「진주지역 감사협의회」 결과

감사실-1199('16.5.19)

▢ 개 요

감사업무 발전을 위한 진주지역에 위치하는 공공기관 감사협의회('16-3차) 개최 결과임

▢ 감사협의회 개최 결과

○ 주관기관 : 국방기술품질원

○ 장소 / 일시 : 송화일식 / '16. 5.10(화), 12:00~13:30

○ 참석자 인원

기관명	참석인원	참석자	비고
한국남동발전	6	감사 외 5명	수행기사 포함 (청렴감찰부 3명)
한국토지주택공사	3	감사 외 1명	수행기사 포함
중소기업진흥공단	2	감사실장 외 1명	
국방기술품질원	2	감사실장 외 1명	
계	13		

○ 협의 및 토의 내용

- 남명 조식 청렴연수원 운영 안내(한국남동발전)
  · 동영상 소개 등
    * 1박 2인 / 1인당 약 28만원
- 정보화 사업 감사 방법 공유
  · 한국남동발전 : 정보화전문 내부 직원 및 외부 회계법인 활용
  ※ 한국남동발전 정보화업무 감사 사례 : 덧붙임 참조
  · 중소기업진흥공단/한국토지주택공사 : 정보화전문 직원 활용
  ***기관마다 IT관련 감사전문가 부재로 실질적인 감사에 애로점 존재**
- 청렴/반부패 행정업무 증가로 자체 감사 업무 애로점 공유

○ 비용 사용

- 식비 등 : 320천원

덧붙임

한국남동발전 정보화 사업(IT) 감사 사례

○ IT 감사 기본 추진 방향

- IT 내부감사 체계 수립
- 전문가를 통한 실지감사 수행

○ 세부 추진 방법

- 위탁 용역 : 안진회계법인

  * 국내 IT감사 가능 회계법인(회계사 외에 IT전문가 별도 운용) : 삼일회계, 안진회계

- 용역 범위
  - IT 내부감사 체계 정립
  - IT 실지감사

  * 남동공단 자체 감사인력과 협업 실시

- 사업기간 : 3개월(실지감사 8일)
- 사업예산 : 9천만원
- 용역참가 인력 : PM포함 5명

○ 업무 추진 관련 담당자 후기

- 남동발전에서도 종전에 IT분야에 실질적으로 감사한 사례가 없어 감사 시 확인/검토하여야 할 사항 많이 존재하여 감사기간 확대 필요성 인식
- 용역 비용 측면에서의 적정성 관련 당시 신용보증기금에서의 IT감사 추진 등과 관련 소요 비용 확인 등을 통해 적정성 판단

※ 남동발전에서 기고하여 「한국감사협회」의 "내부감사저널"에 게재된 "공공기관 IT 내부감사체계 수립의 필요성 및 효과" 자료 덧붙임 참조

공공기관 IT 내부감사 체계 수립의 필요성 및 효과

김낙규
한국남동발전㈜
상임감사위원

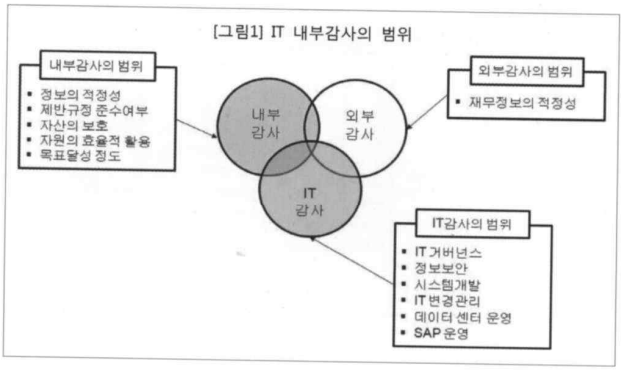
내부감사에서의 IT분야 사각지대 해소

우리 사회는 최근 연이은 은행의 전산장애로 인한 업무마비 사건, 카드사의 개인정보 유출 사건 등의 IT 사고로 고객 불편, 관련 기업의 명예 실추, 금전적 손해 등 막대한 사회적 불안 및 비용을 초래한 바 있다. 또한 사이버 테러, 개인정보보호 등 정보보안 이슈는 금융, 민간기업 뿐만 아니라 공공기관의 경우에도 IT 리스크 증가에 따라 마찬가지로 큰 이슈로 대두되고 있다.

전통적으로 우리나라의 공공기관 내부감사는 회계, 계약 분야 및 각 기관의 고유 업무 분야에 중점을 두고 운영되어 왔으나 최근 들어 IT 관련 사건 · 사고의 증가로 단순한 재무보고 및 통제 그 이상으로 내부감사 역할에 대한 요구가 증가하고 있는 추세이다. 이렇듯 내부감사의 사각지대로 남아 있던 IT 분야의 감사 필요성 증가에 따라 공공기관 또한 IT 리스크를 효율적으로 관리, 점검하기 위한 IT 내부감사 체계 수립의 필요성이 증가하고 있다.

한국남동발전 감사실은 이러한 환경변화에 선제적으로 대응하고자 내부감사의 역할을 IT 분야로까지 확장시키고 각종 사이버 위협 및 IT 리스크에 효율적, 효과적으로 대응하기 위한 노력을 지속적으로 추진해 왔다. IT 전문인력 확보, IT 감사 수행의 전문성 · 객관성 확보 등의 노력을 하였으나 IT 내부감사를 자체적으로 수행하기에는 현실적으로 어려움이 있었다. 이러한 실무적인 어려움을 해소하기 위해 IT 내부감사 체계 수립 및 IT RCM(Risk Control Matrix) 개발을 추진하게 되었다.

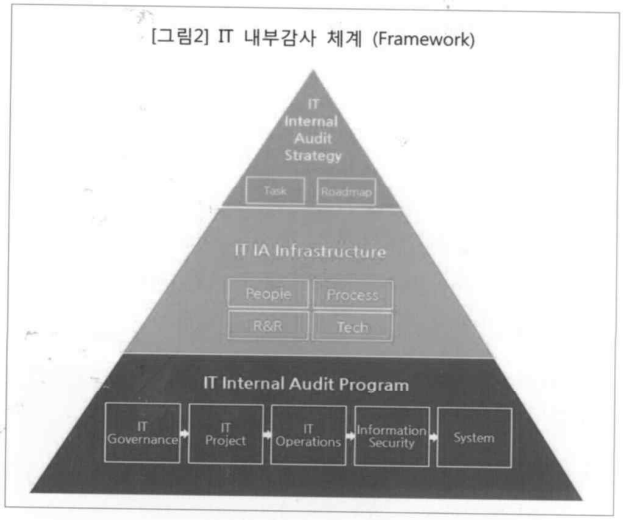
[그림1] IT 내부감사의 범위



IT 내부감사 체계(Framework) 수립

IT 감사는 사전적 의미로 정보시스템의 효율성, 신뢰성, 안전성을 확보하기 위해 독립된 감사인이 일정 기준에 근거하여 정보시스템을 종합적으로 점검 · 평가하고 현업부서 담당자에게 미비점을 개선하도록 조언 · 권고하는 활동을 말한다.

[그림2] IT 내부감사 체계 (Framework)



IT 감사의 목적은 IT 자원이 조직의 목적을 효과적으로 달성하기 위한 방향으로 운영되고 있는지를 점검하는 것이다. 이를 위한 IT 감사의 범위는 다음과 같다.

1) 정보시스템의 적절성과 효과성에 대한 확신을 얻기 위한 통제 검토
2) 시스템 및 그 시스템의 보안에 대한 성과 평가
3) 시스템 개발 프로세스와 절차 점검
4) 급여시스템, 재무회계시스템과 같은 특정 정보시스템의 운영 절차 평가

IT 일반통제는 IT 통제구조를 기반으로 정보시스템을 개발, 운영, 유지하는 일반 환경과 연관되어 IT 활동에 대한 전반적인 통제 체계를 수립하고 전반적 통제목적을 충족하기 위해 시행한다. IT 응용통제는 각 어플리케이션에 대한 고유한 특정 통제로 어플리케이션의 일부분에만 적용된다. 응용통제의 예로는 데이터 입력인증, 전송데이터 암호화, 통제절차 등이 있다.

일반적으로 IT 감사는 해당 조직 IT 업무의 복잡성 등을 감안하여 수행범위를 결정한다. 특히 공공기관의 IT 리스크는 금융기관 등 타 분야와는 다른 양상을 보이기 때문에 획일적인 기준으로 IT 리스크를 관리하고 점검하기 보다는 공공기관 특성에 적합한 IT 리스크 점검 체계를 수립하여 이를 IT 운영 전반의 리스크 점검 도구로 활용할 필요가 있다.

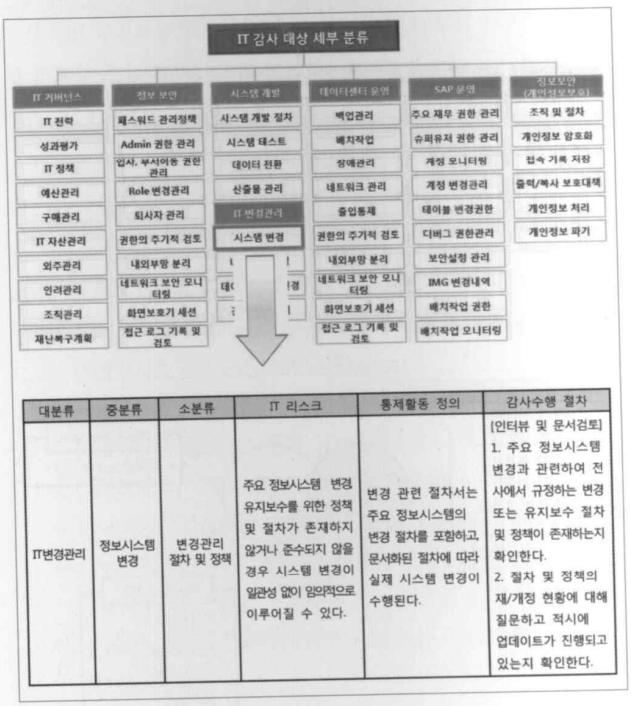
이를 위해 한국남동발전 고유의 IT 내부감사 체계는 「첫째, 날로 증대되는 IT분야의 중요성에 걸맞은 IT 내부감사 전략 및 감사영역별 균형적 발전전략 수립. 둘째, IT분야의 양적, 질적 성장에 맞는 거버넌스 구축. 셋째, IT 내부감사의 지속적 시행에 따른 감사 프로세스 정립. 넷째, IT 전문감사인력 확보 및 전문성 강화」를 토대로 다음과 같이 IT 내부감사 전략(Strategy), IT 내부감사 조직(People), IT 내부감사 프로세스(Process), IT 내부감사 도구(Tool)의 4가지 영역으로 구성하고 각 영역별로 아래와 같은 사항을 정의하여 IT 내부감사 전략 체계를 수립하였다.

1. IT 내부감사 전략(Strategy)
   - 내부감사 전략과 연계되는 IT 내부감사 전략 개발
   - 구체적이고 실현가능성 높은 IT 내부감사 로드맵 및 추진과제 도출
   - IT 감사인의 성과목표와 운용 방향의 적절성 검토
2. IT 내부감사 조직(People)
   - IT 감사인 전문성
   - IT 감사인의 역할과 업무 분담 수준
   - IT 감사인의 IT 관련 교육 수준
3. IT 내부감사 프로세스(Process)
   - IT 감사빈도 설정 및 일정, 기간, 감사대상 업무 범위 선정
   - 감사대상 영역별 감사자원 배분
   - IT 분야의 리스크 기반 감사 수행
   - 현행 내부감사 절차 반영
4. IT 내부감사 도구(Tool)
   - IT 감사 프로그램 보유 여부 고려
   - IT 리스크 반영의 완전성 여부 고려
   - 회사의 IT 현황을 반영한 IT 감사 프로그램 개발로 활용도 극대화

IT RCM(Risk Control Matrix) 개발

IT RCM은 IT 내부감사를 수행하기 위한 도구로서 COSO Framework, ISMS(Information Security Management System), 상장사 IT 체크리스트 및 한국남동발전의 IT 업무별 체크리스트 등 다양한 소스로부터 리스크 정보를 취합·분석한 후 한국남동발전의 IT 환경, 감사의 효과성 등을 고려하여 총 97개의 리스크를 도출하였다. IT 리스크는 IT 거버넌스, 정보보안, 시스템 개발, IT 변경관리, 데이터센터 운영, SAP 운영의 6개 대분류와 27개의 중분류, 97개의 소분류로 구분되며 주요 리스크로는 IT 예산 집행 모니터링, 보안성 검토 절차 준수, 신규 정보시스템 구축 정책 및 절차, 백업 수행, SAP 접근권한 부여 등이 있다.

IT RCM에는 각 소분류별로 리스크와 통제활동이 정의되며 감사 수행 절차에 의해 감사가 진행된다. 감사 수행 방법은 해당 리스크의 통제활동 성격에 따라 달라질 수 있다. 다음은 IT 내부감사 수행 시 사용된 IT 감사대상 분류 및 IT 리스크 통제 매트릭스 예시이다.



대분류	중분류	소분류	IT 리스크	통제활동 정의	감사수행 절차
IT변경관리	정보시스템 변경	변경관리 절차 및 정책	주요 정보시스템 변경 유지보수를 위한 정책 및 절차가 존재하지 않거나 준수되지 않을 경우 시스템 변경이 일관성 없이 임의적으로 이루어질 수 있다.	변경 관련 절차서는 주요 정보시스템의 변경 절차를 포함하고, 문서화된 절차에 따라 실제 시스템 변경이 수행된다.	[인터뷰 및 문서검토] 1. 주요 정보시스템 변경과 관련하여 전사에서 규정하는 변경 또는 유지보수 절차 및 정책이 존재하는지 확인한다. 2. 절차 및 정책의 재/개정 현황에 대해 질문하고 적시에 업데이트가 진행되고 있는지 확인한다.

리스크 기반의 IT 감사체계 구현은 한국남동발전의 IT 리스크를 식별하여 핵심위험을 선정하고, 위험과 관련된 통제활동 설계 및 운영을 검토하기 위한 프로그램 개발 단계로 진행되었다.

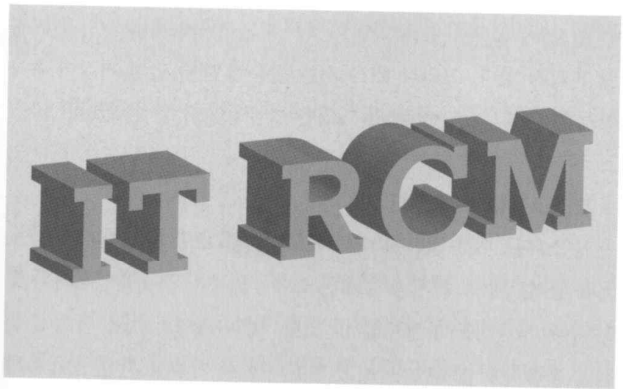
감사계획 수립 단계에서 감사 목적 · 범위에 따라 주요 이슈에 대한 IT RCM을 만들어야 한다. 또한 IT RCM 수립 단계에서 계량화가 가능하고 신뢰할 수 있으며 감사 목적과 이슈에 맞는 감사수행 절차를 마련해야 한다.

추진성과 및 향후계획

한국남동발전 감사실은 금번 IT 내부감사 체계 수립 및 IT RCM 개발의 유효성을 평가하고자 IT 검사역과 IT 감사 외부전문가가 공동으로 참여한 IT 내부감사를 시행하였다. 본 IT RCM을 기반으로 ICT, 정보보안 분야에 약 10일간의 특정감사를 시행하였고 IT 거버넌스, 정보보안, 시스템 개발, IT 변경관리, 데이터센터 운영, SAP 운영의 6개 감사대상 영역(대분류)에서 총 32개의 감사 지적사항을 도출하여 현업부서에 통보하였다.

이번에 마련된 IT 내부감사의 절차와 방법은 한국남동발전에 존재하는 IT 리스크에 대한 단순 적발과 지적이 아닌 한국남동발전만의 컨설팅 IT 감사 모델로 정착시키고 IT분야에 대한 자체 내부감사를 지속적으로 수행할 수 있도록 IT 내부감사 매뉴얼에 반영하였다.

금번 IT 내부감사 수행으로 아래와 같은 시사점을 도출하였다.



1. IT 감사는 업무 이해도 선행이 중요하며 IT 리스크 파악을 위해 예비감사 기간을 충분하게 두어야 한다. IT 환경에 대한 정확한 이해를 통해 고위험 감사대상 선정, 프로세스별 리스크 및 통제활동을 식별하여야 한다.
2. IT 부서의 현황을 가장 잘 아는 내부 IT 검사역의 사전 리스크 파악, Coordinator 역할이 중요하다. 그리고 IT 내부감사 수행 시 감사인별, 직급별 수행역할 분장을 적정하게 하여 감사 배경지식, 업무분야 등을 고려한 감사반을 구성해야 한다.
3. IT 내부감사 수행에 앞서 감사취지 및 필요성에 대한 피감부서의 공감대를 이끌어 내야 한다. IT 부서의 반발이나 자료 제출에 대한 의도적 회피를 방지하기 위해 사전에 IT 부서에 감사 목적을 이해시키려는 노력을 실시하고 피감부서 입장에서의 요구가 분석되어 IT 내부감사 계획 수립 시 이를 반영해야 한다.
4. IT 감사의 한계에 대해서도 보고서에 명시해야 한다. 보통은 정보에 대한 부적절한 접근, 정보화 과정에서의 적절한 문서화 부족, 결론을 도출하기 위한 분석과 조사의 객관성 부족이 그 한계이다. 감사자가 이러한 한계에 직면하게 되었을 때는 보고서에 기록하여야 한다.

IT 내부감사 체계를 성공적으로 도입하고 운영하기 위해서는 감사운영 및 감사 인력, 조직 전반에 미치는 영향을 검토하여 내부감사 부서의 감사방법에 대한 정비가 병행되어야 할 것이다. 각종 사이버 위협 등과 같은 IT 리스크는 끊임없이 변화하고 있으며 그 속도 또한 더욱 더 빨라지고 있으므로 이에 민첩하게 대응하고 내부감사자로서의 역할을 확립하기 위해 IT 내부감사 체계(전략, 조직, 프로세스, 도구) 수립과 이를 지속적으로 개발, 발전시키려는 노력이 뒷받침되어야 한다. 또한, IT 부서와의 신뢰 구축이 선행되어야 하며 이를 위해 IT 리스크에 대한 전문적인 지식을 갖추고 신뢰받는 조언자, 전문가가 되어야 한다.

한국남동발전은 리스크 기반의 IT 내부감사 체계를 수립하고 글로벌 선진 IT 감사기법을 도입함으로써 IT 내부감사 역량을 제고하고 효율적인 IT 내부감사 업무를 추진할 수 있는 기틀을 마련하였다. 이러한 체계 수립을 계기로 체계의 정교화 작업, 적기 업데이트, 적극적 활용 등으로 빠르게 변화하고 있는 IT 환경 및 IT 리스크에 적극 대응해 나아갈 것이다.