제 3 자

Topical Requirement

주제별 요건

The Institute of
Internal Auditors

제 3 자 주제별 요건

국제내부감사직무수행체계(IPPF)®는 국제내부감사표준(Global Internal Audit Standards)™, 주제별 요건(Topical Requirements), 그리고 국제지침(Global Guidance)으로 구성된다. 주제별 요건은 국제내부감사표준과 함께 사용되며, 내부감사 실무의 필수요건을 규정하는 권위 있는 기준을 제공한다.

주제별 요건은 특정 리스크 분야를 감사하기 위한 최소 기준을 설정함으로써 내부감사인이 준수해야 할 명확한 기대치를 제시한다. 다만, 각 조직의 리스크 프로파일에 따라 내부감사인은 필요 시 해당 주제와 관련된 추가적인 사항을 고려해야 할 수도 있다.

주제별 요건을 준수하면 내부감사 서비스 수행의 일관성이 높아지고, 내부감사 서비스와 결과의 품질 및 신뢰성이 향상된다. 궁극적으로 주제별 요건은 내부감사직무의 전문성을 높인다.

내부감사인은 국제내부감사표준에 부합하도록 주제별 요건을 적용해야 한다. 주제별 요건의 준수는 검증(assurance) 서비스에는 필수이며, 자문(advisory) 서비스에는 권장사항이다. 주제별 요건은 해당 주제가 다음에 해당할 때 적용된다:

1. 내부감사 계획에 포함된 감사업무 주제
2. 감사업무 수행 중 식별된 주제
3. 최초 내부감사 계획에 포함되지 않은 요청된 감사업무 주제

주제별 요건의 각 요건이 적용 가능한지 평가한 증거는 반드시 문서화하여 보관되어야 한다. 모든 개별 요건이 모든 감사업무에 적용되는 것은 아니며, 만약 특정 요건이 제외되는 경우에는 그 합리적 근거가 문서화되어 보관되어야 한다. 주제별 요건의 준수는 필수적이며, 이는 감사품질 평가 시 검토 대상이 된다.

제 3 자

제 3 자란 조직("원청조직")이 제품 또는 서비스를 확보하기 위해 비즈니스 관계를 수립하는 외부의 개인, 그룹 또는 법인을 말한다. 이 관계는 계약, 합의 또는 기타 수단을 통해 공식화될 수 있다. 본 주제별 요건에서는 "제 3 자"라는 용어를 판매업체(vendors), 공급업체(suppliers), 계약자, 하도급업체, 아웃소싱 서비스 제공자, 기타 대행사 및 컨설턴트를 지칭하는 데 사용한다. 이 용어에는 제 3 자와 그 하도급업체 간의 계약(재하도급(하위 하도급))도 포함된다.

이 주제별 요건은 내부감사 기능이 제 3 자 및/또는 원청조직과 제 3 자 간의 계약 또는 합의에 의해 허용된 하위 하도급 관계(제 4 자 또는 그 이상의 하위 단계 포함)에 대해 검증 업무를 수행할 때 적용된다. 내부감사인은 아래 리스크 관리 섹션에서 설명된 바와 같이 리스크에 따라 제 3 자 및 하위 단계 당사자의 우선순위를 정해야 한다. 내부감사인은 리스크 평가 결과에 따라 모든 요건을 적용해야 하며, 제외 사항은 반드시 문서화해야 한다.

©2025, The Institute of Internal Auditors. All rights reserved. For individual use only.

본 주제별 요건은 규제기관, 대리인, 수탁자/이사회 구성원과 같은 원청조직과의 간접적인 외부 관계, 이해관계, 또는 관여나 임직원과 같은 내부 관계는 대상으로 하지 않는다.

'제 3 자(third party)'라는 용어는 산업이나 상황에 따라 정의와 사용 방식이 달라질 수 있다. 내부감사인은 이러한 점을 고려하여 유연하게 접근해야 하며, 원청조직이 정한 제 3 자의 정의에 맞추어 주제별 요건을 적용하기 위해 자신의 전문적 판단을 활용해야 한다.

원청조직(제 3 자 계약을 체결하는 조직)은 하나 이상의 목표 달성을 위해 제 3 자를 활용하는 경우에도, 목표 달성과 관련된 리스크에 대한 책임을 여전히 보유한다. 제 3 자와의 거래에는 반드시 식별, 평가 및 관리되어야 할 리스크가 수반된다. 이러한 리스크는 본 주제별 요건에서 제시하는 바와 같이 적절한 거버넌스, 리스크 관리 및 통제 절차를 통해 관리하여야 한다. 제 3 자가 계약상 의무를 이행하지 않거나, 비윤리적 행위에 관여하거나, 영업상 중단을 겪는 경우, 원청조직은 그로 인한 불이익을 입을 수 있다. 제 3 자와 관련된 리스크의 유형과 예시는 다음과 같다:

- 전략 리스크: 조직의 미션 및/또는 상위 목표 달성 역량, 또는 인수합병 영향 관리 역량 등
- 평판 리스크: 환경 훼손 또는 원청조직과 고객, 거래처, 이해관계자 간의 관계 및 신뢰 손상 등
- 윤리 리스크: 진실성 결여, 이해상충, 리베이트, 부패 등
- 운영 리스크: 물리적 보안 및 정보 보안, 내부자 리스크, 서비스 중단, 목표 미달성 등
- 재무 리스크: 제 3 자의 지급불능 및 사기 등
- 컴플라이언스 리스크: 해당 지역, 국가 및 국제 규제 요건 미준수
- 사이버보안 및 기타 데이터 보호 리스크: 민감 데이터의 침해 및 유출 등
- 정보기술 리스크: 핵심 운영을 지원하는 서비스 부족 등
- 법률 리스크: 이해상충, 분쟁, 계약 위반으로 인한 소송 등
- 지속가능성 리스크: 환경 · 사회 · 거버넌스 관련 리스크. 예를 들어 조직이 자연환경에 미치는 영향 관련 리스크, 지역사회와의 상호작용 관련 리스크 등
- 지정학적 리스크: 무역 분쟁/제재 및 정치적 불안정 등

제 3 자 거래 생애주기는 선정, 계약, 거래 개시 절차, 모니터링, 거래 종료 절차로 구성된다. 내부감사인은 거버넌스, 리스크 관리 및 통제 절차 요건을 평가함에 있어 이러한 단계를 고려하여야 한다.

©2025, The Institute of Internal Auditors. All rights reserved. For individual use only.

제 3 자 거버넌스, 리스크 관리 및 통제 프로세스 평가 및 검토

본 주제별 요건은 제 3 자 거버넌스, 리스크 관리 및 통제 프로세스의 설계 및 이행을 평가하기 위한 일관되고 포괄적인 접근방식을 제공한다. 이 요건은 평가를 위한 최소한의 기준을 제시한다.

거버넌스

요건:

내부감사인은 이사회 감독을 포함하여 원청조직의 제 3 자 거버넌스와 관련된 다음 측면을 반드시 평가해야 한다:

A. 제 3 자와 계약을 체결할지 여부를 결정하기 위한 공식적인 접근방식이 수립·이행되고 정기적으로 검토된다. 이 접근방식에는 제품이나 서비스 제공을 통해 목표를 달성하는 데 필요한 자원과 가용 자원을 정의하고 평가하기 위한 적절한 기준이 포함된다.

B. 제 3 자 거래 생애주기 전반에 걸쳐 제 3 자와의 관계 및 관련 리스크를 정의·평가·관리하기 위한 정책과 절차가 수립되어 있다. 이러한 정책과 절차는 관련 규제 요건에 부합하며, 통제 환경을 강화하기 위해 정기적으로 검토되고 업데이트된다.

C. 조직의 제 3 자 관리 역할과 책임이 명확히 정의되어 있으며, 여기에 제 3 자를 선정·지시·관리·커뮤니케이션·모니터링하는 주체와 제 3 자 활동에 대하여 통보받아야 하는 주체가 포함되어 있다. 또한 제 3 자 관련 역할과 책임이 부여된 인원이 적절한 역량을 보유하도록 보장하는 절차가 마련되어 있다.

D. 관련 이해관계자와의 커뮤니케이션을 위한 프로토콜이 정의되어 있으며, 이는 우선순위가 지정된 제 3 자의 성과, 리스크 및 컴플라이언스(특히 법령 및 규정 위반)에 대한 현황을 적시에 보고하는 내용을 포함하고 있다. 제 3 자의 우선순위는 리스크에 따라 결정된다. 관련 이해관계자에는 이사회, 최고경영진, 구매부서, 운영부서, 리스크 관리부서, 컴플라이언스부서, 법무부서, 정보기술부서, 정보보안부서, 인사부서등이 포함될 수 있다.

리스크 관리

요건:

내부감사인은 조직의 제 3 자 리스크 관리에 대한 다음 측면을 반드시 평가해야 한다.

A. 제 3 자 및 그 서비스의 리스크 관리를 위한 프로세스는 표준화되고 포괄적이며, 명확히 정의된 역할과 책임을 포함하고, 조직과 관련된 주요 리스크(예: 전략, 평판, 윤리, 운영, 재무, 컴플라이언스, 사이버보안, 정보기술, 법적, 지속가능성, 지정학적 리스크)를 충분히 반영하고 있다. 프로세스 준수 여부는 모니터링되며, 모든 일탈사항에 대해 시정조치가 이행된다.

©2025, The Institute of Internal Auditors. All rights reserved. For individual use only.

B. 제 3 자와 관련된 리스크는 거래 생애주기 전반에 걸쳐 정기적으로 식별·평가된다. 리스크 평가는 제 3 자, 나아가 하위 협력업체까지 포함하여 순위를 매기고 우선순위를 지정하는 데 활용된다. 리스크 대응 역시 순위를 매기고 우선순위를 부여한다. 리스크 평가는 주기적으로 검토되고 업데이트된다.

C. 리스크 대응은 순위에 상응하여 적절하고 정확하다. 리스크 대응은 필요에 따라 이행, 검토, 승인, 모니터링, 평가 및 조정된다.

D. 제 3 자로부터 발생하는 문제를 관리하고 필요시 상향보고하기 위한 프로세스가 마련되어 있으며, 이를 통해 결과에 대한 책임성을 확보하고 계약 또는 기타 합의 조건의 달성 가능성을 높인다. 제 3 자가 상향보고된 고려사항에 대응하지 않을 경우, 경영진이 해당 사업관계의 지속과 관련된 리스크를 평가하고 적절한 추가 조치, 시정조치 또는 계약 종료를 추진할 수 있는 프로세스가 마련되어 있다.

통제

요건:

내부감사인은 리스크를 토대로 우선순위가 정해진 제 3 자에 대한 다음의 통제 항목을 반드시 평가해야 한다. 평가에는 조직의 제 3 자에 대한 지속적인 평가 및 모니터링을 위한 관리 프로세스가 포함되어야 한다.

A. 제 3 자를 발굴하고 선정하기 위한 견고한 실사 (due diligence) 절차가 마련되어 있으며, 제 3 자와의 관계 필요성과 성격을 설명하고 정당화하는 비즈니스 타당성 검토서 또는 기타 관련 문서가 문서화되고 승인된다.

B. 계약 및 승인은 조직의 제 3 자 리스크 관리 정책과 절차에 따라 수행되며, 조직 내 관련 부서 간의 협업을 포함한다.

C. 최종 계약 또는 합의는 모든 관련 이해관계자(법무 및 컴플라이언스 포함)의 검토 및 승인을 거쳐, 양 당사자의 권한이 있는 개인에 의해 서명되고 안전하게 보관된다. 각 계약마다 계약 관리자 또는 관리 담당자가 책임자로 배정된다.

D. 중앙집중식 계약 관리 시스템 등을 통해 모든 제 3 자 관계에 대한 정확하고 완전하며 최신 상태의 목록을 유지관리한다.

E. 제 3 자가 계약 또는 합의 조건을 충실히 이행할 수 있도록 하기 위하여, 문서화된 거래 개시 절차가 마련되어 준수된다.

F. 제 3 자가 거래 생애주기 전반에 걸쳐 계약 또는 합의 조건에 따라 이행하고 있는지, 그리고 계약상 의무를 충실히 수행하고 있는지를 평가하기 위한 지속적 모니터링 프로세스가 마련되어 있다. 이 프로세스에는 제 3 자가 제공하는 정보의 신뢰성을 검증하는 것과 성과를 주기적으로, 그리고 합의 내용이 변경될 때마다 재평가하는 과정이 포함되어 있다.

©2025, The Institute of Internal Auditors. All rights reserved. For individual use only.

G. 제 3 자가 기대 수준을 충족하지 못하거나 증가된 또는 예기치 못한 리스크를 초래하는 경우 시정 조치를 개시하기 위한 프로토콜이 마련되어 있다. 이 프로토콜에는 사건의 심각도에 따른 보고 및 조치 단계의 격상, 사후 검토의 수행, 사건의 근본 원인 분석이 포함되어 있다.

H. 계약 만료 및 갱신 날짜가 모니터링되며, 필요 시 갱신 조치가 취해진다.

I. 계약 요건에 포함된 일정과 기대사항이 적절히 반영되도록 하기 위하여, 문서화된 거래 종료 계획을 수립하고 이행한다. 이 프로세스에는 다음 방법이 포함된다:

- 제 3 자와의 계약 종료 방법
- 필요시 제 3 자 대체 방법
- 제 3 자가 보관 중인 조직의 민감 데이터에 대한 관리권한의 재할당 및 반환 또는 파기 방법
- 제 3 자의 시스템, 도구 및 시설 접근 권한 회수 방법

About The Institute of Internal Auditors

The IIA is an international professional association that serves more than 265,000 global members and has awarded more than 200,000 Certified Internal Auditor® (CIA®) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

Copyright

© 2025 The Institute of Internal Auditors, Inc. All rights reserved. For permission to reproduce, please contact copyright@theiia.org.

September 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401 Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101