organized to transform data inputs into information outputs to achieve a specified objective. It consists of five key components: infrastructure (facilities, equipment and networks), software (systems, applications and utilities), people (developers, operators, users and managers), procedures (automated and manual) and data (transaction streams, files, databases and tables).

Also, a reliable information system is one that is capable of operating without material error, fault, or failure during a specified period in a specified environment. When an information system meets the four principles listed below, it is concluded that an information system is reliable.

Principle 1: The system is available for operation and use at times set forth in service level statements or agreements（Availability）.

Principle 2: The system is protected against unauthorized physical and logical access（Security）.

Principle 3: System processing is complete, accurate, timely and authorized（Integrity）.

Principle 4: The system can be updated when required in a manner that continues to provide for system availability, security, and integrity（Maintainability）.

Also, as is the case with WebTrust, a total of 58 individual criteria have been established for use as measures for specific evaluation of the four principles. In addition, for each of the 58 criteria, averages of four internal controls are illustrated[7].

3. 3 Overview of Work by the Assurance Provider

The process for providing assurance is similar to that used in the case of WebTrust（see section 2.5 above）. Unlike WebTrust, however, qualified opinion can be issued when the system is in compliance except for certain exceptions.

4. Trust Services

4. 1 Overview of Trust Services

The Trust Services[8] are assurance services designed for e-commerce-based systems and a wide variety of IT-based systems. From a viewpoint of the "continuous reliability chain", the AICPA/CICA integrated both the WebTrust version 3.0 and SysTrust version 2.0 into the Trust Services in April 2003. The newest version was announced in September 2009. Its official name is "Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy."

The accountant association of each country concludes the license agreement on Trust service with AICPA/CICA. Trust Services are already being provided on a commercial basis[9]. The Japanese Institute of Certified Public Accountants（JICPA）has also concluded a license agreement as of December 1, 2003[10].

4. 2 Assurance Evaluation Points

The following five principles have been used in the engagement of Trust Services.

Principle 1: The system is protected against unauthorized access, both physical and logical（Security）.

Principle 2: The system is available for operation and use as committed or agreed（Availability）.

Principle 3: System processing is complete, accurate, timely, and authorized（Processing Integrity）.

Principle 4: Information designated as confidential is protected as committed or agreed（Confidentiality）.

Principle 5: Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice（Privacy）.

In May 2006, AICPA/CICA separated the Privacy principle and established Generally Accepted Privacy Principles（GAPP）independently in order to assist management in creating an effective privacy program that addresses their privacy obligations, risks, and business opportunities. GAPP consists of 10 principles and 68 criteria[11]. Four principles excluding Privacy principle are organized into four broad areas, i.e., Policies, Communications, Procedures and Monitoring for each principle. In addition, a total of 117 criteria have been established for the four principles and a total of 671 internal controls are illustrated.

5. Discussions

5. 1 Financial Auditing Approach

The financial auditing approach nowadays is based on the Risk Approach. Risk Approach is the approach that concentrates auditing resources, auditors and their working hours mainly, on identifying and assessing risks of material misstatement. The risk of material misstatement refers to the risk that the financial statements are not presented fairly in accordance with the Generally Accepted Accounting Principles. It

consists of inherent risk and control risk. Inherent risk can be categorized as the susceptibility to a material misstatement in the absence of related internal controls. Therefore, it is necessary to design and operate appropriate internal controls if an inherent risk exists. Control risk is the risk that an inherent risk will not be prevented or detected in a timely manner by internal controls. If the auditor has missed recognizing that a control risk exists, it has caused the Audit Failure for the auditor. Audit Failure means that the auditor expresses an unqualified opinion although the financial statements are materially misstated. Therefore, audit objectives often focus on substantiating that internal controls exist to minimize inherent risks.

This is the reason why the most important key step for the assurance provider is obtaining and evaluating evidence that attests to the compliance with the principles of WebTrust, SysTrust or Trust Services, and that evaluating compliance means evaluating the effectiveness of internal controls, as stated in point ③ of section 2.5 above.

5. 2 Framework for Managing Reliable Information System Development and Operations

Changing the viewpoint from the position of assuring to the position of being assured, in order to build reliable information systems that satisfy the concepts of WebTrust, SysTrust or Trust Services, I think that it is necessary for the IS manager to understand his or her job responsibility as seen in a framework shown in Figure 1 and adhering to three focus points as follows.

① Establishing and Complying with the Internal Controls

What WebTrust, SysTrust or Trust Services assures is not each individual BtoC electronic commerce transaction or the information system itself, but the effectiveness of the internal controls on the operating environment. The assurance provided by WebTrust, SysTrust or Trust Services is based on the premise that if the internal controls necessary for achieving reliability are designed and operated effectively, then the BtoC electronic commerce or the information system that is subject to those internal controls will be operated reliably.

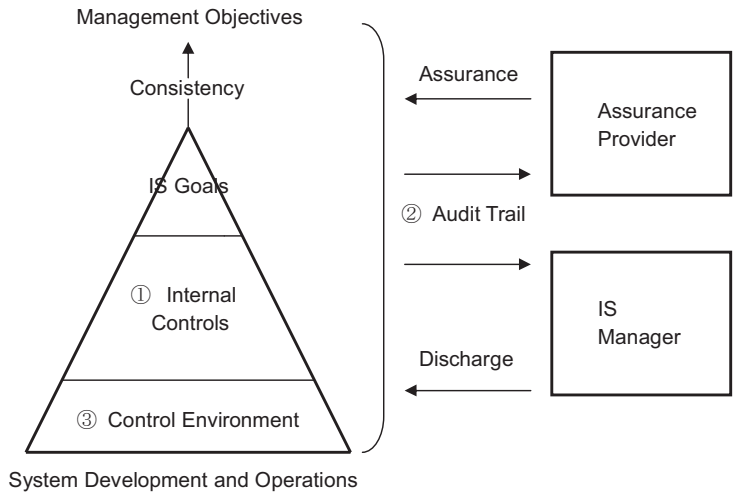

Figure 1: Framework for Managing Reliable Information System Development and Operations, Prepared by author

Internal controls, to put it in an extreme way, are structures intended to allow the convergence of activities from members within an organization that serves as a consistent cooperative body toward the realization of management objectives. Specifically, they are rules. There can be no information system development and operation sites without rules. However, there will likely be no disagreement that there are cases in which the development or operational objectives have not been met because of the inappropriateness of the rules. Everything starts with re-establishing rules based on the current status of practice and complying with those rules.

From the position of an IS manager, a self-assessment, to determine to what degree the four principles established for Trust Services and the many specific examples of criteria and internal controls for each principle are satisfied, may lead to the discovery of weaknesses in his or her managing information system development and operation.

② Securing of the Audit Trail

Cardinal work as an assurance provider is to obtain evidence that attests how effectively the internal controls over the subject information system have functioned, and to evaluate the evidence precisely. Then, the evidence in question is the only one that supports the assurance that is provided.

Evidence can be divided into two types when it pays attention to the instant when it is generated. One type is the evidence generated when an assurance provider obtains it. This is the evidence generated after the internal controls have functioned（"after the fact"）. Typically, it is the answer that an assurance provider can get from inquiring with an IS manager. Another type is the evidence generated in the process where business is carried out by the organization. This is the evidence generated equally when internal controls have functioned. To put it concretely, it is documents logging in the process and the operational circumstance of the subject information system, such as temporary files or log information. It is a so-called an audit trail.

Such documents may be unnecessary for an IS manager if products are complete. However, it is difficult for the assurance provider to conduct examination work effectively if an audit trail is not secured. The reason is that an assurance provider's work is usually conducted after the fact and the competence necessary for admissible evidence is weak only with the former type of evidence. Therefore, when internal controls are designed, it is necessary to build in a mechanism that documents operational conditions for securing an audit trail, too.

Well, it is necessary to secure an audit trail not only for the assurance provider but also for an IS manager. By using an audit trail, I think that an IS manager can be more assertive toward management that he or she has fulfilled his or her job responsibility in managing system development and operations because internal controls have functioned effectively.

③ Establishing a Control Environment

The internal controls for which WebTrust, SysTrust or Trust Services provides an assurance as to effectiveness are based on the previous status of matters. The assurance provided by WebTrust, SysTrust or Trust Services is based on the premise that since the internal controls were functioning effectively in the immediately preceding three months, the internal controls will continue to function effectively in the present and the next three months. The basis for this premise is the existence and sufficient functioning of an effective control environment.

The control environment refers to the management environment within an organization that has an effect on the design and operation of internal controls, such as the integrity of management or the characteristics of control specific to the organization. In other words, no matter how good the internal controls（the assurance provider can provide an assurance as to this fact）, if the members of the organization including management have a weak awareness of the importance of the role

of internal controls, then it will be difficult for those internal controls to continue functioning effectively in the future. As a result, efforts to establish and maintain an effective control environment are also necessary.

6. Concluding remarks

This paper has pointed out two points about the work performed by the assurance provider. One point is that the most important key step is centered on evaluating the design and operation of internal controls necessary for securing the reliability of the information system. Another point is that the logical basis is the Risk Approach which the financial auditing approach nowadays is based on. And through these two points, changing the viewpoint from the position of assuring to the position of being assured, this paper has made proposals for a framework and three specific requirements for managing reliable information system development and operations to the IS manager.

However, some important problems remain which are not discussed sufficiently in this paper. The main problem is how to protect the right to privacy from the viewpoint of GAPP, Generally Accepted Privacy Principles, which has separated from Trust services principles and has become independent. It will be discussed in the near future.

Acknowledgements

The author wishes to give two anonymous referees his sincere appreciation and acknowledgement for their valuable comments and suggestions on this paper.

【Notes】

1） See below for main products.
- AICPA: *Report of the Special Committee on Assurance Services*, AICPA, 1997.
- CICA: *Standards for Assurance Engagements*, CICA, 1997.
- International Federation of Accountants (IFAC): *Reporting on the Credibility of Information*, IFAC, 1997.

2） See below for main paper.
Saito, Takashi: "Information Systems Reliability Assurance by Certified Public Accountants", *Studies on Social Environments*, No. 3, Association for Social Environment Studies, January 2011.

3） We cannot get the original WebTrust Principles (including criteria and illustrated internal controls) from the official website of AICPA or CICA, because WebTrust had integrated into the Trust Services. For your reference, a Japanese translation of WebTrust version 1.1 has been published below.
Saito, Takashi: "Translation WebTrust℠ Principles and Criteria for Business-to-Consumer Electronic Commerce Version 1.1", *Management Information Science*, Vol. 12, Tokyo University of Information Sciences, June 2000.

4） See below for additional details.
Saito, Takashi: "The Systems Audit in the Financial Statements Audit by CPAs", *Journal of Systems Audits*, Vol. 7, No. 1, The Japan Society for Systems Audits, October 1993.

5） VeriSign, Inc. (http://www.verisign.com) is the third-party authorization that was established in 1995 and issues a digital certificate to conduct secure communications and transactions over the Internet.

6） Classes are categories of reliability standards for electronic commerce. VeriSign currently provides three types of certification service. Class 3 is the highest level certificate.
See below for more additional details.
"Certification Practice Statement",
http://www.verisign.com/repository/CPS/index.html
(as of October 10, 2011)

7）We cannot get the original SysTrust Principles (including criteria and illustrated internal controls) from the official website of AICPA or CICA, because SysTrust had integrated into the Trust Services. For your reference, a Japanese translation of SysTrust version 1.0 has been published below.
Saito, Takashi: "Translation SysTrust™ Principles and Criteria for Systems Reliability Version 1.0", *Journal of Tokyo University of Information Sciences*, Vol. 4, No. 2・3, Tokyo University of Information Sciences, March 2001.

8） See paper 2) listed above for additional details.

9） Currently, qualified practitioners are working at 69 accounting firms by 19 nations.
http://www.webtrust.org/

（as of October 10, 2011）

10）For example, JICPA creates a unique pamphlet.
http://www.hp.jicpa.or.jp/ippan/trust/index.html
（as of October 10, 2011）

11）JICPA has translated GAPP into Japanese.
http://www.hp.jicpa.or.jp/specialized_field/files/01217-004025.pdf
（as of October 10, 2011）

【References】

［1］Koreto, Richard J.: "A WebTrust Experience", *Journal of Accountancy*, Vol. 186, No. 4, The American Institute of Certified Public Accountants, October 1998.

［2］American Accounting Association: *A Statement of Basic Auditing Concepts*, American Accounting Association, 1973.
ISBN: 0865390185.