제3자(The Third-Party) 주제별 요건을 활용한 리스크 관리

IIA의 새로운 제3자(Third-Party) 주제별 요건은 조직이 제3자 거버넌스 및 통제 프레임워크를 어떻게 설계하고 구현하는지를 평가하기 위한 구조적이고 일관된 접근방식을 제공한다. 기업들이 클라우드 인프라, 소프트웨어 개발, 물류, 콜센터에 이르기까지 핵심 기능을 외부에 위탁함에 따라, 조직의 위험 범위는 내부 운영을 넘어 지속적으로 확대되고 있다.

세계내부감사인협회(The IIA)의 새로운 「제3자(Third-Party) 주제별 요건(Topical Requirement)」은 제3자 거버넌스, 리스크 관리 및 통제 프로세스의 설계와 구현을 평가하기 위한 일관되고 포괄적인 접근방식을 확립한다. 새로운 주제별 요건은 지정학적 불확실성, 무역 및 공급망 혼란, 그리고 운영·평판·컴플라이언스 리스크를 초래하는 기타 요인과 관련된 제3자 리스크가 증가하는 시점에 도입되었다.

Laurent Berliner

국제내부감사표준위원회(International Internal Audit Standards Board) 위원인 Laurent Berliner는 오늘날 조직이 실제로 네트워크처럼 운영되고 있다고 말한다. 클라우드 인프라, 소프트웨어 개발, 콜센터, 물류, 심지어 핵심 재무 또는 인사 프로세스와 같은 영역까지도 빈번하게 아웃소싱되고 있다. 그는 "이는 속도와 효율성을 가져오지만, 동시에 리스크 범위를 파트너, 하도급업체, 그리고 그들의 공급업체까지 확장시키게 된다"고 말한다.

실제 리스크 사례

이 주제별 요건은 제3자와 관련된 여러 리스크 사례를 제시하고 있으며, 그 예시는 다음과 같다.

Uday Gulvadi

사이버보안 리스크(Cybersecurity risk)

아웃소싱 관계에서 주된 조직(primary organization)은 서비스 제공업체에 개인식별정보(PII)를 포함한 고객 데이터를 제공할 수 있다. Stout의 규제준수·결제·금융범죄(Regulatory Compliance, Payments, and Financial Crimes) 부문 전무이사인 Uday Gulvadi는 "데이터 유출의 규모와 정교함이 증가하고 있다는 사실은 이러한 정보가 위협 행위자와 해커들에게 얼마나 가치 있는지를 보여준다"고 말한다. 그는 이어 "조직은 데이터 보호 및 개인정보보호, 사이버보안 리스크 예방, 사고 대응과 관련된 강력한 통제를 구축해야 한다"고 설명한다.

많은 사고 사례가 보여주듯이, 서비스 제공업체에서 발생한 데이터 유출이나 랜섬웨어 공격은 주된 조직의 평판과 고객 및 기타 비즈니스 파트너와 구축해온 신뢰에 상당한 영향을 미칠 수 있다. 또한 침해 범위를 파악하고, 어떤 기록이 탈취

되었는지를 식별하며, 몸값(ransom) 지급 비용을 부담하는 데에도 막대한 비용이 들 수 있다고 Gulvadi는 지적한다. 그는 "AI의 출현은 리스크를 더욱 악화시켰으며, 딥페이크 기반 공격의 확산은 새로운 차원의 복잡성을 더하고 있다"고 말한다.

그 결과, 내부감사인은 제3자 감사 업무 수행 시 관련 리스크를 평가해야 한다. 여기에는 고객 정보에 접근할 수 있는 모든 핵심 공급업체를 목록화하고 식별하기 위한 통제를 평가하는 것이 포함된다. Gulvadi에 따르면, 내부감사는 서비스 제공업체가 강력한 사이버보안 방어 통제와 사고 대응 통제를 통해 데이터를 보호하고 있는지를 검증·확인하기 위해 조직의 통제를 테스트해야 한다.

제3자의 정의(Defining a Third Party)

제3자(third party)는 벤더, 공급업체, 계약업체, 하도급업체, 아웃소싱 서비스 제공업체, 기타 기관 및 컨설턴트를 의미한다. 이 용어에는 제3자와 그 하도급업체 간의 계약도 포함되며, 이러한 하도급업체는 흔히 "다운스트림(downstream)" 하도급업체로 알려져 있다.

—「Third-Party Topical Requirement」

재무적 리스크(Financial risk)

Berliner는 공급업체가 자금 조달에 실패하거나 지급불능 상태에 직면하거나 갑작스러운 가격 인상을 단행할 수 있으며, 이로 인해 비용이 많이 드는 대체가 필요해지고 계약 조직(hiring organization)의 예산이 불안정해질 수 있다고 설명한다. Gulvadi는 조직이 장기적인 프로세스 아웃소싱 또는 기술 지원 계약에 관여하고 있을 때 이러한 문제가 특히 중요하다고 말한다.

"계약 기간 전반에 걸쳐 제3자의 재무 건전성과 지속적인 운영 역량을 평가하는 것은 매우 중요하다"고 그는 설명한다. 중대한 의존성이 존재하는 경우 조직은 고품질 서비스를 지속적으로 제공할 수 없는 벤더로부터 스스로를 보호해야 한다. 그는 내부감사인이 감사된 재무제표 또는 기타 수단을 활용하여 핵심 벤더의 재무 건전성을 검증·확인하는 것과 관련된 리스크 및 통제를 평가해야 한다고 말한다.

Verizon의 2025 Data Breach Investigations Report에 따르면, 최근 데이터 유출 사고의 30%가 제3자 관여와 연관되어 있었으며, 이는 전년도 비율의 두 배에 해당한다.

운영 리스크

중요한 아웃소싱 프로세스나 플랫폼이 실패할 경우 서비스 제공, 규제 보고 또는 고객 경험이 중단될 수 있다. Berliner는 급여 지급일에 발생하는 급여 서비스 제공업체의 장애나 제품 출시 중 발생하는 데이터센터 장애 등을 그 예로 제시한다.

컴플라이언스 리스크

공급업체가 개인정보를 부적절하게 처리하거나 제재, 반부패 규정 또는 지속가능성 규제를 위반할 경우 조직은 공동 책임을 지게 되고 리스크에 노출될 수 있다.

법적 리스크

제3자가 법률을 위반할 경우, 해당 업체와 거래하는 조직 역시 소송에 휘말리게 되어 법적 제재나 벌금에 직면할 수 있다.

평판 리스크: 핵심 고려사항

Sherry Rodriguez

이 주제별 요건은 평판 리스크를 특별한 주의가 필요한 핵심 범주로 강조하고 있다. 선도적인 금융기관의 글로벌 보증(Global Assurance) 부문 부사장인 Sherry Rodriguez는 조직의 평판이 제3자의 사이버보안, 운영, 재무, 컴플라이언스 또는 법적 취약성으로 인해 부정적인 영향을 받을 수 있다고 강조한다.

Rodriguez는 "내 관점에서 평판 리스크는 이러한 모든 차원을 포괄한다"고 설명한다. 그는 이어 "우리가 제3자를 직접 통제하지는 못하더라도, 그들은 종종 우리를 대신하여 행동한다"며 "평판은 우리의 가장 가치 있는 자산이므로, 우리는 이를 정교하게 보호해야 한다"고 말한다.

이를 위해 내부감사인은 제3자의 운영 및 공급망 내 리스크를 평가하기 위해 선제적으로 제3자와 협력해야 한다. Rodriguez는 감사인이 조직 내부에서도 전략적 • 평판적 노출 리스크와 주제별 요건의 세부 내용에 대한 부서 간 인식을 확보하도록 해야 한다고 조언한다.

그는 이러한 인식이 컴플라이언스, 법무, 재무와 같은 전통적인 리스크 중심 부서를 넘어, 제3자와 상호작용하는 모든 기능 부문까지 확대되어야 한다고 강조한다. 그는 "모든 사람이 리스크를 이해할 때 내부감사인은 자신의 책임을 보다 효과적으로 수행할 수 있는 위치에 서게 된다"고 말한다.

Berliner는 주제별 요건에서 언급된 리스크들이 새로운 것은 아니라고 지적한다. "그러나 현대 공급망의 속도와 상호연결성 때문에 단일 제3자 공급업체의 실패가 여러 리스크 범주, 경우에 따라서는 모든 리스크 범주에 걸쳐 빠르게 연쇄적으로 확산될 수 있다"고 그는 말한다.

거버넌스, 리스크 관리 및 통제 프로세스

Berliner에 따르면, 내부감사인이 거버넌스, 리스크 관리 및 통제를 평가하고 이에 대한 보증을 제공할 때 제기해야 할 핵심 질문은 다음과 같다.

- **거버넌스**: 문서화된 아웃소싱 전략이 존재하는가? 해당 전략은 명확한 규정을 포함하고, 역할을 명확히 하기 위해 3선모델(Three Lines Model)을 반영해야 한다. Gulvadi는 내부감사인이 이사회 차원의 감독 품질도 평가해야 한다고 지적한다. 왜냐하면 거버넌스와 감독의 취약성은 조직에 막대한 리스크를 초래할 수 있기 때문이다.
- **리스크 관리**: 제3자의 선정, 실사, 정기 평가를 위한 표준화된 리스크 기반 프로세스가 존재하는가? 해당 프로세스에는 관련

IPPF의 주제별 요건 (Topical Requirements)

주제별 요건은 The IIA의 국제직무수행방안(IPPF®)를 구성하는 핵심 요소 중 하나이며, 여기에는 국제내부감사표준(Global Internal Audit Standards™)과 국제지침(Global Guidance)도 함께 포함된다. 주제별 요건은 감사 계획에 특정 리스크 영역을 반드시 포함하도록 요구하지는 않지만, 내부감사인이 전 세계 조직에 영향을 미치고 대부분의 감사 계획에 포함될 가능성이 높은 핵심 리스크 영역을 평가할 때 활용할 수 있는 기본 요건을 제공한다.

리스크의 규모에 따라 상위 권한 수준으로 보고해야 하는 시점에 대한 명확한 기준이 포함되어야 한다. 또한 핵심 벤더를 식별하고, 이들이 강화된 모니터링 대상인지 여부를 규정해야 한다. Berliner는 "이는 건전하고 빈틈없는 리스크 관리 시스템이 존재하는지를 보장하는 것에 관한 문제"라고 말한다. Gulvadi는 내부감사인이 리스크 간 상호연결성도 인식해야 한다고 말한다. 그는 "많은 기업이 의존하는 주요 공급업체 한 곳에서 실패가 발생할 경우 도미노 효과가 발생할 수 있다"고 설명한다.

- **통제 프로세스**: 실사는 중요도에 비례하여 수행되는가? 그렇지 않다면 리스크는 적절한 수준의 주의를 받지 못하게 된다. 동시에 Berliner에 따르면 계약 조항(배상책임, 데이터 보안, 감사 권한 및 종료 계획)은 일관되고 지속적으로 적용되어야 한다. 그는 성과 및 리스크 지표는 증거 기반이어야 하며, 계약 종료(offboarding) 체크리스트는 시스템에 대한 유령 접근이나 데이터 유출을 방지해야 한다고 말한다.

주제별 요건 준수

주제별 요건에 대한 준수는 검증 서비스(assurance services)의 경우 의무사항이며, 자문 서비스(advisory services)의 경우 권고사항이다. 다음 중 하나에 해당하는 경우 해당 주제별 요건이 적용된다.

- 내부감사 계획에 포함된 감사 업무의 주제인 경우.
- 감사 업무 수행 중 식별된 경우.
- 최초 내부감사 계획에는 포함되지 않았으나 요청된 감사 업무의 주제인 경우.

주제별 요건의 각 요구사항에 대해 적용 가능성이 평가되었다는 증거는 문서화되어 보관되어야 한다.

— Third-Party Topical Requirement

내부감사의 중대한 역할

제3자 리스크에 대응함에 있어 Berliner는 내부감사인을 건물 검사관에 비유한다. 건물 검사관이 "주택 본체뿐만 아니라 전체 단지 전체에 대해" 배선, 비상구, 보험 증명서 및 기타 핵심 안전장치를 점검하는 것과 같다는 의미이다. 그는 보증 제공에는 다음 사항을 확인하는 것이 포함된다고 말한다.

- 완전하고 리스크 등급화된 제3자 목록(third-party inventory)이 존재하는지 여부.
- 계약상 보호장치와 지속적 모니터링 등의 영역에서 실사가 수행되었는지 여부.
- 이러한 프로세스가 서비스의 중요도에 따라 조정(scale)되고 있는지 여부.
- 계약 종료, 데이터 반환 및 파기, 접근권 철회가 온보딩(onboarding)만큼 엄격하게 수행되고 있는지 여부.

Gulvadi는 대부분의 조직이 조직 차원의 제3자 리스크 관리를 위한 별도의 내부감사 업무를 수행하고 있을 가능성이 높지만, 많은 사업부 또는 기능 부문이 제3자에 중대하거나 핵심적인 의존성을 가지고 있을 수 있다고 지적한다. 그 결과 내부감사는 이러한 사업부 및 기능 부문에 대한 감사에서도 주제별 요건을 적용하는 것을 고려해야 한다. 그는 "요구사항 범위에서 제외되는 사항은 반드시 철저히 문서화되어야 한다"고 말한다.

선도적인 금융기관의 글로벌 보증 부문 부사장인 Sherry Rodriguez는 내부감사인이 먼저 제3자 리스크와 관련된 기존 정책 및 절차를 검토하고, 필요 시 이를 주제별 요건에 부합하도록 조정해야 한다고 조언한다. 또한 벤더들이 유사한 정책 및 절차를 준수하고 있는지를 확인하고, 감사 테스트와 감사 계획을 주제별 요건에 맞추어 정렬해야 한다고 말한다.

자문 역할 측면에서 내부감사인은 이사회와 경영진이 공급망 사고 대응 계획을 스트레스 테스트할 수 있도록 지원할 수도 있다. 예를 들어, 모의훈련을 실시하고 침해 통지, 하도급업체 흐름 조항, 지속가능성 의무와 같은 핵심 계약 조항을 실제 운영에 적용하도록 지원할 수 있다.

가장 과소평가되는 공급망 사이버 리스크 10가지

1. 섀도우 IT(Shadow IT): 보이지 않는 침투 지점
2. 오픈소스 의존성: 트로이 목마 문제
3. 해외 의존성과 관할권 영향력
4. 공급업체 개발 환경에 대한 지속적 통합/지속적 배포(CI/CD) 파이프라인 공격
5. 물리적 인프라 공격 및 하드웨어 백도어
6. 핵심 공급업체 집중: 단일 실패 지점
7. 클라우드 공급망의 복잡성
8. 규제 및 지정학적 변동성
9. 공급망 전반에 걸친 분절된 사고 대응
10. AI 기반 사회공학 공격 및 딥페이크

출처: Risk Ledger

선제적 태세

Berliner에 따르면, 조직 전반에 걸쳐 제3자 프로그램을 처음부터 끝까지(end-to-end) 매핑하고 이를 리스크 등급화(risk tier)하는 것이 매우 중요하다. 이후 내부감사인은 제3자 주제별 요건을 청사진으로 활용하여 "다음 공급망 사고가 헤드라인을 장식하기 전에" 거버넌스, 리스크 관리 및 통제를 테스트할 수 있다고 그는 말한다.
Berliner는 위기가 발생하기 전에 시나리오 리허설, 계약 관리(contract hygiene), 그리고 모니터링 지표에 시간을 투자하는 것이 충분한 가치가 있다고 말한다. 그는 "이러한 선제적 태세야말로 제3자 리스크를 잘 극복하는 조직과 잘못된 이유로 언론의 1면을 장식하는 조직을 진정으로 구분짓는 요소"라고 강조한다.