ARA(감사위험평가) 의 중요성

Danny M. Goldberg(CISA, CGEIT, CCSA, CIA, CPA) 는 국제적 기업 관리, 위험 관리 및 규정 준수 회사인 Sunera(www.sunera.com) 소속의 전문 개발 수행 파트너입니다. Sunera 에 입사하기 전 그는 자문 서비스 및 전문 개발 회사인 SOFT GRC를 창립했습니다. Goldberg는 5년 간 2 개 기업에서 CAE(chief audit executive)/감사 담당 이사를 역임한 경력을 포함해 15여년 간의 감사 업무를 수행해 왔습니다. 그는 BNA 세무 및 회계,내부 감사: 기본 원칙(회계 정책 및 절차 시리즈) 발행물의 공인 전문 해설가 겸 Sawyer의 내부 감사의 공동 저자로 유명한 저자이기도 합니다.

CAE(Chief Audit Executive, 최고감사책임자)라면 ARA(Audit Risk Assessment, 감사위험평가)의 중요성을 잘 압니다. 내부 감사의시작은 언제나 감사 위험 평가에서 출발하기 때문입니다. 이것은 감사 활동을 계획하고 해당 연도에 투입할 자원을 배치하기 위한 토대가 됩니다. 그러나 어려운 경제 시기엔 많은 감사 부서들은 수동적으로 변모해가며 전체 그림을 파악하는 데 어려움을 겪게 됩니다. 또한, 많은 감사부서들이 현실에 안주하며 일상적 업무 처리를 하는 경향이 있습니다. 내부 감사(IA) 부서는 ARA 와 유무형의 편익이 회사 및 부서에 영향을 미친다는 중요성을 간과해서는 안됩니다.

ARA에 대한 IIA 기준 및 관련 해석

IIA(Institute of Internal Auditors, 내부감사인협회) 기준은 IA 부서에 기본 원칙을 안내해줍니다. 여기에 요약한 그 기준들은 ARS의 중요성에 관해 분명합니다.

- **2000 내부 감사 활동 관리**—CAE는 조직에 가치를 더하는 것을 분명하게 하기 위해 내부감사 활동을 효과적으로 관리해야 합니다.
- **2010 계획 수립**—CAE는 조직의 목표와 일관된 내부 감사활동의 우선순위를 정하기 위해 위험 기반계획을 수립해야 합니다.
  - 해석: CAE는 위험기반계획을 개발할 책임이 있습니다. CAE는 다른 활동 혹은 조직의 부문을 위해 경영진들로 하여금 정해지는 위험 선호 레벨을 포함한 조직의 위험 관리 프레임워크를 고려합니다. 프레임워크가 없으면 CAE는 고위간부와 이사회와의 상의 후 그 위험에 그들의 자체적인 판단을 이용합니다.
  - 2010.A1—업무에 대한 내부 감사 활동 계획은 적어도 매년 행해지는 문서화된 위험평가를 기준으로 반드시 이루어져야 합니다. 선임 경영진 및 이사회가 제시한 의견은 이 프로세스에서 고려되어야 합니다.
  - 2010.A2—CAE는 내부 감사 의견 및 기타 결론을 위해 선임 경영진, 이사회 및 기타 이해관계자들이 기대한 내용들을 확인하고 고려해야 합니다.
- **2020 의사 전달 및 승인**—CAE는 내부 감사 활동 계획 및 중간에 변경된 내용 등 자원 요구 사항을 선임 경영진 및 이사회에 전달하고 이사회 및 경영진의 검토 및 승인을 받아야 합니다. CAE는 자원 제약이 미치는 영향에 대해서도 알려야 합니다.
- **2030 자원 관리**—CAE는 승인된 계획을 달성하기 위해 내부 감사 자원이 알맞고 충분하게, 그리고 효과적으로 배치되었는지 확인해야 합니다.

IIA 기준에 명시된 것처럼 감사 부서는 감사 위험 평가를 연 단위로 수행해야 합니다. 위험 기반의 우선순위는 기업의 목표와 일치해야 하지만 대다수의 CAE들이 종종 이를 간과하는 경향이 있습니다. 내부 감사는 객관적이고 독립된 요소이지만 양심 부재로 인한 결과는 위험이라는 인식을 가지고 조직 개선을 위한 방향으로 이루어져야 합니다.

기준 해석에 언급된 것처럼 감사 위험 평가는 경영진 및 감사 위원회가 제시하는 위험 선호에 의해 이루어집니다. 이 프로세스는 ERM(Enterprise Risk Management, 기업위험관리) 프로세스의 위험을 평가하는 ERA(Enterprise Risk Assessment, 기업위험평가)와 유사합니다.

ERM은 "기업 전체 및 전략 수립에 참여하고, 기업 목표 달성과 관련해 기업체에 영향을 미치는 이사회, 경영진 및 기타 담당 직원들로 구성된 단체의 영향을 받으며 단체에 영향을 줄 수 있는 잠재적 이벤트를 파악하고 위험 선호 범위 내에서 적절한 보장이 이루어지도록 위험을 관리하기 위해 고안"된 프로세스로 정의할 수 있습니다.[2] 이에 따라 내부 감사는 일반적으로 ERM 프로세스를 소유하는 것이 아니라 이 프로세스 전반에 걸쳐 관여한다고 할 수 있습니다. 내부 감사는 다음과 같은 방식으로 경영진 및 이사회/감사 위원회에 도움을 줍니다.

- 모니터링
- 검사
- 개선 사항 권고
- 평가
- 보고

또한 내부 감사는 인터뷰/설문조사를 통해 결과를 취합하고 위험을 순서화하는 것으로 기업 위험 평가에 큰 도움을 줄 수 있습니다. 이들이 집중하는 영역에는 약간의 차이가 있습니다. ERA는 기업 전체의 위험에 대해 전반적인 관점을 가진 반면 ARA는 감사할 수 있는 위험에 대해 초점을 둡니다. 예를 들어, ERA는 기업 전체의 성공에 장애가 될 수 있는 위험 영역에 초점을 둡니다. 위험의 많은 부분은 감사할 수 있는 영역이 아닙니다. 반면 감사할 수 있는 위험은 ARA를 통해 다뤄집니다. 단, 각각의 위험 평가에 IA가 관여하면 매우 많은 이점을 얻을 수 있습니다. 위험 평가를 통해 IA가 얻을 수 있는 이점은 다음과 같습니다.

- 여러 계층의 경영진에게 노출될 수 있는 가능성 증대
- 경영진과 친밀한 관계 형성 및 지속적 신뢰 구축
- 조직에 미치는 심각한 위험 및 기록되지 않거나, 문서화되지 않은 주요 위험에 관한 세부적 이해를 통해 조직에 진정한 가치 제공
- 조직의 목표 및 목적 달성을 위해 관리해야 하는 주요 위험 및 목표에 역량 집중

손실된 가치: ARA의 간과로 인한 위험

매년 이루어지는 공식적 위험 평가를 소중히 여기지 않는 내부 감사 기관은 ARA의 간과가 경영에 가져다 줄 수 있는 긍정적 영향과 엄청난 노출 효과를 무시합니다. 많은 경우 이것은 IA가 1년 내내 주요 담당 직원들과 함께 가장 심각하게 나누어야 할 사안이 될 수 있습니다. 또한 IA에 참여하는 직원 수가 많으면, 신뢰적인 관계를 형성할 수 있는 기회는 더 많아집니다. 신뢰 형성이 없으면 IA는 경영진과 IA 간 쌓인 벽을 무너뜨리고 조직 내 탄탄한 조언을 줄 수 있는 역할을 하기가 어려워질 것입니다. 조직 내 진정한 가치를 제공하려면 IA는 경영진과 친밀한 관계를 쌓아야 합니다. 조직내에서 존중받고 신뢰받는 감사 부서의 경우 필요에 따라 부서들을 지원해달라는 요청을 많이 받는 경향이 있습니다. 이것은 위험 평가 프로세스에서 얼굴을 대면하고 같이 참여했기 때문에 가능한 일입니다.

Enjoying this article?

- IT 감사 및 보증 가이드라인 G13 감사 계획 시 위험 평가 사용을 읽어보세요.

  www.isaca.org/guidelines

- IT 감사 및 보증과 관련된 도구 및 기술 P1 IS 위험 평가 측정 및 P5 위험 자체평가 관리를 읽어보세요.

  www.isaca.org/tools-techniques

- 지식센터에서 감사 기준 및 위험관리에 관한 주제로 토론하고 협업해보세요.

  www.isaca.org/knowledgecenter

글로벌 방위 서비스 제공업체의 CAE인 Shelby Faubion은 "IA는 조직 내 서비스 담당 부서 역할을 수행하면서 다른 서비스 제공업체와 같은 방식으로 내부 또는 외부 고객 모두에게 이러한 서비스를 제공해야 합니다. 고객은 이렇게 제공되는 서비스의 특성과 이러한 노력으로 얻을 수 있는 가치를 이해해야 합니다. IA 부서는 타당성을 유지하기 위해 CRM(Customer Relationship Management, 고객관계관리) 계획을 수립하고 명확히 정의된 책임을 부여하여 즉시 이행해야 합니다. CAE가 자사의 비즈니스 리더와 1년에 한 번씩 소통한다면 이 CAE는 실제로 비즈니스가 어떻게 돌아가는지 알 수 없을 것입니다. 오늘날 대다수의 조직이 자사의 전략을 재고하고, 조직에 새로운 위험이 될 수 있는 신규 시장 진입을 모색하고 있습니다. 현재 시장에서 생존하고 투쟁하는 기업들은 전략이 변화하는 것을 이미 알고 있을 것"이라고 말했습니다.

위험 평가가 없으면 IA는 타당성을 잃어버릴 위험에 처할 것입니다. 조직이 신규 시장 진입을 모색하든지, 소셜 미디어, 클라우드 등의 신기술을 활용하든지, 자사의 비즈니스 포트폴리오를 조직적 또는 비조직적으로 확대하든지 상관없이 IA는 조직이 관련 위험에 따른 의미를 파악하고 준비할 수 있게 돕는 역할을 담당해야 합니다. 궁극적으로 IA가 이러한 방식이 기업의 목적 및 전략적 목표와 관련하여 어떻게 작동하는 지 효과적이고 분명하게 표현할 수 없으면, 이는 기업에 이 타당성을 잃게할 수도 있습니다.

마지막으로, 많은 내부 감사 부서은 감사 기간에 늘어난 감사 싸이클에 갇히게 됩니다. 감사 싸이클은 매우 길 수 있고 여러 면에서 매우 고된 일일 수 있습니다. 또한, 감사 후속조치 이후에도 결코 끝나지 않습니다. 조직 내부에 진정한 조언자가 되기 위해 지속적 모니터링과 권고는 필수적입니다. 반면, 끝없는 감사 싸이클에 휘말리기는 쉽습니다. 감사부서가 1년의 대부분을 바쁘게 보내면서 4분기는 다가오고, 또 ARA를 완료하기 위해 해야하는 많은 감사가 기다리고 있습니다. 결과적으로 연말이 되면 전년도 ARA 프로세스가 쌓여지고 또 재생산됩니다.

그러나, 공식적으로 ARA를 수행하는 것은 감사를 진정한 위험 영역 및 조직의 목표에 초점을 맞춰 활동할 수 있게 도와줍니다. 알려진 위험 노출과 관련되어 모든 부분으로부터 공감대가 형성된 위험을 이해하는 것은 감사활동이 경영진의 관점과 조직에 도움이 되는 방향으로 나아갈 수 있게 도움을 줍니다.

끝없는 감사 계획과의 전쟁

많은 내부 감사 담당자들은 감사 일정을 전적으로 통제할 수 없다는 본질적인 믿음으로 인해 매년 위험평가를 수행하지 않습니다. 회사들은 작년 계획을 다시 쓰거나, 조직의 실제 위험보다 활용 가능한 공수를 기반으로 예산을 세우는 경향이 있습니다. 게다가, 조직의 위험보다 공수를 기반으로 한 예산을 책정하는 행위 자체가 감사부서의 책무가 아닐 때도 있습니다. 감사라는 것은 위험과 조직이 노출되는 것에 대해서 개요를 말하고, 감사 위원회가 추가적으로 필요한 자원들을 결정할 수 있게 하는 것입니다. 단지 가용한 공수를 기준으로 감사 예산을 배정했다면 감사 위원회는 조직에 미치는 위험 및 언급되지 않는 위험 영역이 무엇인지 전혀 파악할 수 없을 것입니다.

연말에 감사 부서가 스트레스를 피할 수 있게 해주는 한가지 방법은 조직에 미치는 위험을 토대로 감사 계획을 수립하는 일 외에 유연하게 시간을 조정할 수 있게 근무시간 자유선택제를 도입하는 것입니다. 근무시간 자유선택제는 감사 계획에서 유연성을 만들어주는 감사 스케쥴의 한 부분입니다. 감사부서는 계획이 바뀌지 않는다면 그에 따른 세부 감사들을 확인해야 합니다. 그렇지만 대부분 조직들의 계획은 항상 바뀝니다. 예를 들어, 사기 조사는 원래 계획을 바꿔야 하는 특별한 요구 감사들이 요청되기 때문에 계획하기가 어렵습니다.

마지막으로 IIA 기준의 2010.A에 따르면 위험 평가는 최소 매년 이루어져야 합니다. 그러나, 오늘날처럼 침체된 경제 여건에서 위험 평가를 연 단위로 수행하는 것만으로도 충분할지는 의문으로 남습니다. 많은 조직들은 지속적 위험 평가를 강화하는 데 관여해 왔으며 이러한 단계에서 감사 활동을 통해 일년 내내 단일 프로세스 또는 시스템 내에서 트렌드와 비교 항목을 검토하여 전사적 위험 레벨을 파악하고 평가할 수 있었습니다. 이러한 예는 과거의 성과 및 비즈니스 시스템과 결과를 평가했을 때 나타납니다. Faubion에 따르면 진행 중인 비즈니스 및 컴플라이언스 척도(이윤폭, 금리 및 세금 지불 이전의 수익(EBIT: earnings before interest and taxes), 승률, 오픈 포지션, DSO(days sales outstanding), 고객 클레임 등)가 보편화됨에 따라 문제를 조기에 파악할 수 있습니다. IA에 의해 도구로 사용되는 진행 중인 위험 평가는 IA가 위험 지표에 따라 적극적으로 대처하고 기업이 노출을 최소화할 수 있게 도움을 줄 수 있습니다. 요약하면 위험 평가는 위험 지표를 적극적으로 활용하여 기업 내 한정된 IA 직원의 우선순위를 정할 수 있게 해주는 소중한 도구입니다.

실질적 관점에서 IA는 정밀도에 상관없이 위험을 모니터링 하기 위해 CAAT(Computer-Assisted Audit Techniques)를 사용합니다. 이것은 주요 지표의 모니터링을 수반하여 조직의 위험 프로파일은 물론 ARA 및 감사 계획에도 연이어 변화를 줄 수 있습니다. 감사 계획 수립 시 충분한 감사 기간을 할당함으로써 효율적이고 효과적인 방식으로 계획을 수정하면서 부서의 유연성을 보완할 수 있습니다.

결론

내부 감사 담당자는 내부 ARA의 중요성과 연 단위로 이루어지는 공식적 프로세스의 완수를 과소평가해서는 안됩니다. 경영진과의 노출 및 관계 개발 기회는 계속되고, 거듭되는 재정난 시기에도 중요 조직위험 영역 및 목표의 상위에 ARA를 놓는 것은 지속적인 가치를 추가하기 위한 중요 단계 중 하나입니다. 이러한 이점과 상관없이 ARA의 수행이 연 단위로 이루어진다면 정확한 규모로 감사를 수행하고 부서가 조직의 목표 및 목적을 달성할 수 있습니다.

각주

[1] IIA(국제내부감사인협회), *International Standards for the Professional Practice of Internal Auditing (Standards),* January 2011, *www.theiia.org/guidance/standards-and-guidance/ippf/standards/*

[2] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management—Integrated Framework,* 2004