제28회 한국정보처리학회 추계학술발표대회 논문집 제14권 제2호 (2007. 11)

감리결과 평가를 위한 감리조서 작성방안 연구

노 갑철*
*고려대학교 디지털 정보공학과
e-mail : Clemens@korea.ac.kr

A Study on organization of work paper for Evaluation of Information System Audit Results

Kab-Chul Roh*
Dept of Digital Information Technology, Korea University

요 약

2002 년 미국의 회계부정 문제에 기인해 감사조서의 작성 및 수정, 보관에 관한 규정이 강화되었다. 따라서, 회계감사의 일부로 수행되는 전산감사도 이 규정에 따라 전산 감사조서의 작성이 강화되었다. 최근 정부는 공공기관에서 발주하는 일정규모 이상의 정보화 프로젝트에 대한 감리를 의무화하였으며, 공공부분의 정보시스템 감리는 점차 확대되어 감리시장이 성숙단계에 이르는 것으로 평가되고 있다.

본 연구에서는 정보시스템 감리수행 결과를 평가하기 위한 감리조서의 구성방안을 제안한다. 기존 감리보고서의 불분명한 감리전략과 감리 결과를 지지하는 증거가 불충분한 문제점을 보완하여 감리 전략에 기반한 감리조서의 구성을 제안한다. 이는 기존의 감리절차 진행과정에 감리조서 작성을 추가/보완함으로써 기존의 감리절차를 유지하면서도 감리보고서의 신뢰성을 증진한다.

1. 서론

정보시스템 감리는 공공부문을 중심으로 매우 빠르게 확산되어 점차 민간부문으로 확대되고 있다. 이는 정보시스템 감리를 통하여 정보시스템의 품질향상을 얻을 수 있기 때문이다[1].

정보시스템 감리란 감리대상으로부터 독립적인 감리인이 정보시스템의 효율성, 효과성, 안전성 향상을 위하여 정보시스템의 구축 및 운영에 있어서 시스템의 합목적성, 적용기술의 적합성, 자원사용의 적정성을 점검, 평가하고 감리의뢰인과 피감리인에게 개선이 필요한 사항(Reportable conditions)을 권고하는 것으로 정의되어 진다 [1-3].

그 중요성에 비추어 보면 객관적인 감리결과 평가를 위해 감리조서를 작성하고 감리품질 평가에 활용하는 분야의 연구는 미흡한 실정이다.

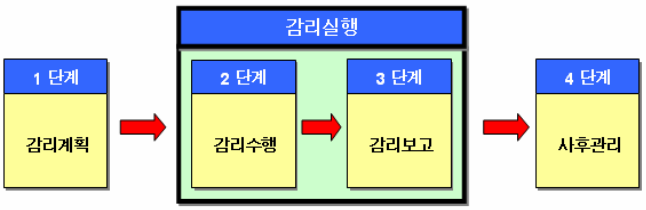
그 이유는 감리법인에서는 개별 감리인의 감리자료 검토 및 면담을 통해 감리근거를 확보하고 감리인의 주관적인 감리기준과 제도에 따라 감리를 수행하기 때문이다. 이는 필연적으로 감리법인과 감리인의 개별적인 역량에 따라 감리품질이 좌우되는 결과를 초래한다[4].

이러한, 문제점을 해결하기 위해 감리과정에서 감리조서를 작성하고 활용하는 노력이 필요하다.

2. 정보시스템감리의 유사제도의 수행절차와 문서화 규정 고찰

2.1 정보시스템 감리절차 및 문서화 규정 고찰

정보시스템 감리는 계획, 실행, 사후관리의 3 부문으로 구성되며, 실행부문은 다시 감리를 수행하는 단계와 이를 관련당사자에게 보고하는 감리보고단계로 나누어 진다. 그림 1 은 정보시스템 감리를 추진하는 과정에서 발생하는 업무를 도식화한 것으로 작업 간의 선후관계를 나타내고 있으며, 선행단계의 작업산출물이나 활동내역이 다음단계를 진행하기 위한 입력물로 활용된다.



(그림 1) 감리절차

또한, 사후관리 단계의 산출물이 최초단계인 감리계획으로 피드백되어 감리의 효과성과 효율성이 증진될 수 있도록 계획을 조정하는데 사용될 수 있다[5].

현재 국내 법/제도에 따른 정보시스템 감리의 문서화 요구는 정보시스템 감리기준에서 규정하고 있으며, 주요 문서는 아래와 같은 사항을 감리보고서에 첨부하도록 규정하고 있다.

- 감리계획의 요약
- 감리대상사업의 개요
- 감리영역별 검토의견
- 기타 권고사항

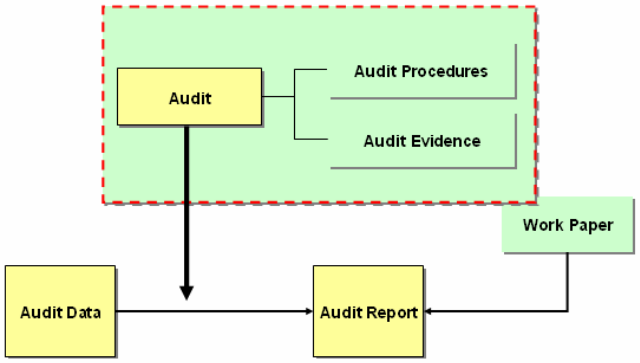
- 감리의견

이외에 감리계약서, 감리계획서, 감리보고서 등 감리관련 중요문서를 감리보고서 제출일로부터 5 년간 보관하도록 규정하고 있다. [6]

2.2 AICPA의 수행절차 및 문서화 규정

미국의 정보시스템에 대한 유사감리제도는 미국정부 및 관계기관 감사 규정(GAS : Government Auditing Standard)에 포함된 컴플라이언스 및 내부통제(Compliance and internal control) 부분 중 OMB-Circular A-130, A-123 에서 규정하고 있다[7]. 위의 기준에 관한 제반 절차는 미국회계사협회(AICPA : American Institute of Certified Public Accountants)에서 마련한 AT Section 601 Compliance Attestation 을 따르도록 규정하고 있다. 이 절차는 다음과 같다.

a. 해당 이행감사에 대한 요구사항의 이해
b. 감사 계획의 수립
c. 해당 조직의 이행감사를 위해 가용한 내부통제에 대한 고찰
d. 해당 요구사항 이행에 관한 테스트 및 충분한 증거의 확보
e. 특정시점 및 계약철수기간의 이벤트 (subsequent events) 고찰
f. 피감 조직이 기 규정된 해당 기준이 요구하는 규정들 중 중요한 모든 규정을 이행하는지에 대한 의견표명[8]



(그림 2) 감사조서의 개념도[9]

그림 2 는 감사조서의 개념을 보여준다. 감사조서는 각각의 감사 상황에 맞추어서 디자인된 감사절차, 감사테스트 결과, 감사과정의 모든 기록물이다.

이러한 감사조서는 감사보고서를 뒷받침하는 중요한 산출물이며 감사보고서와 클라이언트의 데이터 간에 연결고리를 제공한다. 이것은 대체할 수 없으며, 클라이언트의 소유도 아니다. 감사조서는 감사과정의 감사계획, 관리, 리뷰 등의 기반이 된다.

이를 위해 감사조서는 다음사항을 만족해야 한다.

- 클라이언트 이름, 목적(주장), 감사 수행자, 작성된 날짜, 리뷰수행자 등이 적절하게 표시해야 한다.
- 감사조서의 인덱스번호, 상호 참조 등이 포함 되어야 한다.
- 각종 자료의 계산 및 작업과정이 나타나야 한다.
- 감사인이 작업한 내용 및 감사증거의 획득을 검토자가 이해할 수 있도록 작성한다.

또한, 감사 조서는 감사 보고서 발행일로부터 5 년간 보관하도록 규정하고 있으며, 감사조서는 다음과 같은 사항을 포함하도록 하고 있다.

- 클라이언트와 감사 업무에 관한 이해과정(계약서)
- 각 감사의 문서화된 감사전략
- 감사인의 책임 및 사기와 관련된 중요성 관점에서의 감사위험 평가에 관한 증거
- 개선권고사항에 관해 감사위원회와 구두로 협의한 내용
- 통제위험 평가에 관려된 내부통제 이해 내용
- 계획 단계와 검토단계의 분석적 절차 정보
- 경영자로부터 획득한 경영자 확인서
- 각종 공시 및 사업 계속성에 관한 정보[10]

2.3 ISACA의 수행절차 및 문서화 규정

ISACA 의 정보시스템 감사절차는 감사계획, 감사의 수행, 보고 및 사후절차로 이루어진다.

감사조서는 다음과 같은 사항을 만족해야 한다.

- 감사과정에서 정보시스템 감사인은 감사목적에 적합하고 충분하며, 신뢰할만한 감사증거를 획득해야 한다.
- 감사발견사항 및 결과는 감사증거에 의해 적합하게 설명되고 분석되어야 한다[11].

2.3.1 감사조서에 포함되는 내용

정보시스템 감사의 문서화는 감사작업 수행 및 감사증거의 기록이고, 정보시스템 감사 발견사항과 결과의 근간이 된다. 잠재적으로 다음 문서들을 포함한다.

- 정보시스템 감사인이 정보시스템 감사 규정을 준수한 감사조서
- 감사의 계획, 수행, 검토와 관련된 것
- 외부 검토 사항
- 사기와 관련한 증거, 소송, 보험청구 등의 정황
- 스텝의 전문가적인 사항

여기에서 감사조서는 최소한 다음과 같은 기록을 포함하여야 한다.

- 계획 및 준비 단계의 감사범위 및 목적
- 감사 프로그램
- 감사 증거의 수집 및 수행절차
- 감사 발견사항과 결과 및 권고사항
- 감사 결과 관련 모든 보고서
- 스텝들의 감사결과에 대한 관리적 검토

또한, 정보시스템 감사인의 감사조서는 특정 감사의 요구사항에 기반한 다음과 같은 것들을 포함하도록 하고 있다.

- 정보시스템 감사인이 감사 할 영역 및 환경에 대한 이해
- 정보시스템 감사인이 정보처리시스템 및 내부통제환경에 대한 이해
- 감사조서 내용의 출처와 작성자 및 작성일
- 감사 증거와 출처 및 작성일
- 개선권고에 대한 피감자의 반응

이러한 감사조서는 법규에서 요구하는 사항 또는

감사 규정에서 요구한 정보를 포함하여야 하며, 검토자가 이해할 수 있도록 명확하고 완벽하게 작성하여야 한다[11].

3. 감리평가를 위한 감리조서작성 방안

감리조서는 감리 수행 단계 및 감리 대상 부분 별로 구조화되어 작성되어야 하며, 서로 참조 가능하도록 링크되어야 한다.

또한, 감리 과정에서 따라야 할 행위기준의 평가가 용이하도록 구성하여야 한다. 각 조서는 감리의 목적 및 문서의 작성일자와 검토일자 등이 포함되며, 산출물이 적용되는 단계가 포함된 인덱스 및 관리적인 측면에서의 검토를 위한 검토자 표시 등이 포함되도록 한다[12].

3.1 감리계획단계

감리계획단계는 해당감리 프로젝트의 전반적인 성격을 결정하는 단계이다.

이 단계에서 수석 감리인을 비롯한 감리인간의 업무분담이 이루어지며, 감리의 성공적 수행을 위한 브레인스토밍이 이루어진다.

또한, 수석 감리인은 감리 전체의 감리전략(Audit Program 또는 Audit Strategy)을 수립하며, 감리인들은 분담된 업무분야의 감리전략을 수립한다.

그러므로 감리 계획 단계에서는 다음과 같은 내용이 감리조서에 포함되어야 한다.

- 감리 계약서(Engagement Letter) : 감리계약서에는 감리범위, 인력계획, 감리일정 및 감리인의 의무와 피감자의 의무, 이해당사자 등의 의무가 표시된다[13].
- 감리 전략(Audit Program 또는 Audit Strategy) : 감리전략은 감리 계획서를 포함한다. 감리 계획서에 기술된 내용의 모든 내용 및 감리인 별 감사절차가 포함된다. 계획 단계에서 클라이언트의 광범위한 이해를 바탕으로 중요성 기준을 설정하고, 해당 감리에 대한 위험을 평가하고 감사전략에 포함한다[13] [10].
- 분석적 절차 : 분석적 절차는 프로젝트 수행 보직 및 운영조직의 전반적인 사항을 질적, 양적인 방법을 통하여 분석하고, 이 결과가 감리결과에 미치는 영향을 고려하여 감리전략에 반영한다[15][13].
- 고객과 문서 또는 구두로 주고받은 감사 관련사항을 문서화 한다.
- 감리인간의 의견 불일치 내용 및 결론[10].

3.2 감리수행 단계

감리수행 단계는 감리의견을 도출하기 위한 증거를 모으고 분석하는 활동을 포괄한다.

이 단계에서 수집하는 모든 증거 및 활동은 감리조서에 기록되어야 하며, 감리결과를 직접적으로 뒷받침 한다. 따라서, 감리인은 감리대상에 대한 합리적인 확신을 주는 충분하고 신뢰성 있는 증거를 확보하고 감리조서에 기록하여야 한다.

- 감리전략 : 감리전략에 따라 수행되는 모든 문서 및 감리인이 행한 모든 활동과 구두로 확보한 증거를 기록한다. 확보한 증거를 평가하고 추가적인 증거의 확보 및 테스트에 대해 고려한다[13].
- 개선권고사항 (Reportable Conditions) : 감리기간 중 발견한 클라이언트의 취약점들에 대해 문서 또는 구두로 전달한 권고사항을 기록한다[14].

수석감리인은 감리인이 수행한 절차 및 확보한 증거가 감리결과를 뒷받침하기에 신뢰할 수 있고 충분한지에 대해 평가하고 미흡한 부분에 대해서는 지적하고 재수행 또는 추가적인 증거를 확보하도록 지시한다[13][15].

3.3 감리보고 단계

감리보고 단계는 사전에 정의된 검토항목과 기준을 보고서 초안에 기술하고, 문제점과 개선사항을 유형별로 분류한 후, 개선사항 별로 현황과 문제점 그리고 이를 입증할 수 있는 증거를 요약한다.

더불어 문제점을 해결하기 위하여 도움이 될 수 있는 개선사항을 기술하고, 문제점과 개선사항을 각각에 대한 중요도 및 시급성 그리고 개선의 주체를 기술한다.

마지막으로 검토분야 별 결론과 전체 결론을 보고서 초안에 기술한다.

- 클라이언트 책임자 확인서(Representation letter) : 클라이언트가 감리기간 동안 제시한 증거 및 구두로 진술한 내용에 대한 요약으로써 감리와 관련된 중요한 모든 내용을 제시하였음을 문서로 요약하여 확인 받는다[16].
- 감리보고서 : 감리보고서는 감리분야별 현황, 문제점, 개선사항, 결론을 정리하여 중복성과 비일관성, 감리 조서에 의해 확인되지 않은 사실이 배제된 보고서를 작성한다[5].

3.4 사후관리 단계

사후관리 단계는 시정조치계획서 검토, 시정조치결과 확인, 감리품질 평가로 이루어진다.

이 단계에서는 시정조치계획을 검토하고 시정조치결과에 대한 확인이 이루어진다.

또한, 내부적 또는 외부적인 감리평가를 실시하고 감리 시 개선안을 도출한다[5].

- 감리전략 : 시정조치보고서에 대한 검토 내용, 시정조치 결과 관련 확인 및 증거는 모두 문서화한다. 특히, 피감조직의 시정조치 이행여부를 확인하여 문서화한다.

4. 기존의 문서화 방안과의 비교 및 평가

기존 방법은 감리보고서 및 감리관련 일부의 문서만을 보관하고 관리한다. 반면, 회계감사와 병행하여 수행되는 전산감사의 경우 회계감사와 동일한 수준의 문서화가 이루어진다.

표 1 은 기존문서화 방법과 본 논문에서 제안된 문서화 방안을 평가한 결과이다.

<표 1> 기존 문서화 방법과 제안된 문서화 방안의 비교

평가항목	기존의 문서화	제안된 방안
1. 감리 행위요소평가항목 및 평가요소		
1.1 최고 경영층의 지원	불만족	만족
1.2 만족도	대체로 불만족	만족
1.3 의사소통	불만족	만족
1.4 명백한 목표와 목적	만족	만족
1.5 관리	만족	만족
1.6 품질/비용/시간	만족	만족
1.7 조직	대체로 불만족	대체로 만족
1.8 문화	불만족	대체로 만족
2. 감리 산출물 평가항목 및 평가요소		
2.1 실용성	불만족	만족
2.2 편의성	만족	대체로 만족
2.3 신뢰성	대체로 불만족	만족
2.4 효율성	대체로 만족	만족
2.5 통합성	대체로 만족	만족
2.6 상호작용	대체로 불만족	만족
2.7 유연성	불만족	만족
2.8 다양성	대체로 만족	대체로 만족
2.9 간결성	불만족	만족
2.10 구체성	대체로 불만족	만족

상호비교 평가를 위해 감리법인에 보관중인 감리보고서와 회계법인에서 사용하는 감사조서 자동화 시스템에 따라 작성된 전산관련 컴플라이언스 및 내부통제 감사의 감사조서와 보고서를 샘플링하여 사용하였다.

연구를 위해 선별된 감리결과보고서와 감사조서를 위의 평가 항목에 따라 평가하고 그 결과를 만족, 대체로 만족, 대체로 불만족, 불만족 등 4 단계로 나누어 평가하였다.

감리결과 보고서는 80-200 페이지 정도이며, 감사조서의 경우 질의 및 수행조서(감사전략) 150-400 페이지(기관의 규모에 기반함.), 추가로 획득한 감사증거 2000-10,000(기관의 규모에 기반하며, 전산분야에로 제한.)페이지, 개관자료 20-100 페이지로 이루어져 자료의 규모면에서 현격한 차이가 있다.

또한, 전산부문 감사조서는 파일형태의 문서를 감사조서 시스템에 등록/저장함으로써 감리조서의 양을 최소화하여 관리한다.

5. 결론 및 향후연구

본 논문에서는 감리결과의 품질평가를 위한 문서화는 감리전략에 따라 감리조서를 작성하고 관리하는 것이 가장 적합함을 확인하였다. 기존의 개별 문서 및 감리보고서 위주의 문서화 대신 감리전략에 따라 감리조서를 작성하여 체계화함으로써 감리품질 평가 방법을 개선하였다.

감리조서는 기존의 문서화 방식이 감리과정에서 일어난 모든 사항을 문서화하지 않음으로써 발생하는 의사소통 장애를 해결하였다.

감리법인이 수행한 감리 프로젝트를 문서에 담아 감리인의 평가 및 감리프로젝트 자체를 평가하는 자료로 활용이 가능하다. 또한, 감리결과 보고서를 뒷받침하는 근거로서의 감리조서는 감리결과에 대한 신뢰성과 정당성을 부여하여 감리제도 전반의 신뢰성 및 감리의 효과성을 제고하게 된다.

본 연구는 감리결과의 품질평가를 위한 감리조서 작성방안을 수립하고 검증한 것에 의의가 있다.

향후 위의 방안에서 고려하지 않은 감리조서의 평가방안 및 문서화에 따라 추가되는 비용에 관한 연구가 필요할 것으로 판단된다.

참고 문헌

[1] Janes E. Hunton, Stephanie M. Bryant, Nancy A. Bagranoff, Core Concepts of Information Technology Auditing, Wiley, 2003.

[2] 한국전산원, 정보시스템 감리 효과에 관한 연구, 2002.

[3] 한국전산원, 정보시스템 감리 의무화 방안 연구, 2002.

[4] 선우종성, 정보시스템 감리결과의 평가방안, 2005.

[5] 한국전산원, 정보시스템 감리방법론 연구, 2000.12

[6] 정보통신부 정보시스템 감리기준, 1999.

[7] 한국전산원, 해외 정보시스템 감리 유사제도 비교연구, 2004.10.

[8] AICPA, AT Section 601 : Compliance Attestation, 2006.

[9] 권오상, Auditing and attestation 2nd Ed, pp.301, 2006.

[10] AICPA, AU Section 339 : Audit Documentation, 2006.

[11] ISACA, IS Auditing Standards, Guidelines and Procedures, 2007.2.

[12] 한국정보사회 진흥원, 정보시스템감리점검해설서 V2.0, 2007.2.

[13] AICPA, AU Section 311 : Planning and Supervision, 2006.

[14] AICPA, AU Section 325 : Communicating Internal Control Related Matters Identified in an Audit, 2006.

[15] AICPA, AU Section 329 : Analytical Procedures, 1989.

[16] AICPA, AU Section 333 : Management Representations, 1998.

[17] PCAOB, Auditing Standard No. 3 Audit Documentation, 2003.