정보시스템 보안을 위한 위험분석활동과 내부통제평가와의 비교

조 성 백* · 김 귀 남*

요 약

위험분석과 내부통제평가는 조직 내 자산을 보호하기 위한 여러 보안관리 활동들 중 핵심적인 사항이다. 위험분석은 보호가 필요한 영역을 식별하는데 사용되는 활동인 반면, 내부통제평가는 현재의 내부통제시스템이 자산보호에 있어 만족할 수준인지를 확인하는데 사용되는 활동이다. 위험분석은 일반적으로 비인가된 사람으로부터의 비인가된 접근에 그 초점을 두고 있으며 인가된 사람으로부터의 잠재위협에는 상대적으로 적은 관심만을 가졌다. 부정행위에 대한 관심이 증가하는 현 상황에서는, 이들 위협들 또한 적절히 다루어져야 한다. 본 논문은 이 두 가지 활동을 비교하고 그 차이점을 논하는 것을 목적으로 한다.

Comparison of IT Security Risk Analysis and Internal Control Evaluation

Sungbaek Cho* · Kuinam J. Kim*

ABSTRACT

Risk analysis and internal control evaluation are key security management activities for securing organizational assets. Risk analysis is used to identify areas that need safeguarding while internal control evaluation is used to check whether the current control system is effective with a reasonable degree of assurance. Risk analysis usually focuses on unauthorised activities of unauthorised people and has not paid much attention to threats that could be committed by authorized users. As attention to fraud increases, these threats should be appropriately treated within organizations. This paper compares the difference between these two approaches.

* 경기대학교 정보보호기술공학과

1. Introduction

Various management techniques and efforts are made to secure organizational assets. These include risk analysis/management and internal control evaluation/audit. While the latter is closely related to the traditional accounting domain that focuses on completeness and accuracy of data/information [8], the former is rooted in the mechanical engineering school of thought [2]. These days information technology is an essential part of an organization's daily business operations, and the distinction of which control/safeguard belongs to which domain is meaningless. However, the major difference between them should be addressed. Usually, internal control evaluation is concerned about dynamics, that is, the actions and relationships within the business process [1]. In contrast, risk analysis focuses on the static nature of the system or business process in that it first identifies a list of assets involved in the system/process and then assesses the risks associated with each asset. In other words, internal control evaluation includes in-depth analysis of business processes and supporting tasks/activities, whereas risk analysis includes in-depth analysis of physical and logical components of a system and related risks.

One important aspect of internal control evaluation is that it examines the adequacy of the current control system. It enables in depth security analysis from the viewpoint of procedures and operations performed by employees. According to the CSI/FBI computer crime and security survey [7], the respondents were very worried about attacks by disgruntled employees. Moreover, among the various types of attacks examined, financial fraud resulted in the second largest average loss ; the largest was from theft of proprietary information. In order to discover and prevent deliberate actions by internal employees, an understanding of how systems will be used by them is essential [9]. Therefore, a view of the system from the perspective of internal control evaluation should be considered as a complement to the risk analysis view of system.

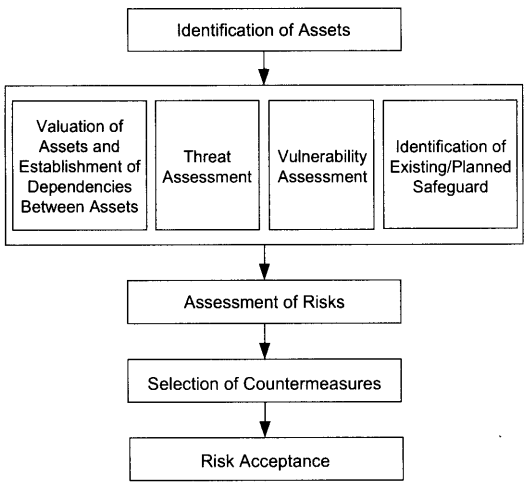
2. Risk Analysis Approach

Risk analysis is a process of identifying risks, determining their magnitude, and identifying areas that require safeguards [10]. The primary reason for conducting risk analysis (as an essential part of risk management) is to identify and assess potential risks in terms of their likelihood and business impacts and provide cost-effective safeguards, ensuring that assets in the organization are protected at a reasonable level of protection.

2.1 Risk Analysis and Management

(Figure 1) shows the general risk management framework (including risk analysis) in GMITS (ISO/IEC Guideline for Management of IT Security)-Part3 [10]. Strictly speaking, this framework represents detailed risk analysis and management, which includes in-depth analysis of asset, threat and vulnerability. Whenever we mention risk analysis and management in this paper, we are assuming that it refers to detailed analysis/management such as CRAMM (UK CCTA Risk Analysis and Management Meth-

odology) [6], one of the most prominent and comprehensive risk analysis and management methodologies.



(Figure 1) Risk Management Framework

As shown in (Figure 1), risk analysis starts from identifying all assets of the system within a review boundary. Then, the asset values which represent the importance of assets to the organization are to be assigned. These values can be expressed in terms of the potential adverse impacts. Dependencies of assets on other assets should also be identified because this might influence the values of the assets (for example, the security requirements for a specific program are directly related to the value of the data/information it is processing). In CRAMM, dependencies between assets are defined in asset models. In asset models, a data asset is linked to other types of assets such as HW, SW and location, which are required for processing this data asset, so that business impacts resulting from insecurity of other asset types can be considered as business impacts on the data asset.

Assets valuation is followed by identification and assessment of threats and vulnerabilities. A threat needs to exploit an existing vulnerability of the asset in order to successfully cause harm. Threats may be natural or human in origin, and could be accidental or deliberate. In threat assessment, both accidental and deliberate threats should be identified and the likelihood of their occurrence should be assessed. The vulnerability assessment includes identifying weaknesses in physical layout, administration, procedures, personnel, HW or SW that may be exploited by a threat source to cause harm to the assets. This assessment identifies vulnerabilities that may be exploited by threats and assesses their likely level of weakness, i.e. ease of exploitation.

Once all the triplets of {asset, threat, vulnerability} have been identified and assessed, then risks can be measured. Risk is a function of the asset value (usually in terms of business impact), threat likelihood, severity of vulnerability, and existing/planned safeguard that reduces the risk. In CRAMM, the existing or planned safeguards are not considered during the risk analysis process to provide more focus on the true nature of risk (inherent risk). On the contrary, in the GMITS framework, the identification of existing or planned safeguards is a part of risk analysis, to avoid unnecessary work or cost in the duplication of safeguards. In this case, it should be checked whether the safeguard is working as intended.

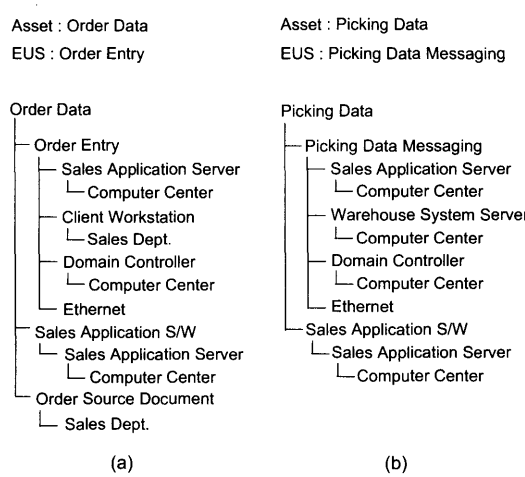
While the above activities represent risk analysis, the remaining activities in (Figure 1), selection of safeguards and risk acceptance are distinctive features of risk management itself. The identification and selection of safeguard is

based on the result of risk analysis; to what extent, which asset is exposed to which threat and what is the potential impact of the threat realization. One important aspect of safeguard selection is the cost factor as it would be inappropriate to implement safeguards which exceed the value of the assets they are designed to protect. After choosing safeguards and identifying how much risk reduction will be achieved by them, the decision on risk acceptance should be made. No system can be made absolutely secure and therefore there will always be residual risks after safeguards have been implemented. If the residual risk is unacceptable the safeguard selection should be performed again.

2.2 Risk Analysis View of Systems

A sound understanding of a system under review is an essential part of risk analysis. To achieve this, risk analysts obtain system relevant information from various sources, such as interviews with appropriate users and system documents (e.g., security policies, operation standards/guidelines, job description, data flow diagrams and network diagrams). Then, the risk analysis begins with identifying key assets and modelling the system using physical and logical links between the assets. However, the modelling is usually done in a static manner, and does not consider the dynamics of the system in terms of sequential interactions such as user-system, user-user and system-system interactions.

This argument becomes clear when we look at a CRAMM example that illustrates a part of a credit sales business process. The credit sales process starts from receiving a customer order document from a customer. A sales clerk in the sales department then enters the order details onto the sales application system via a networked workstation. The sales application server then checks the customer's credit status and the availability of stocks from the customer master file and inventory master file. Once these checks are completed successfully, the order is stored onto the sales order database and the picking list (generated from the order data) is sent to the warehouse system server that runs the shipping process. This example can be expressed as (Figure 2) in CRAMM; some minor variations may be possible.



(Figure 2) CRAMM Asset Model Example

(Figure 2-a) represents the order entry process from the client workstation to the server and (Figure 2-b) represents the application-application messaging process that sends the picking data from the sales application server to the warehouse system server. (Figure 2-a) is a simplified view of the order entry process, which does not represent the order checking activities.

We have to define other end-user services (and therefore asset models) that represent the credit and stock availability checking activities if we want to include the security concerns relating to the credit and stock data assets. However, these end-user services will still not represent what checks are being made and on what condition the order is approved; they will just provide another link relationship between the physical components and the data assets.

As shown in (Figure 2), risk analysis usually focuses on what is involved in a specific data process, rather than how it is involved. Therefore, it tends to be more interested in the system elements than logical activities. Moreover, it does not include any manual process. For example, the manual transfer of an order document from the customer to the sales clerk is not considered in the asset model since the main concerns of risk analysis are the system elements and related security issues. However, the confidentiality, integrity and availability of the source order document could be compromised during the manual process resulting in some adverse impact.

Although the asset model considers the human-computer interactive process (e.g. order entry), it is very limited. As there is no consideration of the conditions under which the sales department clerk is permitted to enter/approve the order, the threats such as deliberate entry/modification with fraudulent data may not be captured. The main concerns for this order entry interactive process would be unauthorised access to the order entry workstation, masquerading of sales clerk identity and input errors. Within the scope of risk analysis, threats from users with adequate access privileges are usually excluded (the only exception is the threat of user errors). This gives focused attention to security issues related to system elements and their exposures to threats from unauthorised people. This limits the security concerns to unauthorised behaviour from unauthorised internal, third party or external entities. Hence deliberate entry/modification by authorized users is not considered.

A well-designed management and technical control structure can prevent and reduce deliberate threats by authorized users. Segregation of duties, corresponding user privilege management and line of authorities and periodic review of user activities are key elements in preventing/reducing/detecting such deliberate threats. In fact, these issues can be covered within the scope of existing risk management practices such as BS7799 [3], GMITS-Part4 [11] and CRAMM, by addressing deliberate actions by authorized employees or third parties. However, we still have to conduct a more detailed analysis of by whom and how these threats may materialize.

3. Internal Control Evaluation

Asset safeguarding can be achieved not only through risk management but also through internal control system design. Internal control covers a broader area than IT security risk management as the latter is more focused on the risks in information systems and relevant assets. However, this distinction has become ambiguous as information systems are actively participating in almost all business processes these days.

According to the COSO (Committee of Sponsoring Organizations of the Tradeway Commission) internal control framework [5], internal

control is a broadly defined process, designed to provide reasonable assurance regarding the achievement of the following three objectives ; (1) economy and efficiency of operations, including achievement of performance goals and safeguarding of assets against loss, (2) reliable financial and operational data and reports, and (3) compliance with laws and regulations. This is a more general term than security safeguard as it is intended not only for the provision of security (in terms of confidentiality, integrity and availability) but also for effectiveness and efficiency.

3.1 Internal Control Evaluation

In the COSO internal control framework, the internal control system consists of five components ; (1) control environment : it provides the foundation for other components. It includes organizational factors such as management's philosophy, organizational structure and assignment of authority and responsibility, (2) risk assessment : it is a means to identify, analyse and manage risks that may result in failure of achieving the objectives, (3) control activities : control activities consist of the policies and procedures management has established to meet its objectives. They include reviews of the control system, physical controls, segregation of duties and information system controls, (4) information processing and communication : it is related to obtaining pertinent information to control the organization's activities and communicating it throughout the organization, and (5) monitorin g : it is an ongoing and periodic assessment of the effectiveness of the internal control system. Therefore, internal control evaluation is a process for determining the soundness of these components to assure the achievement of the above objectives.

As risk assessment is an essential component of the internal control system, a risk management approach has become an integral part of internal control system design. However, the definition of risk in an internal control context is less informative than that of IT security. Risk, more specifically inherent risk, is defined as the susceptibility of an assertion to a material misstatement, assuming that there are no related internal controls. In addition, it is usually framed by business process objectives identified and established prior to risk identification; once these objectives have been established, risks that pose threats to achieving these objectives are identified. There is another risk dimension to internal control, namely control risk. It is the risk that a material misstatement that could occur in an assertion will not be prevented, or detected and corrected on a timely basis by the entity's internal control structure. Control risk is more related to internal control evaluation in that it is a result of through examination of the current internal control system.

The risk assessment component of the internal control system covers not only the security issues arising from elements of information systems but also the management and procedural risks surrounding the systems. On the other hand, IT security risk analysis/management tends to focus on the technical functionality and the risk exposures at a static point; which assets are involved rather than how a specific business process is performed. To include the security concerns of a business process, one must move

from an asset-oriented view to a process-oriented view. Rather than identifying system security at a component/asset level, the evaluation should identify which risks exist in achieving the objectives of the business process. In IT security risk analysis, the business process is constrained by the establishment of dependency relationships between assets and the risks to each asset or group of assets. Besides the complexities of deriving an overall risk measure based on the risks of sets of dependent assets, another problem is that each risk could be localized at an asset level, rather than being incorporated into the impacts on the business process.

Another reason for introducing the internal control evaluation approach is that it validates the adequacy of the current control system. Although the focus of internal control evaluation differs from the focus of risk analysis, the concept of control risk could be used as a measure of vulnerability. In risk analysis, the vulnerability evaluation is often made by using a set of simple high-level questions. For example, one question for assessing the vulnerability to a masquerading threat in CRAMM is 'would a modification of the data be immediately obvious to several people?'. To answer this question, sound examination of how modifications are approved/monitored/reviewed should be made. Therefore, in order to obtain sounder values for vulnerability, the internal control evaluation approach becomes necessary. However, examining all the existing controls (both management and technical) for every threat would be non-practical for risk analysis.

Therefore, one may think of applying the internal control evaluation approach only for deliberate threats from authorized employees; this covers malicious actions of employees who have some form of privileged access. Advances in information and security technology have resulted in a number of technical safeguards that can be used to prevent or reduce attacks from unauthorised people. Examples are various identification and authentication techniques. However, deliberate attacks made by authorized employees are not normally covered by these technical safeguards as they only focus on unauthorised people. The opportunity environment is important in this context; the criminal mind will test the systems for weaknesses and therefore effectiveness of the current control system in preventing/detecting deliberate actions is essential. That is why we consider internal control evaluation for threats from authorized employees.

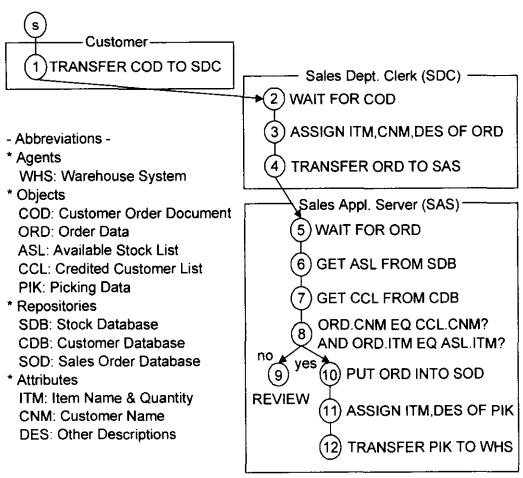
As the scope of general internal control evaluation is very broad, we limit its scope to the evaluation of management and procedural controls, focusing on the identification of the control risks, which might be exploited by authorized employees and third parties both accidentally and deliberately. Therefore in this paper, the primary difference between internal control evaluation and risk analysis is the focus of the review. While risk analysis pays more attention to threats from unauthorised people, physical component failure and natural disasters, internal control evaluation concentrates on threats from authorized people.

3.2 Internal Control Evaluation View

(Figure 3) uses the same example as in (Figure 2), but represents the system from the perspec-

tive of internal control evaluation. This representation is based on the system modelling technique used in TICOM (The Internal Control Model) [1], which is one of the most significant works on internal control evaluation; the TICOM model here is for illustration purposes and shows how auditors think during internal control evaluation. In practice, the system flowchart technique is widely used to understand and document the system.

Originally, TICOM was intended for modelling tasks from a human-oriented perspective. The tasks of the sales application server and interactions between the order entry clerk and server in (Figure 3) are modelled by interpreting the server as a human agent to focus on what is happening to data objects. TICOM uses a set of predefined command languages to capture the essence of tasks in a specific business process. For example, the TRANSFER command is used to represent the transferring of data objects between agents and specifies which data objects are being transferred.



(Figure 3) TICOM Control Model Example

In internal control evaluation, a business process/transaction is expressed in terms of dynamic interactions between participating entities, rather than merely a physical/logical configuration. Therefore, the internal control evaluation approach can identify human-related risks more efficiently than risk analysis can. In our example credit sales process, there is a risk of approving an order from a customer with a poor credit rating. In risk analysis, such a risk is considered in terms of unauthorised access to the customer database and/or a sales application software failure that could result in wrong order approval. By contrast, in the internal evaluation approach, the focus is on the separation of duties between order entry and approval.

As order approval is made by the sales application server in our example, the separation of duties between the order entry and approval seems appropriate at first glance. However, it should be further examined whether the order entry clerk has access to the credit database as the clerk could modify the credit rating deliberately thus allowing approval of the order. This situation could result in the sales department clerk conspiring with a non-creditworthy customer to embezzle goods. Moreover, if the clerk is authorized to create a new customer record as well, he could perpetrate such a fraud by himself. It is almost impossible to prevent a deliberate threat that utilizes the cooperation of several employees. Nevertheless, at least the control risk that could be exploited by a single employee should be properly addressed.

The identification and evaluation of such control risks is based on the heuristics held by expert auditors. The organizational structures,

operational procedures and supported business objects varies from case to case and therefore an evaluation that considers these factors together cannot be easily generalized. Therefore, the evaluation becomes totally dependent on the auditor's expertise and skill. In view of this, extensive research has gone into the provision of a decision-aid that supports the evaluation. For example, in [12], heuristic knowledge of auditors has been derived through knowledge acquisition engineering and it has been formalized into IF -THEN rules so that these rules can be used for evaluation of other cases. In addition, lists of standard controls such as COBIT (Control Objectives for Information and Related Technology) [4] and BS7799 can also be referenced for benchmarking to check whether the existing control structure complies with the standard control structure. However, these rules are still general and they may not be effective for specific cases.

4. Conclusion

We have compared the nature and focus of risk analysis and internal control evaluation. As different roles are assigned to each of them from the different schools of thought, both of them should be addressed through separate management attention. However, ensuring that both of them are performed on a sound and regular basis requires great management effort. Therefore, in this case, organizations might consider including the internal control evaluation's view of a system within a single risk analysis and management framework. Regarding this, a systematic and consistent way of integrating them should be studied further. Moreover, as risk analysis and management is closely related to not only internal control evaluation but also to other security management activities such as incident management, vulnerability assessment and information system audit, a novel approach that minimizes the duplication of effort between them and enhances their relationship should be examined in terms of feasibility and efficiency.

References

[1] Bailey, A. D. Jr., Duke, G. L., Cerlach, J., Ko, C., Meservy, R. D. and Whinston, A. B., "TICOM and the Analysis of Internal Control", The Accounting Review, pp.186-201, April 1985.

[2] Baskerville, R., "Information Systems Security Design Methods : Implications for Information Systems Development", ACM Computing Surveys, Vol.25, No.4, pp.375-414, 1993.

[3] BS7799-Part 2 : Specification for Information Security Management Systems, British Standard Institution, 1999.

[4] COBIT Control Objectives, "IT Governance Institute", 2000.

[5] COSO Internal Control Framework, "The Committee of Sponsoring Organizations of the Tradeway Commission", 1992

[6] CRAMM User Guide 2.0, UK Security Service, 2001.

[7] CSI/FBI Computer Crime and Security Survey, Computer Security Institute, 2002.

[8] Finne, T., "Information Systems Risk Management : Key Concepts and Business Processes", Computers & Security, Vol.19, pp. 234-242, 2000.

[9] Grupe, F. H., Hensley, J. M. and Yamamura, J. H., "Watching Systems in Action : Security at the Periphery", Information Management & Computer Security, Vol.6, pp.155-159, 1999.

[10] Guideline for Management of IT Security-Part3 (GMITS-Part3) : Techniques for the Management of IT Security, ISO/ IEC TR 13335-3, 1997.

[11] Guideline for Management of IT Security -Part4 (GMITS-Part4) : Selection of Countermeasures, ISO/IEC TR 13335-4, 1999.

[12] Meservy, R. D., Bailey, A. D. Jr., and Johnson, P.E., "Internal Control Evaluation : A Computational Model of the Review Process", Auditing : A Journal of Practice & Theory, Vol.6, No.1., pp.44-74.

조 성 백

한국과학기술원 산업공학과 (공학사)
런던대학교 정보보호학과 (공학석사)
런던대학교 정보보호학과 (공학박사)
현재, 경기대학교 정보보호기술공학과 연구교수

김 귀 남

미국 캔자스대학 수학과(응용수학사)
미국 콜로라도주립대학 통계학과(통계학석사)
미국 콜로라도주립대학 기계·산업공학과(기계·산업공학박사)
현재 경기대학교 정보보호기술공학과 주임교수