



The Institute of
**Internal
Auditors**

Global Internal Audit Standards

2023 Draft for Public Comment

국제내부감사표준 – 2023 의견조사용 초안

목차

국제내부감사표준 소개.....	4
용어집	6
내부감사활동의 목적.....	11
영역 II 윤리 및 전문성.....	12
원칙 1 진실성 입증.....	12
국제내부감사표준 1.1 정직과 용기.....	12
국제내부감사표준 1.2 조직의 윤리적 기대.....	13
국제내부감사표준 1.3 법률과 전문가적 행동.....	14
원칙 2 객관성 유지.....	15
국제내부감사표준 2.1 개별감사인의 객관성.....	16
국제내부감사표준 2.2 객관성의 보호.....	17
국제내부감사표준 2.3 객관성의 손상 공개.....	20
원칙 3 감사역량 입증.....	21
국제내부감사표준 3.1 감사역량.....	21
국제내부감사표준 3.2 지속적인 전문성 개발.....	23
원칙 4 전문가로서의 정당한 주의 이행.....	24
국제내부감사표준 4.1 국제내부감사표준과의 적합성.....	25
국제내부감사표준 4.2 전문가로서 정당한 주의.....	26
국제내부감사표준 4.3 전문가적 의구심.....	27
원칙 5 비밀 유지.....	29
국제내부감사표준 5.1 정보의 이용.....	29
국제내부감사표준 5.2 정보의 보호.....	30
영역 III 내부감사부서의 거버넌스.....	32
원칙 6 이사회의 권한 부여.....	32
국제내부감사표준 6.1 내부감사의 임무.....	32
국제내부감사표준 6.2 이사회의 지원.....	35
원칙 7 독립성 보장.....	37
국제내부감사표준 7.1 조직의 독립성.....	37

국제내부감사표준 7.2 최고감사책임자의 역할, 책임 및 자격	39
국제내부감사표준 7.3 독립성의 보호	42
원칙 8 이사회의 감독	44
국제내부감사표준 8.1 이사회의 상호작용	44
국제내부감사표준 8.2 감사자원	46
국제내부감사표준 8.3 감사품질	48
국제내부감사표준 8.4 감사품질에 대한 외부평가	49
영역 IV 내부감사 부서 관리	54
원칙 9 전략적 계획수립	54
국제내부감사표준 9.1 거버넌스, 리스크 관리 및 통제 프로세스의 이해	54
국제내부감사표준 9.2 내부감사 전략	57
국제내부감사표준 9.3 내부감사현장	58
국제내부감사표준 9.4 감사 방법론	60
국제내부감사표준 9.5 내부감사계획	62
국제내부감사표준 9.6 조정 및 의존	65
원칙 10 감사자원 관리	67
국제내부감사표준 10.1 재무 자원 관리	67
국제내부감사표준 10.2 인적 자원 관리	69
국제내부감사표준 10.3 기술적 자원	72
원칙 11 효과적인 커뮤니케이션	73
국제내부감사표준 11.1 이해관계자와의 관계 구축 및 커뮤니케이션	73
국제내부감사표준 11.2 효과적인 커뮤니케이션	75
국제내부감사표준 11.3 감사결과 커뮤니케이션	77
국제내부감사표준 11.4 오류 및 누락	79
국제내부감사표준 11.5 리스크 수용에 관한 커뮤니케이션	80
원칙 12 감사 품질의 향상	82
국제내부감사표준 12.1 감사품질에 대한 내부평가	82
국제내부감사표준 12.2 수행성과 측정	85
국제내부감사표준 12.3 감사업무 수행 성과의 보장 및 개선	87
영역 V 내부감사 서비스 수행	90

원칙 13 효과적인 감사계획 수립	90
국제내부감사표준 13.1 감사업무 커뮤니케이션	91
국제내부감사표준 13.2 감사업무 리스크 평가	93
국제내부감사표준 13.3 감사업무의 목표 및 범위	96
국제내부감사표준 13.4 평가 기준	98
국제내부감사표준 13.5 감사업무의 자원	100
국제내부감사표준 13.6 감사업무 수행 프로그램	101
원칙 14 감사업무 수행	103
국제내부감사표준 14.1 분석 및 평가를 위한 정보 수집	103
국제내부감사표준 14.2 분석 및 잠재적 감사 지적사항	104
국제내부감사표준 14.3 지적사항 평가	106
국제내부감사표준 14.4 권고사항 및 조치 계획	108
국제내부감사표준 14.5 감사 결론 도출	109
국제내부감사표준 14.6 감사업무의 문서화	110
원칙 15 감사결론 커뮤니케이션 및 조치계획 모니터링	113
국제내부감사표준 15.1 최종 감사업무 커뮤니케이션	113
국제내부감사표준 15.2 경영진의 조치계획 이행 확인	115

국제내부감사표준 소개

국제내부감사표준은 전 세계적으로 높은 품질의, 전문적인 내부감사활동 실행에 필요한 필수사항 및 권고사항을 제공한다. 또한 표준은 내부감사 서비스의 성과평가를 위한 기준을 정하고 있다.

국제내부감사표준의 구조

국제내부감사표준은 다음 사항을 포함하고 있다:

- 원칙: 일련의 요건 및 권고사항을 요약한 기본적인 가정이나 규칙에 대한 개략적 설명
- 표준:
 - 전문적인 내부감사활동을 위한 요건
 - 고려사항:
 - 실행: 요건을 실행함에 있어서 일반적이고도 우선시되는 실무기준
 - 적합성 증거: 이 표준의 요건이 실행되었음을 입증하기 위해 권장되는 방법들에 대한 예시

이 표준은 공통 테마 관련 5 개의 주요영역으로 구성된다.

내부감사활동의 목적

II. 윤리 및 전문성

III. 내부감사부서의 거버넌스

IV. 내부감사부서의 관리

V. 내부감사 서비스의 수행

국제내부감사표준의 적용

국제내부감사표준은 전 세계적으로 전문적인 내부감사활동을 위한 필수요건 및 권고사항을 제시한다. 이 표준은 목적, 크기, 규모 및 구조가 다양한 조직을 위해 내부감사 서비스를 제공하는 모든 개인이나 부서에 적용된다. 이 표준은 내부감사인이 조직의 직원인지, 또는 계약을 체결한 외부 서비스 제공자인지, 또는 이 둘의 결합인지와 관계없이 적용된다.

이 표준은 내부감사인 개인과 내부감사부서 전체에 적용된다. 모든 내부감사인에게는 윤리 및 전문성 영역의 원칙과 표준뿐만 아니라 직책의 수행과 관련된 원칙과 표준을 따를 책임이 있다. 최고감사책임자(Chief audit executives)는 내부감사부서가 전반적으로 이 표준을 준수하게 할 책임이 있다.

내부감사인이나 내부감사부서가 법규로 인해 표준의 특정 내용을 준수할 수 없는 경우에는, 해당 내용을 제외한 다른 모든 내용을 준수하고 이러한 사실을 적절하게 공개해야 한다.

이 표준이 다른 권위 있는 기관에서 공표한 요건과 병행하여 사용되는 경우, 내부감사 커뮤니케이션에서 반드시 다른 요건의 사용에 대해서도 적절하게 언급되어야 한다. 그러나 표준은 준수해야 한다.

국제내부감사표준 사용 방법

이 표준의 요건 부문에서 "반드시~해야 한다(must)"라는 표현은 반드시 준수해야 할 사항일 때 사용한다. 이 표준의 실행을 위한 고려사항 부문에서 "~해야 한다(should)"라는 표현은 따르는 것이 더 바람직한 사항일 때 사용한다. 표준의 "~할 수 있다(may)"라는 표현은 필수가 아닌 선택가능한 사항일 때 사용한다.

이 표준의 용어집은 구체적으로 정의된 용어를 사용한다. 이 표준을 정확히 이해하고 적용하려면 용어집에 설명된 용어의 구체적인 의미와 용법을 이해하고 채택해야 한다.

국제내부감사표준설정 프로세스

세계내부감사인협회(IIA)는 폭넓은 공익을 위해 국제내부감사표준위원회가 시행하고 IPPF 감독위원회가 감독하는, 지속적인 프로세스를 포함한 표준을 수립하는 데 전념하고 있다. 국제내부감사표준위원회는 국제내부감사표준의 초안을 작성하고 수정할 때, 이해관계자의 의견 요청을 포함하여 정당한 절차를 거친다. 이 절차에는 표준의 확정 및 발행 전, 전 세계 대중의 의견을 수렴하기 위해 IIA의 웹사이트에 초안을 게시하는 것이 포함된다. 초안은 모든 IIA 지역지부에 배포되고 여러 언어로 번역된다. 번역본 또한 IIA 웹사이트에 게시된다. 독립적인 감독기구인 IPPF 감독위원회는 표준수립 프로세스의 관한 평가와 조언을 제공함으로써 포괄성과 투명성을 촉진하고 궁극적으로 공익에 기여한다.

용어집

검토대상활동(activity under review) – 내부감사업무의 대상. 영역, 조직과 운영, 기능, 프로세스 또는 시스템이 그 예이다.

자문 서비스(consulting services) – 일반적으로 최고경영진, 이사회 또는 현업부서 경영진의 요청에 따라 수행되는 자문업무와 기타 자문활동을 포함하는 서비스를 말한다. 자문 서비스의 성격과 범위는 해당 서비스를 요청한 당사자와의 합의에 따라 결정된다. 자문 업무의 예시로는 내부감사인들이 새로운 규정의 제정 및 실행에 대해, 그리고 프로세스 및 시스템의 설계에 대해 자문 것이 있다. 기타 자문 활동에는 내부감사인이 제공하는 퍼실리테이션(facilitation)과 교육이 포함된다.

검증(assurance) – 기준 대비 실제 상태에 대한 확인 및 의견 진술

검증 서비스(assurance services) – 이 서비스는 내부감사인이 설정된 기준과 비교한 상태에 관한 의견을 제시하고자 객관적인 평가를 실시하는 것이다. 의견 제시의 취지는 이해관계자에게 조직의 거버넌스, 리스크 관리 및 통제 프로세스에 관한 확인 및 의견을 제공하는 것이다. 검증 서비스의 예로 재무감사, 성과감사, 컴플라이언스 감사, 전산감사가 있다.

이사회(board) – 거버넌스를 담당하는 최상위 지배기구로 다음은 그 예이다:

- 이사회 또는 이사회가 특정 기능을 위임한 위원회나 기구(예: 감사위원회)
- 지배 기구가 둘 이상인 조직에서 비상임/감독위원회
- 재단 등의 운영이사회
- 선출직 또는 정무직 공무원 집단

이사회가 존재하지 않는 경우 "이사회"라는 용어는 조직의 거버넌스를 담당하는 집단이나 개인을 의미한다(예를 들면, 일부 공기업 및 민간 부문의 중소기업은 조직의 수장이나 최고경영진이 최상위 지배 기구 역할을 수행하게 할 수 있다).

최고감사책임자(Chief Audit Executive) – 내부감사부서를 효과적으로 관리하고, 내부감사 서비스의 품질을 보장하는 리더. 구체적인 직위 및/또는 직책은 조직마다 다를 수 있다. 예를 들면, "총괄 감사인", "내부감사 책임자", "최고내부감사인", "내부감사 담당 이사", "총괄감사관"과 같은 직함을 "최고감사책임자" 대신 사용할 수 있다.

윤리강령(Code of Ethics) – 국제내부감사표준의 윤리 및 전문성 영역에 기술된 원칙과 표준은 내부감사인의 윤리강령으로 간주된다. 즉, 이 원칙과 표준의 준수는 직업적 윤리강령의 준수와 동일한 의미이다.

역량(competency) – 지식, 스킬(skill) 및 능력

컴플라이언스(compliance) – 법규, 계약, 내규, 절차 또는 기타 요건의 준수

실태(condition) – 검토 대상 활동의 현재 상태

이해충돌(conflict of interest) - 내부감사인이 조직에 최선의 이익이 되지 않는 조치를 취하거나 전문가적 판단을 내리도록 영향을 미치거나 영향을 미치는 것처럼 보일 수 있는 상황, 활동 또는 관계

적합성 증거를 위한 고려사항(Considerations for Evidence of Conformance) - 국제내부감사표준에서 각 표준의 요건이 실행되었음을 보여주는 방식의 예를 제공함.

실행을 위한 고려사항(Considerations for Implementation) - 국제내부감사표준에서 각 표준의 요건을 구현하기 위해 일반적으로 선호되는 실무기준을 제공함.

통제(control) - 리스크를 관리하고 수립된 목적과 목표의 달성 가능성을 높이고자 경영진, 이사회 및 기타 당사자가 취하는 조치

통제 프로세스(control processes) - 조직이 허용한도 내에서 리스크를 관리하기 위해 설계하고 운영하는 내규, 절차 및 활동

기준(criteria) - 검토대상 활동이 바람직한 상태에 있는지를 측정할 수 있는 기준("평가 기준"이라고도 함.)

효과/영향(effect) - 기준과 실태의 차이로 발생할 수 있는 리스크

감사업무(engagement) - 일련의 특정 목표를 달성하기 위해 설계된 여러 형태의 과업 또는 활동을 포함하는 특정의 내부감사 업무 또는 프로젝트를 말함. "검증 서비스" 및 "자문 서비스" 참조

감사 결론(engagement conclusion) - 종합적으로 보았을 때 감사업무 지적사항이 지니는 전체적인 중요성에 대한 내부감사인의 전문가적 판단

감사 목표(engagement objectives) - 감사업무의 목적을 명확하게 설명하고 달성해야 하는 특정한 목표를 설명한 진술

감사계획 수립(engagement planning) - 내부감사인이 감사대상관련 정보를 수집 및 관련 리스크를 평가하여 우선순위화 한 후, 감사업무 목표 및 범위를 설정하고, 평가기준을 식별하여 내부감사업무 수행 프로그램(work program)을 만드는 프로세스

감사업무 감독자(engagement supervisor) - 내부감사업무를 감독할 책임이 있는 내부감사인으로, 감사업무 수행 프로그램, 감사조서, 최종 커뮤니케이션, 성과를 검토 및 승인하는 업무를 담당한다. 내부감사인을 훈련시키고 지원하는 일도 감독업무에 포함될 수 있다. 최고감사책임자가 직접 감사업무 감독자가 될 수도 있고, 그러한 책임을 위임할 수도 있다.

감사업무 수행 프로그램(engagement work program) - 감사업무 목표를 달성하기 위해 수행해야 할 일들과 그 일들을 수행하는 데 필요한 방법론 및 도구와 수단, 그리고 그 일을 수행하도록 배정된 내부감사인이 누구인지를 기술한 문서 또는 서식. 감사업무 수행 프로그램은 감사업무 계획 수립 시에 수집한 정보를 기반으로 작성한다.

외부 서비스 제공자(external service provider) - 내부감사 서비스를 지원하기 위해 관련 지식, 스킬(skill), 경험 및/또는 툴(tool)을 제공하는 조직 외부의 자원

지적사항(finding) – 감사수행 결과, 검토대상활동의 평가기준과 실태 간의 차이를 바탕으로 해당 검토대상에 중대한 리스크가 존재한다고 결정한 사항이다. 예를 들어, 오류, 비리, 불법행위 또는 효율성이나 효과성을 제고할 수 있는 잠재적 기회이다.

부정 행위(fraud) - 사적 또는 사업상의 이득을 위해 개인이나 조직이 자행하는 사기, 은폐, 배임 등과 같은 행위

거버넌스(governance) – 조직의 목표 달성을 위한 활동을 알리고, 지시하고, 관리하고, 모니터링하기 위해 이사회가 구현한 프로세스 및 구조의 조합

충격/영향(impact) – 리스크의 결과 또는 효과. 리스크와 관련하여 다양한 영향이 있을 수 있다. 리스크의 영향은 기업의 전략이나 사업 목표 대비 긍정적일 수도 부정적일 수도 있다.

독립성(independence) – 내부감사부서가 편향되지 않은 방식으로 그 책임을 수행할 수 있는 능력을 손상시키는 상황으로부터의 자유

고유 리스크(inherent risk) – 통제되지 않은 본연의 상태의 내부 및 외부의 리스크 요인들의 조합. 또는 통제가 없다고 가정할 때 존재하는 리스크의 총량.

진실성(integrity) – 내부감사인인 동료 및 다른 사람의 주의 깊고 상세한 검증에서도 아무런 문제가 없을 방식으로 행동하는 것을 말한다. 적절하게 행동할 용기, 정직함 및 공정한 처리를 포함한다.

내부감사헌장(internal audit charter) – 내부감사부서의 권한과 기타 직무수행 요건을 정의한 공식 문서

내부감사부서(internal audit function) – 조직에 검증 및 자문 서비스를 제공할 책임이 있는 전문성을 지닌 개인이나 그룹

내부감사 임무(internal audit mandate) – 내부감사부서의 권한, 역할 및 책임

내부감사 매뉴얼(internal audit manual) – 내부감사부서의 감사인들에게 방향을 제시하고 안내하기 위해 최고감사책임자가 문서화한 감사방법론(내부감사 규정, 프로세스 및 절차)

내부감사계획(internal audit plan) – 정해진 기간 동안 제공할 감사업무 및 기타 내부감사 서비스 내용을 식별하여 작성한 문서로 최고감사책임자가 작성한다. 내부감사계획은 조직의 변화에 적시에 대응하기 위해 역동적이어야 한다.

내부감사활동(internal auditing) – 조직에 가치를 부가하고 조직의 운영을 개선하기 위해 설계된 독립적이고 객관적인 검증 및 자문 활동. 거버넌스, 리스크 관리 및 통제 프로세스의 효과성을 평가하고 개선하기 위해 체계적이고 규율 있는 접근방식을 도입하여 조직이 목표를 달성하도록 돕는다.

국제내부감사직무수행체계(IPPF) – 내부감사수행에 관한 권위 있는 표준 및 지침에 대한 IIA의 개념체계

가능성(likelihood) – 어떤 사건(event)이 발생할 가능성

~할 수 있다(may) – 국제내부감사표준의 실행을 위한 고려사항에서 사용된 "~할 수 있다"라는 표현은 선택적으로 실행할 수 있는 요구사항을 설명할 때 사용한다.

감사방법론(methodologies) – 내부감사부서를 안내하고, 감사활동의 효과성을 제고하기 위해 최고감사책임자가 수립한 내규, 프로세스 및 절차

반드시 ~해야 한다(must) – 국제내부감사표준의 "반드시 ~해야 한다"라는 표현은 반드시 따라야 하는 요구사항을 명시할 때 사용한다.

객관성(objectivity) – 내부감사인 이 타협 없이 전문적인 판단을 내리고 책임을 완전히 수행하여 내부감사활동의 목적을 달성할 수 있도록 해주는 편견 없는 정신적 태도를 말한다.

아웃소싱(outsourcing) – 독립적인 외부 서비스 제공자와 계약을 체결하여 내부감사 서비스를 제공받는 것을 말한다. 내부감사부서의 전면 아웃소싱은 부서 전체의 외주계약을 말하며, 부분 아웃소싱은("코소싱(cosourcing)" 이라고도 함) 내부감사 서비스의 일부분만 아웃소싱하는 것을 나타낸다.

원칙(Principles) – 내부감사활동의 필수 요소를 설명하고 국제내부감사표준의 기초 역할을 하는 규칙

전문가적 의구심(professional skepticism) – 정보의 신뢰성에 의문을 제기하고 비판적으로 평가함.

공공 부문(public sector) – 공적 프로그램, 공공재 또는 공공 서비스를 제공하는 정부와 공적 통제 대상이거나 공적 자금을 지원받는 기관, 기업 및 기타 법인

감사품질 평가 및 개선 프로그램(quality assurance and improvement program) – 내부감사부서가 국제내부감사표준에 부합하고, 성과 목표를 달성하며, 지속적인 개선을 추구하는지 여부를 평가 및 확인하기 위해 최고감사책임자가 수립하는 프로그램이며, 내부 및 외부의 평가를 포함한다.

잔여 리스크(residual risk) – 고유 리스크 중 경영진의 통제 시행 후 남아 있는 리스크("순 위험"이라고도 함)

내부감사 서비스의 결과(results of internal audit services) – 감사결론, 테마(효과적인 실무나 근본 원인 등), 비지니스 단위 또는 조직 차원에서 도출된 결론과 같은 결과물

리스크(risk) – 어떠한 사건(event)이 발생하여 전략 및 비즈니스 목표 달성에 영향을 미칠 가능성

리스크 통제 매트릭스(risk and control matrix) – 내부감사활동의 성과를 촉진시키는 툴(tool). 일반적으로 비즈니스 목표, 리스크, 통제 프로세스 및 주요 정보를 연계한 형태로 내부감사 프로세스를 지원한다.

리스크 성향(risk appetite) – 조직이 전략 및 비즈니스 목표를 추구하는 과정에서 수용하기로 결정한 리스크의 유형과 양을 말한다. 리스크 성향은 조직이 통제 구현의 비용과 효익의 균형을 맞춘 다음 의도적으로 수용하는 리스크의 양을 고려한다.

리스크 평가(risk assessment) – 조직의 목표 달성과 관련된 리스크를 식별 및 분석하는 것을 말한다. 리스크의 중요성은 일반적으로 리스크의 발생가능성과 발생시 영향의 크기의 조합으로 평가한다.

리스크 관리(risk management) – 조직의 목표 달성에 대해 합리적인 확신을 제공하기 위해 잠재적인 사건(event)이나 상황을 평가, 관리, 통제하는 프로세스

리스크 허용한도(risk tolerance) – 비즈니스 목표 달성과 관련하여 수용할 수 있는 성과의 변동범위

근본 원인(root cause) – 검토 대상의 실패와 기준 사이의 차이를 불러일으킨 핵심 이슈 또는 근원적인 이유

최고경영진(senior management) – 한 조직에서 최상위에 있는 경영진

~해야 한다(should) – 국제내부감사표준의 구현을 위한 고려사항에서 사용된 "해야 한다"라는 표현은 필수는 아니지만 따르면 좋은 요구사항을 설명할 때 사용한다.

중대성(significance) – 규모, 성격, 영향, 관련성 및 영향과 같은 정량적 및 정성적 요인을 포함하여, 고려 대상인 맥락 내에서 한 문제가 지니는 상대적인 중요성을 말한다. 관련 목표의 맥락에서 문제의 중대성을 평가할 때 내부감사인은 전문가적 판단이 필요하다. 리스크의 중대성은 대개 리스크의 발생 가능성과 발생 시 충격/영향의 조합으로 측정된다.

이해관계자(stakeholder) – 한 조직의 활동 및 결과에 직간접적인 이해관계가 있는 당사자. 조직의 이해관계자의 예로 직원, 고객, 공급업체, 주주, 규제 기관, 금융기관이 있다. 내부감사부서의 이해관계자의 예로 조직의 이사회, 경영진, 직원, 고객, 공급업체, 외부감사인, 규제 기관이 있다. 대중도 이해관계자가 될 수 있다.

표준(standard) – 국제내부감사표준위원회(International Internal Audit Standards Board)가 공표한 전문 선언문은 다음 사항을 기술하고 있다:

- 전문적인 내부감사활동 수행에 요구되는 사항
- 실행을 위한 고려사항
- 적합성 증거를 위한 고려사항

감사조서(workpapers) – 감사업무계획 수립 및 현장감사 수행 시 작업한 사항을 문서화한 것을 말한다. 감사 지적사항 및 결론의 기반이 되며, 이를 뒷받침하는 정보와 증빙을 제공한다.

내부감사활동의 목적

내부감사활동의 목적에서는 내부감사인 및 내부감사 이해관계자가 내부감사활동의 가치를 이해하고 이를 명확하게 설명할 수 있도록 도움을 주고자 한다.

목적

내부감사활동의 목적은 이사회 및 경영진에게 객관적인 검증과 조언을 제공함으로써 조직의 성과를 향상시키는데 있다.

내부감사활동은 조직의 다음 사항을 강화한다:

- 가치 창출 및 보호, 지속가능성
- 거버넌스, 리스크 관리 및 통제 프로세스
- 의사결정 및 감독
- 이해관계자의 평판과 신뢰
- 공익 기여 능력

내부감사활동은 다음과 같은 상황일 때 가장 효과적이다:

- 공익을 위해 정립된 국제내부감사표준에 따라 자격을 갖춘 내부감사인이 수행한다.
- 내부감사부서가 이사회에 직접적인 책임을 지는 독립적인 위치에 있다.
- 내부감사인은 편견이 없으며, 부당한 영향력을 받지 않으며, 객관적인 평가를 위해 최선을 다한다.

영역 II 윤리 및 전문성

내부감사인의 윤리강령은 윤리 및 전문성의 원칙과 표준으로 구성된다. 이러한 원칙과 표준은 내부감사 서비스를 제공하는 개인과 단체뿐만 아니라, 전문 내부감사인의 행동에 대한 기대치를 설명해 준다. 이를 준수하면 내부감사활동에 대한 신뢰를 심어주고 내부감사활동의 윤리적 문화를 조성하며 내부감사인의 업무수행과 판단을 신뢰할 수 있는 근간을 제공한다.

"내부감사인"이란 IIA 에서 인증한 전문자격증 소지자나 예비자격자, 그리고 IIA 의 지부와 지사의 구성원을 포함하여 IIA 의 모든 회원을 의미한다. 내부감사인은 윤리 및 전문성 표준을 준수해야 한다. 내부감사인이 소속된 조직의 윤리 강령과 같은 다른 행동 강령을 준수해야 하는 경우에도 본 체계에 포함된 윤리 및 전문성의 원칙과 표준을 반드시 지켜야 한다. 이러한 원칙과 표준에 언급되어 있지 않은 행동도 용납할 수 없거나 신뢰할 수 없는 것으로 간주될 수 있다.

원칙 1 진실성 입증

내부감사인은 자신의 업무수행과 행동에 있어 진실성을 입증한다.

진실성은 다른 감사인이 검증하여도 동일한 결론에 이를 수 있도록 행동하는 것이다. 진실성에는 공정한 처리, 진정성 및 적절하게 행동할 수 있는 용기가 필요하며, 이는 다르게 행동하라는 압력이 있거나 자신 또는 조직에 불리한 결과를 초래하게 될 수도 있는 경우에도 마찬가지이다. 간략히 말하면, 내부감사인은 불편하거나 어려운 때에도 진실을 말하고 올바른 일을 해야 한다.

진실성은 객관성, 역량, 전문가로서의 정당한 주의, 기밀유지를 포함하여 기타 윤리 및 전문성 원칙의 근간이다. 내부감사인의 진실성은 신뢰를 구축하고 존경을 받는 데 필수적이다.

국제내부감사표준 1.1 정직과 용기

요건

내부감사인은 반드시 정직하고 용기 있게 업무를 수행해야 한다.

내부감사인은 모든 업무 관계자와의 커뮤니케이션 시 반드시 진실하고 정확하며 명료하고 개방적이며 상대를 존중해야 한다. 내부감사인은 거짓, 오해의 소지가 있거나 기만적인 진술을 해서는 안 되며, 감사업무 커뮤니케이션 시 지적사항이나 기타 관련 정보를 숨기거나 생략해서는 안 된다. 내부감사인은 공개하지 않을 경우 정보에 입각한 결정을 내리는 조직의 능력에 영향을 줄 수 있는 모든 중대한 사항을 반드시 공개해야 한다.

내부감사인은 딜레마와 어려운 상황에 직면하더라도 진실되게 소통하고 적절한 조치를 취함으로써 반드시 용기를 보여야 한다. 내부감사인은 의구심이나 반대 의견을 표명하는 경우에도 반드시 다른 사람을 정중하며 전문가 다운 태도로 대해야 한다.

최고감사책임자는 내부감사인이 유불리와 무관하게 적법하고 증거에 기반한 지적사항, 결론, 권고사항을 표명할 때 지지를 받는 업무 환경을 반드시 유지해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

내부감사인은 윤리적 책임에 대한 인식과 이해를 높이기 위해 매년 최소 2시간의 윤리 관련 보수교육(CPE)을 받아야 한다. 최고감사책임자는 내부감사인이 교육을 받을 수 있는 기회를 갖도록 해야 한다. 최고감사책임자는 또한 내부감사인에게 진실성과 기타 윤리적 원칙을 설명하는 교육을(예를 들면, 윤리적 선택이 필요한 상황에 대해 논의하는) 제공함으로써 진실성이 중요함을 강조할 수 있다.

효과적인 내부감사부서 관리에는 적절한 업무 감독과 주기적 실적 검토가 있으며, 이는 실제상황에서 진실성이 어떻게 도전 받고 적용되는지에 관하여 내부감사인과 감독자 간 논의할 기회를 제공한다. 예를 들면, 감사업무의 감독자가 감사업무수행 프로그램을 승인하거나 감사조서를 검토하면서 진실성에 위협이 될 수 있는 잠재적 또는 실질적 상황을 해결하는 데 도움이 되는 적절한 지침을 제공할 수 있다.

공공 부문

공공 부문의 내부감사인은 항상 공익을 보호해야 하며 지적사항, 권고사항 및 결론을 제시할 때 용기를 보여야 한다.

적합성 증거

- 모든 내부감사인을 위한 연간 윤리교육이 포함된 교육훈련 계획
- 참석자명부, 교육일정, 수료증 또는 내부감사인의 윤리교육 참석이나 참여를 증명할 수 있는 기타 문서

국제내부감사표준 1.2 조직의 윤리적 기대

요건

내부감사인은 조직의 합법적이고 윤리적인 기대사항을 반드시 존중하고 그에 기여해야 한다.

내부감사인은 반드시 조직의 윤리적 기대를 이해하고 충족시켜야 하며, 이에 반하는 행동을 인지할 수 있어야 한다. 내부감사인은 반드시 조직의 윤리 문화를 장려하고 촉진시켜야 한다.

내부감사인은 적절한 윤리와 가치를 향상시키기 위해 반드시 조직의 목표, 내규, 프로세스를 개선하기 위한 평가를 실시하고 권고사항을 제시해야 한다. 내부감사인이 조직의 윤리적 기대와 일치하지 않는 행동을 조직 내에서 식별하는 경우, 그 문제를 최고감사책임자가 수립한 내규에 따라 반드시 보고해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

내부감사계획은 윤리와 관련된 리스크 평가를 포함하여 조직의 현행 내규, 프로세스 및 기타 통제가 이러한 리스크를 적절하고 효과적으로 다루고 있는지 판단해야 한다. 예를 들면, 조직의 내규에서 윤리 관련 이슈에 대해 소통하고 처리하는 기준 및 프로세스, 소통 대상자, 미해결

이슈를 해결하기 위한 실시요강(protocol)을 지정할 수 있다. 또한, 최고감사책임자는 윤리적 이슈를 해결하기 위한 방법론을 결정하고, 최고경영진 및 이사회와 이 방법론을 논의하여 접근방식을 일치시켜야 한다.

내부감사인은 개별 감사업무 수행 시 윤리 관련 리스크와 통제를 고려해야 한다. 내부감사인이 조직의 윤리적 기대와 일치하지 않는 조직 내 행동을 식별할 경우, 조직의 내규 및 프로세스를 고려하여 최고감사책임자가 정한 방법론에 따라 내부적으로 문제에 대해 소통해야 한다.

행동강령 및 윤리강령 등의 문서화 여부와 무관하게, 내부감사인이 최고경영진이 조직의 윤리적 기대를 위반했다고 판단한 경우, 최고감사책임자는 이 문제를 이사회에 보고해야 한다. 윤리 관련 문제가 이사회 의장과 관련된 경우, 최고감사책임자는 전체 이사회에 이 문제를 보고해야 한다. 내부감사인은 최고경영진이나 이사회와 관련된 모든 윤리 관련 문제에 대해 사후관리하고, 이를 해결하기 위해 적절한 조치가 실행되었음을 검증해야 한다.

적합성 증거

- 윤리적 기대 및 문제가 논의된 워크숍, 교육 행사 또는 회의에 내부감사인이 참여한 기록
- 조직의 윤리관련 내규 및 프로세스를 이해하고 준수한다는 약속을 인정하는 내부감사인 개개인이 서명한 문서
- 조직의 윤리관련 내규 및 프로세스의 평가서
- 윤리적 문제가 조직의 내규와 관련 법규에 따라 최고경영진, 이사회 및 규제당국에 효과적으로 전달되었음을 입증하는 문서

국제내부감사표준 1.3 법률과 전문가적 행동

요건

내부감사인은 어떤 경우에도 불법적이거나 조직 또는 내부감사활동의 전문성에 대한 신뢰를 손상시킬 수 있는 활동에 가담하거나 당사자가 되어서는 안 된다. 내부감사인은 어떤 경우에도 조직이나 직원에게 해가 될 수 있는 활동에 가담하거나 당사자가 되어서는 안 된다.

내부감사인은 의무 공시를 포함하여, 조직이 속한 산업 및 사법관할권과 관련된 법규를 반드시 이해하고 준수해야 한다. 내부감사인이 법규 위반을 식별하는 경우 법규 및 내부감사 내규에 명시된 바에 따라 적절한 조치를 취할 권한이 있는 개인이나 단체에 해당 사건을 반드시 보고해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

최고감사책임자는 내부감사인이 조직이 속한 산업 및 사법관할권과 관련된 법규를 준수하도록 방법론을 수립하고 실행해야 한다. 이러한 방법론은 조치가 위반사항을 적절하게 처리하는지

검증하기 위해 확립된 절차를 포함하여 법규 위반에 대해 내부감사인이 취할 것으로 기대되는 조치를 명시해야 한다.

최고감사책임자는 내부감사인들이 적절하게 감독됨을 확인하고, 국제내부감사표준을 준수하고, 윤리적 및 직업적 가치에 따라 행동하기 위한 방안들을 수립해야 한다. 다음은 신뢰를 저해할 수 있는 행동의 예이다:

- 괴롭힘, 희롱 또는 차별함.
- 실수에 대한 책임 회피함.
- 감사보고서나 총평에서 의도적으로 최소화, 은폐, 생략하는 방법을 통해 감사 지적사항, 감사 결론 혹은 감사 등급 내용을 허위로 보고하거나 또는 커뮤니케이션하고, 다른 사람도 그렇게 하도록 허용 또는 조장함.
- 거짓말하거나, 속이거나, 자신의 역량이나 자격을 허위로 표시하는 등 고의로 타인을 오해하게 행동함(예를 들면, 자격을 소지하고 있다고 주장하거나, 만료 또는 비활성화, 말소된 자격 혹은 취득한 사실이 없는 자격 증명의 표시).
- 동료들 사이에서나 공공 장소에서 조직, 동료 직원 혹은 이해관계자에 대해 비방함.
- 객관성 또는 독립성의 손상 상태를 알리지 않고 내부감사 서비스 수행함.
- 적절한 승인 없이 기밀 정보를 요구하거나 공개함.
- 내부감사부서가 국제내부감사표준을 준수하며 운영되고 있다는 근거가 없음에도 그러하다고 명시함.
- 조직이 용납하거나 수용할 수 있는 불법 행위를 간과함.

적합성 증거

- 법규 및/또는 전문가적 행동 교육에 내부감사인이 참여한 기록
- 관련 법률과 전문가적 기대사항을 이해하고 이에 부합하게 행동하겠다는 약속을 확인한 내부감사인 개개인이 서명한 문서
- 내부감사인 사이에 불법적이거나 평판을 떨어뜨리는 행동과 조직 내 개인의 법규 위반을 처리하는 방안들을 기록한 문서
- 불법적이거나 전문가답지 않은 행동에 대한 우려에 관하여 내부감사인과 감독자 간의 대화를 기록한 문서나 감사조서에 감독자가 기록한 검토 의견

원칙 2 객관성 유지

내부감사인은 내부감사 서비스를 수행하고 의사 결정을 내릴 때 공정하고 편견 없는 태도를 유지한다.

객관성은 내부감사인이 타협 없이 전문가적 판단을 내리고, 책임을 다하며, 내부감사활동의 목적을 달성할 수 있도록 하는 편견 없는 정신 자세이다. 내부감사부서의 독립적인 위치는 내부감사인의 객관성 유지 능력을 뒷받침한다.

국제내부감사표준 2.1 개별감사인의 객관성

요건

내부감사인은 내부감사 서비스의 모든 측면을 수행하는 과정에서 반드시 직업적인 객관성을 유지해야 한다. 직업적인 객관성은 내부감사인이 공정하고 편견 없는 사고 방식을 적용하고 모든 관련 상황에 대해 균형 잡힌 평가를 기반으로 판단을 내릴 것을 요구한다.

내부감사인은 다음 사항 이외에도 잠재적 편견을 반드시 인식하고 관리해야 한다:

- 자체검토 편향 - 자신이 수행한 업무를 자신이 직접 검토할 경우 비판적 시각이 부족하여 실수나 결점을 간과할 수 있다.
- 친숙성 편향 - 과거 경험을 바탕으로 가정함으로써 전문가적 의구심을 손상시킬 수 있다.
- 편견 또는 무의식적 편향 - 판단에 부당하게 영향을 미칠 수 있는 문화, 민족, 성별, 이데올로기, 인종 또는 기타 특성에 대한 편견을 포함하여 정보를 잘못 해석한다.

최고감사책임자는 내부감사인의 객관성을 지원하고 촉진하기 위한 내규, 절차 및 교육을 반드시 제공해야 한다. 내부감사인은 반드시 자신의 책임과 관련된 기대를 이해하고 내규 및 절차를 적용해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

객관적인 평가를 하려면 편견과 부당한 영향이 없는 공정한 사고방식이 필요하며, 이는 최고경영진과 이사회에 객관적인 검증과 조언을 제공하는 데 필수적이다. 내부감사인은 상황, 활동 및 관계에서 객관성 유지에 영향을 미칠 수도 있는 방식들에 대한 인지능력을 강화해야 한다.

또한, 내부감사인은 정보 및 증거를 객관적으로 평가하는 감사인의 능력을 저해하고, 판단과 결정에 부당한 영향을 미치는 방식으로 정보를 잘못 해석하고, 추측하고, 실수하고, 정보를 무시 또는 간과하게 만드는 인간의 경향이나 성향을 고려해야 한다.

객관성은 내부감사인이 타인의 판단에 타협하거나 복종하지 않고 직무를 수행하는 것을 의미한다. 국제내부감사표준은 최고감사책임자가 확립한 내규 및 교육훈련과 더불어, 검토 대상 활동에 대한 균형 있는 평가를 제공하기 위해, 정보를 수집하고 평가하는데 체계적이고, 규율화된 접근방식을 규정한 요건, 절차, 지침을 제공함으로써 객관성을 뒷받침한다. 교육은 내부감사인이 객관성 손상이 발생하는 상황들과 이를 해결하는 최선의 방법들을 더 잘 이해하는 데 도움이 될 수 있다.

매년 내부감사인은 객관성의 중요성에 대한 인식, 관련 내규 및 절차에 대한 이해, 잠재적 손상요인의 공개 의무를 확인하는 증명서에 서명해야 한다.

적합성 증거

- 내부감사현장 중 객관성을 유지해야 할 내부감사인의 책임에 관해 기술한 부분
- 객관성과 관련된 내규 및 절차
- 참가자 목록을 포함하는 객관성 교육 계획 및 이수 기록
- 객관성의 중요성과 잠재적 손상요인을 공개할 의무에 대한 내부감사인의 인식을 확인하는 증명서
- 잠재적 이해충돌이나 기타 객관성 손상요인의 공개 문서
- 감독자의 검토 및 내부감사인 멘토링 기록

국제내부감사표준 2.2 객관성의 보호

요건

내부감사인은 객관성에 대한 실질적, 잠재적, 그리고 인식된 손상을 반드시 인지, 회피 및 경감해야 한다.

내부감사인은 다음을 반드시 회피해야 한다:

- 객관성을 손상할 수 있거나 손상한다고 추정되는 선물, 보상 또는 호의와 같은 유무형의 품목을 받는 행동
- 상황, 활동 및 관계를 포함하여 이해충돌은 다음 사항일 수 있다:
 - 조직에 반대하거나, 조직과 경쟁하거나, 조직의 이익에 저촉되는 행위
 - 금전적 또는 기타 사적 이득을 취할 가능성 촉발
 - 잠재적 또는 실제적 손실 또는 손해로부터 자신을 보호하려는 의도
 - 혈연을 중시하거나 특정 개인의 편의를 봐주려는 의도

내부감사인은 어떠한 경우에도 자신의 이익이나 최고경영진 또는 기타 권위있는 자를 포함한 다른 사람의 이익, 혹은 정치적 환경이나 주변의 다른 여건에 의해 부당하게 영향을 받아서는 안 된다.

내부감사 서비스를 수행할 때:

- 내부감사인은 과거 1 년간 자신이 자문 서비스를 제공했거나, 중책을 맡았거나, 중대한 영향력을 행사할 수 있었던 업무활동에 대해 검증업무를 수행할 수 없다. 동일한 상황에서 자문 서비스 요청을 받았을 경우, 수락 전에 요청자에게 그러한 상황을 공개하는 경우에만 자문 서비스를 수행할 수 있다. 공개 이후에 내부감사인은 자문업무를 수락할 수 있다.
- 내부감사업무 수행을 감독하고, 감독 대상 감사의 적정한 문서화 여부에 대한 검토는 반드시 자격을 구비한 유능한 내부감사인이 수행해야 한다. 내부감사인이 최고감사책임자가 책임을

맡고 있는 영역에 대한 검증업무를 수행할 때에는 반드시 독립적이고 자격을 구비한 자가 해당 업무를 감독해야 한다.

최고감사책임자는 객관성 손상을 해결하기 위한 내규 및 절차를 반드시 수립해야 한다. 내부감사인은 최고감사책임자 또는 그 역할을 수행하도록 지명된 자와 손상요인을 반드시 논의하고, 관련 내규 및 절차에 따라 적절한 조치를 취해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

객관성 손상요인은 내부감사인의 판단과 결정에 영향을 미쳐 감사 지적사항 및 결론을 변경할 수 있게 만드는 상황, 활동 및 관계를 말한다. 표준 2.2의 객관성의 보호는 내부감사인이 공정하고 편견 없는 사고방식을 유지하기 위해 피해야 하는 상황, 활동, 관계의 유형을 명시하고 있다. 감사인이 의도하지 않은 경우에도 객관성 손상요인은 실제로 또는 외관상 존재할 수 있다. 객관성이 실제로 손상되지 않은 경우에도 다른 사람들은 객관성이 손상된 것으로 인식할 수 있다. 내부감사인은 객관성을 손상시킬 수 있거나 손상되었을 것으로 추정되는 추가적인 상황에 대해 판단해야 한다.

이해충돌은 내부감사인이 내부감사 임무를 공정하게 수행하기 어렵게 하는 업무적 또는 사적 이해관계가 서로 경합하는 상황을 말한다. 이해충돌은 비윤리적이거나 부적절한 행위를 유발하지 않더라도 내부감사인, 내부감사부서 및 내부감사직 전체에 대한 신뢰를 약화시킬 수 있는 부적절한 외관을 초래할 수 있다.

내부감사부서의 내규 및 절차는 다음과 관련하여 내부감사인에게 기대 및 요건을 명시해야 한다.

- 선물, 호의 및 보상의 수락
- 객관성을 손상시킬 수 있는 상황의 식별
- 객관성의 손상을 인지했을 때 적절한 대응

선물로 받을 수 있는 금액을 제한하는 규정과 같이 대부분의 조직에는 선물, 보상 및 호의 수락과 관련된 내규가 있다. 내부감사활동 수행 시 객관성이 지니는 중요성 때문에 최고감사책임자는 조직보다 엄격한 내규를 정할 수 있다. 내부감사인은 조직의 내규와 최고감사책임자의 내규 중에서 보다 엄격한 내규를 따라야 하며, 선물, 보상 또는 호의의 수락이 자신의 판단에 영향을 미치거나 호의적인 감사 지적사항, 결론 혹은 결과를 제공하는 대가로 수수한 것으로 인식될 수 있는지 신중히 고려해야 한다.

조직 및/또는 내부감사부서의 내규는 이해충돌을 야기할 수 있는 특정 활동이나 관계를 금지할 수 있다. 피해야 할 활동에는 조직의 임직원, 외부 납품업체 및 공급업체와 업무 외적으로 친목을 다지는 것이 포함될 수 있다. 내부감사인은 투자와 같은 금전적 유대 관계 및 사적 친분 관계를 피해야 하는데 있어 사실상이든 표면상이든 이해충돌에 해당될 수 있기 때문이다.

최고감사책임자는 성과평가 및 보상체계, 상여금, 인센티브 제도로 인해 발생할 수 있는 내부감사인의 잠재적인 객관성 손상을 줄이기 위한 예방책을 마련해야 한다. 다음은 내부감사인의 객관성을 손상시킬 수 있는 보상 체계의 예이다:

- 감사대상부서 경영진의 의견 또는 동 경영진을 대상으로 실시한 설문조사 결과에 기반한 성과평가 및 보상
- 감사업무수행 중 형성한 지적사항의 개수, 감사대상부서의 매출증가나 비용절감, 인원감축 기여에 기반한 성과 측정
- 감사대상부서 경영진이 선물 및 사례하는 방법으로 감사인에게 간접적인 보상을 하도록 허용

내부감사인은 객관성에 대해 자신이 이해한 바와 관련 내규 및 절차를 적용하여 어떤 상황, 활동 또는 관계가 객관성을 손상시킬 수 있거나 손상시키는 것으로 추정되는지 평가해야 한다. 여기에는 다른 사람들의 인식도 고려되어야 한다.

표준 2.2 객관성의 보호에서 언급된 감사업무의 인원배정 및 감독 요건은 업무에 배정된 내부감사인이 점검 대상 업무의 일부분을 최근에 담당한 적이 없음을 확인하기 위함이다. 그로 인해 관점이 편향되거나, 특정 결과를 도출해야 할 이해관계가 발생하거나, 객관성이 손상되었다는 인식이나 외관을 형성할 수 있기 때문이다. 감사업무 전체를 수행하고 감독하는 내부감사인은 점검 대상 업무로부터 독립성을 유지해야 한다.

감사업무자원 계획을 수립할 때 최고감사책임자나 최고감사책임자 역할을 대행하도록 지명된 감독자는 내부감사인과 감사업무에 대해 논의하여 객관성에 대한 현재 또는 잠재적인 손상요인을 식별해야 한다. 논의 시 이전에 공개된 손상요인도 고려해야 한다.

감사업무 감독 프로세스의 일환으로 감사조서를 검토하여 지적사항과 결론이 적절하게 뒷받침되었는지 확인한다. 또한, 감사업무의 감독은 경험 많은 내부감사인이 잠재적인 객관성 우려사항에 대한 피드백과 멘토링을 제공할 수 있는 기회를 제공한다. (표준 12.3 감사업무 성과의 보장 및 개선, 표준 13.5 감사업무 자원 참조)

객관성 손상을 피할 수 없는 경우 표준 2.3 객관성의 손상 공개에서 설명된 대로 이를 공개하고 경감해야 한다.

공공 부문

공공 부문 내부감사인의 자문 서비스에 잠재적인 손상요인이 있는 경우, 관련 법규는 해당 자문 서비스의 요청자가 이러한 요인을 이해하고 지적사항, 권고사항 및 결론에 대한 책임을 수락함을 확인하도록 요구할 수 있다. 또한 내부감사인은 최종 감사업무 커뮤니케이션에서 잠재적 손상요인을 공개해야 할 수도 있다.

적합성 증거

- 잠재적 손상요인과 필요한 보호장치를 식별하기 위한 내규 및 절차
- 객관성 교육 기록
- 감독자의 검토 기록
- 증명서
- 보상 계획

- 객관성 손상요인을 논의한 이사회 의사록
- 객관성 손상요인을 공개한 문서
- 객관성 손상을 피할 수 없는 경우, 내부감사 활동계획을 완수하기 위한 대안을 제시하고 있는 계획
- 내부감사부서의 이해관계자에게 실시한 설문조사와 같이, 최고감사책임자의 객관성 인식에 대한 피드백의 출처
- 외부의 독립적인 평가자가 수행한 감사품질에 대한 외부평가 결과

국제내부감사표준 2.3 객관성의 손상 공개

요건

실질적으로나 외관상으로 객관성이 손상된 경우, 그 세부사항을 내부감사 서비스를 수행하기 전에 해당 당사자에게 반드시 공개해야 한다.

내부감사인인 자신의 객관성에 영향을 미칠 수 있는 손상요인에 대해 알게 되는 경우, 내부감사인인 최고감사책임자 또는 지정된 감독자에게 반드시 그 사실을 공개해야 한다. 최고감사책임자가 내부감사인의 객관적인 직무 수행 능력에 영향을 미치는 손상요인이 존재한다고 판단하는 경우, 최고감사책임자는 점검 대상 부서의 경영진, 최고경영진 및/또는 이사회와 반드시 그러한 요인을 논의하고, 상황 해결을 위해 적절한 조치를 취해야 한다.

감사지적사항, 권고사항 및/또는 결론의 신뢰성이나 신뢰성 인식에 영향을 미치는 손상요인이 업무 종료 후 발견된 경우, 최고감사책임자는 점검 대상 부서의 경영진, 최고경영진, 이사회 및/또는 영향을 받는 기타 이해관계자와 반드시 해당 우려사항을 논의하고, 상황 해결을 위해 적절한 조치를 취해야 한다. (표준 11.4 오류 및 누락 참조)

최고감사책임자의 객관성이 사실상 또는 외관상 손상되는 경우, 최고감사책임자는 반드시 손상요인을 이사회에 공개해야 한다. (표준 7.2 최고감사책임자의 역할, 책임 및 자격과 표준 7.3 독립성의 보호 참조)

실행 및 적합성 증거를 위한 고려사항

실행

객관성 손상요인을 공개하라는 요건은 각각의 객관성 손상요인을 해결하기 위해 취해야 할 조치를 설명하는 것으로, 일반적으로 내부감사 내규 및 절차에 정의되어 있다. 객관성 손상요인을 공개하고 경감하는 전반적인 접근방식은 일반적으로 최고경영진 및 이사회와의 합의하에 최고감사책임자가 결정한다.

객관성 손상이 불가피한 경우, 최고감사책임자는 다음을 포함하여 손상을 경감하기 위한 방법을 고려할 수 있다:

- 객관성이 손상된 감사인을 해당업무에서 제외하고 다른 내부감사인을 배정한다.

- 적정하게 조정된 감사인력을 고려하여 감사업무일정을 다시 수립한다.
- 감사업무의 범위를 조정한다.
- 감사업무 수행이나 감독을 아웃소싱(outsourcing)한다.

객관성 손상에 관한 문제가 감사업무계획 수립 중에 발생하면 최고감사책임자는 점검 대상 부서의 경영진 및/또는 최고경영진과 우려사항에 대해 논의하고, 리스크 노출이 최소화된 이유와 관리 방법을 설명할 수 있으며, 이러한 논의를 문서화할 수 있다.

최고감사책임자 또는 기타 내부감사인인 내부감사활동이 아닌 역할이나 책임을 담당할 것을 요청받는 경우, 최고감사책임자는 보고 관계, 책임, 기대 역할에 대해 최고경영진 및 이사회와 논의해야 한다. 이 같은 논의 중 최고감사책임자는 객관성 및 제안된 역할과 책임이 야기할 수 있는 잠재적 객관성의 손상, 이러한 손상을 경감하기 위해 필요한 안전장치에 관한 IIA의 표준을 강조해야 한다. (표준 6.1 내부감사의 임무, 표준 7.2 최고감사책임자의 역할, 책임 및 자격, 표준 7.3 독립성의 보호, 표준 9.3 내부감사현장 참조)

적합성 증거

- 객관성 손상 공개에 대한 내부감사 내규 및 절차
- 객관성 손상 공개 문서
- 손상 공개에 대해 커뮤니케이션한 기록과 수령 기록, 적절한 당사자의 대응/승인 기록

원칙 3 감사역량 입증

내부감사인은 자신의 역할과 책임을 성공적으로 완수하기 위해 필요한 지식, 스킬(skill) 및 역량을 적용한다.

감사역량을 입증하려면 내부감사 서비스를 제공하기 위한 지식, 스킬 및 능력을 개발하고 적용해야 한다. 내부감사인이 경제적, 환경적, 법적, 정치적, 사회적 맥락뿐만 아니라 비즈니스, 경영 및 신기술에 대한 이해를 증진시키는 것이 여기에 포함된다.

국제내부감사표준 3.1 감사역량

요건

내부감사인은 반드시 자신의 책임을 성공적으로 수행할 수 있는 지식, 기술 및 역량을 소유하거나 획득해야 한다.

내부감사인은 반드시 필요 역량을 소유하고 있거나 획득할 수 있는 서비스에만 참여해야 한다. 감사인 개개인에게는 직책 완수에 필요한 역량을 지속적으로 개발하고 적용할 책임이 있다.

내부감사인의 역량은 다음과 관련된 지식, 스킬 및 능력의 소유로 입증된다:

- IIA의 국제내부감사표준 및 현행 내부감사직무수행기준

- 감독, 리더십, 커뮤니케이션 및 협업
- 거버넌스, 리스크 관리 및 통제 프로세스
- 재무 관리 및 정보 기술과 같은 비즈니스 기능과 부정행위 등과 같은 상시적 리스크
- 산업별 법규 및 관행
- 데이터 수집, 분석 및 평가를 위한 툴(tool)과 기법
- 현재의 감사활동, 동향 및 새로 등장하는 이슈

또한 최고감사책임자는 반드시 내부감사부서가 내부감사현장에 기술된 서비스를 수행할 수 있는 역량을 집합적으로 소유하고 있음을 보장하거나, 필요한 역량을 확보하기 위한 조치를 취해야 한다. (표준 7.2 최고감사책임자의 역할, 책임 및 자격과 표준 10.2 인적 자원 관리 참조)

실행 및 적합성 증거를 위한 고려사항

실행

내부감사인원은 어떤 경력 단계에 해당하건 다음 사항을 이행해야 한다:

- 국제공인내부감사사(CIA) 및 IIA 와 다른 전문가 단체에서 제공하는 기타 인증과 자격증 같은 적절한 전문 자격을 취득함.
- 이해관계자, 동료 및 감독자가 제공한 피드백을 기반으로 개발이 필요한 역량과 개선 기회를 파악함.
- 내부감사 방법론뿐만 아니라 내부감사인이 서비스를 제공하는 조직과 관련된 비즈니스 활동에 대해서도 교육을 이수함. 예를 들면, 투자회사에 내부감사 서비스를 제공하는 내부감사인은 투자 회사와 관련된 비즈니스 프로세스에 대해 교육을 받아야 한다. 교육 기회에는 강좌 수강, 멘토와의 협업 또는 감사업무 기간 중 감독자의 감독 하에 새로운 과업 배정이 포함될 수 있다.

내부감사부서가 서비스를 수행할 수 있는 역량을 집합적으로 소유했음을 보장하기 위해, 최고감사책임자는 다음을 이행해야 한다:

- 감사업무를 배정하고, 교육 필요성을 파악하고, 공석을 채우기 위해 내부감사인을 채용할 때 활용가능한 내부감사인의 역량 목록을 관리함.
- 내부감사인 개개인의 연례 고과 평가 참여함.
- 내부감사부서의 역량 향상이 필요한 분야 파악함.
- 내부감사인의 지적 호기심을 장려하고 교육 및 내부감사 성과를 개선할 수 있는 기타 기회에 투자

- 내부감사부서가 보유하고 있지 못한 특수한 역량 또는 추가가 필요한 전문역량을 제공할 수 있는 다른 검증 및 자문 서비스 제공자를 파악하고 이러한 역량을 이들에게 위탁하는 것을 고려
- 내부감사부서가 요청받은 서비스를 수행할 수 있는 역량을 집합적으로 소유하지 않은 경우, 독립적인 외부 서비스 제공자와의 계약을 고려
- 감사품질 평가 및 개선 프로그램(QAIP)을 효과적으로 실행

적합성 증거

- 내부감사인의 인증, 교육, 경험, 업무 경력 및 기타 자격을 나열한 목록이나 문서
- 역량 및 전문성 개발 계획에 대한 내부감사인의 자체 평가
- 강좌, 컨퍼런스, 워크숍 및 세미나와 같은 보수 교육(CPE)을 내부감사인이 이수한 문서
- 최고감사책임자의 내부감사인 성과 검토 문서
- 감사업무 감독자의 검토 문서, 내부감사 이해관계자가 감사 종료 후 작성한 설문조사, 내부감사인 개인 및 내부감사부서 전체가 보여준 역량에 대해 표현한 기타 피드백(feedback)
- 감사품질에 대한 내부 및 외부의 평가 결과
- 내부감사계획 이행을 위해 필요한 역량의 목록, 차이분석, 격차를 메우기 위해 필요한 교육 및 예산 파악을 포함하여 내부감사계획 자원을 확충하기 위해 최고감사책임자가 작성한 관련 문서
- 내부감사부서가 의뢰할 수 있는 기타 검증 및 자문 서비스 제공자의 역량을 나타내는 검증 지도(assurance map) 등의 문서

국제내부감사표준 3.2 지속적인 전문성 개발

요건

내부감사인은 내부감사 서비스의 효과와 품질을 제고하기 위해 자신의 역량을 유지하고 지속적으로 개발해야 한다.

내부감사인은 반드시 매년 최소 20 시간의 보수교육(CPE)을 이수함으로써 지식, 스킬(skill) 및 능력을 향상시켜야 한다. 전문 내부감사 인증을 취득한 내부감사 실무자는 반드시 보수교육에 대한 추가 요건을 충족하여 인증을 최신 상태로 유지해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

내부감사인은 매년 최소 20 시간의 보수교육을 이수함으로써 최신 지식을 습득하고 관련 주제에 대한 이해를 심화하여 내부감사 서비스의 효과와 품질을 제고할 수 있다. 내부감사인은 자신이 근무하는 조직과 내부감사직무에 영향을 미칠 수 있는 새로운 주제, 리스크, 추세 및 변화에 대해

배울 수 있는 기회에 초점을 맞춰야 한다. 국제공인내부감사사(CIA) 등 전문자격을 취득한 내부감사인은 자격을 유지하기 위한 추가적인 요건을 알고 있어야 한다. 요건을 충족하지 못한 경우, 내부감사인의 자격 사용 승인이 취소되는 등의 결과를 초래할 수 있다.

필수 보수교육의 일환으로 IIA 는 자격 소지자가 매년 윤리 교육을 이수하도록 요구한다. 이 요구사항은 특히 IIA 인증과 관련되어 있으며, 모든 내부감사 전문가는 정기적으로 윤리 중심의 보수교육이나 훈련을 받아야 한다.

내부감사부서 전체에 대한 교육 및 훈련 기회를 제공할 책임은 최고감사책임자에게 있지만, 궁극적으로 역량을 개발하고 배움의 기회를 모색해야 하는 것은 내부감사인의 개인의 책임이다. 예를 들어, 내부감사인은 익숙하지 않거나 경험이 제한적인 조직의 프로세스나 영역과 관련된 감사업무를 배정해 달라고 요청할 수 있다. 또한, 내부감사인은 피드백과 제안을 제공하고 자신의 경험과 통찰력을 공유하는 감독자로부터 멘토십(mentorship) 및 긴밀한 지도를 받을 기회를 모색하고 환영해야 한다.

내부감사인은 뉴스 서비스 및 뉴스레터를 구독하여 내부감사직무와 자신이 근무하는 조직과 관련된 업계의 최신 동향을 파악할 수 있다. 또한, 최고감사책임자가 온라인 또는 대면 세미나에 참석하거나 내부감사 직원에게 추천할 수 있다. 최고감사책임자는 주기적으로 내부감사 직원 교육 행사를 기획하여 내부감사 직무수행에 새로운 기술이나 변화를 도입할 수 있다.

전문성 개발 계획에는 내부감사인의 진로 및 전문성 개발 필요성에 대한 정기 검토와 평가가 포함되어야 한다. 최고감사책임자는 훈련 계획과 예산 분배 시 내부감사부서 전체의 역량 개발에 투자하는 것과 내부감사인 개인의 직업적 성장 목표를 달성할 수 있는 기회를 제공하는 것 사이에 균형을 유지해야 한다.

적합성 증거

- 교육 행사 및 기타 보수교육 계획 문서
- 내부감사인이 이수한 보수교육 및 취득한 자격증에 대한 기록
- 내부감사인의 성과 검토 및/또는 전문성 개발 계획
- 감사인 대회 참석 및 자원봉사와 같이, IIA 와 기타 유관 전문 단체활동에 적극적으로 참여했다는 증거

원칙 4 전문가로서의 정당한 주의 이행

내부감사인은 내부감사 서비스를 계획하고 수행할 때 전문가로서 정당한 주의를 기울인다.

전문가로서 정당한 주의 이행과 관련된 표준은 다음을 사항을 요구한다:

- 국제내부감사표준과의 적합성
- 수행할 업무의 성격, 상황 및 요건에 대한 고려
- 정보를 비판적으로 평가하고 질문하기 위해 전문가적 의구심을 적용

전문가로서 정당한 주의를 기울여야 합리적으로 신중하고 유능한 다른 내부감사인 지닌 성실성, 판단력 및 의구심을 가지고 내부감사 서비스를 계획하고 수행해야 한다. 내부감사인은 서비스를 제공받는 자들의 최선의 이익을 위해 전문가로서 정당한 주의를 이행하지만 그렇다고 완전 무결한 것은 아니다.

국제내부감사표준 4.1 국제내부감사표준과의 적합성

요건

내부감사인은 반드시 국제내부감사표준에 따라 내부감사 서비스를 계획하고 수행해야 한다.

내부감사부서의 방법론은 반드시 이 표준을 준수하면서 수립, 문서화 및 관리되어야 한다. 내부감사인은 내부감사 서비스 계획을 수립하고 이행할 때와 내부감사 지적사항, 권고사항, 결론 및 기타 결과를 전달할 때 이 표준과 내부감사부서의 방법론을 반드시 따라야 한다.

내부감사인 또는 내부감사부서가 이 표준의 일부를 준수하는 것이 법규로 금지된 경우, 이를 제외한 다른 표준은 모두 준수되어야 하며 반드시 적절하게 공개되어야 한다.

이 표준과 다른 권위 있는 기관에서 발행한 요건 간에 불일치가 존재할 경우, 내부감사인과 내부감사부서는 반드시 이 표준을 따라야 하며, 다른 요구사항이 더 엄격한 경우 해당 요구사항을 따를 수도 있다.

실행 및 적합성 증거를 위한 고려사항

실행

최고감사책임자는 매년 이 표준을 검토하고 내부감사부서의 방법론을 업데이트(update)하여 둘 사이의 정합성을 보장해야 한다.

최고감사책임자 또는 지정된 감사업무 감독자는 감사업무 수행 프로그램이 이 표준의 요건과 일치하고, 내부감사 업무가 이 표준의 요건에 따라 수행됨을 보장해야 한다.

내부감사인은 이 표준을 준수하며 업무를 수행할 수 없는 경우, 최고감사책임자 또는 지정된 감독자와 부적합 사유 및 그러한 부적합이 감사업무에 미치는 영향에 대해 논의해야 한다. 표준 8.3 품질, 표준 12.1 내부 품질 평가, 표준 15.1 최종 감사업무 커뮤니케이션은 이 표준과의 적합성 및 부적합에 관한 커뮤니케이션과 관련 추가 요건을 제공한다.

적합성 증거

- 내부감사부서의 감사방법론과 최신 업데이트(update)에 관한 기록문서
- 최종 감사업무 커뮤니케이션과 최고경영진 및 이사회와의 커뮤니케이션에서 이 표준과의 적합성에 관한 진술과 부적합 사실의 공시
- 내부감사인이 따라야 하지만, 이 표준을 준수하는 것은 방해하는 법규에 관한 참조 문서
- 이 표준 외에도 내부감사부서가 따르는 기타 권위 있는 요건에 관한 참조목록

- 감사품질 평가 및 개선 프로그램(QAIP)의 결과

국제내부감사표준 4.2 전문가로서 정당한 주의

요건

내부감사인은 다음을 포함하여 제공할 서비스의 성격, 상황 및 요건을 고려하여 반드시 전문가로서 정당한 주의를 기울여야 한다:

- 조직의 전략 및 목표
- 내부감사 서비스를 제공받는 자와 기타 이해관계자의 최선의 이익
- 거버넌스, 리스크 관리 및 통제 프로세스의 적정성 및 실효성
- 수행할 내부감사 서비스의 잠재적 효익과 관련된 비용
- 감사업무 목표를 달성하는 데 필요한 업무의 범위와 적시성
- 검토대상 업무에 대한 리스크의 상대적 복잡성, 중대성 또는 중요성
- 심각한 오류, 부정행위, 컴플라이언스 실패와 목표, 운영 또는 자원에 영향을 미칠 수 있는 기타 리스크의 발생확률
- 적절한 기법, 툴(tool) 및 기술의 사용

실행 및 적합성 증거를 위한 고려사항

실행

내부감사인이 전문가로서 정당한 주의를 기울여 서비스를 수행하기 위해서는 내부감사활동의 목적과 제공할 내부감사 서비스의 성격을 고려하고 이해해야 한다. 내부감사인은 내부감사현장, 최고감사책임자의 내부감사계획 및 계획에 포함시킬 감사업무를 결정하는데 도움이 되는 상황을 이해하는 것부터 시작해야 한다. 내부감사 서비스 계획을 수립하고 수행할 때 내부감사인은 조직의 고객 및 조직의 조치에 의해 영향을 받는 기타 이해관계자(일반 대중 포함)의 최선의 이익도 고려한다. 여기에는 이해관계자의 기대(공정하고 정직한 비즈니스 수행 등), 요구(안전 등), 조직의 전략 및 목표와 뚜렷하게 관련되지 않을 수도 있는 기저의 리스크에 대한 잠재적 노출이 포함된다.

관련 상황에는 조직의 전략 및 목표와 조직의 거버넌스, 리스크 관리 및 통제 프로세스의 적정성과 실효성이 포함된다. 최고감사책임자는 내부감사계획의 기반이 되는 리스크 평가를 수행할 때 이러한 상황을 고려한다. 또한 내부감사인은 감사 수행 시 검토대상 업무활동과 관련하여 이러한 상황을 고려한다. 내부감사인은 이러한 이해를 기반으로 수행하게 될 내부감사 서비스에 접근함으로써 전문가로서 정당한 주의를 기울인다.

내부감사인은 내부감사 서비스 계획 수립 초기 단계에서 검토대상 업무활동 조직의 경영진과 커뮤니케이션하고 정보를 수집하여 감사업무 목표 및 범위를 결정한다. (표준 13.1 감사업무 커뮤니케이션 및 표준 13.2 감사업무 리스크 평가 참조). 검토대상 조직 또는 업무활동과 관련된 리스크의 우선순위를 정할 때, 전문가로서 정당한 주의를 이행하기 위해서는 경영진이 저지른

심각한 오류, 법규 위반, 부정행위 및 검토대상 조직이나 업무운영, 자원에 영향을 미칠 수 있는 기타 리스크의 발생확률을 고려해야 한다. 이는 다시 감사업무 목표 달성에 영향을 미친다.

평가 대상 리스크의 복잡성, 중대성 및 중요성은 상대적이다. 한 리스크가 조직 전체에는 중대하거나 중요하지 않을 수 있지만, 특정 감사업무나 검토대상 업무활동과 관련해서는 중대하거나 중요할 수 있다. 따라서 관련 리스크를 적절하게 평가하고, 추가적인 평가를 위해 리스크의 우선순위를 결정하려면 맥락 속에서 복잡성, 중대성 및 심각성을 이해하는 것이 필요하다.

또한, 전문가로서 정당한 주의는 내부감사 서비스 비용(필요한 자원의 양 등)의 결과로 얻을 수 있는 효익과 비교할 것을 요구한다. 예를 들어, 검토대상 업무활동의 통제 설계 자체가 적절하지 않은 경우 해당 통제장치의 효과성을 종합 평가하는 것은 투입 비용 대비 가치가 없을 것이기 때문이다. 내부감사인은 조직의 내부감사 서비스에 대한 투자 대비 최대의 가치 또는 효익 제공을 추구한다. 또한, 내부감사인은 철저한 계획수립을 위해서 감사업무 목표를 가장 효율적으로 달성하는 데 필요한 기법, 툴(tool), 기술과 감사업무의 범위 및 적시성을 고려해야 한다. 내부감사인, 특히 최고감사책임자는 점검과 평가 프로세스를 지원하는 데이터 분석 소프트웨어 및 기타 기술의 이용을 고려해야 한다.

표준 4.2의 전문가로서 정당한 주의 조항에서 직접 요구하고 있는 사항은 아닐지라도, 감사업무를 적절하게 감독하고 감사품질 평가 및 개선 프로그램(QAIP)을 실행할 때에도 전문가로서 정당한 주의를 이행해야 한다. (표준 8.4 감사품질에 대한 외부평가, 표준 12.1 감사품질에 대한 내부평가, 표준 12.2 성과 측정, 표준 12.3 감사업무 수행의 보장 및 개선 참조)

적합성 증거

- 검토 대상인 조직과 업무활동의 전략 및 목적을 문서화한 기록
- 거버넌스, 리스크 관리 및 통제 프로세스 평가서
- 오류, 컴플라이언스의 실패 및 부정행위를 포함한 리스크 평가 문서
- 수행할 내부감사 서비스의 잠재적 비용과 효익 및 감사업무 수행 범위와 적시성에 관한 회의 및 논의 내용을 기록한 기록물
- 감사업무 감독자의 검토내용이 기재된 감사조서
- 내부감사인의 수행 검토
- 전문가로서 정당한 주의에 관한 회의, 교육 또는 기타 논의 내용을 기록한 기록물
- 설문조사나 기타 툴(tool)을 통해 수집한 이해관계자의 피드백
- 내부감사부서의 감사품질 평가 및 개선 프로그램(QAIP)의 일환으로 수행된 내부 및 외부의 평가

국제내부감사표준 4.3 전문가적 의구심

요건

내부감사인은 내부감사 서비스를 계획하고 수행할 때, 반드시 전문가적 의구심을 가져야 한다. 전문가적 의구심을 갖기 위해 내부감사인은 반드시 다음을 수행해야 한다:

- 의문을 제기하는 마음을 지닌 태도를 유지한다.
- 정보의 신뢰성을 비판적으로 평가한다.
- 일관성 없는 정보에 대해 우려를 제기하거나 질문을 할 때에는 솔직하고 직선적이어야 한다.
- 불완전하거나, 일관성이 없거나, 거짓이거나, 오해의 여지가 있는 정보 및 진술에 대해 판단을 내릴 때는 추가적인 증거를 찾는다.

실행 및 적합성 증거를 위한 고려사항

실행

전문가적 의구심은 내부감사인이 신뢰나 믿음이 아니라 사실, 정보 및 논리를 기반으로 객관적인 판단을 내릴 수 있게 해준다. 의구심은 주장, 진술 및 기타 정보의 타당성과 진실성에 대해 항상 질문하거나 의심하는 태도이다. 감사인은 경영진의 진술을 뒷받침하고 검증하기 위한 증거를 찾을 때 전문가적 의구심을 가져야 한다. 감사인은 사실 또는 진실이라고 제시된 정보를 질문이나 의심 없이 단순히 신뢰하지 않는다. 전문가적 의구심에는 주어진 주제의 피상적 수준을 넘어 탐구하려는 의지와 호기심이 필요하다.

내부감사업무를 수행할 때 감사인은 관련성 있고 신뢰할 수 있으며 충분한 정보를 수집하고 해당 정보를 분석 및 평가하기 위해 전문가적 의구심을 가져야 한다. 내부감사인이 정보가 불완전하거나 일관성이 없거나 거짓이거나 오해의 여지가 있다고 판단하는 경우, 추가 분석을 수행하여 정확하고 완전한 정보를 식별하고 감사 지적사항, 권고사항 및 결론을 뒷받침하는 증빙을 생성해야 한다. 최고감사책임자나 지정된 감사업무 감독자가 감사조서 및/또는 감사업무 커뮤니케이션을 검토하고 승인함으로써 추가적인 검증이 제공된다.

최고감사책임자는 내부감사인이 전문가적 의구심과 관련된 역량을 개발하도록 지원해야 한다. 워크숍 및 기타 교육 기회는 내부감사인이 전문가적 의구심을 개발하고 적용하는 법을 배우며, 편견을 피하고 개방적이며 호기심 많은 사고방식 유지의 중요성을 이해하는데 도움이 될 수 있다. 내부감사인은 일관성이 없거나 불완전하거나 거짓이거나 오해의 여지가 있는 정보를 인식하는 방법을 배울 수 있다. 또한, 최고감사책임자는 주어진 감사 기간 내에서 증거를 찾기 위해 투자해야 할 적절한 시간에 대한 기대치를 설정해야 한다.

적합성 증거

- 참가자 목록을 포함하여, 관련 교육의 기획 및 이수 기록
- 내부감사인이 감사업무 수행 중 수집한 정보를 평가하고 검증하는 방식이 표시된 감사조서
- 거짓 또는 오해의 여지가 있는 정보를 감사 지적사항으로 문서화

- 감사업무 감독자가 검토하고 서명 또는 이니셜을 기재한 감사조서 및 감사업무 커뮤니케이션 기록

원칙 5 비밀 유지

내부감사인은 정보를 적절하게 이용하고 보호한다.

내부감사인은 감사업무 수행 과정에서 기밀, 재산권 및/또는 개인 식별이 가능한 정보를 입수하게 된다. 여기에는 물리적 및 디지털 형식의 정보와 공식 또는 비공식 회의와 같은 구두 커뮤니케이션이 포함된다. 내부감사인은 이러한 정보를 승인된 목적으로만 사용하고, 내부 및 외부의 무단 접근이나 유출로부터 보호함으로써 입수한 정보의 가치와 소유권을 존중한다.

국제내부감사표준 5.1 정보의 이용

요건

내부감사인은 내부감사 서비스 수행을 위해 정보를 이용할 경우 반드시 조직과 내부감사부서의 내규 및 절차를 따른다.

내부감사인은 반드시 배정된 감사업무나 서비스를 수행하는 데 필요한 정보만 수집하고 문서화해야 한다. 이러한 정보는 반드시 승인된 목적으로만 이용해야 한다.

내부감사인은 절대로 사적 이익을 위해서나, 위법적이거나 조직의 정당하고 윤리적인 목표에 해가 되는 방식으로 정보를 이용해서는 안 된다.

실행 및 적합성 증거를 위한 고려사항

실행

내부감사인은 정보를 취급하고 이용할 때 조직과 내부감사부서의 내규 및 절차를 따라야 한다. 최고감사책임자는 내부감사인이 접근할 수 있는 정보의 적절한 이용과 관련하여 내규, 절차 및 기대사항을 내부감사인과 논의해야 한다. 최고감사책임자는 이러한 내규 및 절차에 대한 이해를 확인하기 위하여 내부감사인에게 증명서나 기타 양식에 서명하도록 요구할 수 있다.

내부감사인은 감사업무 수행 시 종종 기밀 정보, 독점 정보 및/또는 개인 식별 정보에 접근할 수 있다. 이러한 정보를 부적절하게 이용하면 평판 손상 및 법규 위반과 같이 의도치 않은 결과를 초래할 수 있다.

감사업무수행 프로그램이나 감사조서의 양식에는 정보 이용에 대한 인가를 상기시켜주는 문구가 포함되어야 한다. 전자 양식에는 내부감사인이 문서에 접근하여 작성하기 전에 이러한 문구를 확인하도록 요구하는 자동 통제장치가 포함될 수 있다.

내부감사인은 사적 이익을 위해 조직 내부의 재무, 전략 또는 운영 지식이나 기타 조직에 관한 정보를 이용해서는 안 된다. 예를 들어 주식의 매수나 매도, 또는 경쟁관계에 있는 상품 제작에

정보를 제공하기 위해 내부감사 서비스를 통해 입수한 정보를 이용, 매매 혹은 유출해서는 안 된다. 내부감사인은 제공 서비스와 관련이 없는 정보에 접근해서는 안 된다.

적합성 증거

- 정보의 적절한 이용에 관한 내규, 절차 및 교육 관련 문서
- 정보의 적절한 이용에 관한 회의 회의록
- 정보이용 관련 내규, 절차 및 법규에 관하여 이해하는 것으로 인정되는 교육 참석 기록
- 정보이용 관련 내규 및 절차를 준수했음을 입증하는 수행 검토
- 효과적으로 설계 및 운영되는 정보 접근 통제장치

국제내부감사표준 5.2 정보의 보호

요건

내부감사인은 반드시 정보보호에 대한 책임을 인지하고 내부감사를 수행하거나 직무 관계의 결과로 얻은 정보의 기밀성, 프라이버시(privacy) 및 소유권을 존중하는 방식으로 행동해야 한다.

내부감사인은 반드시 소속 조직이 운영되는 지역 사법관할권의 기밀유지, 정보 보안 및 정보 프라이버시와 관련된 법규를 이해하고 준수해야 한다. 또한 내부감사인은 다음 관련하여 반드시 소속 조직과 내부감사부서의 내규 및 절차를 따라야 한다:

- 감사업무 기록의 보관, 보존 및 폐기
- 내부 및 외부의 당사자에게 감사업무 기록 공개
- 더 이상 필요하지 않은 기밀 정보에 대한 접근이나 사본의 취급

법적 또는 직업적 책임이 있는 경우를 제외하고, 내부감사인은 인가되지 않은 자에게 절대로 기밀 정보를 공개하면 안 된다. 이는 내부감사인이 조직 내에서 인사 이동되거나 퇴직하는 경우에도 적용된다.

내부감사인은 사회적 환경이나 동료 또는 가족을 포함하여 정보가 부주의하게 공개, 노출 또는 유출될 가능성에 대해 반드시 경계해야 한다.

최고감사책임자는 반드시 내부감사부서와 내부감사부서를 지원하는 개인이 동일한 정보보호 요건을 따르도록 보장해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

내부감사부서가 취득, 이용, 생산한 정보는 법규와 조직 및 내부감사부서의 내규와 절차에 의해 보호된다. 법규, 내규, 절차는 일반적으로 물리적, 디지털적 보안과 접근, 보존 및 폐기를 다룬다.

최고감사책임자는 법규상의 요건과 보호(예: 법적 특권 또는 변호사-의뢰인 특권)의 충격/영향을 더 잘 이해하기 위해 법률 고문과 상의해야 한다. 사업정보를 외부에 공개하기 전에 조직의 내규 및 절차에 따라 정당한 권한을 가진 자가 이를 검토하고 승인하도록 요구될 수도 있다.

정보는 데이터 암호화, 이메일 배포, 소셜 미디어 사용 제한, 정보에 대한 물리적 접근 제한과 같은 통제장치를 통해 의도적이거나 의도하지 않은 유출로부터 보호될 수 있다. 내부감사인이 이러한 데이터에 더 이상 접근할 필요가 없으면 디지털 허용 권한을 회수하고 출력한 사본은 정해진 내규 및 절차에 따라 처리해야 한다.

유출로부터 보호되어야 하는 정보의 전형적인 예는 개인정보이다(예: 급여, 징계 기록 또는 감독자 및 인사 담당자와 논의한 인사 문제). 이러한 정보에 대한 접근은 종종 패스워드 사용과 데이터 암호화를 포함한 물리적 및/또는 전산 통제를 통해 제한되거나 모니터링된다.

최고감사책임자는 내부감사인의 정보 접근 요구와 접근 통제의 효과적인 작동 여부를 주기적으로 평가 및 확인해야 한다.

공공 부문

공공 부문의 내부감사인은 정보 공개와 관련된 모든 법적 요건을 반드시 이해하고 준수해야 한다.

적합성 증거

- 감사 기록의 접근 통제, 보관, 보존 및 폐기, 내부 및 외부 당사자에 대한 감사 기록의 공개, 더 이상 필요하지 않은 기밀 정보의 취급과 관련된 내규, 프로세스, 절차의 적용을 보여주는 문서
- 접근을 제한하고, 통제장치를 우회하거나 위반할 리스크를 경감하는 메커니즘의 실행에 관한 문서
- 기밀유지 및 관련 내규, 절차, 법규에 대한 이해를 확인하는 정보보호 교육 참석 기록
- 정보보호 및 공개와 관련된 내규와 절차가 준수되었음을 입증하는 수행 검토
- 감사조서와 감사보고서 등 최종 커뮤니케이션 배포 제한사항에 관한 문서
- 모든 정보공개에 대한 허가서 및 승인된 배포 목록
- 법규상 요구되거나, 법률고문(해당 시), 최고경영진 및 이사회가 승인하여 공개한 정보의 기록
- 내부감사 업무 관련 정보의 기밀성이 유지되었음을 확인하는 증명서

영역 III 내부감사부서의 거버넌스

내부감사부서가 효과적이기 위해서는 확실한 거버넌스 체계 마련이 필수적이다. 이 영역에서는 내부감사부서에 권한을 부여하고, 독립적인 위치를 보장하며, 그 성과를 감독할 이사회에 책임을 설명하고 있다. 최고감사책임자는 이사회와 효과적으로 커뮤니케이션하고, 이사회에 정보를 제공할 책임이 있다. 이사회는 내부감사활동의 목적을 달성할 수 있는 내부감사부서의 능력에 관하여 중요한 역할 및 책임이 있다. 이 영역의 표준은 최고감사책임자 및 이사회가 공동으로 수행해야 하는 책임과 개별적으로 수행해야 하는 책임을 구분한다.

국제내부감사표준에서는 거버넌스를 담당하는 최상위 지배기구로서 "이사회"라는 용어로 사용하고 있는데, 이 용어는 다음을 지칭한다.

- 이사회 또는 이사회가 특정 기능을 위임한 위원회나 기구 (예: 감사위원회)
- 지배 기구가 둘 이상인 조직에서 비상임/감독 위원회
- 재단 등의 운영이사회
- 선출직 또는 정무직 공무원 집단

이사회가 존재하지 않는 경우 "이사회"라는 용어는 조직의 거버넌스를 담당하는 집단이나 개인을 의미한다(예를 들면, 일부 공기업 및 민간 부문의 중소기업은 조직의 수장이나 최고경영진이 최상위 지배 기구 역할을 수행하게 할 수 있다).

표준에서 제시하고 있는 이사회에의 책임은 내부감사부서가 내부 직원으로 구성되는지 또는 외부 서비스 제공자와 계약이 체결되었는지 여부와 관계없이 적용된다. 최고감사책임자의 책임은 내부 직원이든 외부 서비스 제공자의 직원이든 관계없이 이사회에서 지정한 자가 수행한다. 이사회는 내부감사부서의 표준 적합성을 확인할 책임이 있다.

원칙 6 이사회에의 권한 부여

이사회는 내부감사부서의 권한, 역할 및 책임을 정립하고, 승인하며 지원한다.

내부감사부서의 권한, 역할 및 책임은 내부감사의 임무에 정의되어 있다. 이에 따르면, 내부감사부서는 최고경영진과 이사회에 객관적인 검증과 조언을 제공함으로써 조직의 성공을 촉진하는 임무를 부여받았다. 내부감사부서는 조직 전체의 거버넌스, 리스크 관리 및 통제 프로세스의 효과성을 평가하고 개선하기 위해 체계적이고 규율화된 접근방식을 사용하여 임무를 수행한다.

국제내부감사표준 6.1 내부감사의 임무

요건

이사회의 책임

이사회는 내부감사부서의 권한, 역할 및 책임을 정의하고 내부감사 서비스의 범위와 유형을 명시한 내부감사의 임무를 반드시 승인해야 한다.

이사회는 효과적인 내부감사기능의 근간이 될 임무를 이해하고 지원하기 위해 최고감사책임자가 제공하는 정보를 반드시 고려해야 한다.

이사회는 새로운 최고감사책임자의 고용이나, 조직에 대한 리스크의 유형, 심각성 및 상호의존성 변화와 같이 조직에 영향을 미치는 변화들을 고려하기 위해 최소 연 1 회 내부감사의 임무를 반드시 검토해야 한다.

최고감사책임자의 책임

최고감사책임자는 내부감사의 임무를 정립하는 데 필요한 정보를 이사회에 반드시 제공해야 한다. 이 정보에는 내부감사부서의 거버넌스와 관련된 국제내부감사표준, 내부감사 서비스의 잠재적 범위 및 유형, 내부감사부서에 공통적인 기타 책임이 포함된다.

이사회가 내부감사 서비스의 범위와 유형을 결정하는 데 도움을 주기 위해, 최고감사책임자는 반드시 내부 및 외부의 다른 검증 제공자 및 규제기구와 협력하여 서로의 역할과 책임에 대한 상호 이해를 확보해야 한다. 이러한 상호 이해는 이사회와 공유되어야 한다.

공동의 책임

이사회와 최고감사책임자는 내부감사부서의 임무에 대해 반드시 논의하고 합의를 도출해야 한다. 최고감사책임자는 내부감사현장에 합의된 내부감사의 임무를 반드시 기술해야 하며, 이 현장은 이사회에 의해서 승인되어야 한다.

이사회와 최고감사책임자는 내부감사부서가 그 목표를 달성하는 데 있어 권한, 역할 및 책임이 충분한 지 평가하기 위해 적어도 연 1 회 내부감사의 임무와 현장에 대해 반드시 논의해야 한다. 최고감사책임자는 개정된 내부감사현장의 변경사항을 반드시 문서화해야 한다. 내부감사의 임무와 현장의 변경사항은 반드시 이사회의 승인을 얻어야 한다. (표준 9.3 내부감사현장 참조)

실행 및 적합성 증거를 위한 고려사항

실행

이사회의 실천사항

내부감사의 임무를 결정하기 위해 이사회가 이해해야 하는 정보의 예는 다음과 같다:

- 표준에 정의된 내부감사활동의 전반적인 목표
- 표준에 명시된 내부감사활동의 원칙
- 내부감사부서가 조직에 가치를 부가하고, 조직의 성공에 기여할 수 있는 기회
- 내부감사부서의 권한, 역할 및 책임에 대한 선진 사례
- 관련된 사법관할권의 준거 법규

이사회와 최고감사책임자는 이러한 이해를 바탕으로 내부감사부서에 대한 기대사항을 논의하고, 적절한 권한, 역할 및 책임을 정립해야 한다.

이사회는 내부감사부서의 넓은 업무범위를 고려할 때, 경영진이 가치를 창출하고 보호하는 기회를 지원하는 데 있어 내부감사부서의 검증과 조언이 지니는 가치를 인식하고, 조직이 이를 수용하도록 촉진해야 한다.

조직 또는 상황의 변화가 타당하다면, 1년에 한번 이상 내부감사의 임무 및 현장을 검토하고 업데이트하도록 요구할 수 있다. 그러한 경우에는 정해진 연례 검토기준을 따르기 보다는 수시로 논의해야 한다.

최고감사책임자의 수행

최고감사책임자는 효과적인 내부감사부서의 특성에 대해 이사회에 조언함으로써 이사회가 적절한 내부감사의 임무를 고려하도록 지원한다. 이를 위해 최고감사책임자는 표준, 사법관할권 관련 법규, 내부감사기능의 선진 활동 및 실무에 관한 연구 결과들을 이사회와 공유한다.

최고감사책임자는 조직 내 검증 제공자를 조정하는 과정에 참여하고, 조직 내 타 부서가 내부감사의 임무에 어떻게 기여할 수 있는지에 대해 이사회에 조언해야 한다. 최고감사책임자는 이사회가 내부 및 외부의 다른 검증 제공자 및 규제기구의 역할과 책임을 이해하도록 돕고, 적절한 내부감사 임무에 대해 명확성을 제공할 수 있다.

최고감사책임자는 이사회에 내부감사현장 승인을 받기 전에, 최고경영진과 내부감사현장안을 검토함으로써 이사회에 기대를 이해하고, 이를 지원하고 있음을 보장해야 한다.

공동 이행사항

최고감사책임자는 이사회가 내부감사현장의 적절한 내용과 형식을 결정하는 데 도움이 되도록 내부감사현장의 구성요소에 대한 권장 사례, 템플릿 또는 기타 지침을 이사회에 제공할 수 있다.

내부감사현장은 내부감사부서의 임무의 근거가 되는 관련 법규도 참조할 수 있다. 예를 들면, 규정이나 증권 거래소 상장요건이 내부감사부서에 적용될 수도 있다.

최고감사책임자는 최고경영진과 함께 이사회에 기대를 이해하고 이를 지원하기 위해 제안된 내부감사의 임무와 현장 및 모든 업데이트 사항을 검토해야 한다.

최고감사책임자는 최소 연 1 회 내부감사현장에 대한 검토사항 이사회 안전에 포함되도록 해야 한다.

공공 부문

공공 부문에서는 내부감사부서가 대중에게 지니는 책무성과 투명성 임무를 인지하고, 공익을 위해 업무를 수행하도록 요구할 수 있다.

내부감사의 임무는 법이나 규정과 같은 거버넌스 문서에 명시될 수 있는데, 이러한 문서가 내부감사현장을 대신할 수 있다. 그 결과 내부감사의 임무에 대한 연례 검토가 보장되지 않을 수도 있다. 만일 이러한 법규가 내부감사의 임무와 현장에 일반적으로 명시되는 모든 측면을

다루지 않을 경우, 최고감사책임자는 이사회의 검토 및 승인을 위해 추가적인 내용을 정리하고 문서화해야 한다.

공공 부문의 최고감사책임자는 임명 또는 선출될 수 있는데, 보고 관계와 관련된 고유한 요구사항을 반드시 인지하고 있어야 한다.

적합성 증거

- 내부감사의 임무에 대하여 토의하고 승인한 이사회 의사록
- 내부감사의 임무변경을 토의하고 승인한 이사회 의사록(필요 시)
- 내부감사 임무에 대한 연례검토가 포함된 이사회 회의 안건 및/또는 의사록
- 최고감사책임자가 매년 내부감사헌장을 검토한 문서
- 날짜 및 연혁(version) 관리 증빙이 포함된 내부감사헌장
- 감사헌장 승인 및 후속 변경사항을 확인할 수 있는 이사회 의사록

국제내부감사표준 6.2 이사회의 지원

요건

이사회의 책임

이사회는 반드시 내부감사부서를 지원하여 조직 전체에서 인정받도록 보장해야 한다.

이사회는 내부감사부서가 데이터, 기록 및 기타 정보는 물론 내부감사 임무를 완수하는데 필요한 인적 및 물적 자원에 제한 없이 접근할 수 있도록 반드시 보장해야 한다.

이사회는 반드시 직접적이고 정기적인 커뮤니케이션을 통해 최고감사책임자를 지원해야 한다.

이사회는 다음을 통해 내부감사부서를 지원함을 보여준다:

- 내부감사 임무를 정립하고 승인함.
- 내부감사부서가 그 임무를 완수할 수 있도록 조직 내 특정 지위에 최고감사책임자가 보고하도록 함.
- 내부감사헌장, 내부감사계획, 예산 및 자원 계획을 승인함.
- 내부감사부서의 범위, 접근, 권한 또는 자원에 관한 규정이 효과적인 직무 수행 능력을 제한하는지에 대한 여부를 판단하기 위해 최고경영진과 최고감사책임자에게 적절히 질의함.
- 필요 시 최고경영진의 배석 없이 최고감사책임자와 회의함.

최고감사책임자의 책임

최고감사책임자는 조직 전체에 걸쳐 내부감사의 임무를 인정하고 지원하는 데 필요한 정보를 이사회에 반드시 제공해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

이사회 이행사항

경영진이 배석하지 않은 가운데 이사회와 최고감사책임자가 최소 분기별로 만나는 것은 선진적인 거버넌스 관행이다. 종종 이러한 회의는 이사회 정례 회의 후 비공개 또는 비밀 회의의 형태로 소집된다. 이사회는 공식적인 회의가 아니어도 최고감사책임자와 통화나 기타 비공식적인 논의를 통해 지속적인 지원을 입증하고, 내부감사부서의 진행상황을 알고 있어야 한다.

이사회는 최고감사책임자가 내부감사부서가 추구하는 임무를 지원할 수 있는 조직 내의 개인에게 행정적으로 보고하도록 보장해야 한다. 가장 바람직한 대상은 CEO 나 그와 동등한 직위여야 한다.

이사회는 내부감사부서가 데이터, 기록 및 기타 정보는 물론 인적 및 물적 자원에 접근해야 하는 필요성을 이해해야 한다. 이사회는 접근, 감사 범위 또는 자원의 제한으로 인해 내부감사부서의 서비스 수행과 내부감사의 임무를 완수하는 데 방해가 되는지를 주기적으로 평가해야 한다. 만일 최고감사책임자가 난관에 봉착했다고 보고하는 경우, 필요하다면 이사회는 최고경영진과 소통함으로써 지원을 입증해야 한다.

최고감사책임자 수행사항

최고감사책임자는 내부감사부서에 대한 지원을 입증하는 방법에 대해 이사회에 조언해야 한다. 또한, 최고감사책임자는 내부감사부서가 서비스를 수행하고 내부감사 임무를 완수하는 데 방해가 되는 모든 제한에 대해 이사회에 알려야 한다.

공동 수행사항

최고감사책임자가 이사회에 소통하는 정보의 유형과 상세 수준은 양측이 합의해야 한다.

공공 부문

공공 부문의 이사회는 내부감사부서의 예산 및/또는 자원 계획을 승인할 직접적인 권한이 없을 수 있다. 최고경영진이 조직 외부의 예산 당국에 예산을 신청하는 경우, 이사회는 내부감사 임무를 완수하기에 충분한 자원 확보할 수 있도록 옹호해야 한다.

공공 부문의 최고감사책임자는 공적 진실성 보장을 위해 정책이나 사법관할권의 법규(공공 기록과 관련된 규정 등)가 비공식적인 논의를 금지 또는 제한하고, 이사회와의 비공개 회의를 특정 주제로 제한하는 등의 규칙을 제정할 수 있음을 반드시 인식해야 한다.

적합성 증거

- 내부감사헌장, 내부감사계획, 내부감사 예산 및 자원 계획에 대한 이사회 검토와 승인을 명시하고 있는 이사회 의사록
- 최고감사책임자와 이사회 간의 시의적절하고 유익한 커뮤니케이션 내용을 명시하고 있는 기록
- 최고감사책임자가 제공할 정보의 성격과 수준에 대해 이사회와 합의한 문서

- 내부감사부서의 제한 없는 접근에 대해 논의한 이사회와 최고경영진 간의 커뮤니케이션 문서나 의사록
- 최고감사책임자가 이사회에 전달해야 하는 정보가 담긴 상호 합의된 매트릭스(matrix)나 유사한 문서
- 내부감사 서비스를 수행하는 데 필요한 데이터, 기록, 인적 및 물적 자산에 대한 접근을 논의한 문서

원칙 7 독립성 보장

이사회는 내부감사부서의 독립성을 확립하고 보호한다.

이사회는 내부감사부서의 독립성을 보장할 책임이 있다. 독립성이란 편향되지 않은 방식으로 내부감사책임자를 수행하는 내부감사부서의 능력을 손상시키는 상황으로부터의 자유로 정의된다. 독립성은 이사회에 대한 책무성, 관련 자원에 대한 접근, 간섭 받지 않을 자유를 통해 확립된다. 내부감사부서는 최고감사책임자가 이사회에 직접 보고하고 내부감사부서가 간섭 없이 서비스와 책임을 수행할 수 있는 조직 내 위치에 있을 때 내부감사활동의 목적을 완전하게 달성할 수 있다.

국제내부감사표준 7.1 조직의 독립성

요건

이사회는 책임

이사회는 내부감사부서가 임무를 완수할 수 있도록, 최고감사책임자 및 내부감사부서와 직접적인 보고 관계를 수립해야 한다.

이사회는 직접적인 보고 관계의 일환으로 반드시 다음 사항을 수행해야 한다:

- 최고감사책임자의 임명, 해임, 성과 평가, 보수에 관한 결정을 승인 및/또는 참여
- 최고경영진이 배석하지 않은 회의를 포함하여, 최고감사책임자에게 이사회와 중대하고 민감한 사안을 논의할 수 있는 기회를 제공
- 최고감사책임자가 조직 내에서 경영진의 간섭 없이 내부감사 서비스와 책임을 수행하고, 최고경영진 및/또는 이사회와 직접 사안을 논의하거나, 필요 시 이사회에 단계적으로 보고(escalation)할 수 있는 지위에 위치하도록 보장
- 내부감사부서가 감사범위를 결정하고 내부감사 업무를 수행하고 결과를 전달할 때 간섭 받지 않음을 보장

최고감사책임자의 책임

최고감사책임자는 반드시 최소 연 1 회 내부감사부서의 조직 내 독립성을 이사회에 확인해야 한다. 독립성이 손상되었을 수 있는 사건이나 그러한 손상을 해결하기 위해 채택한 조치 또는 보호장치에 대한 소통도 이에 포함된다. (7.3 독립성의 보호 참조)

공동책임

최고감사책임자는 반드시 내부감사현장에 이사회가 결정한 보고 관계 및 조직 내 지위를 문서화해야 한다. 이사회는 반드시 내부감사현장을 승인해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

이사회 이행사항

최고감사책임자의 보고 관계와 내부감사부서의 조직 내 지위는 최고감사책임자에 의해서만 결정되는 것은 아니다. 일반적으로 이사회, 최고경영진 및 최고감사책임자는 내부감사부서가 그 임무를 가장 잘 완수할 수 있도록 해주는 보고 관계에 대해 논의한다.

내부감사활동은 내부감사부서가 검증과 조언을 제공하는 감사대상부서의 경영진에게 직접적으로 보고하는 책임을 가지는 것보다 이사회에 직접적으로 보고하는 책임을 가지고 있을 때("이사회에 기능적으로 보고" 또는 "이사회에 기능적으로 보고하는 관계에 있음"이라고도 함) 가장 효과적이다. 이사회는 이사회와 최고감사책임자 간 직접적인 보고 관계를 구축으로써 내부감사부서가 간섭이나 부당한 제한없이 감사업무를 수행하고, 감사 지적사항, 결론 및 기타 결과를 전달할 수 있도록 보장할 수 있다. 간섭의 예는 요청한 정보를 경영진이 적시에 제공하지 않고, 정보, 인적 또는 물적 자산에 대한 접근을 제한하는 것이다. 내부감사부서의 효과적인 운영 능력을 방해하는 방식으로 예산이나 자원을 제한하는 것도 부당한 제한의 예이다. (표준 7.3 독립성의 보호 및 표준 11.3 감사결과 커뮤니케이션 참조)

또한 내부감사부서의 조직 내 독립성은 이사회에 직접 보고하는 최고감사책임자에 달려 있다. 최고감사책임자가 이사회에 직접 보고할 경우 지적사항이나 결론의 수정을 요구하는 감사대상부서 경영진의 과도한 압력과 같이, 내부감사부서의 공정한 업무 수행 능력을 손상시키는 상황을 피할 수 있다.

이사회는 내부감사현장 외에도 이사회 현장에 이러한 관계가 문서화되어 있음을 확인하여, 최고감사책임자의 직접 보고가 지니는 중요성에 대한 이해를 입증할 수 있다.

이사회는 최고감사책임자가 최고경영진에게 접촉할 수 있고, 경영진의 판단에 이의를 제기할 수 있는 권한을 가진 조직 내 지위에 보고할 수 있도록 보장해야 한다(종종 최고감사책임자의 "행정적 보고 관계"라고 한다). 최고감사책임자가 이러한 권한을 발휘하기 위해서는 일반적으로 CEO 나 그에 상응하는 직위에 행정적으로 보고하는 것이 가장 바람직하지만, 적절한 안전장치가 구현되어 있을 경우에는 다른 고위 책임자에게 보고해도 동일한 목적을 달성할 수 있다. 내부감사기능을 담당하는 자회사, 지점, 지역본부의 총괄책임자도 해당 영역을 담당하는 최고경영진과 상응하는 직급에 보고해야 한다.

최고감사책임자 이행사항

최고감사책임자는 이사회가 내부감사부서의 보고 관계와 조직 내 위치가 공정한 방식으로 책임을 수행할 수 있는 능력을 뒷받침하는지 평가할 수 있도록 필요한 정보를 제공해야 한다. 최고감사책임자는 최고경영진 및 이사회와 문제를 논의하기 위한 기준과 프로세스를 수립한다. (추가 요건과 고려사항은 표준 7.3 독립성의 보호, 원칙 11 효과적인 커뮤니케이션 및 관련 표준 참조)

공공 부문

공공 부문의 조직에서 이사회는 최고감사책임자의 임명, 해임 또는 보수 결정에 대한 권한이 없을 수 있다. 또한 선출직 이사나 비상임 이사와 같이 조직 외부에 있는 이사진은 최고감사책임자 임명에 관여할 권한이 없을 수 있다. 그럼에도 불구하고 이사회는 성과 평가 및 최고감사책임자의 임명과 해임 결정에 대해 경영진에게 조언해야 한다.

또한 공공 부문의 최고감사책임자 중 일부는 공개 투표로 결정되는 선출직이다. 이사회가 아닌 지배 기구에서 임명하는 최고감사책임자도 있다. 경우에 따라 최고감사책임자의 보고 관계와 공공 부문 내부감사부서의 조직 내 위치는 법규에 의해 정립된다.

적합성 증거

- 내부감사부서의 보고 관계를 기술한 내부감사헌장
- 최고감사책임자가 최고경영진 및 이사회와 직접 의사 소통한 의사록이나 기타 증빙
- 최고감사책임자가 이사회와 함께 내부감사부서의 지속적인 독립성을 확인했거나, 내부감사부서의 임무 수행 능력에 영향을 미치는 손상요인과 이를 관리하기 위한 안전장치에 관해 논의한 내용을 보여주는 이사회 의사록이나 기타 문서
- 최고감사책임자의 임명, 해임, 성과 평가 및 보상에 관한 결정에 이사회가 관여했음을 보여주는 이사회 의사록이나 기타 문서

국제내부감사표준 7.2 최고감사책임자의 역할, 책임 및 자격

요건

이사회 의 책임

이사회는 반드시 최고감사책임자의 역할과 책임을 승인하고, 그러한 역할을 이행하는 데 필요한 자격과 역량을 확인하여야 한다.

이사회는 최고감사책임자가 내부감사부서를 효과적으로 관리하고, 내부감사서비스의 수행품질을 보장할 수 있는 자격과 역량을 갖추도록 해야만 한다.

최고감사책임자의 주요 역할은 「영역 IV. 내부감사부서 관리」에서 설명하고 있는 것처럼 내부감사 서비스를 포함, 내부감사부서를 관리하는 것이다. 이사회는 최고감사책임자에게 내부감사활동 범위를 벗어난 추가적인 역할이나 책임을 부여하기 전에 이로 인해 발생할 수 있는 내부감사부서의 독립성에 대한 실질적 또는 잠재적인 손상요인을 반드시 이해해야 한다

감사 외의 역할 및 책임이 내부감사부서의 독립성을 손상시키거나 손상시키는 것처럼 보이는 경우, 이사회는 반드시 적절한 안전장치의 구현을 보장해야 한다. (표준 7.3 독립성의 보호 참조)

최고감사책임자의 책임

최고감사책임자는 이사회가 내부감사부서를 관리하는데 필요한 자격, 역량 및 조건을 이해하기 위해 알 필요가 있는 정보를 반드시 제공해야 한다.

최고감사책임자는 감사 외의 역할 및 책임을 맡기 전에 반드시 이사회에 그 시사점을 전달하고, 실질적, 잠재적 및 인식상의 손상요인을 관리하기 위한 안전장치를 제안해야 한다.

이사회는 승인을 받아 감사 외의 역할 및 책임을 맡은 최고감사책임자는 내부감사부서의 독립성 보장을 위해 적절한 안전장치가 구현되어 효과적으로 운영되고 있음을 이사회에 반드시 입증해야 한다,

최고감사책임자에게는 반드시 이사회가 기대하는 역할과 책임을 수행하는 데 필요한 자격과 역량을 유지하고 강화할 책임이 있다. (원칙 3 역량의 입증 및 관련 표준 참조)

실행 및 적합성 증거를 위한 고려사항

실행

이사회는 최고경영진과 협력하여 최고감사책임자에게 기대되는 역량과 자격이 무엇인지 결정한다. 기대 역량은 내부감사의 임무, 조직의 복잡성과 특수한 필요사항, 조직의 리스크 프로파일, 조직이 속한 산업과 관할권, 기타 요소에 따라 다를 수 있다. 최고감사책임자에게 기대되는 역량과 자격은 일반적으로 직무기술서 형태로 문서화되며, 다음 사항을 포함한다:

- 국제내부감사표준 및 선진 내부감사 실무에 대한 전반적인 이해
- 산업 또는 부문에 대한 경험
- 내부 감사인을 모집, 채용 및 교육하고 관련 역량을 개발하도록 지원하여 효과적인 내부감사부서를 구축
- 국제공인내부감사사(CIA) 자격이나 기타 관련 전문 교육, 인증 및 자격증

위 목록은 가장 바람직한 역량과 자격 요건을 포함하고 있다. 특히, 다른 산업이나 분야에서 일하거나, 또는 다른 역할을 수행하고 있는 사람을 최고감사책임자로 영입한 경우, 그 부족한 역량과 자격을 감사부서의 다른 구성원의 역량으로 보완이 가능하다면 여타 영역에 대한 전문성 또는 리더로서의 역량을 고려하여 최고감사책임자로 선택할 수 있다. 이러한 경우 최고감사책임자는 경험이 부족한 분야에 대한 지식을 얻기 위하여 지식이 풍부한 내부감사부서의 구성원과 협력해야 한다.

또한, 이사회는 최고감사책임자가 보수교육, 전문협회 회원자격, 전문 인증 및 기타 전문성 개발 기회를 추구하도록 권장해야 한다. (원칙 3 역량의 입증 및 관련 표준 참조)

최고감사책임자는 내부감사부서를 관리하는 책임 외에도 종종 경영진이 통상적으로 책임지고 있는 감사업무 이외의 역할을 수행하도록 요청을 받는데, 이는 내부감사부서의 독립성을 손상시키거나 손상시키는 것처럼 보일 수 있다. 다음은 그 상황의 사례이다:

- 새로운 규제요건 따라 컴플라이언스 준수를 보장하기 위한 정책, 절차, 통제 및 리스크 관리 활동을 즉시 개발할 필요가 있는 경우
- 최고감사책임자가 기존의 리스크 관리 활동을 새로운 사업 부문 또는 지리적 시장에 맞게 적용할 수 있는 가장 적절한 전문성을 갖추고 있는 경우
- 조직의 자원이 한정적이거나 별도의 컴플라이언스 부서를 두기에 너무 작은 조직의 경우
- 조직의 리스크 관리 프로세스가 충분하지 못한 상황에서 최고감사책임자가 리스크 관리 계획이나 프로그램을 주도하기에 가장 적합한 전문지식을 보유하고 있음
- 조직이 내부통제제도 및 특정 통제 프로세스의 효과성을 내부감사부서가 관리해야 한다고 기대함
- 최고감사책임자가 지난 12 개월 동안 검토 대상 업무를 담당한 경우

이사회 이행사항

이사회는 최고감사책임자를 고용하기 전에 채용 및 임명 과정에 참여해야 한다. 예를 들면, 이사회는 최고감사책임자가 내부감사부서를 관리하고 조직에서 기대하는 추가적인 역할 및 책임을 수행하는 데 필요한 자격과 역량에 대해 논의할 수 있다. 이사회는 기대되는 자격과 역량을 반영하도록 최고감사책임자의 직무 기술서를 검토 및 승인할 수 있다. 또한, 이사회는 후보자를 선정하기 전에 후보자의 이력서를 검토하고 인터뷰에 참여함으로써 최고감사책임자 임명 결정에 관여해야 한다.

이사회는 최고감사인의 감사 외의 역할과 책임에 대해 최고감사책임자 및 최고경영진과 논의하여 근거, 리스크, 독립성 손상 관리 계획에 대한 이해가 공유되도록 보장해야 한다. (표준 7.3 독립성의 보호 참조) 이러한 역할과 책임이 최고감사책임자의 책임 중 장기 또는 영구적인 부분인지 아니면 일시적이고 경영진에게 이전될 예정인지도 고려해야 한다.

최고감사책임자 이행사항

최고감사책임자는 감사 외의 역할과 책임에 대해 논의할 때, 독립성과 관련된 표준 및 고려사항, 이러한 표준 및 고려사항이 객관성을 지원하는 방법, 제안된 역할과 책임이 지니는 손상 리스크를 강조해야 한다. 최고감사책임자는 이러한 리스크의 관리가 가능한 안전장치에 대해 잘 알고 있을 가능성이 높으며, 표준 7.3 독립성의 보호에 부합하는 제안을 해야 한다.

적합성 증거

- 최고감사책임자의 직무 기술서 및/또는 임명에 대한 이사회 승인서. 혹은 위원회가 최고감사책임자의 역할에 필요한 자격과 역량을 평가했다는 기타 증거
- 감사 외의 역할 및 책임과 잠재적 손상요인에 대한 논의 내용을 기록한 의사록이나 기타 메모 그리고, 안전장치에 대해 이사회가 승인한 계획서

- 감사 외의 역할 및 책임을 장기간 수행함에 따른 독립성 보호장치에 대해 이사회의 승인을 기술한 내부감사헌장(역할, 책임 및 보호장치의 예상 기간과 보호장치의 효과를 주기적으로 평가하는 방법 포함)

국제내부감사표준 7.3 독립성의 보호

요건

내부감사부서의 독립성 손상을 관리하기 위한 안전장치는 반드시 마련되어야 한다.

이사회의 책임

이사회는 독립성 손상 리스크 관리를 위한 안전장치가 적절하게 설계되고 효과적으로 운영되도록 보장함으로써 내부감사부서의 독립성을 반드시 보호해야 한다.

최고감사책임자의 책임

최고감사책임자는 내부감사부서의 독립성이 실질적으로 또는 외관상으로 손상될 가능성이 있는 현재의 또는 제안된 역할 및 책임에 대해 이사회와 반드시 논의해야 한다. 최고감사책임자는 각각의 손상요인을 해결하는 데 적절한 여러 유형의 안전장치에 대해 이사회에 반드시 조언해야 한다.

최고감사책임자는 독립적으로 직무를 수행하는 내부감사부서의 능력에 영향을 미치는 모든 손상요인을 반드시 최고경영진 및 이사회와 논의하고, 그러한 상황을 해결하기 위해 이사회와 최고경영진의 협조를 구해야 한다.

또한, 최고감사책임자는 현존하는 손상요인을 최고경영진 및 기타 적절한 당사자에게 반드시 공개해야 한다. 최고감사책임자는 공개해야 하는 기타 당사자를 결정할 때, 손상의 특성, 내부감사 서비스 결과의 신뢰성에 이러한 손상이 미치는 충격/영향 및 관련 이해관계자의 기대사항을 반드시 고려해야 한다. 감사업무가 종료된 후에 손상요인이 발견되어 감사 지적사항, 권고사항 및/또는 감사결론의 신뢰성이나 신뢰성 인식에 영향을 미치는 경우, 최고감사책임자는 검토대상 부서의 경영진, 최고경영진, 이사회 및/또는 영향을 받는 기타 이해관계자와 우려사항을 논의하고, 상황을 해결하기 위한 적절한 조치를 결정해야 한다. (표준 11.4 오류 및 누락 참조)

공동책임

최고감사책임자가 상시적으로 맡고 있는 감사 이외의 책임이 있는 경우, 이 책임과 업무의 성격, 독립성 보장을 위해 마련된 안전장치를 내부감사헌장에 반드시 기술해야 한다. 만일 이 책임 영역의 대상이 내부감사활동인 경우, 이사회에 독립적으로 보고하는 객관적이고 유능한 외부 검증 제공자와 계약을 결하는 등 검증 확보를 위한 대안적 프로세스가 반드시 수립되어야 한다.

최고감사책임자가 맡고 있는 감사 이외의 책임이 한시적인 경우, 해당 영역에 대한 검증은 그 한시적 업무를 수행하는 동안과 이후 12 개월 동안은 반드시 독립적인 제 3 자가 감독해야 한다. 최고감사책임자의 감사 이외 책임이 일시적인 경우, 이러한 책임을 경영진에게 이양하는 계획을 반드시 수립해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

다음은 독립성을 손상시킬 수 있는 상황이다:

- 최고감사책임자와 이사회 간의 직접적인 커뮤니케이션이나 상호작용이 부족함.
- 경영진이 이사회가 이미 승인하여 내부감사현장에 기술된 내부감사서비스의 범위를 제한하려 시도함.
- 경영진이 내부감사서비스를 수행하는 데 필요한 인적 및 물적 자원뿐만 아니라 데이터, 기록 및 기타 정보에 대한 접근을 제한하기 위해 시도함.
- 경영진이 내부감사 지적사항을 보류하거나 변경하도록 내부감사인에게 압력을 가함.
- 내부감사부서의 예산이 내부감사현장에 명시된 책임을 수행할 수 없는 수준으로 축소됨.
- 최고감사책임자가 담당 또는 감독하거나 중대한 영향력을 행사할 수 있는 부문에 대해 내부감사부서가 수행하거나 최고감사책임자가 감독하는 검증업무 (표준 7.2 최고감사책임자의 역할, 책임 및 자격 참조)
- 최고감사책임자가 행정적으로 보고하는 고위 임원이 관리하는 활동과 관련하여 내부감사부서가 검증 업무를 수행하거나 최고감사책임자가 감독함. 예를 들면, 최고감사책임자가 최고재무책임자에게 보고하도록 되어있는 상황에서 본 최고재무책임자에게 보고하는 재무부서의 감사를 담당함.

이사회 이행사항

이사회는 감독 활동에는 내부감사부서의 독립성 손상을 모니터링하고, 모든 손상요인을 관리하기 위한 안전장치를 마련하는 것이 포함된다. 이사회는 최고경영진 및 최고감사책임자와 잠재적, 인식적 및 실질적 손상의 성격과 원인 및 제안된 독립성 보호장치에 대해 논의해야 한다. 보호장치는 보고라인과 책임을 주기적으로 평가하는 것, 독립성이 손상될 수도 있는 영역에서 검증을 받기 위한 대안 프로세스를 개발하는 것과 같은 활동들을 포함한다.

이사회는 안전장치를 누가, 어떻게, 언제 실행할 것인지에 대해 구체적으로 확인하여야 한다. 영구적인 보호장치가 구현될 때까지 임시 보호장치를 적용할 수 있다. 이사회는 최소 연 1 회, 그리고 최고감사책임자의 책임이 바뀔 때마다 보호장치가 여전히 효과적으로 작동하는지 검증해야 한다.

최고감사책임자 이행사항

최고감사책임자는 독립성과 관련된 표준의 이해를 바탕으로, 실질적, 잠재적 또는 인식 수준의 독립성 손상요인이 존재하는지 판단하기 위해 보고관계, 역할 및 책임을 포함한 관련 상황을 평가하여야 한다. 최고책임자는 독립성 및 손상요인에 대해 이사회와 최고경영진의 기대사항을 이해하고 이들을 교육시키기 위해 적극적으로 소통하여야 한다. 또한, 최고감사책임자는 관련

당사자와의 논의를 통해 공정한 방식으로 책임을 수행하는 내부감사부서의 능력에 아직 실질적인 영향을 미치지 않는 인식 수준의 손상상황을 해결할 수 있다.

공동 이행사항

감사 이외 역할과 책임을 수락하기 위한 최고감사책임자의 계획은 다음 사항을 포함하여야 한다:

- 독립성 보호장치
- 내부감사계획 및 자원에 대한 잠재적 충격/영향을 식별
- 적용 가능하다면, 임시로 맡고 있는 감사 외의 책임을 경영진에게 이양하는 일정을 명시

적합성 증거

- 최고경영진, 이사회, 기타 이해관계자와 독립성 손상에 대해 논의하였음을 보여주는 의사록 및 기타 문서
- 독립성 손상 리스크를 관리하기 위한 보호장치가 적절한 당사자와 합의되었고, 적절하게 설계되어, 효과적으로 운영되고 있음을 보여주는 의사록 및 기타 문서
- 손상이 의심되거나 식별될 때 따라야 할 규정 및 절차서
- 독립성 관련 우려사항을 해결하기 위한 구체적인 안전장치를 설명한 공식적인 활동 계획
- 독립성 보호장치로서 내부 및 외부의 기타 제공자가 제공할 검증 서비스에 대한 문서

원칙 8 이사회의 감독

이사회는 내부감사부서를 감독하여 그 효과성을 보장한다.

이사회의 감독은 내부감사부서의 전반적인 효과성을 보장하는 데 필수적이다. 이 원칙을 달성하려면, 이사회와 최고감사책임자 사이의 협력적인 양방향 커뮤니케이션이 필요하며, 내부감사부서가 내부감사 임무를 완수하는 데 충분한 자원을 확보할 수 있도록 이사회의 지원이 필요하다. 또한, 이사회는 감사품질에 대한 외부평가 결과에 대한 이사회의 직접 검토를 포함하여 감사품질 평가 및 개선 프로그램(QAIP)을 통해 최고감사책임자 및 내부감사부서의 수행 품질을 검증한다.

국제내부감사표준 8.1 이사회의 상호작용

요건

이사회의 책임

이사회는 조직의 거버넌스, 리스크 관리 및 통제 프로세스의 효과성을 이해하기 위해 반드시 내부감사부서와 상호작용해야 한다.

이사회 감독에는 내부감사부서가 내부감사의 임무를 완수하고 있는지 확인하기 위한 최고감사책임자와의 지속적인 커뮤니케이션이 반드시 포함되어야 한다. 이사회는 최고감사책임자가 내부감사 우선순위를 결정하는데 도움이 될 수 있도록 조직의 전략, 목표 및 리스크에 대한 이사회 관점을 전달해야 한다.

이사회는 다음의 기대사항을 반드시 설정해야 한다:

- 최고감사책임자와의 커뮤니케이션 빈도
- 이사회 리스크 허용 범위를 초과한 심각하거나 중대한 리스크와 같이 이사회에 단계적으로 보고해야 하는 문제를 판단하는 기준
- 경영진에서 이사회까지 단계적 소통을 위한 프로세스

최고감사책임자의 책임

최고감사책임자는 이사회가 감독 책임을 수행하는 데 필요한 정보를 반드시 이사회에 제공해야 한다. 최고감사책임자는 내부감사의 임무 및 독립성에 대한 커뮤니케이션 외에도 이사회가 그 책임을 다할 수 있도록 감사결론, 검증내용, 조언 및 통찰력을 포함하여 내부감사 서비스의 결과물을 반드시 전달해야 한다. (표준 11.3 감사결과 커뮤니케이션 참조)

실행 및 적합성 증거를 위한 고려사항

실행

이사회 이행사항

이사회와 최고감사책임자 간의 커뮤니케이션의 빈도는 중요한 문제에 대한 적시적 커뮤니케이션의 필요성을 고려해야 한다. 이사회는 재무 리스크 관리뿐만 아니라 전략적 중요 계획, 사이버보안, 보건 및 안전, 지속가능성, 비즈니스 복원력, 평판을 포함하여 광범위한 비재무적 거버넌스와 리스크 관리 문제에 대한 이해 및 감독과 관련된 관점과 기대사항을 커뮤니케이션해야 한다. 이사회는 최고감사책임자가 최고경영진 이상의 단계까지 보고해야 할 것으로 예상되는 문제를 식별하기 위해, 이사회가 허용한 리스크 범위를 초과하는 중요성과 중대성에 대한 기준을 설정할 수 있다. 이 기준은 최고감사책임자가 경영진에서 이사회까지 단계적인 커뮤니케이션을 위해 따라야 할 프로세스와 연계되어야 한다.

일반적으로 정식 이사회를 통해서만 최소 분기기준으로 공식적 커뮤니케이션을 허용할 수 있다. 또한, 흔히 최고감사책임자와 이사회 구성원은 필요한 경우 정식 이사회 사이에 종종 비공식적으로 커뮤니케이션을 할 수 있다.

이사회는 최고감사책임자 및 최고경영진과의 논의를 통해 최고감사책임자가 보고한 정보가 최고경영진에 의해 정보의 의미가 변질되거나, 보고의 충격/영향을 축소시키는 방식으로 제한되거나 수정되지 않는다는 합리적인 확신을 얻어야 한다.

최고감사책임자 이행사항

최고감사책임자는 이사회에 적시에 커뮤니케이션을 제공하기 위해 서면 및 구두 보고, 프레젠테이션, 공식 회의, 비공식 논의와 같은 다양한 방법을 사용할 수 있다. 최고감사책임자는 이사회에 기대사항을 규정 및 절차에 공식적으로 문서화할 수 있다. 최고감사책임자는 이사회에 기대사항을 충족하고 이사회가 감독 책임을 달성하는데 도움이 되는 커뮤니케이션의 빈도, 성격 및 내용을 이사회와 주기적으로 확인해야 한다.

적합성 증거

- 최고감사책임자와 논의한 사항의 성격과 빈도를 문서화한 이사회 안건 및 의사록
- 최고감사책임자가 이사회에 제출한 프레젠테이션
- 이사회 구성원에 대한 내부감사의 커뮤니케이션
- 이사회가 주목해야 할 문제를 식별하기 위한 기준과 이러한 문제를 전달하는 프로세스("단계적 보고 매트릭스(escalation matrix)"라고도 함)
- 최고감사책임자의 커뮤니케이션이 이사회 현장에 명시된 이사회에 기대사항을 어떻게 지원하는지 보여주는 문서

국제내부감사표준 8.2 감사자원

요건

이사회에 책임

이사회는 내부감사부서가 내부감사의 임무를 완수하고, 내부감사계획을 달성할 수 있는 충분한 자원을 확보했는지 반드시 확인해야 한다.

이사회는 최소 연 1 회 이상 최고감사책임자에게 내부감사의 임무를 완수하고, 내부감사계획을 달성하기 위한 내부감사자원이 충분한지 반드시 질문해야 한다. 이사회는 내부감사 임무와 계획 달성에 불충분한 자원이 미치는 충격/영향을 반드시 고려해야 한다. 이사회는 감사자원이 충분하지 않다고 판단되면, 반드시 최고경영진에게 이러한 문제와 내부감사계획에 미칠 수 있는 잠재적 충격/영향을 알리고 필요한 자원을 지원하도록 지지해야 한다.

최고감사책임자의 책임

최고감사책임자는 충분한 감사자원을 확보하기 위한 전략을 반드시 제안해야 하며, 내부감사 자원이 내부감사의 임무를 완수하고 내부감사계획을 달성하기에 충분하지 않은 경우 반드시 이사회에 이를 알려야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

이사회 이행사항

이사회는 매년 의안에 내부감사 자원의 충분성에 대한 논의를 포함하는 것 이외에도, 최고감사책임자의 감사자원 조달 전략과 관련된 문서 검토를 요청해야 하며, 내부감사부서가 임무를 완수하고 감사계획을 달성할 수 있는 능력과 감사자원 사이의 관계를 분석해야 한다. 이사회는 최고감사책임자가 충분한 자원을 확보하도록 지원하는 데 도움이 되도록 최고경영진에게 조언하거나 정보를 제공하는 프로세스를 구현해야 한다.

최고감사책임자 이행사항

최고감사책임자는 감사자원이 내부감사 임무를 완수하고, 내부감사계획을 달성하기에 충분한지 주기적으로 평가해야 하며, 감사자원 조달 관련 우려사항은 적시에 이사회에 알려야 한다. 최고감사책임자는 내부감사 임무를 완수하고 감사계획을 달성하는 데 필요한 재정적, 인적 및 기술적 자원의 충분성을 분석하기 위해 내부감사부서가 보유하고 있는 자원목록과 내부감사 서비스를 수행하는 데 필요한 자원 간의 차이 분석을 수행해야 한다. (원칙 10 감사자원 관리 참조) 최고감사책임자의 전략에는 예산요청을 포함한 감사자원 충당계획이 포함되어야 하며, 감사업무 서비스 수행을 위한 기술의 사용뿐만 아니라 내부감사부서 직원채용 방안도 포함되어야 한다. 최고감사책임자는 이사회에 제시할 다양한 접근방식에 대한 비용 효익 분석을 수행해야 한다.

공동 이행사항

이사회와 최고감사책임자 사이의 감사자원에 대한 논의는 최소 연 1 회 이상 필요하지만, 분기기준으로 논의하는 것이 선진적인 관행이다. 논의에는 아웃소싱 또는 초청감사인(guest auditor) 활용을 포함하여, 원하는 내부감사 범위를 달성하기 위한 방안의 고려와 내부감사부서의 효율성 및 효과성을 개선하기 위한 기술 구현이 포함되어야 한다.

공공부문

공공 부문의 이사회는 법률, 법령 또는 거버넌스로 인해 내부감사부서에 자원을 배분할 권한이 없을 수도 있다. 또한, 예산은 의회나 입법부와 같은 정부의 다른 기능에 의해 승인될 수 있다. 특히, 지방정부와 같은 지방 자치 단체에서는 지방의회가 각 기관의 예산을 승인한다. 그럼에도 불구하고 최고감사책임자는 반드시 이사회에 감사자원의 제한을 알림으로써, 이사회가 내부감사 임무를 완수하고 내부감사계획을 달성하는 데 필요한 자원에 대해 최고경영진이나 예산책정 권한이 있는 정당한 권리자에게 의견을 제공할 수 있다.

적합성 증거

- 내부감사 자원의 충분성에 대한 논의를 기록한 의안, 의사록, 최고감사책임자와 이사회 및/또는 최고경영진 간의 커뮤니케이션
- 내부감사계획을 달성하는 데 필요한 자원의 충분성을 나타내는 내부감사 자원 계획
- 내부감사자원과 관련된 예산 신청
- 내부감사계획과 파악된 감사자원 간의 차이 분석서
- 최고감사책임자의 감사자원조달 전략서

국제내부감사표준 8.3 감사품질

요건

이사회의 책임

이사회는 최고감사책임자가 감사품질 평가 및 개선 프로그램(QAIP)을 수립, 실행 및 유지하는지 반드시 확인해야 한다.

감사품질 평가 및 개선 프로그램(QAIP)은 내부감사부서가 이 표준에 부합하고 성과 목표 달성하는지 여부를 평가하도록 설계되어 있다. 또한, 이 프로그램의 취지는 내부감사부서가 지속적인 성장을 추구하도록 보장하는 것이다.

이 프로그램은 반드시 다음 두 가지 유형의 평가를 포함해야 한다:

- 외부평가 (표준 8.4 감사품질에 대한 외부평가 참조)
- 내부평가 (표준 12.1 감사품질에 대한 내부평가 참조)

이사회는 반드시 최소 연 1 회 내부감사부서의 성과 목표를 승인해야 한다. (표준 12.2 성과 측정 참조)

이사회는 반드시 최고감사책임자의 성과에 대한 연례 평가를 최고경영진과 함께 수행하거나 참여해야 한다. 이러한 평가에는 다음이 포함된다:

- 표준 및 추가 규정에 대한 적합성, 내부감사업무 충족 능력, 내부감사계획 이행현황을 포함하여 내부감사부서의 성과 목표를 검토
- 내부감사부서의 감사품질 평가 및 개선 프로그램(QAIP) 실행결과 고려
- 내부감사부서의 수행 목표 충족 정도 판단
- 최고감사책임자의 수행내용에 대한 조직의 평가 검토 및 기여

최고감사책임자의 책임

최고감사책임자는 반드시 내부감사부서의 모든 측면을 다루는 내부감사 품질평가 및 개선 프로그램을 수립, 실행 및 유지해야 한다. 최고감사책임자는 최소 연 1 회 감사품질에 대한 내부평가 결과를 이사회에 반드시 보고해야 한다. 보고내용에는 다음 사항이 포함된다:

- 내부감사부서의 표준 적합성과 성과목표의 달성
- 내부감사기능의 결함과 개선 계획

실행 및 적합성 증거를 위한 고려사항

실행

이사회 이행사항

최고감사책임자에 대한 이사회의 연례 평가에는 다음이 포함되어야 한다:

- 거버넌스, 리스크 관리 및 통제 프로세스 개선에 대한 기여 수준
- 내부감사 직원의 생산성 향상
- 내부감사 프로세스의 비용 효율성 향상
- 적절한 감사업무 계획수립과 감독
- 이해관계자와 관계를 구축하고 그 요구를 충족시키는 효과성

이사회의 평가에는 정성적 및 정량적 평가가 포함되어야 한다. 성과의 측정은 조직에 따라 다르며 내부감사부서에 의미가 있어야 한다.

최고감사책임자 이행사항

최고감사책임자는 이사회가 내부감사부서의 감사품질 평가 및 개선 프로그램(QAIP)을 감독하는데 필요한 정보를 얻을 수 있도록 보장해야 한다. 여기에는 다음이 포함된다:

- 최고감사책임자의 지시 또는 지원 하에 수행된 감사품질에 대한 내부 및 외부평가의 범위, 빈도 및 결과
- 개선조치를 위한 활동계획. 활동계획은 이사회와 합의해야 함.
- 이사회와 합의한 개선활동계획의 진행상황

공공 부문

감사품질 평가 및 개선 프로그램(QAIP)은 조직이 운영되는 관할권 내에서 내부감사부서가 지켜야 하는 모든 법규준수를 포함해야 한다.

적합성 증거

- 내부감사부서의 감사품질 평가 및 개선 프로그램(QAIP)에 대한 최고감사책임자와의 논의를 문서화한 이사회의 의안 및 의사록
- 감사품질 평가 결과와 모든 개선계획을 언급한 활동계획의 상태에 대한 최고감사책임자의 프레젠테이션 및 기타 커뮤니케이션
- 이사회가 최고감사책임자의 수행 평가에 대해 검토 및 기여했다는 것을 보여주는 이사회 의사록이나 기타 문서

국제내부감사표준 8.4 감사품질에 대한 외부평가

요건

이사회는 내부감사부서의 감사품질에 대한 외부평가가 최소 5년마다 수행되도록 반드시 보장해야 한다.

감사품질에 대한 외부평가는 반드시 품질평가 프로세스뿐만 아니라 전문적인 내부감사활동 실무 자격을 갖춘 독립적인 평가자나 평가팀이 수행하여야 한다. 독립적인 평가자나 평가팀은 조직 외부에 있어야 하며, 내부감사부서가 속한 조직의 직원이거나, 그 조직의 일부이거나 통제 하에 있어서는 안 된다. 독립적인 평가자, 평가팀 및 그들이 속한 조직은 객관성을 손상시킬 수 있는 실질적, 잠재적 또는 인식된 이해 상충이 없어야 한다.

감사품질에 대한 외부평가는 내부감사부서의 다음 사항의 적정성에 대한 포괄적인 검토가 필요하다:

- 임무, 헌장, 전략, 방법론, 프로세스, 리스크 평가 및 내부감사계획
- 국제내부감사표준과의 적합성
- 평가수행기준 및 측정과 평가결과
- 툴(tool) 및 기법의 충분한 사용과 프로세스 개선에 대한 초점을 포함하는 역량
- 해당 프로세스에 관련된 자들 간의 관계를 포함하여 조직의 거버넌스 프로세스와의 통합
- 조직의 거버넌스, 리스크 관리 및 통제 프로세스에 대한 기여
- 조직의 운영과 목표 달성 능력 향상에 대한 기여
- 이사회, 최고경영진 및 이해관계자가 체계적으로 정한 기대사항을 충족하는 데 있어서의 효과성과 효율성

감사품질에 대한 외부평가는 두가지 방식으로 수행된다: 독립적인 제 3 자가 수행하는 평가 또는 독립적인 검증을 받는 자체평가

이사회 의 책임

이사회는 반드시 감사품질에 대한 외부평가의 범위와 빈도를 결정해야 한다. 이사회는 그 범위를 정의할 때, 내부감사현장에 포함된 내부감사부서 및 최고감사책임자의 책임과 내부감사부서에 영향을 미칠 수 있는 규제 요건을 반드시 고려해야 한다.

이사회는 최고감사책임자의 감사품질에 대한 외부평가 수행 계획을 반드시 검토하고 승인해야 한다. 이러한 승인은 최소한 다음을 반드시 포함해야 한다:

- 평가의 범위 및 빈도
- 자체평가에 대한 검증을 위해 선택된 외부평가자, 평가팀 또는 개인의 역량 및 독립성
- 독립적인 제 3 자가 수행하는 감사품질에 대한 외부평가 대신 독립적인 검증을 받는 자체평가를 수행하는 근거

이사회는 반드시 외부평가자가 실시한 감사품질에 대한 평가 결과 또는 독립적인 검증과 함께 실시된 자체평가 결과 전부를 직접 해당 평가를 수행한 평가자로부터 받아야 한다. 이사회는

파악된 미비사항과 개선조치를 위한 최고감사책임자의 활동계획을 반드시 검토하고 승인해야 한다. 또한 이사회는 반드시 활동계획의 완료 일정을 승인하고 최고감사책임자의 진행상황을 모니터링해야 한다.

최고감사책임자의 책임

최고감사책임자는 반드시 내부감사품질에 대한 외부평가 수행계획을 수립하고, 이사회에 승인을 얻어야 한다. 외부평가는 반드시 조직 외부의 자격을 갖춘 독립적인 평가자나 평가팀에 의해서 수행되어야 한다. 최고감사책임자는 독립적인 평가자, 평가팀 또는 자체평가를 검증할 개인을 선택할 때, 다음과 같은 기준을 충족함을 반드시 보장해야 한다. 독립적인 평가자나 평가팀은 자격이 있음을 입증하기 위해서는 반드시 다음 기준을 충족하고 있다는 증거를 제시해야 한다:

- 표준 및 주요 내부감사 실무에 대한 경험과 지식
- 최고감사책임자 또는 이에 상응하는 내부감사부서의 고위 직급으로 근무한 경력
- 이전에 내부감사품질에 대한 외부평가를 수행한 경험
- IIA 에서 인정한 내부감사품질에 대한 외부평가 교육과정 이수
- 평가 팀원 중 최소 1 인은 활성화 상태인 CIA 자격을 보유해야 함
- 사실상 또는 외관상의 이해 상충이 없음을 증명

독립적인 검증을 받는 자체평가

감사품질에 대한 외부평가 요건은 독립적인 검증을 받는 자체평가를 주기적으로 실시할 경우 충족될 수 있다. 그러나, 독립적 검증을 받는 자체평가는 감사품질에 대해 외부평가를 받아야 하는 내부감사부서의 요건을 완전히 충족하지는 못한다. 자체평가는 10 년에 한 번씩 감사품질에 대한 외부평가와 번갈아 실시할 수 있다.

자체평가는 일반적으로 내부감사부서에서 평가를 수행한 다음 자격을 갖춘 독립적인 외부평가자가 검증한다. 독립적인 검증을 받는 자체평가는 범위가 더 제한적이며, 다음으로 구성된다:

- 내부감사부서의 국제내부감사표준 적합성 평가와 관련하여 외부평가자의 품질평가 프로세스를 모델로 한, 포괄적이고 완전하게 문서화된 자체 평가 프로세스.
- 자격을 갖춘 독립적인 외부평가자의 현장 검증. 독립적인 검증 시, 자체평가가 완전하고 정확하게 수행되었는지 반드시 확인해야 한다.
- 벤치마킹, 선진 사례, 그리고 이사진 및 최고경영진, 현업경영진 등 주요 이해관계자와의 인터뷰 사안

실행 및 적합성 증거를 위한 고려사항

실행

최고감사책임자

최고감사책임자는 평가자의 독립성이 손상될 수도 있음을 알고 있어야 한다. 잠재적 손상요인의 예로는 조직, 직원 또는 내부감사부서와의 과거, 현재 또는 미래의 관계(예를 들면, 재무제표의 외부감사, 내부감사부서에 대한 지원, 개인적 친분, 거버넌스, 리스크 관리, 재무보고, 내부통제 또는 기타 관련 영역에서 과거나 미래의 감사품질에 대한 내부평가나 자문 서비스 참여)가 포함된다.

잠재적인 평가자가 조직에서 퇴직한 전 직원인 경우, 퇴직 이후 경과기간을 고려해야 한다.

조직 내 다른 부서에 속한 개인은 비록 내부감사부서와 조직적으로는 분리되어 있으나, 외부평가자로서의 감사품질 평가를 수행할 수 있는 독립성이 있는 것으로 간주되지는 않는다. 공공 부문에서 동일한 정부 계층 내의 타 기관에 있는 내부감사부서는 같은 최고감사책임자에게 보고하는 경우 독립성이 있다고 간주되지 않는다. 마찬가지로, 관련된 조직(예: 모기업, 그룹 계열사 또는 대상 조직에 대해 정기적인 감시, 감독, 감사품질 평가 책임이 있는 조직)에 속한 개인은 독립성이 있다고 간주되지 않는다.

두 조직 간의 상호 동료평가(peer review)는 독립적인 것으로 간주되지 않는다. 그러나, 3 개 이상의 동료(peer) 조직(동일한 산업, 지역 협회 또는 기타 동호 단체에 속한 조직) 간의 상호 평가는 독립적인 것으로 간주될 수 있다. 독립성과 객관성이 손상되지 않으며, 모든 팀원이 자신의 책임을 온전히 수행할 수 있도록 반드시 주의를 기울여야 한다.

공동 이행사항

이사회는 감사품질에 대한 외부평가 관련 프로세스를 포함하여, 표준에 대한 적합성과 감사품질을 보장하기 위한 내부감사부서의 프로세스를 이해해야 한다.

표준에 따르면, 내부감사부서는 최소 5년에 1회 감사품질에 대한 외부평가를 받아야 한다. 그러나, 이사회와 최고감사책임자는 외부평가를 더 자주 수행하는 것이 적절하다고 결정할 수 있다. 리더(예를 들면, 최고경영진 또는 최고감사책임자)가 교체되거나, 내부감사 규정 또는 절차에 중대한 변경이 있거나, 둘 이상의 내부감사 조직을 하나의 부서로 통합하거나, 상당한 수준의 직원 이직 등 보다 빈번한 품질평가를 고려해야 할 몇 가지 이유에 해당이 된다. 또한, 규제가 심한 산업이나 대중에게 직접 서비스를 제공하는 조직과 같은 경우에는 감사품질에 대한 외부평가의 빈도 또는 범위를 늘리는 것을 선호하거나 요구할 수 있다.

일반적으로 이사회와 최고감사책임자는 그러한 조정이 필요한지 여부를 결정하기 위해 협력한다.

조직은 감사품질에 대한 외부평가를 실시하기 위해 관련 평가서비스를 공급하는 제공자와 계약하는 대신, 동일한 산업 또는 지리적 위치에 있는 둘 이상의 조직과 협력하여 일련의 품질평가를 수행함으로써 비용을 절감할 수 있다. 독립성 요건 충족을 위해, 두 조직은 서로를 직접 평가할 수 없다. 그러나 세 개 이상의 조직으로 구성된 그룹은 예를 들면 A가 B를 평가하고 B가 C를 평가하고 C가 A를 평가하는 계약을 체결할 수 있다.

외부평가자의 자격 및 역량

이 표준에서 제시된 자격요건 및 독립성 기준 외에도, 감사품질에 대한 외부평가팀의 책임자는 활성화된 CIA 자격을 보유하는 것이 바람직하다.

공공 부문

공공 부문 내부감사부서의 감사품질에 대한 외부평가에는 공공 부문의 업무활동 및 거버넌스 구조에 대해 잘 알고 있는 인원이 포함되어야 한다.

적합성 증거

- 자격을 갖춘 독립적인 감사품질 평가자가 작성한 감사품질에 대한 공식적인 감사품질에 대한 외부평가 보고서
- 외부평가자가 이사회에 제출한 감사품질에 대한 외부평가 결과 프레젠테이션
- 적절한 경우, 최고감사책임자가 이사회에 제출한 외부평가 결과 및 조치 계획에 대한 프레젠테이션
- 최고감사책임자의 감사품질에 대한 외부평가 계획에 대한 논의하고, 승인한 내용이 포함되어 있는 이사회 의사록
- 감사품질에 대한 외부평가자의 자격과 독립성에 대해 논의하고, 확인한 내용이 포함되어 있는 이사회 의사록
- 독립적인 검증을 받는 자체평가를 수행하기로 한 근거에 대해 최고감사책임자가 작성한 문서

영역 IV 내부감사 부서 관리

최고감사책임자는 내부감사헌장 및 국제내부감사표준에 따라 내부감사부서를 관리할 책임이 있다. 이 책임에는 전략적 계획수립, 자원의 확보와 배치, 이해관계자와의 관계 구축 및 의사소통을 통한 객관적인 검증과 조언 제공, 내부감사부서의 성과 보장과 향상이 포함된다.

내부감사부서를 관리할 책임이 있는 자는 조직에 직접 고용된 자든, 외부 서비스 제공자를 통해 계약된 자든 이 영역에서 설명한 책임을 수행하는 것을 포함해서 이 표준을 준수해야 한다.

구체적인 직함과 책임은 조직마다 다를 수 있다. 예를 들어, 최고감사책임자는 "총괄 감사인", "내부감사 책임자", "최고내부감사인", "내부감사 담당이사", 또는 "총괄감사관"과 같은 직함을 가질 수 있다. 최고감사책임자는 자신의 책임을 내부감사부서 내의 자격을 갖춘 전문가에게 위임할 수 있지만 궁극적인 책임은 최고감사책임자 자신에게 있다.

내부감사부서는 이사회와 최고감사책임자 간의 직접적인 보고 관계를 통해 임무를 완수할 수 있다. (표준 7.1 조직의 독립성 참조) 또한, 최고감사책임자는 일반적으로 일상적인 업무활동을 지원하고 내부감사 서비스의 결과가 충분히 고려되도록 보장하는 데 필요한 지위 및 권한을 확립하기 위해, 최고경영책임자와 같은 최고경영진에게 행정적으로 보고한다.

원칙 9 전략적 계획수립

최고감사책임자는 내부감사부서가 임무를 완수하고, 장기적 성공을 위한 위상 정립을 보장하기 위한 전략적 계획을 수립한다.

최고감사책임자는 전략적 계획을 수립하기 위해서, 내부감사의 임무와 조직의 거버넌스, 리스크 관리 및 통제 프로세스를 이해해야 한다. 내부감사 전략은 감사부서가 조직의 성공을 지원할 수 있는 충분한 자원과 위치를 확보하도록 해준다. 내부감사헌장은 내부감사의 임무, 내부감사 서비스의 범위 및 우선순위, 임무를 완수하기 위한 부서의 능력을 뒷받침하는 조건을 문서화한 것이다. 또한, 최고감사책임자는 내부감사부서에게 지침이 될 방법론과 전략을 제공하기 위한 내부감사계획을 수립하고 이행한다.

국제내부감사표준 9.1 거버넌스, 리스크 관리 및 통제 프로세스의 이해

요건

최고감사책임자는 효과적인 내부감사 전략, 헌장 및 계획을 수립하기 위해 조직의 거버넌스, 리스크 관리 및 통제 프로세스를 반드시 이해해야 한다.

최고감사책임자는 거버넌스 프로세스를 이해하기 위해 조직이 다음사항들을 수행하는 방식을 반드시 고려해야 한다:

- 전략적 목표를 수립하고 전략상, 운영상의 결정을 함.
- 리스크 관리 및 통제를 감독함.
- 윤리적 문화를 장려함.
- 효과적인 성과 관리와 책임을 보장함.
- 경영진 및 현업 부서를 구조화함.
- 리스크 및 통제 정보를 조직 전체에 전달함.
- 이사회와 내부 및 외부의 검증 서비스 제공자, 그리고 경영진 간의 활동 및 커뮤니케이션의 조정을 보장함.

최고감사책임자는 리스크 관리 및 통제 프로세스를 이해하기 위해 조직이 중대한 리스크를 식별 및 평가하고, 적절한 통제 프로세스를 선택하는 방법에 대해 반드시 고려해야 한다. 여기에는 조직이 다음의 핵심 리스크 영역을 식별하고 관리하는 방법에 대한 이해가 포함된다:

- 재무 및 운영 정보의 신뢰성과 무결성
- 운영 및 프로그램의 효과성과 효율성
- 자산의 보호
- 법규의 준수

실행 및 적합성 증거를 위한 고려사항

실행

최고감사책임자의 이해력은 정보를 광범위하게 수집하고 포괄적으로 바라봄으로써 증진된다. 정보의 출처에는 최고경영진 및 이사회와의 논의, 내부감사 업무 커뮤니케이션과 감사조서, 다른 검증 및 자문 서비스 제공자가 작성한 평가서와 보고서가 포함된다.

거버넌스(governance) 프로세스의 이해

최고감사책임자는 선진적인 거버넌스 원칙, 전세계적으로 인정되는 거버넌스 체계 및 모델, 조직이 운영되는 산업과 부문에 해당되는 특정한 수행 지침에 대해 잘 알고 있어야 한다. 최고감사책임자는 이러한 지식을 기반으로 상기 사항이 조직에서 구현되었는지 확인하고, 조직의 거버넌스 프로세스의 성숙도를 측정해야 한다. 조직의 거버넌스 구조, 프로세스와 관행은 유형, 크기, 복잡성, 구조 및 프로세스 성숙도와 같은 조직의 고유한 특성과 조직이 따라야 하는 법적 및 규제 요건의 영향을 받을 수 있다.

최고감사책임자는 이사회가 조직의 거버넌스 차원에서 수행하는 역할, 특히 전략적 및 운영적 의사결정 관련 역할에 대한 추가적인 통찰력을 얻기 위해, 이사회와 위원회의 헌장, 의제 및 회의록을 검토할 수 있다.

최고감사책임자는 핵심적인 거버넌스 역할을 수행하는 개인(예: 이사회 의장, 정부 기관의 최고 선출직 또는 임명직 공무원, 최고윤리책임자, 인사책임자, 준법감시인 및 최고리스크책임자)과 대화하여 조직의 프로세스와 검증 활동에 대한 명확한 이해를 얻을 수 있다. 최고감사책임자는

이전에 완료된 거버넌스 검토 보고서 및/또는 결과를 검토할 수 있으며, 식별된 우려사항에 특히 주의를 기울인다.

리스크 관리 프로세스의 이해

최고감사책임자는 조직이 운영되는 산업 및 부문에 해당되는 특정한 수행 지침뿐만 아니라 전세계적으로 인정되는 리스크 관리 원칙, 체계(frameworks) 및 모델을 이해해야 한다.

최고감사책임자는 조직이 리스크 성향을 정의하고 리스크 관리 전략 및/또는 체계를 구현했는지 여부를 식별하는 것을 포함하여 조직의 리스크 관리 프로세스의 성숙도를 평가하기 위한 정보를 수집해야 한다. 최고경영진 및 이사회와의 논의는 최고감사책임자가 조직의 리스크 관리와 관련된 그들의 관점과 우선순위를 이해하는 데 도움이 된다.

최고감사책임자는 리스크 정보를 수집하기 위해 최고경영진 및 현업 경영진, 리스크 관리 책임자, 외부 감사인, 규제기관, 기타 내부 및 외부의 검증 서비스 제공자가 발행한 최근 완료된 리스크 평가와 관련된 보고서 등 커뮤니케이션을 검토해야 한다.

통제 프로세스의 이해

최고감사책임자는 전세계적으로 인정되는 통제 체계(controls frameworks)에 익숙해져야 하고, 조직에서 사용하는 통제 체계를 고려해야 한다. 최고감사책임자는 식별된 조직의 목표 각각에 대해 조직의 통제 프로세스와 그 효과성에 대한 폭 넓은 이해를 높이고 유지해야 한다. 최고감사책임자는 다음 사항들을 이행하기 위해 조직 전반의 리스크 및 통제 매트릭스(matrix)를 개발할 수 있다:

- 조직의 목표 달성 능력에 영향을 줄 수 있는 리스크를 문서화함.
- 리스크의 상대적 중대성을 구분함.
- 조직 프로세스의 핵심 통제장치를 파악함.
- 통제의 설계 적정성에 대해 검토하여 의도대로 작동하는지 여부에 대해 파악함.

최고감사책임자는 조직의 거버넌스, 리스크 관리 및 통제 프로세스에 대한 철저한 이해를 통해 조직의 성공을 향상시킬 수 있는 내부감사 서비스를 제공할 기회를 식별하고 우선순위를 지정할 수 있다. 식별된 기회는 내부감사 전략 및 계획의 근간이 된다.

적합성 증거

- 거버넌스, 리스크 관리 및/또는 통제를 위해 조직에서 사용하는 문서화된 체계(controls frameworks)와 프로세스
- 리스크 성향 정의서
- 각각의 전략, 접근법 및 감독을 포함하여 조직의 거버넌스, 리스크 관리 및 통제 프로세스에 대한 논의를 나타내는 이사회 회의 의제와 의사록
- 이사회 및 위원회 헌장
- 거버넌스 및 리스크 관리 역할을 맡은 조직 내 담당자들과의 회의록 또는 기록
- 거버넌스, 리스크 관리 및 통제에 대한 법규와 기타 요건

- 규제당국으로부터 받은 커뮤니케이션
- 사업 전략과 계획
- 전사적 리스크 및 통제 매트릭스(matrix)

국제내부감사표준 9.2 내부감사 전략

요건

최고감사책임자는 조직의 전략적 목표와 성공을 지원하고 최고경영진, 이사회 및 기타 핵심 이해관계자의 기대에 부합하는 내부감사부서를 위한 전략을 반드시 수립하고 실행해야 한다.

내부감사 전략에는 내부감사부서를 위한 비전, 전략적 목표 및 그를 뒷받침하는 계획이 반드시 포함되어야 한다.

최고감사책임자는 적어도 연 1 회 최고경영진 및 이사회와 함께 내부감사 전략을 반드시 검토해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

내부감사 전략은 내부감사부서가 내부감사 임무를 완수하도록 인도하는데 도움이 된다.

최고감사책임자는 내부감사 전략의 비전과 전략적 목표를 수립하기 위해 조직의 전략과 목표, 최고 경영진 및 이사회와의 기대치를 고려하는 것부터 시작해야 한다. 또한 최고감사책임자는 내부감사 임무에서 합의된 대로 수행할 서비스 유형과 내부감사부서가 충족시켜야 할 기타 이해관계자의 기대치를 고려할 수 있다. 최고감사책임자는 최고경영진 및 이사회와 함께 최소 연 1 회 내부감사 전략을 검토해야 하는 요건을 충족시키는 것 외에도, 내부감사전략에 대해 이사회와의 승인을 구하여야 한다.

비전은 내부감사부서의 바람직한 미래(예: 향후 3~5 년) 상태를 설명하고, 해당 부서가 임무를 완수하는 데 도움이 되는 방향을 제시한다. 또한, 비전은 내부감사인에게 영감을 주고 동기를 부여하며 내부감사부서가 지속적으로 개선되도록 설계된다. 전략적 목표는 비전을 달성하기 위해 실행에 옮길 수 있는 목표를 정의한다. 이를 뒷받침하는 계획은 각 전략적 목표를 달성하기 위한 보다 구체적인 방법과 단계를 설명한다.

전략 수립에 대한 한 가지 접근법은 내부감사부서의 강점, 약점, 기회 및 위협을 식별하고 분석하는 것이다. 이는 내부감사부서를 개선시키는 방법을 결정하기 위해 고안된 과정이다. 또 다른 접근법은 내부감사부서의 현재 상태와 원하는 상태 사이의 차이 분석을 수행하는 것이다.

전략을 뒷받침하는 계획에는 다음이 포함되어야 한다:

- 내부감사인의 역량 개발을 도울 수 있는 기회
- 내부감사기능의 효율성과 효과성을 향상시키는 기술의 도입 및 적용
- 내부감사부서를 전반적으로 개선할 수 있는 기회

최고감사책임자가 전략적 목표와 이를 뒷받침하는 계획을 수립할 때, 취해야 할 조치의 우선순위를 정하고 목표 달성 시기를 설정해야 한다.

내부감사 전략은 조직의 전략적 목표나 이해관계자의 기대에 변화가 있을 때마다 조정되어야 한다. 내부감사 전략을 보다 자주 검토해야 하는 변화요인은 다음과 같다:

- 조직의 전략 또는 거버넌스, 리스크 관리 및 통제 프로세스의 성숙도에 발생한 변화
- 조직의 규정 및 절차 또는 조직이 따라야 하는 법규의 변경
- 최고경영진, 이사회 구성원 또는 최고감사책임자의 변경
- 내부감사부서에 대한 내부 및 외부 평가 결과

최고감사책임자는 내부감사부서의 구성원 중에서 전략적 목표 및 계획과 관련된 특정 책임을 위임할 수 있다. 또한, 최고감사책임자는 전략 달성 여부를 측정하기 위한 핵심성과지표(KPI) 및 자체 평가 프로세스뿐만 아니라, 실행 일정을 설계할 수 있다. 내부감사 전략의 연례 검토에는 계획에 대한 내부감사부서의 진척도에 대한 논의가 포함되어야 한다.

적합성 증거

- 비전, 전략적 목표 및 이를 뒷받침하는 계획을 포함한 내부감사 전략서
- 최고경영진, 이사회 및/또는 기타 이해관계자와의 회의에서 기대사항이 논의된 회의록이나 관련 문서
- 전략 관련 정보 및 이에 대한 분석 기록
- 내부감사 전략을 수립 및 검토하고 이행을 모니터링하기 위한 내부감사 규정과 절차
- 계획의 진행상황에 대한 자체 평가 또는 기타 검토 결과

국제내부감사표준 9.3 내부감사현장

요건

최고감사책임자는 최소한 내부감사부서에 대해 다음 사항을 명시하는 내부감사현장을 반드시 마련하고 관리해야 한다:

- 내부감사활동의 목적
- 국제내부감사표준을 준수하겠다는 약속
- 임무와 내부감사부서를 지원하는 이사회의 책임
- 조직 내 지위와 보고 관계
- 감사 서비스 제공 범위와 유형을 포함한 내부감사부서의 책임
- 감사품질 검증 및 개선에 대한 약속

조직 외부에 있는 당사자에게 검증서비스를 제공하는 경우, 이러한 검증서비스의 성격도 내부감사현장에 반드시 정의되어야 한다.

최고감사책임자는 최고경영진 및 이사회와 내부감사현장에 대해 반드시 논의하고, 이사회 승인을 얻어야 한다. 최고감사책임자와 이사회는 주기적으로 이 현장을 반드시 검토해야 한다. 최고감사책임자는 내부감사현장의 변경이 필요한 경우, 수정된 현장에 대하여 이사회 승인을 반드시 받아야 한다. (표준 6.1 내부감사의 임무 참조)

실행 및 적합성 증거를 위한 고려사항

실행

내부감사현장은 조직마다 다를 수 있지만, 일반적으로 다음과 같은 주제를 포함한다:

- 개요 - 내부감사활동의 목적과 내부감사부서의 윤리 및 전문성, 표준 적합성과 관련 법규(필요 시 지정된) 준수를 나타낸다. (영역I과 영역II 참조)
- 임무 - 이사회가 승인한 내부감사부서와 최고감사책임자의 권한, 역할 및 책임을 지정한다. (표준 6.1 내부감사의 임무 참조)
- 조직 내 지위 및 보고 관계 - 조직의 독립성이 보장되는 최고감사책임자의 보고 관계 및 내부감사부서의 조직 내 지위를 문서화한다. (표준 7.1 조직의 독립성과 7.2 최고감사책임자의 역할, 책임 및 자격 참조) 이 부분에서는 내부감사부서의 보고 관계를 명확히 하기 위해 "이사회" 및 "최고경영진"이라는 용어를 정의하고, 내부감사부서를 지원하고 감독하는 이사회 책임을 정해야 한다. (원칙 6 이사회가 부여하는 권한, 원칙 8 이사회 감독 및 관련 표준 참조) 또한, 조직 내 정보 흐름의 지원과 내부감사부서의 인적 자원 관리 및 예산 승인과 같은 행정적 책임도 설명할 수 있다.
- 독립성 및 객관성에 대한 보호조치 - 손상요인이 존재하는 경우 실행해야 할 보호조치를 설명한다. (표준 2.2 객관성의 보호 및 표준 7.3 독립성의 보호 참조)
- 책임 - 제공할 내부감사 서비스의 범위와 유형, 최고경영진 및 이사회와의 의사소통 방식을 설명한다. 거버넌스, 리스크 관리 및 통제 프로세스에 대한 검증과 조언을 제공할 모든 책임을 식별해야 한다. (예: 교육 제공, 윤리 위반 보고서 모니터링, 부정행위 조사 수행 등)
- 감사품질 평가 및 개선 - 내부감사부서의 품질에 대한 내부 및 외부 평가 프로그램의 개발 및 유지와 평가 결과의 전달에 관한 기대사항을 설명한다. (표준 8.3 감사품질, 표준 8.4 감사품질에 대한 외부평가, 원칙 12 감사품질의 향상 및 관련 표준 참조)
- 서명 - 최고감사책임자, 지정된 이사회 대표 및 최고감사책임자가 행정적으로 보고하는 자 간의 동의를 나타낸다. 이 부분에는 날짜, 서명인의 이름 및 직위가 포함된다.

내부감사현장의 초안이 작성되면, 내부감사부서에 대한 이해와 기대를 정확하게 반영하고 있는지 확인하기 위해 최고경영진 및 이사회와 제안된 현장에 대해 논의해야 한다. 최고감사책임자는 이사회 회의에서의 논의 및 승인을 위해 초안의 최종본을 제시해야 한다.

또한, 최고감사책임자와 이사회는 내부감사현장의 조항이 내부감사부서가 그 목적을 지속적으로 달성하는데 충분한지 여부를 검토하고 재확인하는 빈도에 대해 동의해야 한다. 선진적인 관행은 매년 현장을 검토하고, 내부감사의 임무에 대한 질문 발생 시 필요한 내용을 참조하고, 필요 시 업데이트(update)하는 것이다.

공공 부문

내부감사의 임무가 법규와 같은 다른 준거 문서에 명시되어 있는 경우, 해당 문서가 현장 역할을 할 수 있다.

행정적 보고 관계는 법으로 설정될 수 있으며 경영진이 아닌 이사회에만 해당될 수 있다.

적합성 증거

- 내부감사현장에 대한 논의와 승인 내용이 기록된 이사회 의사록
- 날짜, 서명자의 이름 및 직함이 기재되어 있는 승인된 현장
- 최고감사책임자가 최고경영진 및 이사회와 함께 내부감사현장을 주기적으로 검토한다는 증거가 포함된 이사회 의사록

국제내부감사표준 9.4 감사 방법론

요건

최고감사책임자는 내부감사부서가 임무를 달성하고, 표준에 부합하도록 안내하는 감사 방법론(정책, 프로세스 및 절차)을 반드시 수립해야 한다.

감사방법론은 다음 사항을 포함한 내부감사 프로세스 및 서비스에 대해 반드시 지침을 제시해야 한다:

- 조직 전체 및 개별감사업무를 위한 리스크 평가
- 내부감사계획을 수립
- 검증과 자문 업무 사이의 균형을 결정
- 내부 및 외부 검증 제공자와의 조정
- (이용 시) 외부 서비스 제공자를 관리
- 감사인이 접근할 수 있는 데이터 및 정보를 보호
- 내부감사업무를 수행:

- 검토대상활동의 거버넌스, 리스크 관리, 통제 고려사항을 뒷받침하는 권위 있는 체계와 지침을 식별
- 비즈니스 프로세스 및 테스트할 리스크의 우선순위 분석
- 통제 프로세스의 설계 및 운영을 테스트
- 근본 원인 규명
- 필요한 문서와 승인을 확보
- 내부감사 업무 수행 및 문서화 감독
- 감사 지적사항 및 결론의 중대성 판단
- 내부감사 서비스의 결과 커뮤니케이션
- 조직의 지침, 관련 규정 또는 기타 요건에 따른 업무 기록 및 기타 정보를 유지 및 공개
- 경영진의 조치 계획 완료 모니터링
- 내부감사부서의 품질 및 개선 검증
- 내부감사 임무에 포함되어 있는 추가 서비스 수행

최고감사책임자는 반드시 내부감사부서가 감사 방법론에 대한 교육을 받도록 해야 한다.

최고감사책임자는 반드시 감사 방법론의 효과성을 평가하고, 내부감사부서를 개선하고 부서에 영향을 미치는 중대한 변화에 대응하기 위해 필요에 따라 그 방법론을 개정해야 한다.

(원칙 13 효과적인 감사계획 수립, 원칙 14 감사업무 수행, 원칙 15 감사결론 커뮤니케이션 및 조치계획 모니터링에 제시된 표준 참조)

실행 및 적합성 증거를 위한 고려사항

실행

감사 방법론의 형식, 내용, 세부 수준 및 문서화 정도는 내부감사부서의 규모, 구조, 성숙도 및 업무의 복잡성에 따라 다를 수 있다. 방법론은 개별 문서(표준 운영 절차 등)로 존재하거나, 내부감사 매뉴얼에 포함되거나 내부감사 관리 소프트웨어에 통합될 수 있다.

최고감사책임자는 내부감사부서의 성공을 보장하기 위해 표준에 부합하고 이를 지원하는 감사 방법론을 수립하고, 내부감사 프로세스 수행 및 서비스를 실행하기 위한 체계적인 접근방식을 내부감사인들에게 안내한다. 내부감사 방법론은 내부감사인이 표준을 실행하고 양질의 서비스를 수행하는 데 도움이 되는 특정 지침과 기준을 제공함으로써 표준을 보완한다. 예를 들어, 최고감사책임자는 감사 지적사항 및 결론을 평가할 때, 내부감사인을 지원하기 위해 전체 감사지적사항을 고려하여 개별 감사지적사항의 중대성과 감사결론의 중대성을 나타내는 방법론, 등급 척도, 순위 등을 마련해야 한다. (표준 14.3 지적사항의 평가, 14.5 감사 결론의 구성 참조)

일부 감사 방법론에는 프로세스 또는 시스템 개발이 필요하다. 예를 들어, 최고감사책임자는 경영진이 감사 지적사항을 해결하기 위한 조치를 이행했는지 여부를 모니터링하는 프로세스를

수립해야 한다. 내부감사인은 최고감사책임자가 수립한 방법론과 프로세스를 이용한다. (표준 15.2 조치 계획의 이행 확인 참조)

또한, 감사 방법론은 최고감사책임자가 최고경영진 및 이사회와 합의하여 결정하는 검증 업무 외에 의사소통, 운영 문제 처리, 서비스 수행을 위한 프로세스와 절차를 설명한다. 이러한 서비스의 예로는 교육 제공, 윤리 위반 보고서 모니터링, 부정행위 조사 수행, 환경과 보건 및 안전(EHS) 평가 수행이 있다. 최고감사책임자는 내부감사부서가 그러한 서비스를 제공할 것으로 예상되는 경우 감사 방법론을 수립하고, 내부감사인을 적절하게 교육시켜야 한다.

내부감사부서의 품질을 평가하는 동안 감사 방법론의 효과성을 검토해야 한다. 최고감사책임자는 내부감사 직무 표준 및 지침의, 법규요건의, 그리고 기술 혁신에서의 중대한 변화가 있을 때 방법론을 업데이트(update)할 필요가 있다.

적합성 증거

- 감사 방법론을 포함하는 문서 또는 소프트웨어 프로그램
- 회의 안건 및 회의록, 이메일, 서명된 확인서, 교육 일정 또는 감사 방법론에 대해 내부감사 직원과의 커뮤니케이션을 증명하는 유사 문서
- 감사 방법론의 준수를 입증하는 감사 작업 문서

국제내부감사표준 9.5 내부감사계획

요건

최고감사책임자는 조직의 목표 달성을 지원하는 내부감사계획을 반드시 마련해야 한다.

최고감사책임자는 조직의 전략, 목표 및 리스크에 대한 문서화된 평가를 기반으로 내부감사계획을 반드시 수립해야 한다. 이 평가에는 조직의 거버넌스, 리스크 관리 및 통제 프로세스에 관한 이해뿐만 아니라 최고경영진과 이사회의 의견도 반드시 반영해야 한다. 평가는 적어도 연 1 회 반드시 수행되어야 한다.

내부감사계획은 다음을 반드시 충족해야 한다:

- 내부감사 전략과 전체 범위의 내부감사 서비스를 고려
- 조직의 거버넌스, 리스크 관리 및 통제 프로세스의 평가와 개선을 지원하는 내부감사 서비스를 명시
- IT 거버넌스의 범위, 부정행위 리스크, 조직의 컴플라이언스 및 윤리 프로그램의 효과성 고려
- 필요한 재정적, 인적 및 기술적 자원을 파악
- 조직의 비즈니스, 리스크, 운영, 프로그램, 시스템, 통제 및 조직 문화의 변화에 따른 변동 및 적시 업데이트(update)

최고감사책임자는 반드시 필요할 때마다 내부감사계획을 검토 및 수정하고, 최고경영진과 이사회에 다음사항을 적시에 전달해야 한다:

- 감사자원의 제한이 내부감사범위에 미치는 충격/영향
- 리스크가 높은 영역이나 활동에 대한 검증 업무를 계획에 포함하지 않은 근거
- 새롭게 등장한 리스크를 이유로 먼저 감사를 해달라는 요청과 계획된 검증업무를 자문업무로 대체 해달라는 요청과 같이 주요 이해 관계자 간에 감사서비스에 대해 상충하는 요구
- 감사범위에 대한 또는 감사정보 접근에 대한 제한

최고감사책임자는 중요한 중간 변경사항을 포함하여, 내부감사계획을 최고경영진 및 이사회와 반드시 논의해야 한다. 계획에 대한 중대한 변경은 반드시 이사회에 승인을 받아야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

내부감사계획의 수립과 수정 빈도는 조직과 리스크 환경의 변화 정도와 빈도 등과 같은 요소에 따라 결정되어야 한다. 표준은 내부감사계획의 기초로, 조직 전체의 리스크 평가를 최소 1년에 한번 실시하도록 요구한다. 그러나, 최고감사책임자는 리스크 정보를 지속적으로 파악하고, 이에 따라 리스크 평가 및 내부감사계획을 업데이트(update)해야 한다. 조직의 환경이 역동적인 경우 내부감사계획을 반기, 분기 또는 월 별로 업데이트(Update)해야 할 수도 있다.

초기에 내부감사계획을 준비하는 한 가지 접근방식은 감사모집단("리스크 모집단"이라고도 함)을 파악하여 조직 내에서 잠재적으로 감사 가능한 단위를 구성하고, 리스크의 식별 및 평가를 용이하게 하는 것이다. 감사모집단은 조직의 목표 및 전략적 계획에 대한 이해를 기반으로 하고, 조직의 구조 또는 리스크 체계(frameworks)와 일치할 때 가장 유용하다. 감사 가능한 단위에는 비즈니스 단위, 프로세스, 프로그램 및 시스템이 포함될 수 있다. 최고감사책임자는 포괄적인 리스크 평가 및 조직 전체의 검증 범위 식별을 준비하기 위해 해당 조직 단위를 주요 리스크에 연결할 수 있다. 최고감사책임자는 이 프로세스를 통해 내부감사 업무 중에 추가로 평가할 리스크의 우선 순위를 지정할 수 있다.

내부감사부서는 감사 모집단 및 리스크 평가가 조직의 주요 리스크를 포함하는지 확인하기 위해 일반적으로 조직의 리스크 관리 시스템 내에서 식별된 주요 리스크를 독립적으로 검토하고 검증한다. 내부감사부서는 조직의 리스크 관리 프로세스가 효과적이라는 결론을 내린 경우에만 리스크 및 통제에 대한 경영진의 정보에 의존해야 한다.

최고감사책임자는 조직 전체 또는 포괄적인 리스크 평가를 완료하기 위해 광범위한 조직차원에서 뿐만 아니라 특정한 감사대상 단위에서도 목표와 전략을 고려해야 한다. 또한, 최고감사책임자는 윤리, 부정행위, IT, 제 3자 관계, 규제 요건 미준수와 관련된 리스크와 같이 하나 이상의 사업 단위나 프로세스와 연결되거나 보다 복잡한 평가가 필요한 리스크를 적절히 고려해야 한다.

최고감사책임자는 리스크 평가를 뒷받침하기 위해 최근 수행한 내부감사 업무와 이사회 및 최고경영진과의 논의로부터 정보를 수집할 수 있다. (표준 9.1 거버넌스, 리스크 관리 및 통제 프로세스 이해, 표준 11.3 결과의 의사소통 참조) 최고감사책임자는 리스크를 지속적으로

평가하는 방법론을 구현할 수 있다. 리스크는 목표 달성에 부정적 영향과 장애물로서의 관점뿐만 아니라 조직의 목표 달성 능력을 향상시키는 기회 측면에서도 고려되어야 한다.

최고감사책임자는 감사계획에 중대하고, 새롭고, 발생 중인 리스크가 모두 적절하게 식별 및 고려될 수 있도록 전략을 수립해야 한다. 특히 규모가 작은 내부감사부서에서는 자원 제한 때문에 매년 감사 모집단에 있는 모든 리스크를 평가하기 어려울 수 있다. 이 경우 최고감사책임자는 경영진의 리스크 평가, 최고경영진 및 이사회와의 회의, 이전의 감사업무 및 기타 감사 수행 결과와 같은 리스크 정보 출처에 대해 의존도를 높여야 할 수 있다. 최고감사책임자는 주기적으로 의존도를 재평가하는 계획을 세워야 한다.

최고감사책임자는 내부감사계획 수립을 위해 최고경영진 및 이사회와의 의견과 요청사항, 조직 전체에 대한 검증 범위, 다른 검증 제공자의 업무수행에 의존할 수 있는 내부감사부서의 능력 등을 포함하여, 표준의 기타 요건은 물론 조직 전체에 대한 리스크 평가를 통해 식별된 잔여 리스크 수준의 결과를 고려한다. 내부감사계획수립은 지속적 감사 또는 민첩한 감사의 개념을 통합할 수 있기 때문에 내부감사계획은 "반복적(rolling)", "유동적(fluid)" 또는 "역동적(dynamic)"으로 간주되며, 내부감사부서가 연중 발생하는 변화에 기민하고 역동적으로 대응할 수 있도록 해준다.

내부감사인원은 내부감사계획이 모든 의무적이고 리스크를 기반으로 한 감사업무가 포함하는 것을 보장하기 위해 다음 사항을 고려해야 한다:

- 법규에 의해 요구되는 감사업무
- 조직의 미션 또는 전략에 중요한 감사업무
- 상당한 수준의 잔여 리스크가 존재하는 영역 및 업무
- 모든 중대한 리스크가 검증서비스 제공자에 의해 충분히 검증되는지 여부
- 자문 요청 및 수시로 발생하는 요청
- 잠재적 감사업무 각각에 대해 필요한 시간과 자원
- 조직의 거버넌스, 리스크 관리 및 통제 프로세스 개선에 기여할 수 있는 감사업무와 같이, 각각의 감사업무가 조직에 가져올 수 있는 잠재적 효익

최고감사책임자는 내부감사 업무 일정을 수립하기 위해 다음 사항을 고려해야 한다:

- 조직의 운영상 우선순위
- 외부감사인 및 규제기관의 검토일정
- 내부감사인의 역량 및 가용성
- 검토대상활동에 접근할 수 있는 능력

예를 들어, 특정 시기에 감사업무를 수행해야 하는 경우, 해당 감사를 완료하는 데 필요한 자원으로 해당 기간에 가용할 수 있어야 한다. 마찬가지로 검토대상활동이 연중 특정 기간 동안 제공되지 않거나 제약이 있는 경우, 해당 기간을 피하도록 감사업무 일정을 수립해야 한다.

제안된 내부감사계획에는 일반적으로 다음이 포함된다:

- 감사가 검증 또는 자문 업무인지 명시한 감사업무 제안 목록
- 제안된 각 감사업무를 선택한 근거. 예를 들면, 리스크의 중요성, 조직의 테마(theme)나 추세(근본 원인), 규제 요건 또는 마지막 감사 이후 경과 기간
- 제안된 각 감사업무의 전반적인 목적 및 예정 감사 범위
- 내부감사부서를 개선하기 위한 감사 외 활동이나 프로젝트의 목록
- 우발상황 및 수시 요청을 위해 유보되어야 할 시간의 비율

최고감사책임자, 최고경영진 및 이사회는 감사계획의 수정을 요하는 중대한 변화를 정의하는 기준에 동의해야 한다. 합의된 기준 및 프로토콜(protocol)은 내부감사부서의 방법론에 통합되어야 한다. 중대한 변화의 예로는 중요한 리스크 또는 중대한 전략적 목표와 관련된 감사업무의 취소나 연기가 있다. 이사회와의 공식 논의 일정을 잡기 전에 감사계획을 수정해야 하는 리스크가 발생하는 경우, 이사회에 변경사항을 즉시 알리고 가급적 빨리 공식 승인을 받아야 한다.

적합성 증거

- 승인된 내부감사계획
- 감사계획의 기반이 되는 정보를 포함하는 리스크 평가서, 우선순위 정의서
- 최고감사책임자가 최고경영진 및 이사회와 함께 감사 모집단, 조직차원의 리스크 평가, 내부감사계획, 계획의 중요한 변경을 처리하기 위한 기준과 프로토콜(protocol)에 대해 논의한 회의록
- 조직차원의 리스크 평가 및 내부감사계획을 알리기 위해 정보 수집 논의를 문서화한 기록
- 내부감사계획을 배포 받은 사람들의 명단
- 중요한 변경 처리를 위한 조직차원의 리스크 평가 및 프로토콜(protocol)에 대해 문서화된 방법론

국제내부감사표준 9.6 조정 및 의존

요건

최고감사책임자는 반드시 내부 및 외부의 검증 서비스 제공자와 조정하여 그들의 업무수행에 의존하는 것을 고려해야 한다.

서비스의 조정은 서비스 수행에 드는 노력의 중복을 최소화하고, 핵심 리스크 적용범위의 차이를 강조하며, 모든 서비스 제공자가 제공하는 전체적인 부가가치를 향상시킨다.

최고감사책임자는 반드시 다른 검증 및 자문 서비스 제공자를 평가하는 방법론을 수립해야 한다. 평가 시, 서비스 제공자의 역할, 책임, 조직적 독립성, 역량 및 객관성뿐만 아니라 업무수행 시 적용해야 하는 전문가로서의 정당한 주의도 반드시 고려해야 한다. 최고감사책임자는 서비스 제공자가 수행한 업무의 범위, 목표 및 결과를 반드시 이해해야 한다.

내부감사부서가 다른 검증 서비스 제공자의 업무수행에 의존하는 경우에도 최고감사책임자에게는 내부감사부서가 도달한 결론에 대한 책임이 있으며, 적절한 정보로 이러한 결론을 입증할 책임이 있다.

실행 및 적합성 증거를 위한 고려사항

실행

최고감사책임자는 최고경영진과 소통하고, 조직의 보고 체계와 이사회의 회의 안건 또는 의사록을 검토하여 조직의 검증 및 자문 서비스 제공자를 식별해야 한다. 내부의 검증 및 자문 서비스 제공은 컴플라이언스, 환경, 재무통제, 보건 안전, 정보 보안, 법무, 리스크 관리 및 품질 검증을 담당하는 부서와 같이 최고경영진에게 보고하는 부서에서 수행하거나, 일부 최고경영진이 수행한다. 외부의 검증 제공자는 최고경영진, 외부 이해관계자 또는 최고감사책임자에게 보고할 수 있다.

다음은 조정의 예이다:

- 계획된 업무의 성격, 범위 및 시기 공유
- 검증 기법, 방법 및 용어에 대한 공통의 이해 보장
- 서로의 업무수행 프로그램, 감사조서 및 보고서에 대한 접근 허용
- 공통 리스크 평가를 제공하기 위한 경영진의 리스크 관리 정보의 활용
- 감사업무 일정 조율
- 공유할 리스크 모집단 생성
- 합동 보고를 위해 결과 취합

검증 활동 조정 프로세스는 소규모 조직의 비공식 프로세스부터, 규제가 심한 대규모 조직의 복잡한 공식 프로세스에 이르기까지 조직에 따라 다양하다. 최고감사책임자는 서비스를 조정하는데 필요한 정보를 수집하기 위해 다양한 제공자와 만나기 전에, 조직의 기밀유지 요건을 고려한다. 종종 서비스 제공자들은 예정된 감사업무의 목표, 범위 및 시기와 이전 감사의 결과를 공유한다. 또한, 이들은 서로의 업무수행에 의존할 것인지에 대해 논의한다.

검증 범위를 조정하는 한 가지 방법은 식별된 중대한 리스크 범주를 관련된 검증 출처와 연결하고, 각 리스크 범주에 제공되는 검증 수준을 평가하여 검증 지도를 만드는 것이다. 이 지도는 포괄적이기 때문에, 검증 범위의 차이와 중복을 드러내, 최고감사책임자가 각 리스크 영역에서 검증 서비스의 충분성을 평가할 수 있다. 당사자들이 업무를 조정하는 방법에 대해 합의에 도달할 수 있도록, 다른 검증 제공자와 그 결과를 논의할 수 있다. 최고감사책임자는 합동 검증 접근방식을 통해 내부감사부서의 검증 업무를 다른 검증 제공자와 조정하여 감사업무의 성격, 빈도 및 중복을 줄이고, 검증 범위의 효율성을 극대화한다.

최고감사책임자는 내부감사부서의 전문 분야가 아닌 특수 영역을 평가하고, 감사업무를 완료하는데 필요한 테스트의 양을 줄이고, 내부감사계획을 넘어선 리스크에 대한 검증을 강화하기 위해서 등 여러가지 이유로 기타 서비스 제공자의 업무수행에 의존하는 것을 선택할 수 있다.

내부감사부서가 다른 서비스 제공자의 업무수행에 의존할 것인지 결정하기 위해, 감사방법론에 제공자의 다음 사항을 고려해야 한다:

- 잠재적 또는 실질적인 이해충돌 및 공개 여부
- 보고 관계와 서비스 제공자의 업무수행에 의존하는 것이 미칠 수 있는 잠재적인 충격/영향
- 전문적인 경험, 자격, 인증 및 제휴 관계의 관련성과 타당성
- 업무계획 수립, 감독, 문서화 및 검토에 적용되는 방법론과 주의사항
- 지적사항과 그 지적사항이 충분하고 신뢰할 수 있으며 관련성 있는 증거에 기반하여 합리적으로 보이는지 여부

최고감사책임자는 다른 검증 제공자의 업무수행을 평가한 후, 내부감사부서가 해당 업무수행에 의존할 수 없다고 결정할 수 있다. 내부감사인인 수행업무를 다시 테스트하고 추가 정보를 수집하거나 검증 서비스를 독립적으로 수행할 수 있다.

내부감사부서가 지속적으로 또는 장기적으로 다른 검증서비스 제공자의 서비스업무에 의존하려는 경우, 당사자는 제공할 검증서비스에 대해 합의한 사항과 검증 내용, 테스트와 검증 수행 사실을 뒷받침하는 증빙을 문서화해야 합니다.

적합성 증거

- 검증 및 자문 서비스의 개별 제공자 또는 고위 경영진 및 이사회와의 회의의 회의록에 기록될 검증 및 자문 서비스의 역할과 책임에 관한 명확한 커뮤니케이션
- 각 영역에서 검증 서비스를 담당할 제공자를 식별한 검증 지도 및/또는 합동 검증 계획
- 내부감사부서가 서비스 제공자의 업무수행에 의존할 수 있는지 결정하기 위해 최고감사책임자가 수립한 방법론 문서
- 현장 등 수행할 검증 작업의 명세 확인이 가능한 다른 보증 제공자와 체결한 약정서

원칙 10 감사자원 관리

최고감사책임자는 내부감사부서의 전략을 실행하고 계획을 완수하며 그 임무를 달성하기 위해 감사자원을 관리한다.

감사자원을 관리하려면 재정적, 인적 및 기술적 자원을 효과적으로 확보하고 배치해야 한다.

최고감사책임자는 조직의 프로세스를 따라 내부감사의 책임을 수행하는 데 필요한 감사자원을 확보하고, 내부감사부서를 위해 수립된 방법론에 따라 자원을 배치한다.

국제내부감사표준 10.1 재무 자원 관리

요건

최고감사책임자는 반드시 내부감사부서의 재무 자원을 관리해야 한다.

최고감사책임자는 반드시 내부감사의 임무와 계획을 성공적으로 달성할 수 있는 예산을 수립해야 한다. 예산에는 교육 및 기술과 툴(tool)의 획득을 포함하여, 부서 운영에 필요한 자원이 포함된다. 최고감사책임자는 반드시 예산에 맞춰 내부감사부서의 일상 업무를 효과적이고 효율적으로 관리해야 한다.

최고감사책임자는 반드시 이사회에 예산안을 제출하여 승인을 받아야 한다. 최고감사책임자는 불충분한 재원의 충격/영향을 최고경영진 및 이사회에 적시에 전달해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

최고감사책임자는 최소 월 1 회 예산 계획과 실적을 검토하고 중대한 차이를 분석하여 조정이 필요한지 결정해야 한다. 예산에는 예상치 못한 내부감사계획 변경 필요 시를 대비한 준비금이 포함될 수 있다.

최고감사책임자는 예상치 못한 상황으로 인해 상당한 추가 자원이 필요한 경우, 최고경영진 및 이사회와 이러한 상황을 논의해야 한다.

공공 부문

최고감사책임자는 예산이 법규에 따라 설정된다 하더라도 주어진 예산 내에서 내부감사부서의 자원을 할당하는 방법을 반드시 결정해야 하며, 편성된 재원이 부족할 경우 이사회 및 경영진에게 반드시 알려야 한다.

소규모 내부감사부서

최고감사책임자는 내부감사부서의 규모가 작아 그 예산이 타 부서, 사업 단위 또는 권한자가 관리하는 더 큰 예산 내에서 설정되는 경우에도, 내부감사부서에 배정된 자금을 이해하고, 지출을 추적하고, 내부감사부서에 배정된 재원의 충분성을 모니터링해야 하며, 이사회에 그러한 정보를 제공해야 한다.

아웃소싱

내부감사부서를 아웃소싱하는 조직의 경우에도(개별 프로젝트 예산이 아닌) 내부감사부서를 위한 포괄적이고 총체적인 예산을 반드시 수립하고, 주기적으로 검토하여 그 충분성을 확인해야 하며, 이사회는 필요 시 충분한 자원을 지원해야 한다.

적합성 증거

- 예산, 예측 및 실제 지출 비용에 대한 내부감사계획의 문서화
- 최고감사책임자가 내부감사 예산에 대해 최고경영진 및 이사회와 논의한 회의록
- 내부감사부서의 예산 및 승인을 논의한 이사회 회의록

국제내부감사표준 10.2 인적 자원 관리

요건

최고감사책임자는 내부감사현장을 성공적으로 이행하고 내부감사계획을 달성하는 데 필요한 자격을 갖춘 내부감사인 채용, 개발 및 유지하는 프로그램을 반드시 수립해야 한다.

최고감사책임자는 반드시 승인된 내부감사계획을 달성하기 위해 인적 자원이 적절하고 충분하며 효과적으로 배치되도록 해야 한다. 적절함은 지식, 기술 및 능력의 혼합을 가리킨다. 충분함은 자원의 양을 의미한다. 효과적인 배치는 내부감사계획의 달성을 최적화하는 방식으로 자원을 할당하는 것을 뜻한다.

최고감사책임자는 내부감사부서의 인적 자원의 적합성과 충분성에 대해 반드시 최고경영진 및 이사회와 소통해야 한다. 이사회는 반드시 자원 계획을 승인해야 한다. 내부감사부서에 내부감사계획을 달성하기 위한 적절하고 충분한 인적 자원이 부족한 경우, 최고감사책임자는 반드시 자원 확보 방법을 결정하거나, 그러한 제한의 충격/영향을 적시에 최고경영진 및 이사회에 전달해야 한다.

최고감사책임자는 반드시 내부감사부서 내에서 개별 내부감사인의 역량을 반드시 평가하고 전문성 개발을 장려해야 한다. 최고감사책임자는 반드시 내부감사인과 협력하여 교육, 감독자의 피드백 및/또는 멘토링을 통해 개인적인 역량을 개발하게 한다.

실행 및 적합성 증거를 위한 고려사항

실행

내부감사부서의 자원조달에 대한 구조 및 접근방식은 내부감사현장과 일치해야 하며, 내부감사계획과 전략적 목표 달성을 지원해야 한다.

최고감사책임자는 내부감사부서의 인적 자원 관리 프로그램을 만들 때, 다음을 수행해야 한다:

- 구조 및 복잡성, 지리적 운영 지역, 문화와 언어의 다양성, 조직이 운영되는 리스크 환경의 변동성과 같은 조직적 특성 고려
- 내부감사 예산과 비용의 효과성 및 다양한 인력배치 방식의 유연성 고려해야 한다(예: 직원 고용 대 외부 서비스 제공자에게 외주).
- 내부감사현장을 이행하고 내부감사계획을 달성하는 데 필요한 인적 자원 확보 방법의 이해
- 최고경영진 및 이사회와 소통하여 접근방식에 대한 합의 도출

최고감사책임자는 자격을 갖춘 내부감사인 채용 프로그램을 지원하기 위해 다음을 수행해야 한다:

- 인사부서와 협력하여 표준 3.1 역량 및 전문 역량 체계의 요건에 부합하는 직무 명세서 또는 기술서를 마련
- 다양한 배경, 경험 및 관점을 가진 내부감사인을 채용하고 효과적인 협업과 다양한 견해를 공유할 수 있는 포괄적인 업무 환경을 조성하는 이점을 고려

- 취업 박람회, 학생 행사, 전문 네트워킹 기회 및 채용 후보자와의 면접과 같은 채용 활동에 참여

최고감사책임자는 내부감사인을 개발하고 보유하기 위해 다음 사항을 수행해야 한다:

- 내부감사부서의 전략적 목표 달성을 지원하는 보상, 승진 및 포상활동 실행
- 내부감사인의 교육, 성과 평가 및 전문성 개발 촉진을 위한 방법론 실행
- 지식의 부서간 공유 및 승계 계획과 같은 내부감사부서와 조직의 인적 자원 목표 고려
- 윤리적이고 전문적인 환경을 조성하고 내부감사인이 적절하게 교육받고 효과적으로 협업하도록 보장함. (영역 II. 윤리 및 전문성 참조)

최고감사책임자는 인적 자원이 내부감사계획을 달성하는데 적절하고 충분한지 평가하기 위해 다음 사항을 고려해야 한다:

- 내부감사인의 역량 및 내부감사 서비스를 수행하는 데 필요한 역량
- 서비스를 완료하는 데 필요한 시간
- 서비스의 성격 및 복잡성
- 내부감사인의 수와 생산적인 업무가 가능한 시간
- 내부감사인, 조직의 정보, 인력, 자산의 가용성을 포함한 일정 제약조건
- 다른 검증 제공자의 업무수행에 의존할 수 있는 능력 (표준 9.6 조정 및 의존 참조)

최고감사책임자는 역량 체계(-frameworks)를 이용하여 내부감사부서의 역량 및 경험 목록을 식별, 평가 및 작성할 수 있다. 최고감사책임자는 내부감사계획을 달성하는 데 필요한 역량을 검토한다. (표준 3.1 역량 참조)

최고감사책임자는 역량 외에도 개별 내부감사인의 일정과 검토대상활동을 담당하는 직원의 가용성을 기반으로 내부감사 업무의 시기 또는 일정을 고려한다. 특정 감사업무는 연중 특정 시기에 실시되어야 할 수 있으며, 해당 감사를 완료하는 데 필요한 자원도 해당 시간에 반드시 이용가능해야 한다.

최고감사책임자는 계획된 감사업무를 처리하는데 자원이 충분하지 않은 경우 기존 직원에 대한 교육을 제공하고, 조직 내에서 전문가를 초청감사인(guest auditor)으로 요청하고, 직원을 추가로 고용하고, 다른 검증 제공자에게 의존하고, 순환 감사 프로그램을 개발하거나 외부의 서비스 제공자와 계약을 체결할 수 있다. 외부의 서비스 제공자는 전문 기술을 제공하거나, 특별 프로젝트를 완료하거나, 제한된 수의 감사업무를 수행할 수 있다.

내부감사부서가 내부 직원으로 구성되는 경우, 내부감사 인력은 순환 배치 방식으로 보완될 수 있다. 예를 들어, 타 사업 단위의 직원이 내부감사부서에 일시적으로 합류했다가 나중에 원래의 사업 단위로 복귀하는 것이다. 내부감사부서로 파견된 직원은 전문 기술과 지식은 물론 고유한 관점 및 통찰력을 제공할 수 있다. 또한, 원래의 사업 단위로 복귀한 직원은 내부감사 경험을 통해 조직의 거버넌스, 리스크 관리 및 통제 프로세스에 대한 이해를 심화할 수 있다. 최고감사책임자는

순환 배치 방식을 이용할 경우 잠재적인 객관성 손상 및 필요한 안전장치를 인식해야 한다. (표준 2.2 객관성의 보호 참조)

내부감사인은 개인의 전문성 개발을 보장할 책임이 있으며, 역량 체계(-frameworks)를 이용하여 자신의 기술과 발전 기회를 평가해야 하며, 최고감사책임자는 내부감사인의 전문성 개발을 지원해야 한다. 최고감사책임자는 전문성 개발에 대한 최소한의 기대치를 설정할 수 있으며, 전문 자격 취득을 장려해야 한다. 최고감사책임자는 내부감사 예산에 교육 및 전문성 개발을 위한 비용지원을 포함해야 하며, 보수교육, 훈련 및 대회참석을 통한 내부 및 외부의 기회를 제공해야 한다. (표준 3.1 역량, 표준 10.1 자원 관리 참조)

감사업무 감독을 위한 내부감사 방법론에는 내부감사인이 감독 역할을 맡은 보다 경험 많은 내부감사인으로부터 건설적인 피드백을 받을 수 있는 충분한 기회가 포함되어야 한다. 이러한 피드백은 감독자가 감사조서 및 기타 커뮤니케이션을 검토할 때 서면이나 구두 형태로 제공될 수 있다. 멘토십(mentorship) 프로그램은 경험이 적은 내부감사인이 지식이 풍부한 감사인과 동행하면서 업무 수행을 직접 관찰할 수 있는 현장 경험 기회를 제공한다. 내부감사부서의 내부평가에 해당하는 상시 모니터링 및 주기적인 자체 평가는 내부감사인의 효과성을 높이기 위한 피드백(feedback)과 제안을 받을 수 있는 추가적인 기회를 제공한다. (표준 12.1 내부평가 참조) 연 1 회와 같이 정기적으로 수행되는 개인의 성과 평가는 내부감사인의 전문성 개발에 기여할 수 있는 또 다른 정보의 원천이다.

공공 부문

공공 부문의 최고감사책임자는 보상 결정을 내릴 권한이 없을 수 있으나, 인사부서와 협력하여 직무 분류기준에 내부감사인의 적절한 역량과 자격이 명시되고, 내부감사인의 채용과 유지, 역량의 평가 내용이 포함되도록 보장해야 한다.

적합성 증거

- 내부감사인 담당 직원의 역량과 내부감사인에게 요구되는 역량 간의 차이에 대한 분석서
- 직무 기술서
- 현 감사부서 감사인의 이력서
- 교육 계획서
- 교육과정 이수에 대한 증빙
- 내부감사인의 성과 평가서
- 외부 서비스 제공자와 체결한 계약서 및 해당 제공자가 투입한 내부감사인의 이력서
- 내부감사 예산에 관한 논의를 기록한 회의록
- 감사업무 예상 일정 및 자원 할당이 포함된 내부감사계획
- 감사업무 수행 후 계획 근무시간과 실제 근무한 시간의 비교
- 내부감사부서 및 개별 내부감사인의 성과 평가서

국제내부감사표준 10.3 기술적 자원

요건

최고감사책임자는 내부감사부서가 내부감사 프로세스를 뒷받침하는 적절한 기술을 보유하고 있는지 반드시 확인해야 한다.

최고감사책임자는 반드시 내부감사부서에서 사용하는 기술을 정기적으로 평가하고 효과성과 효율성을 개선할 수 있는 기회를 추구해야 한다.

최고감사책임자는 새로운 기술을 도입할 때 내부감사인 이 기술 자원을 효과적으로 사용하기 위해 적절한 교육을 받도록 반드시 보장해야 한다. 최고감사책임자는 반드시 조직의 IT 및 정보 보안 부서와 협력하여 기술 자원이 적절하게 도입되고, 적절한 통제가 효과적으로 작동하도록 해야 한다.

최고감사책임자는 기술적 제약이 내부감사부서의 효과성 또는 효율성에 미치는 충격/영향을 최고경영진 및 이사회에 반드시 전달해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

내부감사부서는 효과성 및 효율성을 개선하기 위해 기술을 이용해야 한다. 다음은 이러한 기술의 예이다:

- 감사 관리 시스템
- 프로세스 매핑 애플리케이션(Process mapping applications)
- 데이터 사이언스(data science) 및 분석을 지원하는 툴(tool)
- 커뮤니케이션과 협업을 지원하는 툴(tool)

최고감사책임자는 내부감사부서가 책임을 수행하기 위해 적절한 기술 자원을 확보할 수 있도록 다음 사항을 수행한다:

- 내부감사부서의 프로세스 전반에 걸쳐 기술로 구현되는 개선사항의 취득 및 실행에 대한 타당성 평가
- 승인을 위해 최고경영진 및 이사회에 충분한 보충자료와 함께 기술 자원 신청서 제출
- 승인된 기술을 도입하기 위한 계획을 수립하고 이행. 계획에는 내부감사인 교육과, 최고경영진 및 이사회를 대상으로 효익 실현에 대한 입증 포함한다.
- 정보 보안 및 개인 정보 보호와 관련된 리스크를 포함하여 기술의 이용으로 발생하는 리스크를 식별하고 대응

적합성 증거

- 기술 요청 및 도입과 관련된 논의의 기록이나 계획서
- 내부감사부서에서 사용 중인 기술 애플리케이션(technology applications) 목록
- 감사업무 중 기술의 이용을 증명하는 감사조서를 포함하여 기술 도입, 교육 및 이용에 대한 기록
- 내부감사인 이름과 이들의 기술 관련 인증 및 자격증
- 내부감사부서의 기술 자원 사용과 관련된 정보 보안, 기록 관리 및 기타 규정과 절차서

원칙 11 효과적인 커뮤니케이션

최고감사책임자는 내부감사부서가 이해관계자와 효과적으로 커뮤니케이션하도록 보장한다.

효과적인 커뮤니케이션을 위해서는 이해관계자와 관계를 구축하고 신뢰를 확립해야 하며, 이들이 내부 감사 서비스 결과로부터 이익을 얻도록 보장해야 한다. 최고감사책임자는 내부감사부서가 이해관계자와 지속적인 커뮤니케이션 체계를 확립하고 신뢰를 구축하고 관계를 증진하도록 도와줄 책임이 있다. 또한 최고 감사 책임자는 감사품질 보장하고 내부 감사 서비스의 결과에 기반한 통찰을 제공하기 위하여 고위경영진과 이사회에 대한 감사부서의 공식적인 커뮤니케이션을 감독한다.

국제내부감사표준 11.1 이해관계자와의 관계 구축 및 커뮤니케이션

요건

최고감사책임자는 이사회, 최고경영진, 현업부서의 경영진, 규제당국, 내부 및 외부 서비스 제공자를 포함한 주요 이해관계자와의 관계 및 신뢰를 구축하기 위해 내부감사부서가 취해야 할 접근방식을 반드시 수립해야 한다.

최고감사책임자는 내부감사부서와 이해관계자 간의 공식 및 비공식 커뮤니케이션을 촉진하여 다음에 대해 상호간에 이해할 수 있도록 반드시 기여해야 한다:

- 조직의 이익 및 우려사항
- 리스크를 식별 및 관리하고 검증을 제공하기 위한 접근방식
- 모든 당사자의 역할과 책임 및 협업 기회
- 관련 규제 요건
- 재무보고를 포함하여 중요한 조직의 프로세스

실행 및 적합성 증거를 위한 고려사항

실행

상시적인 정기 커뮤니케이션은 최고경영진, 이사회 및 내부감사부서 간에 조직의 리스크 및 검증 우선순위에 대한 공통의 이해에 기여하고, 변화에 대한 적응을 촉진한다. 조직의 목표와 리스크에

영향을 미칠 수 있는 주요 동향 및 계획된 업무활동에 대해 최신 상태를 유지하기 위해, 조직의 커뮤니케이션 채널에 최고감사책임자를 포함시켜야 한다. 또한, 최고감사책임자는 이사회와 주요 거버넌스 위원회는 물론 최고경영진 및 컴플라이언스, 리스크 관리, 품질 관리와 같이 최고경영진에게 직접 보고하는 그룹과의 회의에 참석해야 한다.

또한 최고감사책임자는 최고경영진 및 이사회와 커뮤니케이션 방법론을 논의하여 공식적인 커뮤니케이션이 필요한 심각한 문제를 정의하는 기준, 공식적인 커뮤니케이션의 형식과 내용, 그러한 커뮤니케이션의 주기를 결정해야 한다.

최고감사책임자는 최고경영진 및 이사회와 개별 구성원과 독립적으로 만남으로써 그들과 관계를 구축하고 그들의 우려사항과 관점에 대해 배울 수 있다. 내부감사인은 비즈니스 목표와 프로세스를 더 잘 이해하기 위해 사업 단위 책임자 및 운영 업무 담당자와 같이 현업부서 경영진의 핵심 구성원과 만날 수 있다. 규제가 엄격한 산업이나 부문에서는 최고감사책임자와 외부 감사인 및 규제당국 간의 회의가 적절할 수 있다.

최고감사책임자와 내부감사인은 전략, 목표 및 리스크는 물론 업계 뉴스, 추세(trends), 규제상의 변화에 대해 경영진 및 이사회와 논의를 개시할 수 있다. 이러한 논의는 설문조사, 인터뷰 및 집단 워크숍과 함께 새롭게 나타난 리스크와 부정 리스크에 대한 정보를 얻는 데 유용한 도구이다. 웹사이트, 뉴스레터, 프레젠테이션과 기타 형태의 커뮤니케이션은 내부감사부서의 역할과 효익을 직원 및 기타 이해관계자와 공유하는 효과적인 방법이 될 수 있다.

규모가 큰 내부감사부서의 최고감사책임자는 내부감사인 개인에게 글로벌 운영, IT, 컴플라이언스 및 HR(human resources)과 같은 핵심 부서의 경영진과 상시 커뮤니케이션을 유지할 책임을 위임할 수 있다. (표준 9.6 조정 및 의준 참조)

커뮤니케이션에는 내부감사인과 조직의 직원 간의 상시적이고 비공식 접촉 기회가 포함되어야 한다. 비공식 접촉이 지속적으로 이루어지면, 직원은 내부감사인을 신뢰하게 되어 공식 회의에서는 일어날 수 없는 솔직한 논의가 이루어질 가능성이 높아진다. 비공식 접촉은 관계 구축의 일환으로, 조직 및 통제 환경에 대한 내부감사인의 포괄적인 이해를 향상시킬 수 있다. 내부감사인을 특정 사업 단위나 지역의 업무에 순환 배치할 경우 내부감사인의 객관성 보호 필요성과 비공식 커뮤니케이션의 이점 사이에 균형을 유지할 수 있다.

공공 부문

내부감사인은 일반 대중을 조직의 직접적인 이해관계자로 고려해야 한다. 내부감사부서는 대중에게 봉사하기 위해 유틸리티(utilities), 대중 교통 시스템, 공원 및 여가 시설을 포함한 공공 서비스 이용자와 같은 대중의 의견을 고려할 수 있다. 추가적인 이해관계자에 선출직 공무원이 포함될 수 있다. 그러나, 내부감사인은 조직에 직접적인 거버넌스를 제공하지 않는 공무원의 지시를 받기 전에, 경영진 및 이사회를 관여시켜야 한다.

적합성 증거

- 문서화된 내부감사부서의 관계관리 계획서
- 내부감사부서 구성원 및 이해관계자 간의 회의 안건 또는 회의록
- 내부감사인이 내부 이해관계자의 의견을 구하는 설문조사, 인터뷰 및 집단 워크숍

- 내부감사부서가 조직의 이해관계자와 소통하는 웹사이트나 웹페이지, 뉴스레터, 프레젠테이션 및 기타 매체

국제내부감사표준 11.2 효과적인 커뮤니케이션

요건

최고감사책임자는 반드시 내부감사 커뮤니케이션이 정확하고, 객관적이며, 명확하고, 간결하고, 건설적이며, 완전하고, 적시에 이루어지도록 해야 한다.

커뮤니케이션은 반드시 다음과 같아야 한다.

- 정확성: 오류 및 왜곡이 없고, 관련 사실에 충실함.
- 객관성: 공평하고 편향적이지 않으며, 모든 관련 사실 및 상황에 대한 공정하고 균형 잡힌 평가의 결과.
- 명확성: 논리적이고 관련된 이해관계자가 쉽게 이해할 수 있으며, 불필요한 전문용어 사용을 지양함.
- 간결성: 간결하고, 불필요한 상세함 및 장황함이 없음.
- 건설적: 이해관계자 및 조직에 도움이 되며, 필요 시 개선을 유도함.
- 완전성: 내부감사 서비스의 결과를 뒷받침하며 관련 있고 신뢰할 수 있는 충분한 정보 및 증거.
- 적시성: 문제의 중요성에 따라 경영진이 적시에 적절한 시정 조치를 취할 수 있도록 함.

실행 및 적합성 증거를 위한 고려사항

실행

최고감사책임자는 내부감사 커뮤니케이션이 정확하고 객관적이며 명확하고 간결하고 건설적이며 완전하고 적시에 이루어지도록 보장하기 위해 내부감사부서의 커뮤니케이션을 감독하고, 일관성을 달성하기 위한 규정, 기준 및 절차를 포함할 수 있는 방법론을 수립한다. 커뮤니케이션 방법론은 최고경영진, 이사회 및 기타 이해관계자의 기대치를 고려해야 한다. (표준 9.4 방법론 참조) 최고감사책임자는 내부감사인에게 감사업무 보고서 작성이나 최종 커뮤니케이션 프레젠테이션 준비 교육과 같이, 커뮤니케이션 교육을 제공할 수 있다.

감독자의 검토를 통해 감사보고서를 비롯한 감사업무 커뮤니케이션이 다음의 특성 및 고려사항을 준수하였는지를 확인한다:

- 정확성 - 내부감사인은 커뮤니케이션 시 수집된 정보를 바탕으로 정확한 용어와 표현을 사용해야 한다. 내부감사인은 표준 11.4 오류 및 누락을 포함하여, 정확성과 관련된 다른 표준도 고려해야 한다.
- 객관성 - 내부감사 서비스의 지적사항, 권고사항, 결론 및 기타 결과는 반드시 모든 관련 상황에 대한 균형 잡힌 평가에 기반해야 한다. 커뮤니케이션은 사실에 입각한 정보를

식별하고, 해당 정보를 목표와 연결하는 데 중점을 두어야 한다. 내부감사인은 편향된 것으로 인식될 수 있는 용어를 피해야 한다. (원칙 2 객관성의 유지 및 표준 2.1 개별 감사인의 객관성 참조)

- **명확성** - 명확성은 내부감사인이 사용하는 언어가 조직에서 사용되는 용어와 일치하고, 듣는 사람이 쉽게 이해할 수 있을 때 높아진다. 내부감사인은 불필요한 전문용어 사용을 지양하고, 보고서나 프레젠테이션에 특정 또는 고유한 방식으로 사용되거나 일반적이지 않은 중요한 용어를 정의해야 한다. 내부감사인은 지적사항, 권고사항 및 결론을 뒷받침하는 중대한 세부정보를 포함하는 것으로 커뮤니케이션의 명확성을 제고한다.
- **간결성** - 중복을 피하고 불필요하거나 중요하지 않거나 업무 또는 서비스와 관련 없는 정보를 배제해야 한다.
- **건설적** - 내부감사인은 검토대상부서가 개선기회 및 조치 계획을 결정하는 것을 촉진하는데 협조적이고 도움이 되는 어조로 정보를 표현해야 한다.
- **완전성** - 완전성은 독자가 내부감사인이 도달한 것과 동일한 결론에 도달할 수 있게 한다. 내부감사인은 다양한 수신자를 위한 커뮤니케이션을 준비하고, 커뮤니케이션의 성격은 각 수신자 그룹에 맞게 조정되어야 한다. 예를 들어, 최고경영진 및 이사회에 대한 커뮤니케이션은 검토대상 활동의 경영진에게 전달되는 커뮤니케이션과 다를 수 있다. 내부감사인은 완전성을 보장하기 위해 수신자가 담당하는 조치를 취하는데 필요한 정보를 고려한다.
- **적시에** - 적시성은 조직마다, 감사업무의 성격에 따라 다를 수 있다.

최고감사책임자는 감사업무의 감독 이외에도 내부감사 커뮤니케이션의 효과성을 측정하고 모니터링하기 위해 핵심성과지표(KPI)를 정할 수 있으며, 이는 내부감사부서의 감사품질 평가 및 개선 프로그램(QAIP)의 일부로 사용될 수 있다. (표준 8.3 품질, 원칙 12 품질의 향상, 관련 표준 참조)

적합성 증거

- 효과적인 커뮤니케이션 기술에 대한 교육 또는 회의 참여 기록
- 최고감사책임자가 승인한 최종 커뮤니케이션 및 기타 문서와 효과적인 커뮤니케이션의 특징을 보여주는 보충 문서
- 효과적인 커뮤니케이션의 특징을 보여주는 프레젠테이션 슬라이드나 회의록
- 커뮤니케이션의 적시성을 입증하는 기록
- 효과적인 커뮤니케이션의 특징을 보여주는 감사조서
- 커뮤니케이션 효과성 향상에 대한 감독자의 검토가 포함된 감사조서
- 내부감사 커뮤니케이션의 품질에 관한 이해관계자 설문조사 결과
- 감사품질 평가 및 개선 프로그램(QAIP)의 결과

국제내부감사표준 11.3 감사결과 커뮤니케이션

요건

최고감사책임자는 반드시 내부감사 서비스의 결과를 주기적으로 전달해야 한다.

최고감사책임자는 커뮤니케이션의 성격과 시기에 대한 최고경영진 및 이사회에 기대치를 반드시 이해해야 한다.

다음은 내부감사 서비스의 결과이다:

- 감사 결론
- 효과적인 관행이나 근본 원인과 같은 테마(themes)
- 사업 단위나 조직 차원의 결론 등

감사 결론

최고감사책임자는 반드시 감사보고서를 비롯한 최종 감사업무 커뮤니케이션을 검토하고 승인해야 하며, 발행 전에 누구에게 어떻게 배포할지 결정해야 한다. 이 의무를 다른 내부감사인에게 위임할 때에도, 전반적인 책임은 최고감사책임자에게 있다. 최고감사책임자는 법규에 의한 의무 또는 제한이 없는 한, 최종 커뮤니케이션을 조직 외부에 공개하기 전에 반드시 법률 고문 및/또는 최고경영진의 조언을 구해야 한다. (표준 11.4 오류 및 누락, 표준 11.5 리스크 수용에 대한 커뮤니케이션 참조)

테마(Themes)

여러 감사업무의 지적사항 및 감사결론을 전체적으로 바라볼 경우 근본 원인과 같은 패턴이나 추세를 확인할 수 있다. 최고감사책임자가 조직의 거버넌스, 리스크 관리 및 통제 프로세스와 관련된 테마를 식별할 때 이러한 테마는 통찰력, 조언 및/또는 결론과 함께 적시에 최고경영진과 이사회에 전달되어야 한다.

사업 단위나 조직 차원의 결론

최고감사책임자는 업계 요구사항, 법규 또는 최고경영진, 이사회 및/또는 기타 이해관계자의 기대로 인해 거버넌스, 리스크 관리 및/또는 통제 프로세스의 효과성에 대해 사업 단위나 조직 차원에서 결론을 내려야 할 경우가 있다. 감사 결론은 여러 감사업무를 기반으로 최고감사책임자의 전문가적 판단을 반영하며, 반드시 관련성 있고 신뢰할 수 있으며 충분한 정보로 뒷받침되어야 한다.

최고감사책임자는 감사 결론을 최고경영진이나 이사회에 전달할 때 반드시 다음사항을 포함시켜야 한다:

- 감사결론에 대한 요청 요약
- 등급, 의견 또는 기타 설명으로 표현될 수 있는 결론
- 거버넌스 체계 또는 리스크 및 통제 체계와 같이 감사결론의 근거로 사용된 기준
- 감사결론과 관련된 제한 및 기간을 포함한 감사범위

- 감사결론을 뒷받침하는 정보의 요약
- 다른 검증 제공자의 업무에 대한 의존도 공개(해당 시)

실행 및 적합성 증거를 위한 고려사항

실행

내부감사 서비스의 결과는 개별 감사업무, 여러 감사업무, 시간 경과에 따른 최고경영진 및 이사회와의 상호작용에 기반할 수 있다.

감사보고서 등 감사업무 커뮤니케이션

표준 13.1의 감사업무 커뮤니케이션에서는 내부감사인이 검토대상활동의 담당자들과 감사 기간 전반에 걸쳐 커뮤니케이션할 것을 요구하지만, 최고감사책임자에게는 감사보고서 등 최종 감사업무 커뮤니케이션이 적절한 당사자에게 배포되도록 보장할 책임이 있다. 적절한 당사자에는 최고경영진, 이사회 및/또는 경영진의 조치 계획을 마련하고 실행할 책임이 있는 자들이 포함될 수 있다. (표준 13.1 감사업무 커뮤니케이션, 표준 15.1 최종 감사업무 커뮤니케이션 참조)

최고감사책임자는 내부감사인이 감사업무 커뮤니케이션에 검토대상부서의 만족스럽고 긍정적인 성과를 포함하도록 장려해야 한다. 여러 감사를 통해 식별된 모범 사례의 예는 조직의 다른 부분으로 전파될 수 있거나 조직 전체의 벤치마크 역할을 할 수 있다.

테마(themes)

다수의 감사를 통해 도출된 지적사항, 권고사항 및 결론을 추적하면 기준 대비 실제 상태의 개선이나 악화, 실제 상태의 기저 원인 또는 효과성이나 효율성을 높이는 관행을 공유할 수 있는 기회와 같이 추세(trends)를 식별할 수 있다.

최고경영진 및 이사회에 대한 커뮤니케이션에는 다음이 포함되어야 한다:

- 심각한 통제 취약점 및 확실한 근본 원인 분석
- 여러 감사업무나 사업 단위에 걸친 테마별 혹은 체계적 이슈, 조치 또는 진행상황

테마를 식별할 때 다른 검증 제공자로부터 얻은 통찰력을 고려할 수 있다. (표준 9.6 조정 및 의존 참조)

사업 단위나 조직 차원의 감사 결론

최고감사책임자는 사업 단위나 전체 조직 차원에서 감사 결론을 전달할 때, 결론이 조직의 전략, 목표 및 리스크와 어떻게 관련되는지 고려해야 한다. 또한, 최고감사책임자는 감사 결론이 문제를 해결하고, 가치를 부가하고, 경영진이나 기타 이해관계자에게 감사대상 테마나 실태 전반에 대해 확신을 줄 수 있는지 고려해야 한다.

또한, 최고감사책임자는 감사결론과 관련된 감사기간과 감사범위 제한을 고려하여 전반적인 감사업무에 대한 결론을 결정한다. 다른 내부 및 외부 검증 제공자가 완료한 감사업무를 포함하여, 모든 감사 또는 프로젝트가 고려된다. (표준 9.6 조정 및 의존 참조)

예를 들면, 전체 감사 결론은 독립적인 제 3 자나 규제당국과 같은 외부 기관에서 보고된 결과와 함께 조직의 지역 및 국가 차원에서 수집된 감사 결론을 기반으로 할 수 있다. 감사범위에는 감사 기간, 감사대상 업무활동, 감사제한 및 감사결론의 경계를 설명하는 기타 변수를 명시함으로써 전체 감사결론에 대한 맥락을 제공한다.

최고감사책임자는 전체 감사 결론의 기반이 되는 정보를 요약하고, 관련 리스크 또는 통제 체계나 전체 결론의 기초로 사용된 기타 기준을 식별해야 한다. 최고감사책임자는 전체 감사 결론이 조직의 전략, 목표 및 리스크와 어떻게 관련되는지를 명확히 설명해야 한다. 전체 감사 결론은 일반적으로 서면으로 전달되지만, 표준에 그렇게 해야 한다는 요건이 있는 것은 아니다.

공공 부문

대중 또는 조직 외부의 핵심 이해관계자와의 커뮤니케이션이 내부감사부서의 임무의 일부인 경우, 관련 법규나 규정에 명시된 바에 따라 적시에 최종 감사업무 커뮤니케이션을 할 수 있어야 한다.

공공 부문의 내부감사부서는 공개 회의에서 내부감사 결과를 발표해야 하는 경우가 많다. 표준 13.1 감사업무 커뮤니케이션에 따르면, 내부감사부서가 이사회나 선출된 기구에 보고하는 경우 최고경영진 및 법률 고문의 조언을 구하지 않고 감사 결과를 공개할 수 있으나, 이러한 경우에도 감사종료 보고 시 경영진에게 그 결과를 반드시 전달해야 한다.

적합성 증거

- 감사 지적사항, 권고사항 및 결론을 포함한 최종 감사업무 커뮤니케이션
- 최고감사책임자의 요약본, 회의록, 연설문, 슬라이드 또는 최고경영진 및 이사회와의 커뮤니케이션을 나타내는 문서
- 추세(trends)를 보여주는 데이터 보고서, 다이어그램(diagrams) 및 그래프(graphs)를 포함하는 분석
- 총평의 근거로 사용되는 관련 리스크 또는 통제 프레임워크나 기타 기준

국제내부감사표준 11.4 오류 및 누락

요건

감사보고서 등 최종 감사업무 커뮤니케이션에 심각한 오류나 누락이 존재할 경우, 최고감사책임자는 적시에 오류나 누락된 정보를 수정하여 최초의 커뮤니케이션을 받은 모든 이에게 반드시 전달해야 한다.

중요성은 이사회와 합의한 기준에 따라 결정된다.

실행 및 적합성 증거를 위한 고려사항

실행

최고감사책임자와 이사회는 오류나 누락의 심각성을 결정하는 기준과 정정사항을 전달하는 프로토콜(protocol)에 대해 합의해야 한다. 최고감사책임자는 심각성을 결정하기 위해 오류가 존재하거나 누락된 정보가 법규상의 조치를 초래하거나 지적사항, 결론, 권고사항 또는 조치 계획을 변경시킬 수 있는지 평가해야 한다.

최고감사책임자는 원래의 커뮤니케이션을 받은 모든 이에게 정정된 정보가 전달됨을 보장할 수 있는 가장 적절한 커뮤니케이션 방법을 결정한다. 최고감사책임자는 정정된 정보를 전달하는 것 외에도 오류 또는 누락의 원인을 파악하고, 향후 유사한 상황이 발생하지 않도록 시정 조치를 취해야 한다.

적합성 증거

- 오류 및 누락의 처리를 위한 내부감사 규정과 절차
- 중요성을 결정하기 위해 최고감사책임자가 이사회와 합의하여 사용하는 기준
- 최고감사책임자가 오류 또는 누락의 심각성과 원인을 어떻게 확정하는지 보여주는 통지문서 및 기타 기록
- 오류 또는 누락을 논의한 최고감사책임자의 일정, 이사회나 기타 회의 기록, 내부 메모 및 이메일
- 원본 및 정정한 최종 커뮤니케이션 문서
- 정정한 커뮤니케이션 수신에 관련된 당사자 전원에게 받은 서류

국제내부감사표준 11.5 리스크 수용에 관한 커뮤니케이션

요건

최고감사책임자는 허용할 수 없는 수준의 리스크에 대해 반드시 알려야 한다.

최고감사책임자가 경영진이 조직의 리스크 허용범위를 초과하는 수준의 리스크를 수용했다고 결론을 내리면, 해당 사안을 반드시 최고경영진과 논의해야 한다. 최고감사책임자가 이 사안이 최고경영진에 의해 해결되지 않았다고 판단하는 경우, 이를 반드시 이사회에 상정해야 한다. 리스크를 해결하는 것은 최고감사책임자의 책임이 아니다.

실행 및 적합성 증거를 위한 고려사항

실행

최고감사책임자는 최고경영진과 이사회와의 논의, 이해관계자와의 관계와 상시적인 커뮤니케이션, 내부감사 서비스의 결과를 통해 조직의 리스크와 리스크 허용범위를 이해한다. (표준 8.1 이사회와의 상호작용, 표준 9.1 거버넌스, 리스크 관리 및 통제 프로세스의 이해, 표준 11.1 이해관계자와의 관계 설정 및 커뮤니케이션 참조). 이러한 이해는 최고감사책임자에게 조직이 수용가능 하다고 간주하는 리스크 수준에 대한 관점을 제공한다. 조직에 공식적인 리스크 관리 프로세스가 존재하는 경우 리스크 수용 규정이 포함될 수 있으며, 최고감사책임자는 이를 이해해야 한다.

최고감사책임자는 조직에서 명시하고 있는 리스크 허용범위를 초과하는 리스크의 수용을 기록하고 전달하는 방법론에 대해 논의하고, 이사회에 동의를 구할 수 있다. 방법론은 이 표준의 요건과 조직의 리스크 관리 프로세스, 규정 및 절차를 고려해야 한다. 리스크 관리 프로세스에는 중대한 리스크 이슈를 전달하기 위해 선호하는 접근방식이 포함될 수 있다. 명세서에는 커뮤니케이션의 적시성, 보고 체계 및 조직의 법률 고문이나 준법감시인과의 협의 요건이 포함될 수 있다. 내부감사 방법론에는 리스크에 대한 설명, 우려되는 사유, 내부감사 권고사항 또는 기타 조치를 실행하지 않은 경영진의 이유, 리스크를 수용한 책임자의 이름 및 논의 날짜를 포함하여 논의와 취한 조치를 기록하는 절차가 포함되어야 한다.

최고감사책임자는 감사지적사항에 대한 경영진의 대응 내용을 검토하고, 합의된 조치 계획에 대한 경영진의 이행현황을 모니터링하는 과정에서 경영진이 리스크를 수용한 사실을 인지할 수 있다. 이해관계자와의 관계 설정 및 커뮤니케이션 유지는 경영진의 리스크 수용을 포함하여 리스크 관리 활동에 대한 정보를 유지하는 추가적인 수단이다.

다음은 조직의 리스크 허용범위를 초과하는 리스크를 수용함으로써 발생할 수 있는 리스크 사례이다:

- 조직의 평판을 실추시킴
- 조직의 구성원이나 기타 이해관계자에게 피해를 줌
- 규제당국의 중대한 벌금 부과, 영업제한 또는 기타 재정상 또는 계약상의 불이익
- 중대한 허위진술
- 이해충돌, 부정행위 또는 기타 불법 행위
- 전략적 목표 달성에 심각한 장애가 됨

최고감사책임자의 전문가적 판단은 경영진이 조직의 리스크 허용범위를 초과하는 수준의 리스크를 수용했는지 결정하는 데 기여한다. 예를 들어, 최고감사책임자는 이전에 합의한 조치 계획에 대한 경영진의 이행상태가 불충분한 경우, 경영진이 조직의 리스크 허용범위를 초과하는 수준의 리스크를 수용했다고 결론을 내릴 수 있다. 최고감사책임자는 최고경영진 및/또는 이사회에 우려를 제기하기 전에 해당 리스크 영역을 담당하는 경영진과 직접 만나 우려사항을 공유하고, 경영진의 관점을 이해하고, 조치 계획을 포함한 해결책에 대한 합의를 통하여 문제를 해결해야 한다.

이 표준의 요건은 최고감사책임자가 해당 리스크의 관리를 담당하는 경영진과 합의에 도달할 수 없는 경우에만 시행된다. 최고감사책임자는 허용할 수 없는 것으로 식별된 리스크가 최고경영진과 논의한 후에도 해결되지 않은 경우, 이사회에 이에 대한 문제를 보고한다. 이사회는 경영진과 함께 문제 해결 방법을 결정할 책임이 있다.

공공 부문

내부감사부서가 조직 외부의 기관이나 감독 기구로부터 자금을 지원받는 경우, 최고감사책임자는 규정에 따라 이사회 이외에도 자금 지원 기관이나 기구에 이를 통보해야 할 수 있다.

적합성 증거

리스크 우려를 전달하는 방법론에 대한 이사회와의 논의 및 합의 기록

- 회의록을 포함하여, 리스크 및 현업 경영진과 최고경영진에게 권고한 조치에 대한 논의 기록
- 현업부서 경영진에서 최고경영진으로 단계별로 논의하도록 정하고 있는 프로세스를 포함하여, 우려되는 리스크와 이에 대응하기 위해 내부감사부서가 취한 조치를 설명하고 있는 기록
- 개인적 또는 비공개 회의를 포함한 이사회에서 보고된 우려사항에 대해 회의한 기록

원칙 12 감사 품질의 향상

최고감사책임자는 국제내부감사표준과의 적합성을 보장하며, 내부감사부서의 성과를 지속적으로 개선한다.

감사품질은 국제내부감사표준과의 적합성과 내부감사부서의 수행 목표 달성을 종합적으로 측정하는 것이다. 감사품질 평가 및 개선 프로그램(QAIP)은 내부감사부서가 표준을 준수하고, 수행 목표를 달성하며, 지속적인 개선을 추구함을 보장하고 평가하도록 설계되었다. 이 프로그램에는 내부 및 외부 평가가 포함된다. (표준 8.3 품질 및 표준 8.4 감사품질에 대한 외부평가 참조)

최고감사책임자는 내부감사부서의 지속적인 개선을 보장할 책임을 가지고 있다. 이를 위해서는 내부감사업무, 내부감사인 및 내부감사부서의 수행내용을 평가하기 위한 기준 및 측정방법을 수립해야 한다. 이러한 측정방법은 수행목표 대비 진척도를 평가하는 기반을 구성한다.

국제내부감사표준 12.1 감사품질에 대한 내부평가

요건

최고감사책임자는 내부감사부서의 국제내부감사표준 적합성과 수행목표 대비 진척도에 대한 내부 평가 방법론을 반드시 마련하고 실시해야 한다.

최고감사책임자는 다음을 포함하는 내부 평가 방법론을 반드시 수립해야 한다:

- 내부감사부서의 수행목표 대비 진도율과 표준 적합성을 상시 모니터링
- 이 표준의 모든 요소에 대한 적합성을 평가하기 위해, 내부감사 실무에 대한 충분한 지식을 갖춘 조직 내 다른 자의 평가나 주기적인 자체 평가
- 내부 평가 결과에 대해 최소 연 1 회 이사회와 커뮤니케이션

최고감사책임자는 주기적인 자체 평가 결과에 따라 표준과의 부적합 사례 및 개선 기회를 다루기 위한 조치 계획을 반드시 수립해야 하며, 조치 일정도 제안해야 한다. 최고감사책임자는 주기적인 자체 평가 결과와 조치 계획을 반드시 이사회에 전달해야 한다. (표준 8.1 이사회와의 상호작용 및 표준 9.4 방법론 참조)

내부평가는 반드시 기록으로 남겨야 하고 조직의 감사품질에 대한 외부평가의 일부로 독립적인 제 3자가 수행하는 평가에 포함되어야 한다. (표준 8.4 감사품질에 대한 외부평가 참조).

최고감사책임자는 표준 부적합 수준이 내부감사부서의 전반적인 업무범위 또는 운영에 충격/영향을 주는 경우, 부적합한 내용과 받게 될 충격/영향을 최고경영진 및 이사회에 반드시 공개해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

상시 모니터링

상시 모니터링은 내부감사부서의 일상적인 감독, 검토 및 성과측정을 위해 반드시 필요한 활동이다. 상시 모니터링은 내부감사부서 관리에 사용되는 일상적인 규정 및 실무에 포함되어 있으며, 표준 적합성을 평가하는 데 필요한 프로세스, 툴(tool) 및 정보를 포함한다.

내부감사부서의 표준 적합성과 수행 목표 대비 진척도는 주로 감사업무의 계획과 감독, 확립된 내부감사 방법론, 감사조서 절차 및 승인, 감사조서와 최종 커뮤니케이션에 대한 감독 검토와 같은 지속적인 활동을 통해 모니터링된다. 이러한 활동에는 개선이 필요한 취약점이나 영역의 식별 및 이를 해결하기 위한 조치 계획이 포함된다. 최고감사책임자는 내부감사인인 감사 기간 중 사용할 템플릿(template) 또는 자동화된 감사조서를 마련하여 감사업무 수행의 표준성 및 일관성을 보장할 수 있다.

적절한 감독은 모든 감사품질 평가 및 개선 프로그램(QAIP)의 기본요소이다. 감독은 계획수립에서 시작하여 감사가 종료될 때까지 계속된다. 감독에는 기대치 설정, 감사 기간 중 팀원 간의 커뮤니케이션 장려, 감사조서의 적시 검토와 승인이 포함될 수 있다. (표준 12.3 감사업무 성과의 보장 및 개선 참조)

상시 모니터링에 일반적으로 사용되는 추가적인 방법은 다음과 같다:

- 내부감사인이 확립된 관행 및 절차를 준수하는지 확인하고, 수행 표준의 적용에서 일관성을 보장하기 위한 체크리스트 또는 자동화 툴(tool)
- 내부감사 팀의 효율성 및 효과성에 대한 내부감사 이해관계자의 피드백(feedback). 피드백은 감사업무 직후 또는 주기적으로(예: 반년 또는 매년) 설문조사 툴(tool)이나 최고감사책임자와 경영진 간의 논의를 통해 얻을 수 있다.
- 내부감사부서의 효율성과 효과성 결정에 유용할 수 있는 기타 측정방법에는 자원 할당의 적정성을 표시하는 지표(예: 예산 대비 실적 차이), 감사업무 종료의 적시성, 내부감사계획의 달성, 이해관계자 만족도 설문조사가 있다.

상시모니터링은 표준 적합성을 검증하는 것 외에도 내부감사부서를 개선할 수 있는 기회를 식별하게 할 수 있다. 이 경우 최고감사책임자는 이러한 기회를 다루고, 핵심성과지표를 포함한 조치 계획을 마련할 수 있다. 변경사항이 실행되면 지표를 사용하여 성공 여부를 모니터링할 수 있다.

주기적인 자체 평가

주기적인 자체 평가는 표준 및 내부감사부서에 대한 보다 총체적이고 포괄적인 검토를 제공한다. 주기적인 자체 평가는 모든 표준과의 적합성을 다루는 반면, 상시 모니터링은 감사업무 수행과 관련된 표준에 중점을 둔다. 주기적인 자체 평가는 내부감사부서의 선임 직원, 품질평가 전담 팀, 표준에 관한 풍부한 경험이 있는 내부감사부서 내의 개별 감사인, 국제공인내부감사사(CIA) 또는 조직의 다른 부서의 유능한 내부감사 전문가가 수행할 수 있다. 최고감사책임자는 표준에 관한 내부감사인의 이해를 향상시킬 수 있도록, 자체 평가 프로세스에 내부감사인을 포함하는 것을 고려해야 한다.

주기적인 자체 평가를 통해 내부감사부서의 표준 적합성을 검증할 수 있다. 외부평가자의 평가 직전에 자체 평가를 수행하면, 일반적으로 외부 평가를 완료하는 데 필요한 시간과 노력이 감소된다.

주기적인 자체 평가 시에는 다음을 평가한다:

- 내부감사부서 방법론의 적정성 및 적절성
- 내부감사부서의 조직 성공 증진 기여도
- 수행된 내부감사 서비스와 및 제공된 감독의 품질
- 이해관계자의 기대 충족도와 수행 목표의 달성도

자체 평가를 수행하는 개인 또는 팀은 일반적으로 각 표준에 대한 내부감사부서의 적합성을 평가하고, 내부감사부서의 이해관계자를 인터뷰하고 설문조사 할 수 있다. 최고감사책임자는 이 프로세스를 통해 일반적으로 내부감사부서의 방법론의 품질과 감사업무 수행을 위한 규정 및 절차의 준수 정도를 평가할 수 있다.

주기적인 자체 평가의 일부로 내부감사부서는 다음을 수행할 수 있다:

- 사후 검토 - 내부감사부서는 특정 기간 중 수행된 감사업무 샘플(sample)을 선택하고 검토하여 내부감사부서의 방법론 및 표준 적합성을 평가할 수 있다. 이러한 검토는 일반적으로 해당 감사업무에 관여하지 않은 내부감사 직원이 수행한다. 규모가 크거나 성숙한 조직에서는 품질 검증 전문가 또는 팀이 이 프로세스를 수행할 수 있다.
- 성과 측정 분석 - 내부감사부서는 내부감사 실무의 효율성과 관련된 성과 측정을 모니터링하고 분석할 수 있다. 성과 측정의 예는 다음과 같다:
 - 계획 대비 실제 감사 시간
 - 내부감사계획 완료 비율
 - 현장감사 종료 후 감사보고서 등 최종 감사업무 커뮤니케이션이 실시되기까지의 기간
 - 감사 후 완료된 경영진의 조치 계획 비율
- 직원 중 전문가격을 보유한 내부감사인 수, 이들의 내부감사활동 경력년수, 이들이 해당 연도에 이수한 보수교육 시간

공공 부문

내부 평가 시스템에는 준거 규정 준수에 대한 상시 모니터링도 반드시 포함되어야 한다.

소규모 내부감사부서

소규모 내부감사부서는 재정 및 인원의 제약으로 인해 감사품질에 대한 내부평가를 수행하는 데 어려움을 겪을 수 있다. 따라서, 소규모 내부감사부서의 최고감사책임자는 주기적인 평가를 수행하기 위해 조직 내 타인(예를 들면, 전직 내부감사인이나 내부감사활동에 관한 적절한 지식이 있는 자)에게 협조를 요청할 것을 고려할 수 있다. 최고감사책임자는 그러한 평가를 감독해야 한다.

최고감사책임자는 상시 모니터링을 수행하기 위해 각 감사기간 중 표준 적합성 여부를 모니터링하기 위한 체크리스트 또는 기타 자동화된 툴(tool)의 사용을 늘릴 필요가 있을 수 있다.

적합성 증거

- 내부감사부서의 효율성 및 효과성과 관련하여 감사조서 검토, 설문조사 결과, 수행 측정을 뒷받침하는 완전한 체크리스트
- 검토 계획과 범위, 감사조서, 커뮤니케이션을 포함하는 주기적인 평가 결과 문서
- 내부 평가 결과를 포함하고 있는 이사회 및 경영진 대상 프레젠테이션 자료와 회의록
- 시정 조치 계획을 포함하여 상시 모니터링 및 주기적인 자체 평가 결과 기록
- 내부감사부서의 적합성, 효율성 및 효과성을 개선하기 위해 취한 조치

국제내부감사표준 12.2 수행성과 측정

요건

최고감사책임자는 내부감사부서의 수행성과를 평가하기 위한 목표를 반드시 마련해야 한다. 최고감사책임자는 수행 목표를 마련할 때 반드시 최고경영진 및 이사회의 의견과 기대치를 반드시 고려해야 한다. 최고감사책임자에게는 내부감사부서가 수행 목표를 달성하도록 보장할 책임이 있다.

최고감사책임자는 내부감사부서의 수행 목표 달성 진척도를 평가하기 위한 수행 기준 및 측정방법을 포함하는 수행성과 측정 방법론을 반드시 수립해야 한다. 최고감사책임자는 내부감사부서의 수행성과를 평가할 때, 최고경영진 및 이사회로부터 피드백(feedback)을 받아야 한다.

최고감사책임자는 모든 문제와 개선 기회를 다루는 조치 계획을 반드시 수립해야 한다.

실행 및 적합성 증거를 위한 고려사항

구현

수행성과 측정방법의 설정은 내부감사부서가 표준 및 현장에 부합하게 수행 목표를 달성했는지 결정하는데 중요하다. 첫 번째 단계 내부감사 서비스가 조직의 가치를 부가하고, 리스크 대응을 지원하고, 운영을 개선하고, 통제 강화에 기여한다고 이해관계자가 믿는 내부감사 서비스에 대한 핵심 수행성과 측정방법을 최고감사책임자가 식별하는 것이다.

내부감사부서의 효과성 및 효율성에 대한 핵심 수행성과 측정방법을 식별할 때 고려해야 할 대상에는 국제내부감사표준, 내부감사부서의 임무 및 현장, 준거 법규, 내부감사부서의 전략과 수행 목표가 포함된다. 효과성 및 효율성 측정은 정량적 또는 정성적일 수 있다.

내부감사부서의 수행성과 측정에는 운영 및 전략적 결과가 포함되어야 한다. 내부감사계획의 달성이 성과의 유일한 척도가 되어서는 안 된다. 수행성과 측정에는 다음이 포함될 수 있다:

- 리스크 관리, 통제 및 거버넌스 프로세스 개선에 대한 기여도
- 주요 목적 및 목표의 달성
- 내부감사계획 대비 진척도 평가
- 중대한 것으로 식별된 리스크의 범위
- 직원의 생산성 향상
- 감사 프로세스의 효율성 제고
- 프로세스 개선을 위한 조치 계획 증가
- 감사업무 계획수립 및 감독의 적정성
- 이해관계자의 니즈(needs) 충족 여부 평가
- 내부감사부서의 감사품질 개선 프로그램 및 감사품질 평가 결과
- 이해관계자와의 명확한 커뮤니케이션
- 감사 테스트 종료 후 최종 감사업무 커뮤니케이션이 발행되기까지 평균 경과 시간
- 경영진이 수락한 권고사항의 비율
- 투자수익률(ROI)
- 감사업무를 수행할 때 형평성 고려 수준

최고감사책임자는 효과성 및 효율성을 측정하는 핵심지표와 목표가 확인되면, 모니터링 프로세스와 이해관계자와의 커뮤니케이션 방법(예: 형식, 시기 및 측정지표)을 수립해야 한다. 내부감사부서는 핵심 이해관계자로부터 감사의 효과성에 대한 피드백(feedback)을 받고 필요 시 조정해야 한다.

적합성 증거

- 진행상황을 모니터링하는 데 사용되는 수행측정방법에 대한 내부 커뮤니케이션
- 최고경영진 및 이사회에 제출한 요약 감사보고서 등 커뮤니케이션 요약본

국제내부감사표준 12.3 감사업무 수행 성과의 보장 및 개선

요건

최고감사책임자는 반드시 적절한 감사업무 감독과 감사품질 평가, 감사역량 개발이 이루어지도록 보장해야 한다.

- 최고감사책임자는 적절한 감독을 보장하기 위해 반드시 감사기간 중 내부감사인에게 지침을 제공하고, 수행 프로그램의 완전함을 확인하고, 감사조서가 지적사항, 결론 및 권고사항을 적절하게 뒷받침하는지 확인해야 한다.
- 최고감사책임자는 감사품질 보증을 위해 감사업무가 표준 및 내부감사부서의 방법론에 따라 수행됨을 반드시 보장해야 한다.
- 최고감사책임자는 감사역량 개발을 위해 반드시 내부감사인에게 수행성과 및 개선 기회에 대한 피드백(feedback)을 제공해야 한다.

필요한 감독의 범위는 내부감사부서의 성숙도, 내부감사인의 숙련도와 경험, 감사업무의 복잡성에 따라 다르다.

최고감사책임자는 감사업무 수행의 주체가 내부감사 직원이든 다른 서비스 제공자이든 관계없이 감사업무를 감독할 책임이 있다. 적절하고 자격을 갖춘 개별 감사인에게 감독 책임을 위임할 수 있지만, 궁극적인 책임은 최고감사책임자에게 있다.

최고감사책임자는 반드시 내부감사부서의 확립된 방법론에 따라 적절한 감독이 수행되었다는 증거가 기록되고 유지되도록 해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

최고감사책임자 또는 지정된 감사업무 감독자는 감사업무 감독을 계획할 때, 감사 목표를 검토해야 한다. 감사를 수행한 내부감사인과 최고감사책임자 또는 지정 감독자 간의 사후 회의와 같은 직원 역량 개발 기회가 감독에 포함될 수 있다.

내부감사인의 기술을 평가하는 것은 감사조서 검토 수준 이상의 상시적인 감독 프로세스이다. 최고감사책임자는 기술 평가 결과에 따라, 감사업무를 감독하고 이에 기반하여 감사업무를 할당 받을 자격이 있는 내부감사인을 식별할 수 있다.

감사업무의 감독은 감사의 계획에서 시작하여 감사가 종료될 때까지 계속된다. 감독자는 감사계획 단계에서 감사업무 수행 프로그램을 승인하고, 감사의 다른 측면에 대한 책임을 맡을 수 있다(원칙 13 효과적인 감사계획 수립 및 관련 표준 참조).

감사업무 수행 프로그램 승인의 주요 기준은 감사업무 목표의 효율적 달성 여부이다. 수행 프로그램에는 감사업무 정보를 식별, 분석, 평가 및 기록하는 절차가 포함된다. 감사업무 감독에는 수행 프로그램의 완료 여부 확인과 수행 프로그램 변경 승인도 포함된다.

감사업무 감독자는 감사를 수행하도록 배정된 내부감사인 및 검토대상 영역 또는 프로세스의 경영진과 상시적인 커뮤니케이션을 유지해야 한다. 감사업무 감독자는 수행된 감사 절차, 식별된 정보, 감사 중 발견된 지적사항 및 잠정적 결론을 설명하는 감사조서를 검토한다. 감독자는 정보, 테스트 및 결과 증거가 감사업무 목표를 달성하고, 감사 결론을 뒷받침하기에 충분하며 관련성 있고 신뢰할 수 있는지 평가한다.

표준 11.2 효과적인 커뮤니케이션은 감사업무 커뮤니케이션이 정확하고 객관적이며 명확하고 간결하고 건설적이며, 완전하고 시기 적절할 것을 요구한다. 감사조서는 감사업무 커뮤니케이션을 일차적으로 뒷받침하므로, 감독자는 이러한 요소에 대해 감사업무 커뮤니케이션 및 감사조서를 검토한다.

감사업무 감독자 및/또는 최고감사책임자는 감사기간 중 해당 감사업무를 수행하도록 배정된 내부감사와 만나 감사 프로세스를 논의하여, 해당 감사인을 교육, 역량 개발 및 평가할 수 있는 기회를 제공한다. 감독자는 감사 프로세스의 모든 측면을 기록한 감사업무 커뮤니케이션 및 감사조서를 검토할 때 추가적인 증빙이나 설명을 요청할 수 있다. 내부감사인은 감사업무 감독자가 제기한 의문에 답함으로써 업무를 개선할 수 있다.

일반적으로 감독자의 검토 의견은 적절한 증거가 제공되거나, 감독자의 우려사항 및/또는 의문을 해결하는 추가 정보와 함께 감사조서가 수정되면 최종 기록에서 지워진다. 또는, 내부감사부서는 감사업무 감독자의 우려사항 및 의문, 이를 해결하기 위해 조치한 단계 및 이러한 단계의 결과에 대한 별도의 기록을 유지할 수 있다.

최고감사책임자는 감사업무 수행 주체가 내부감사부서인지 다른 검증 제공자인지 관계없이, 모든 내부감사 업무 및 감사기간 중 내려진 중대한 전문가적 판단에 대해 책임을 진다.

최고감사책임자는 내부감사인이 최고감사책임자의 전문가적 판단과 일치하지 않는 판단을 내리거나 감사업무에 부정적인 영향을 미칠 수 있는 조치를 취할 리스크를 최소화하기 위한 정책 및 절차를 수립한다. 최고감사책임자는 전문가적 판단의 차이를 해결할 수 있는 수단을 마련한다. 여기에는 관련 사실에 대한 논의, 추가적인 조사나 연구 수행, 감사조서 및 결론에 대한 다양한 관점의 문서화 등이 포함될 수 있다. 윤리적 문제에 대해 전문가적 판단에 차이가 있는 경우, 조직에서 윤리 문제를 담당하는 자에게 해당 문제를 회부하여 판단을 구할 수 있다.

소규모 내부감사부서

감독 및 지속적인 내부 평가를 담당할 감사인이 없을 수 있는 소규모 감사부서에게는 감사업무 수행 보장이 어려운 일이다. 최고감사책임자는 체크리스트나 기타 자동화 툴(tool)과 같은 도구를 사용하여, 각 감사업무 수행 시 표준과의 기본적인 적합성을 보장하는 것을 고려할 수 있다.

적합성 증거

- 서명이나 이니셜(initial)이 있고, 감사업무 감독자가 날짜를 기입한 감사조서(수기 문서일 경우). 또는 전자 승인된 감사조서(감사조서 프로그램으로 문서화한 경우)
- 감사조서 검토사항을 뒷받침하는 완전한 체크리스트
- 내부감사인 및 감사업무에 직접 관여한 다른 자의 감사 경험에 대한 피드백(feedback)을 포함하는 인터뷰와 설문조사 결과

- 감독자와 내부감사인 직원 간의 감사업무에 관한 커뮤니케이션 기록



영역 v 내부감사 서비스 수행

내부감사 서비스 수행 시 내부감사인들은 효과적으로 감사업무(지적사항, 권고사항 및 결론을 개선하기 위해 수행하는) 계획을 수립해야 하며, 검토대상활동에 책임이 있는 경영진과 직원들은 감사업무 전체기간과 종료 후에도 공동으로 커뮤니케이션해야 한다.

표준은 감사업무 수행에 관하여 순차적으로 제시하고 있으나, 감사업무 수행 단계가 항상 명확하게 구분되고 순차적이며 연속적인 것은 아니다. 실제 단계별 수행 순서는 업무별로 중복 및 반복되는 경우 다를 수 있다. 예를 들어, 계획수립 단계에 포함된 정보수집 및 위험평가 업무는 감사업무 내내 계속될 수도 있다. 각각의 수행 단계는 다른 단계 또는 감사업무 전체에 영향을 미칠 수도 있다. 따라서 내부감사인은 업무 프로세스 시작 전에 이 영역의 모든 표준을 검토하고 이해해야 한다.

내부감사 서비스는 검증 또는 자문, 아니면 둘 모두를 제공하는 것으로 간주된다. 개별 표준에 별도로 명시된 경우를 제외하고, 내부감사인은 검증 또는 자문업무 수행 시 이 표준을 적용하고 준수해야 한다.

내부감사인은 검증 서비스를 통해 검토대상활동의 현상태와 평가기준 간의 차이에 관한 객관적인 평가를 제공한다. 내부감사인은 이 차이점에 유의미한 지적사항이 있는지 여부를 결정하고 지적사항에 대한 업무 결론을 종합적으로 제공한다. 보증 서비스는 조직의 이해관계자, 특히 이사회, 고위 경영진 및 검토 중인 활동의 관리에게 거버넌스, 위험 관리 및 제어 프로세스에 대한 확신을 제공하기 위한 것입니다.

내부감사인은 이사회, 고위경영진 또는 검토대상활동 경영진의 요청에 따라 자문업무 및 기타 자문활동을 수행한다. 자문 서비스의 성격과 범위는 서비스를 요청하는 당사자와의 합의를 따른다. 자문업무의 예로는 내부감사인이 프로세스나 시스템의 설계, 또는 신규 정책의 개발 및 수행에 대해 자문을 제공하는 것이 있다. 기타 자문 활동으로는 내부감사인이 촉진 및 교육을 제공하는 것이 포함된다. 내부감사인은 자문업무 수행 시 경영상의 책임을 떠맡지 않음으로써 객관성을 유지한다.

원칙 13 효과적인 감사계획 수립

내부감사인은 체계적이고 규율화된 접근방식을 적용하여 개별 감사업무 계획을 수립한다.

국제내부감사표준은 최고감사책임자가 수립한 감사방법론과 함께, 감사업무 계획 수립 시 내부감사인이 채택하는 체계적이고 규율화된 접근방식의 근간이다. 내부감사인은 감사업무의 모든 단계에서 효과적으로 커뮤니케이션할 책임이 있다.

감사업무 계획수립은 해당 감사에 대한 최초의 기대치와 해당 감사가 내부감사계획에 포함된 이유를 이해하는 것으로 시작된다. 내부감사인은 감사업무를 계획할 때 검토대상 조직과 활동을 이해하고, 해당 활동과 관련된 리스크를 평가하기 위해 정보를 수집한다. 내부감사인은 이러한 리스크 평가를 통해 리스크를 식별하고 우선순위를 정하여 감사업무의 목표 및 범위를 정할 수

있다. 또한, 내부감사인인 해당 감사를 수행하는 데 필요한 기준과 자원을 식별하고, 수행되어야 할 특정 감사 단계를 설명하는 감사업무 수행 프로그램을 만든다.

국제내부감사표준 13.1 감사업무 커뮤니케이션

요건

내부감사인인인 감사기간 중 반드시 효과적으로 커뮤니케이션해야 한다.

효과적인 감사업무 커뮤니케이션이란 표준 11.2 효과적인 커뮤니케이션에서 정의한 바와 같이 반드시 정확하고 객관적이며 명확하고 간결하고 건설적이며 완전하고 시기적절해야 한다.

감사업무 커뮤니케이션에는 반드시 검토대상활동 경영진과의 초기, 상시, 종료 및 최종 커뮤니케이션이 포함되어야 한다.

초기 감사업무 커뮤니케이션은 다음 사항과 같이 구성된다:

- 감사 실시 통보
- 감사업무 리스크 평가, 목표, 범위 및 시기에 대한 논의
- 감사업무를 수행하는 데 필요한 정보와 자원 요청
- 추가적인 커뮤니케이션에 대한 기대치 설정

상시 커뮤니케이션을 위해서는 감사업무 진척상황에 대한 업데이트(update)를 제공해야 한다. 상시 커뮤니케이션의 범위는 감사업무의 성격과 기간에 따라 다르다. 내부감사인인인 다음 사항에 대해서는 반드시 커뮤니케이션을 실시해야 한다:

- 즉각적인 주의가 필요한 거버넌스, 리스크 관리 또는 통제 이슈
- 감사업무 범위, 목표, 시기 또는 기간의 변경

내부감사인인인 감사가 종료되고 최종 커뮤니케이션을 실시하기 전에 반드시 검토대상활동의 경영진과 종료단계 커뮤니케이션(일반적으로 회의)을 실시해야 한다. 종료단계 커뮤니케이션은 내부감사인인과 경영진에게 최종 감사보고서 등 최종 커뮤니케이션이 실시되기 전에 감사 지적사항, 권고사항 및 결론과 관련된 의견의 차이를 해결할 수 있는 기회를 제공한다.

종료단계 커뮤니케이션에는 반드시 다음 사항에 대한 논의가 포함되어야 한다:

- 감사 지적사항, 권고사항 및 결론
- 지적사항을 처리하기 위한 경영진의 조치 계획
- 권고사항 및/또는 조치 계획의 타당성
- 각 감사지적사항 조치 완료 기한
- 감사지적사항 조치 이행책임자

내부감사인과 경영진이 지적사항, 권고사항 또는 결론에 합의하지 못하는 경우, 내부감사인은 반드시 종료단계 커뮤니케이션 시 검토대상활동의 경영진과 해당 문제에 대해 논의하고 상호 이해가 일치되도록 노력해야 한다. 여전히 이견이 존재하는 경우, 내부감사인은 타당한 이유가 없는 한 절대로 감사 결과의 일부를 수정해야 할 압박감을 가져서는 안 된다. 내부감사인은 감사보고서 등 최종 감사업무 커뮤니케이션 내용에 있는 차이점에 대해 양측의 입장이 다를 경우 그 이유를 반드시 명시해야 한다. (표준 15.1 최종 감사업무 커뮤니케이션 참조)

실행 및 적합성 증거를 위한 고려사항

실행

효과적인 커뮤니케이션을 위해서는 공식 및 비공식, 서면 및 구두 등 다양한 방법을 이용해야 한다. 감사업무 커뮤니케이션은 예정된 회의, 프레젠테이션, 이메일 및 기타 문서, 비공식 토론을 통해 이루어질 수 있다. 감사업무 커뮤니케이션의 품질과 내용에 대한 요건은 일반적으로 최고경영진 및 이사회의 기대치에 따라 최고감사책임자가 정하고 내부감사 방법론에 문서화된다. (표준 11.2 효과적인 커뮤니케이션 참조)

내부감사인은 감사 실시 통보를 통해 적절한 이해관계자, 일반적으로 검토대상활동의 경영진 및/또는 담당 직원에게 감사업무에 대해 사전 통보하여 협조와 열린 대화의 기반을 다진다. 내부감사인은 최고감사책임자가 수립한 규정에 따라 통보 대상을 결정해야 한다. 감사 실시 통보 시, 감사 이유, 예정된 감사착수 시기 및 대략적인 감사 기간에 대해 경영진에 알려야 한다.

감사실시 통보형식은 다양하지만 메시지, 알림, 메모 또는 서신과 같은 서면 통보형식이 일반적이다. 감사 실시 통보에는 계획된 감사가 검토대상활동에서 발생하는 다른 중대한 일정과 충돌하지 않도록 보장하기 위해, 감사 시기가 포함된다. 또한, 내부 감사인은 리스크를 평가하고, 감사업무 수행 프로그램을 준비하기 위해 필요한 정보와 문서를 요청한다.

또 다른 일반적인 초기 커뮤니케이션은 일반적으로 리스크 평가가 완료되고 내부감사인이 초기 감사업무 목표 및 범위를 정한 후에 발생하는 감사착수 회의이다. 내부감사인은 이 회의에서의 논의를 통해 검토대상활동의 경영진이 감사업무의 목표, 범위 및 시기를 이해하고 지원하도록 보장할 수 있는 기회를 가질 수 있다. 또한, 이 회의를 통해 당사자들은 의견을 상호 조정하고, 커뮤니케이션의 빈도 및 최종 커뮤니케이션 대상을 포함하여 추가적인 커뮤니케이션에 대한 기대치를 설정할 수 있다.

내부감사인은 착수 회의 후 회의에서 논의한 내용을 문서화하기 위해 감사 계획 메모를 작성해야 한다. 이러한 문서는 감사조서에 포함되어야 한다.

내부감사인과 검토대상활동 경영진 간의 감사업무 전반에 걸친 상시 커뮤니케이션은 즉각적인 주의가 필요한 정보를 전달하고, 감사업무 진척상황 또는 범위 변경에 대해 관련 당사자에게 알리는 데 있어 필수적이다. 상시 커뮤니케이션은 내부감사인과 검토대상활동 경영진이 명확성을 확보하고, 오해 및 차이점을 피하거나 해결하는 데 도움이 된다.

필수사항인 종료단계 커뮤니케이션("종료 회의"라고도 함)은 내부감사인, 검토대상활동의 경영진 및 기타 관련 직원이 최종 감사보고서 발행 등 최종 커뮤니케이션 실시 전에 감사 지적사항, 권고사항 및 결론을 검증하고 확정하도록 하기 위해 계획된 체계적인 기회이다. 또한 종료단계 커뮤니케이션은 경영진과 내부감사인이 지적사항, 권고사항 및/또는 결론에 대한 차이점이나

불일치를 논의하고 잠재적으로 해결할 수 있는 기회를 제공한다. 그 목적은 합의에 도달하는 것이지만, 그에 실패할 경우 이 표준에서는 감사보고서 등 최종 감사업무 커뮤니케이션 내용에 경영진과 내부감사인 양측의 관점을 포함시키도록 요구한다.

내부감사인의 권고사항에 대한 타당성을 논의할 때 리스크의 심각도 대비 권고사항 이행의 효익과 같이, 비용 분석이 포함될 수 있다. 경영진의 조치 계획은 최종 감사보고서 발행 등 종료 커뮤니케이션 실시 전에 완전히 수립되지 않을 수 있지만, 경영진은 지적사항을 해결하기 위해 취할 조치에 대한 방법을 가질 수 있다. 경영진이 조치 계획을 완전히 수립하지 않았더라도, 방법을 논의하고 평가할 수 있다. 경영진은 논의 후 조치 계획, 예상 이행 시기 및 이행 담당자를 확인할 수 있다.

적합성 증거

초기 커뮤니케이션

- 감사업무가 사전에 실시 통보되었음을 나타내는 이메일, 회의록 또는 사전 계획 문서(예: 메모)
- 리스크 평가, 감사 목표와 범위 및 시기를 논의한 증빙을 포함한 감사 개시 회의 기록
- 착수회의 내용을 기록한 감사계획 메모
- 검토대상활동의 경영진의 피드백 (설문조사 등을 통한)

상시 커뮤니케이션

- 감사 진척상황 업데이트(update), 긴급 이슈 및 변경사항에 대한 필수 통보, 검토대상활동 경영진의 정보를 포함하여 감사업무 전반에 걸친 커뮤니케이션을 보여주는 문서 (이메일, 회의록, 감사조서 또는 메모)

종료 단계 커뮤니케이션

- 내부감사 지적사항, 권고사항 및 결론, 경영 실천계획에 대한 체계적인 양방향 커뮤니케이션을 보여주는 회의록이나 메모
- 내부감사 지적사항, 권고사항, 결론과 경영진의 대응을 포함한 경영 실천 계획의 초안
- 검토대상활동 경영진에게 요청하여 받은 피드백(feedback)의 기록문서(설문조사를 통해서 등)

국제내부감사표준 13.2 감사업무 리스크 평가

요건

내부감사인은 반드시 검토대상활동에 대해 이해하고 관련 리스크를 평가해야 한다.

내부감사인은 반드시 충분한 정보를 식별 및 수집하고, 감사업무 리스크 평가를 실시하여 검토대상활동에 대한 이해를 제고해야 한다.

내부감사인은 다음을 반드시 이해해야 한다.

- 검토대상활동과 관련된 조직의 전략, 목표 및 리스크
- 조직의 리스크 허용범위
- 내부감사계획을 뒷받침하는 리스크 평가
- 검토대상활동의 목표
- 검토대상활동의 거버넌스, 리스크 관리 및 통제 프로세스
- 해당 통제프로세스의 효과성을 평가하는 데 사용할 수 있는 권위 있는 체계(frameworks), 지침 및 기준

내부감사인원은 감사업무 리스크를 평가하기 위해 다음을 반드시 수행해야 한다:

- 검토대상활동의 목표에 대한 중대한 리스크를 식별
- 해당 검토대상활동이 조직의 리스크 허용범위 내에서 리스크를 통제하는 수단을 식별
- 리스크의 중요성(충격/영향 및 발생가능성)을 평가
- 해당 검토대상활동 관련 통제 프로세스의 설계 적정성 평가
- 부정행위, IT 및 시스템과 관련된 리스크를 포함하여 구체적인 리스크를 고려

실행 및 적합성 증거를 위한 고려사항

실행

내부감사인원은 검토대상활동에 대해 이해하고 관련 리스크를 평가하기 위해 내부감사계획, 내부감사계획 수립에 이르기까지의 논의, 해당 감사업무가 계획에 포함된 이유를 이해해야 한다. 내부감사계획에 포함된 감사업무는 내부감사부서의 전사적 리스크 평가로부터 기인한다. 내부감사인원은 감사업무를 시작할 때 해당되는 리스크를 고려하고, 내부감사계획이 수립된 이후 변화가 있었는지 여부를 문의해야 한다. 내부감사인이 전사적 리스크 평가 및 최근에 실시된 기타 리스크 평가(경영진이 작성한 평가 등)를 검토하면, 검토대상활동과 관련된 리스크를 식별하는 데 도움이 될 수 있다.

내부감사인원은 조직과 검토대상활동 간의 일관성 여부를 점검해야 한다. 내부감사인은 조직의 목표, 규정, 절차뿐만 아니라 거버넌스, 리스크 관리 및 통제를 위한 조직의 전략과 프로세스에 대한 정보를 수집하고 고려한다. 다음으로, 내부감사인은 감사업무 리스크 평가를 시작할 때 조직의 이러한 측면이 검토대상활동 및 감사와 어떻게 관련되는지 고려한다.

유용한 정보는 다음 사항에서 발견될 수도 있다:

- 내부감사부서나 경영진이 최근에 실시한 리스크 평가
- 내부감사부서와 기타 검증 및 자문 서비스 제공자가 이전에 수행한 감사업무 결과
- 재무, 환경, 사회적 책임 및 거버넌스와 같은 기타 검증 및 자문 서비스 제공자의 보고서
- 전사적 리스크 평가 및 내부감사계획
- 이전 감사업무의 감사조서

내부감사인은 정보를 수집하기 위해 다음을 수행할 수 있다:

- IIA의 권위 있는 지침과 조직이 속한 부문, 산업 및 사법관할권과 관련된 기타 표준, 지침, 법규를 포함하는 참고 자료를 검토
- 조직도와 직무 기술서를 이용하여 검토대상활동과 관련된 정보, 프로세스 및 기타 측면을 담당하는 자를 파악
- 검토대상활동 조직의 물리적 자산
- 경영진의 규정, 절차, 업무흐름도 및 보고서를 포함하여 정보 담당자나 외부 출처로부터 확보한 문서를 조사
- 웹사이트, 데이터베이스(database) 및 시스템 조사
- 인터뷰, 토론 또는 설문조사를 통한 질의
- 프로세스 진행 관찰
- 다른 검증 및 컨설팅 서비스 제공자와의 회의

내부감사인은 수집된 정보를 검토하여 검토대상 프로세스의 운영 방식을 이해하고, 검토대상활동이 그 목표를 달성하는지 측정하기 위해 경영진이 사용하는 기준을 식별한다. 내부감사인은 설문조사, 인터뷰, 물리적 검사 및 프로세스 추적조사(walk-through)를 통해 검토대상활동의 현재 실태를 관찰할 수 있다. 내부감사인은 감사조서로 보관되는 개별 계획 문서에 관련 정보를 기록하고 요약해야 한다. (표준 14.6 감사업무의 문서화 참조)

내부감사인은 감사업무 리스크 평가를 수행하기 위해 수집된 정보를 사용하여 검토대상활동의 목표, 각 목표의 달성에 영향을 미칠 수 있는 리스크 및 각 리스크를 관리하기 위한 통제를 이해하고 문서화한다.

내부 감사인은 차트, 스프레드시트 또는 유사한 툴(tool)을 만들 리스크와 이러한 리스크를 관리하도록 설계된 통제를 문서화할 수 있다. 내부감사인은 종종 리스크 통제 매트릭스(Risk Control Matrix)라고 하는 문서 작성을 통해 자신의 전문가적 판단, 경험 및 논리를 기반으로 검토대상 활동의 맥락에서 수집된 정보를 고려하고, 리스크의 발생가능성과 충격/영향, 그리고 기타 잠재적 리스크 요인을 조합하여 대략적인 리스크의 중대성을 추정할 수 있다.

내부감사인은 전문가로서의 정당한 주의의 일환으로 검토대상활동의 경영진으로부터 얻은 정보를 고려해야 한다. 검토대상 영역 또는 프로세스의 경영진과의 논의는 종종 비즈니스 목표, 고유 리스크, 통제 및 관련 리스크의 중대성에 대한 추가적인 관점과 통찰력을 제공한다. 검토대상활동의 리스크에 대한 상호 이해를 확립하면, 리스크 평가의 유용성이 제고된다. 또한, 내부감사인은 감사계획 수립 중 감사업무 감독자와 상의해야 한다.

리스크 통제 매트릭스(Risk Control Matrix)는 일반적으로 감사업무 과정 전반에 걸쳐 수립된다. 이 매트릭스(matrix)는 테스트 단계를 통해 감사가 진행됨에 따라 원인, 리스크 사건, 영향(결과), 고유 리스크 평가 및 통제 유형(즉, 예방, 적발 또는 시정)에 대한 설명을 기록하는 데 사용될 수 있다. 감사업무 중에 해결해야 할 리스크는 중대성에 따라 우선순위를 지정할 수 있다. 이는 종종

히트맵(heat map)과 같은 기본적인 그래프에 변수를 위치시켜 설명된다. 이러한 문서는 감사조서의 일부로 보관해야 한다.

가장 중대한 리스크의 경우, 통제 설계의 적정성을 평가하면, 내부감사인이 테스트가 계속 필요한 통제를 결정하는 데 도움이 된다. 가장 높은 우선순위로 평가된 리스크는 표준 13.3 감사업무의 목표 및 범위에 설명된 감사 목표와 범위의 기초가 된다. 내부감사인은 감사 분석 시 잔여 리스크를 결정하고, 검토대상활동의 허용 가능한 범위를 초과하는 모든 리스크를 기록해야 한다. (표준 14.2 분석 및 잠재적 감사 지적사항 참조)

적합성 증거

감사조서의 문서화 대상:

- 관련된 조직의 전략, 목표 및 리스크
- 검토대상활동의 목표
- 검토대상활동의 거버넌스, 리스크 관리 및 통제 프로세스
- 조직도 및 직무 기술서
- 직접 관찰하거나 검사한 메모 및/또는 사진
- 검토대상활동을 위한 규정 및 절차
- 관련 법규 및 컴플라이언스 평가서
- 웹사이트, 데이터베이스(database) 및 시스템에서 수집한 관련 정보
- 인터뷰 메모, 토론 또는 설문조사
- 다른 검증 제공자의 수행업무와 이전에 완료된 리스크 평가 및 감사업무의 관련 정보
- 각 리스크의 중대성과 통제 설계의 적정성을 나타내는 리스크 통제 매트릭스(Risk Control Matrix)나 기타 문서

국제내부감사표준 13.3 감사업무의 목표 및 범위

요건

내부감사인은 반드시 감사업무의 목표와 범위를 정하고 문서화해야 한다.

감사업무의 목표는 반드시 감사의 목적을 명확히 하고, 감사업무 리스크 평가 결과를 고려해야 한다.

감사 범위는 감사 시 검토할 활동, 위치, 프로세스, 시스템, 구성요소 및 기타 요소와 수행 기간을 명시하여 감사업무의 초점과 경계를 정한다. 감사 범위는 반드시 감사 목표를 달성하기에 충분해야 한다. 감사 범위의 제한은 반드시 감사착수 시 및 감사보고서 등 최종 감사업무 커뮤니케이션 내용에 공개되어야 한다.

최고감사책임자 또는 지명된 자는 반드시 감사업무의 목표 및 범위를 승인해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

내부감사인은 감사업무의 목표와 범위를 통해 검토대상활동의 중대한 리스크에 감사노력을 집중하고, 감사업무 수행 프로그램을 개발하며, 경영진 및 이사회와 명확하게 커뮤니케이션할 수 있다. 또한 감사목표와 범위는 내부감사인이 감사업무 일정, 예산 및 자원 요건을 결정하는 데 도움이 되는 기반을 제공한다.

내부감사인은 감사업무의 목표 및 범위를 결정하기 위해 다음에 필요한 정보를 수집해야 한다:

- 감사업무의 목적과 내부감사계획에 포함된 이유를 이해한다.
- 검토대상활동의 전략과 목표를 고려한다.
- 감사업무 리스크 평가를 통해 감사와 관련된 리스크를 우선순위화 한다. (표준 13.2 감사업무 리스크 평가 참조)

내부감사인은 감사업무 유형에 따라 이해관계자의 기대와 이 표준의 요건이 달라지기 때문에 감사업무가 검증 요청인지 자문 서비스인지 고려해야 한다. 검증 감사의 목표 및 범위는 자문 업무의 목표 및 범위와 상당히 다를 수 있다. 검증 감사의 경우 목표와 범위는 주로 내부감사인이 결정하는 반면, 자문 업무의 경우 목표는 일반적으로 자문 업무를 요청한 당사자가 결정한다.

내부감사인은 감사를 시작하기 전에 감사 목표와 범위를 적절하게 정의한 후에, 다음을 수행할 수 있다:

- 검토대상활동의 중대한 리스크에 초점을 맞춤
- 노력의 중복 또는 가치를 부가하지 않는 업무 수행회피
- 감사업무를 완료를 위해 적절하고 충분한 자원을 할당

감사업무의 목표는 내부감사인의 의도된 감사 성과를 광의의 문장으로 정의한 것이다. 감사목표는 감사를 통해 달성하고자 하는 목적을 명시하고, 내부감사인이 수행할 절차를 결정하는데 도움을 준다. 내부감사인은 감사업무의 목표가 조직뿐만 아니라 검토대상 영역이나 프로세스의 비즈니스 목표와 일치하는지 확인해야 한다.

검증 감사는 조직의 영역에 비즈니스 목표를 달성하는 데 방해가 될 수 있는 리스크를 관리하기 위해 통제가 적절하게 설계 및 운영되고 있다는 검증을 제공하는 데 중점을 둔다. 이러한 감사업무의 목표는 감사기간 동안 프로세스 및 시스템 통제를 테스트하는 우선순위를 정하는 것이다. 여기에는 다음과 관련된 리스크를 관리하도록 설계된 통제가 포함된다:

- 권한 및 책임의 분장
- 규정, 계획, 절차 및 법규 준수
- 정확하고 신뢰할 수 있는 정보의 보고
- 자원의 효과적이고 효율적인 사용

- 자산의 보호

내부감사인은 감사목표가 수립되면 전문가적 판단을 행사하고, 필요 시 감사업무 감독자와 협의하여 감사 업무의 범위를 결정해야 한다. 감사범위는 감사 목표를 달성하기에 충분할 만큼 넓어야 한다. 내부감사인은 감사범위 결정 시 해당 범위 내에서 각 감사업무 목표가 달성될 수 있도록 독립적으로 고려해야 한다.

내부감사인은 일반적으로 감사범위에 포함되거나 제외될 항목에 대한 감사업무 이해관계자의 요청 및 모든 범위 제한을 고려하고 문서화한다. 감사범위 제한의 예는 다음과 같다:

- 감사수행 기간
- 자원 제한(재정적, 인적 및 기술적)
- 데이터, 기록, 기타 정보와 인적 및 물리적 자산에 대한 접근

내부감사인은 감사 개시 또는 착수 회의 시에 감사업무의 목표, 범위 및 시기를 전달한다. 이러한 정보는 감사 계획 메모에 기록되고, 감사조서에 통합되어야 한다. (표준 13.1 감사업무 커뮤니케이션 참조)

적합성 증거

- 감사 계획 메모
- 감사보고서 등 최종 감사업무 커뮤니케이션 내용
- 다음을 문서화한 감사조서:
 - 감사 목표와 리스크 평가의 일관성
 - 감사업무 목표를 달성하는 범위
 - 감사 목표 및 범위를 포함하는 감사업무 수행 프로그램 승인
 - 감사 목표 및 범위에 대한 이해관계자와의 회의록
 - 감사업무 이해관계자의 감사범위 포함 또는 제외항목에 대한 요청 및 감사범위 제한

국제내부감사표준 13.4 평가 기준

요건

내부감사인은 감사업무 목표 및 범위에 정의된 검토대상활동의 평가에 사용하는 데 적합한 기준을 반드시 식별해야 한다.

내부감사인은 검토대상활동이 그 목적과 목표를 달성했는지 판단하기 위해 경영진 또는 이사회가 적절한 기준을 수립한 정도를 반드시 확인해야 한다. 해당하는 경우, 내부감사인은 이러한 기준을 반드시 평가에 사용해야 한다.

부적절한 경우, 내부감사인은 경영진 및/또는 이사회와의 논의를 통해 적절한 평가 기준을 식별해야 한다.

다음 사항은 기준의 예이다:

- 내부(규정, 절차, 핵심성과지표 또는 해당 활동의 목표)
- 외부(법규 및 계약상의 의무)
- 권위 있는 관행(산업, 활동 또는 직종의 특수한 체계(frameworks), 표준, 지침 및 벤치마크(benchmarks)).

실행 및 적합성 증거를 위한 고려사항

실행

내부감사인은 정보 수집 및 감사업무 계획 수립의 일환으로 검토대상활동의 거버넌스, 리스크 관리 및 통제 프로세스의 효과성과 효율성을 평가하기 위해 조직에서 사용하는 기준을 식별한다. 다음으로, 감사인은 해당 감사업무와 가장 관련성이 높은 평가 기준에 중점을 둔다. 이러한 기준은 활동의 바람직한 상태를 나타내고, 기존 상태(실태)를 비교할 실용적이고 측정가능한 대상을 제공해야 한다. 예를 들어 감사업무 목표가 검토대상활동에서 통제 프로세스의 효과성을 평가하는 것이라면, 기준 또는 바람직한 상태는 검토대상활동의 통제 프로세스의 예상 결과일 수 있으며, 실태는 실제 결과에 의해 드러난다.

적정한 기준은 잠재적 지적사항이 될 수 있는 바람직한 상태와 실제 상태 간의 차이를 식별하고, 지적사항의 중요성을 판단하고, 의미 있는 결론에 도달하는데 필수적이다. 내부감사인은 조직의 기준이 적정한지 결정하기 위해 전문가적 판단을 행사한다. 적정한 기준은 관련성이 있고, 조직 및 검토대상활동의 목표와 일치하며, 신뢰할 수 있는 비교결과를 생성한다. 이 표준에 열거된 기준의 예 이외에도, 기준에는 확립된 조직의 관행, 통제설계에 기반한 기대 및 공식적으로 문서화되지 않을 수 있는 절차가 포함될 수 있다.

내부감사인은 기준의 적정성을 평가할 때, 조직이 적절한 거버넌스, 리스크 관리 및 통제 관행을 구성하는 기본 원칙을 확립했는지 판단해야 한다. 내부감사인은 경영진이 다양한 사업 단위, 부서 또는 프로세스에 대한 중요성 기준치를 포함하여 리스크 허용범위를 명확하게 표현했는지 고려해야 한다. 또한 내부감사인은 조직이 통제의 정의를 채택했거나 명확하게 표현했는지 확인하고, 충족 수준의 통제가 무엇인지에 대한 경영진의 이해를 식별해야 한다. 예를 들어, 충족은 한 통제목표 내에서 거래 중 특정 비율이 수립된 통제 절차에 따라 수행되었거나, 통제 전반에서 특정 비율이 의도된 대로 작동하고 있다는 의미이다.

또한, 내부감사인은 권고 사례를 조사하고, 경영진의 기준을 다른 조직에서 사용하는 기준과 비교해야 한다. 감사업무 목표를 달성하는 데 최선의 기준을 결정하려면, 내부감사인이 전문가적 판단을 적용해야 한다. 내부감사인은 문서화된 규정, 절차 및/또는 기타 기준에 세부사항이 부족하거나 부적절하다고 판단할 수 있다. 내부감사인은 경영진이 적정한 기준을 결정하는 데 도움을 주거나, 관련 기준을 식별하거나 수립하는 것을 지원하기 위해 전문가의 의견을 구할 수 있다. 내부감사인은 경영진의 기준이 전반적으로 적정해 보일 수 있지만, 감사업무를 위해 더 나은 기준을 제안할 수 있다.

내부감사인은 검토대상활동이 사용하는 기준이 부적절하거나 부재할 경우, 경영진이 내부감사인이 식별한 기준을 실행하도록 권할 수 있다. 적절한 기준의 부재에 대한 논의는 자문 서비스 제공 결정으로 이어질 수 있다.

내부감사인은 검토대상활동의 경영진이 감사업무 중에 사용될 기준을 이해하고 있는지 확인해야 한다. 검토대상활동의 담당자가 오해하거나 이의를 제기하는 것을 방지하기 위해, 합의된 기준은 문서화되어야 한다.

적합성 증거

- 고려한 기준의 출처와 기준의 적합성을 판단하는 데 사용된 프로세스를 문서화한 감사조서
- 기준에 대해 검토대상활동의 경영진 및/또는 이사회와 내부감사인의 논의를 나타내는 회의록, 계획 메모, 이메일과 같은 문서

국제내부감사표준 13.5 감사업무의 자원

요건

내부감사인은 감사업무 계획을 수립할 때 감사 목표를 달성하는 데 필요한 자원을 반드시 식별해야 한다.

내부감사인은 반드시 감사업무를 수행하는 데 필요한 자원의 유형과 양을 결정해야 한다. 결정 시 다음 사항을 고려해야 한다:

- 감사업무의 성격과 복잡성
- 감사업무를 반드시 완료해야 하는 시한
- 이용가능한 재정적, 인적 및 기술적 자원이 감사업무 목표를 달성하기에 적절하고 충분한지 여부

내부감사인은 이용가능한 자원이 부적절하거나 불충분한 경우, 최고감사책임자 또는 자원 확보를 담당하는 지명된 자와 우려사항을 반드시 논의해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

자원의 식별 및 할당은 일반적으로 감사업무를 지휘하고 감독하도록 지정된 내부감사인이 수행하는 감사 계획수립의 한 단계이다. 감사업무 감독자는 감사업무에 필요한 자원의 유형과 양을 결정하기 위해 수행할 업무의 성격과 복잡성에 특별한 주의를 기울이면서 감사업무 계획수립 전반에 걸쳐 수집되고 전개된 정보를 이해해야 한다. 다음으로, 감독자는 감사업무의 목표를 달성하기 위해 취해야 하는 단계와 각 단계에 소요될 것으로 예상되는 시간을 식별하기 위해 전문가적 판단을 적용한다. 또한, 감사업무에 배정된 시간, 시기, 언어 및 이동과 같이 감사의 성과에 영향을 미칠 수 있는 정해진 조건 및 제약을 고려하는 것도 중요하다.

내부감사인은 감사업무를 계획할 때, 이용가능한 재정적, 인적 및 기술적 자원의 가장 효율적이고 효과적인 적용을 고려해야 한다. 감사업무 감독자는 내부감사부서의 구성원이 보유한 전문 역량에 대한 최고감사책임자의 정보에 접근할 수 있다. 감사업무 자원을 계획하려면 이용가능한 자원이 적절하고 충분한지 또는 감사를 완료하기 위해 추가 자원을 확보해야 하는지 여부를 결정해야 한다.

감사업무 감독자는 감사자원 제한이 감사업무 목표를 달성하기 위한 내부감사부서의 능력을 방해하는 경우, 이러한 우려사항을 최고감사책임자에게 보고할 책임이 있다. 최고감사책임자는 최고경영진 및 이사회와 자원 제한의 시사점을 논의하고, 취해야 할 조치를 결정할 책임이 있다. 예를 들어, 최고감사책임자가 필요한 자원을 확보할 수 없는 경우, 감사업무 범위를 줄여야 할 수 있다. (표준 10.1 재원 관리, 표준 10.2 인적 자원 관리 및 표준 10.3 기술 자원 참조)

내부감사인은 감사자원의 효과적인 실행을 개선하기 위해, 계획된 시간 대비 감사업무를 수행하는데 소요된 실제 시간을 문서화할 수 있다. 향후 감사자원 계획수립을 개선하기 위해 이러한 문서를 검토할 수 있다.

적합성 증거

- 최고감사책임자가 작성한 내부감사부서의 역량 목록
- 감사업무 자원조달에 대한 내부감사부서의 규정 및 절차서
- 적절하고 충분한 감사자원의 활용을 보여주는 승인된 감사업무 수행 프로그램
- 감사업무의 자원조달 필요성(needs)을 분석하고 자원 할당을 기록한 계획서(감사조서)
- 검토대상활동의 경영진을 대상으로 적시성 및 감사자원의 적정성에 대해 질문한 사후 설문조사
- 외부 서비스 제공자와의 계약 및/또는 관계

국제내부감사표준 13.6 감사업무 수행 프로그램

요건

내부감사인은 감사업무의 목표를 달성할 감사업무 수행 프로그램을 개발하고 문서화해야 한다.

감사업무 수행 프로그램은 감사업무 리스크 평가 결과를 포함하여, 감사계획 수립 중에 얻은 정보를 기반으로 한다.

감사업무 수행 프로그램은 다음 사항을 반드시 식별해야 한다:

- 감사업무의 목표를 달성하기 위한 과업
- 과업을 수행하기 위한 방법론 및 툴(tool)
- 과업 수행을 위해 배정된 내부감사인

최고감사책임자 또는 지명된 자는 감사업무 수행 프로그램이 실행되기 전에 반드시 해당 프로그램을 검토하고 승인해야 한다. 이후 감사업무 수행 프로그램을 변경해야 할 경우에는 반드시 최고감사책임자 또는 지명된 자와 논의하고 승인을 얻어야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

감사업무 수행 프로그램은 감사업무에서 완료해야 할 과업과 감사팀의 각 구성원에게 할당된 역할 및 책임을 문서화한다. 감사업무 수행 프로그램은 최고감사책임자 또는 지명된 감사업무 감독자가 검토하며, 일반적으로 과업을 완료한 내부감사인인 이름 및 완료일과 함께, 완료된 다양한 과업의 검토와 승인을 표시하는 방법을 포함한다.

감사업무 수행 프로그램은 감사계획 수립 중에 수집하여 개발한 정보를 기반으로 하며, 내부감사인이 감사 지적사항, 권고사항 및 결론을 작성할 때 정보를 분석하고 평가하는 데 사용될 절차를 자세히 설명한다. 계획 수립 단계에서 수행된 업무는 일반적으로 감사조서에 기록되고, 감사업무 수행 프로그램에서 참조된다.

내부감사인은 감사업무 수행 프로그램을 수립하기 위해 사용할 테스트 접근방식과 리스크 및 통제를 연결하여 리스크 통제 매트릭스(Risk Control Matrix)를 확장할 수 있다. 분석과 평가가 수행됨에 따라, 리스크 및 통제를 지적사항, 권고사항 및 결론에 연결하도록 매트릭스(matrix)를 확장할 수 있다. 감사업무 수행 프로그램은 본 표준에 설명된 내용 외에도 핵심 통제의 효과성을 테스트하는 데 사용할 분석 절차와 같은 테스트 목표, 기준 및 방법론을 명시해야 한다. 감사업무 수행 프로그램에는 표본추출 방법론, 모집단 및 크기도 포함되어야 한다.

감사계획 수립단계에서 적용되는 분석 및 세부정보의 수준은 내부감사부와 감사업무에 따라 다르다. 통제 설계의 적정성 평가는 내부감사인이 유효성을 추가로 테스트할 핵심 통제를 명확하게 식별하는 데 도움이 되므로, 감사업무 계획수립의 일부로 완료되는 경우가 많다. 감사업무 수행 프로그램에는 통제 설계의 적정성에 대한 서면 평가가 포함될 수 있다.

그러나, 이러한 평가를 수행하는 가장 적절한 시기는 감사업무의 성격에 따라 다르다. 통제 설계 평가는 감사계획 수립 중에 완료되지 않은 경우, 감사업무 수행의 특정 단계에서 이루어지거나 내부감사인이 통제의 효과성 테스트를 수행하는 과정에서 이루어질 수 있다.

적합성 증거

- 감사업무 수행 프로그램 수립을 지원하는 감사조서
- 테스트 접근방식이 설명된 리스크 통제 매트릭스(Risk Control Matrix)
- 통제 프로세스 지도(map) 또는 설명
- 통제 설계의 적정성 평가에 대한 기록
- 추가 테스트 계획
- 과업 및 절차가 결정된 계획 수립 회의의 회의록, 메모 또는 문서
- 서면 승인을 받은 감사업무 수행 프로그램

- 감사업무 수행 프로그램 변경 승인 문서

원칙 14 감사업무 수행

내부감사인은 감사의 목표를 달성하기 위해 감사업무 수행 프로그램을 사용한다.

내부감사인은 감사업무계획을 수립할 때, 감사업무 수행 프로그램을 만들기 위해 정보를 수집하고 정리한다. 감사업무 수행 프로그램은 감사업무 목표를 달성하는 데 사용될 과업과 방법론을 설명한다.

내부감사인은 감사업무 수행 프로그램을 이행하기 위해 정보를 수집 및 분석하고, 평가를 수행한다. 내부감사인은 이러한 단계를 통해 잠재적 지적사항을 식별하고, 지적사항의 원인, 영향 및 중대성을 판단하고, 권고사항 및 결론을 도출할 수 있다.

국제내부감사표준 14.1 분석 및 평가를 위한 정보 수집

요건

내부감사인은 분석 및 평가를 수행하기 위해 반드시 관련성이 있고 신뢰할 수 있으며 충분한 정보를 수집해야 한다.

내부감사인은 감사 지적사항을 도출하고 이를 뒷받침하기 위해 반드시 감사정보를 수집하고 분석해야 한다.

내부감사인은 정보가 적절하고 신뢰할 수 있는지 여부와 분석 결과가 잠재적인 감사 지적사항을 구성할 수 있는 합리적인 근거를 제공하기에 충분한지 평가해야 한다. 분석 결과 및 보충 정보를 통칭하여 "증거"라고 부른다. (표준 14.2 감사정보 분석 및 잠재적 감사 지적사항 참조)

정보는 감사업무 목표와 일치하고, 감사 범위 내에 있으며, 감사 지적사항, 권고사항 및 결론의 도출에 기여할 때 관련성이 있다.

정보는 사실에 입각한 최신 정보일 때 신뢰할 수 있다. 내부감사인은 전문가적 의구심을 발휘하여 정보의 신뢰성을 평가한다. 다음 사항의 경우에는 정보의 신뢰성이 보장된다:

- 내부감사인이 직접, 또는 독립적인 출처로부터 얻은 정보
- 확증된 정보
- 효과적인 거버넌스, 리스크 관리 및 통제 프로세스를 갖춘 시스템에서 수집한 정보

정보는 내부감사인의 분석 수행과 평가 완료 가능성이 가능할 때 충분한 정보로 인정된다. 신중하고 정보에 입각한 유능한 사람이 감사업무 수행 프로그램을 반복했을 때, 내부감사인과 동일한 결론에 도달할 수 있으면 증거가 충분하다고 여긴다. 내부감사인은 증거가 감사 지적사항을 도출하거나 뒷받침하기에 충분하지 않은 경우, 반드시 분석 및 평가를 위해 추가적인 정보를 수집해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

내부감사인은 감사업무 수행 프로그램의 각 단계를 완료하기 위해 정보를 수집할 때, 감사업무의 목표 및 범위 내에서 관련된 정보에 중점을 둔다. 내부감사인은 전문가적 의구심을 적용할 때, 정보가 사실에 입각한 최신 정보인지, 직접(관찰 등을 통해) 입수했는지 또는 검토대상활동 책임자와 독립적인 관계에 있는 출처에서 입수했는지 비판적으로 평가해야 한다. 정보를 단일 출처 이상과 비교하여 입증하는 것은 신뢰성을 높이는 또 다른 방법이다.

분석을 위한 정보 수집 절차에는 다음 사항이 포함될 수 있다:

- 검토대상활동에 관련된 개인과의 인터뷰 또는 설문조사 수행
- 프로세스를 직접 관찰[추적조사(walkthrough)라고도 함]
- 검토대상활동과 무관한 개인으로부터 정보의 확인 또는 검증을 구함
- 문서, 재고, 장비와 같은 물리적 증거를 검사하거나 조사
- 데이터를 관찰하거나 추출하기 위해 조직의 시스템에 직접 접근
- 시스템의 사용자 및 관리자와 협력하여 데이터 확보

내부감사인은 정보를 수집할 때, 데이터 모집단을 전수 조사할지 또는 표본을 테스트할지 고려한다. 표본을 추출하기로 선택한 경우, 모집단을 가장 잘 대표하는 표본을 추출할 수 있는 방법을 적용해야 한다.

적합성 증거

- 감사업무 목표와 관련된 데이터 수집절차를 포함하는 감사업무 수행 프로그램
- 출처, 수집 날짜 및 관련 기간을 포함한 수집된 정보에 대한 설명
- 수집한 정보가 분석을 수행하기에 충분하다고 내부감사인이 판단한 근거를 기술한 문서

국제내부감사표준 14.2 분석 및 잠재적 감사 지적사항

요건

내부감사인은 반드시 관련성 있고 신뢰할 수 있으며 충분한 정보를 분석하여 잠재적 감사 지적사항을 도출해야 한다.

내부감사인은 평가 기준과 검토대상활동의 현 상태("실제 상태") 사이에 차이가 있는지 판단하기 위해 반드시 정보를 분석해야 한다. (표준 13.4 평가 기준 참조) 내부감사인은 감사업무 수행 중에 수집한 정보와 증거를 사용하여 실제 상태를 판단한다. 기준과 실제 상태 사이의 차이는 반드시 주의를 기울여서 추가로 평가할 필요가 있는 잠재적 감사 지적사항을 의미한다. 잠재적 감사 지적사항의 일반적인 예로는 오류, 비리, 불법 행위 및 효율성 또는 효과성을 개선할 수 있는 기회를 들 수 있다.

내부감사인은 초기 분석 결과가 잠재적 감사 지적사항을 뒷받침할 만한 충분한 증거를 제공하지 못할 경우, 추가적인 분석이 필요한지 여부를 결정할 때 반드시 전문가로서 정당한 주의를 행사해야 한다. 이후 이에 따라 감사업무 수행 프로그램을 조정해야 하며, 반드시 최고감사책임자 또는 지명된 자의 승인을 받아야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

감사업무 수행 프로그램에는 다음과 같이 실시할 필요가 있는 특정 분석의 목록이 포함될 수 있다:

- 프로세스 또는 업무활동의 정확성이나 효과성 테스트
- 합리성 테스트
- 비율, 추세 및 회귀 분석
- 현재 기간의 예산정보와 예상 또는 이전 기간의 유사 정보 간 비교
- 일련의 정보(예: 기록된 급여 비용 등 재무 정보 및 평균 직원 수의 변화 등 비재무 정보) 간의 관계 분석
- 내부 벤치마킹(benchmarking) 또는 조직 내 여러 다른 영역의 정보 비교
- 외부 벤치마킹(benchmarking) 또는 다른 조직의 정보를 이용한 비교

내부감사인은 한 개의 표본이 아닌 모집단을 전수 검사할 수 있는 소프트웨어 애플리케이션(application)과 같이, 분석의 효율성과 효과성을 개선하는 기술을 이해하고 사용해야 한다.

분석은 평가 기준과 실제 상태 사이의 의미 있는 비교로 귀결되어야 한다. 분석 결과 기준과 상태 사이에 차이가 있을 경우, 그 원인과 결과를 파악하고 잠재적 지적사항의 중대성을 결정하기 위해 후속 감사 절차를 사용해야 한다. 특히 자문 업무에서 지적사항은 "의견"이라고도 한다.

내부감사인은 잠재적 지적사항을 평가하고 그 원인, 결과 및 중대성을 결정하는 데 사용해야 하는 추가적인 절차의 범위와 유형을 정하기 위해 전문가로서 정당한 주의를 행사한다. 최고감사책임자 및 내부감사 방법론은 추가 분석 수행 여부를 결정하기 위한 지침을 제공할 수 있다. 고려사항은 다음을 포함한다:

- 통제 프로세스의 적정성을 포함한 감사업무 리스크 평가 결과
- 검토대상활동 및 잠재적 지적사항의 중대성
- 분석 결과가 잠재적 감사 지적사항을 뒷받침하는 정도
- 추가적인 평가를 위한 정보의 이용가능성 및 신뢰성
- 추가 분석 수행의 비용 대비 효익

적합성 증거

- 수행한 분석 결과를 문서화한 감사조서(사용된 데이터 분석 프로그램 또는 소프트웨어, 테스트 모집단, 표본추출 프로세스 및 표본추출 방법 포함)
- 감사업무 수행 프로그램과 상호 참조되는 감사조서 및/또는 감사보고서 등 최종 커뮤니케이션 내용
- 감사보고서 등 최종 커뮤니케이션과 관련된 문서
- 감사업무에 대한 감독자의 검토의견
- 내부자 및 외부자가 수행한 평가 결과 (표준 8.4 감사품질에 대한 외부평가 및 표준 12.1 감사품질에 대한 내부평가 참조)

국제내부감사표준 14.3 지적사항 평가

요건

내부감사인은 반드시 개별적인 잠재적 지적사항을 평가하여 그 중대성을 결정해야 한다.

내부감사인은 잠재적 감사 지적사항을 평가할 때 반드시 근본 원인을 식별하고 잠재적 영향을 판단하며 문제의 중대성 평가해야 한다. 내부감사인은 리스크의 중대성을 판단하기 위해 리스크의 발생가능성과 이러한 리스크가 조직이나 조직의 거버넌스, 리스크 관리 또는 통제 프로세스에 미칠 수 있는 충격/영향을 고려한다.

내부감사인이 조직이 중대한 리스크에 노출되어 있다고 판단한 경우, 반드시 해당 문제를 문서화하여 지적사항으로 알려야 한다.

내부감사인은 최고감사책임자가 수립한 방법론을 이용하여, 각 감사 지적사항의 중대성에 따라 등급, 순위 또는 기타 우선순위를 구분 표시하여 반드시 제공해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

감사 지적사항의 도출을 위해 내부감사인은 확립된 기준을 검토대상활동의 현재 상태와 비교하는 것에서부터 시작한다. (표준 14.2 분석 및 잠재적 감사 지적사항 참조) 내부감사인은 비교 결과 차이가 존재하는 경우, 잠재적 지적사항을 추가로 조사하여 다음 사항을 탐색한다:

- 차이의 근본원인은 일반적으로 통제 결함과 관련 있다. 근본 원인을 파악하기 위한 가장 단순한 방법에는 차이가 존재하는 이유에 대해 일련의 질문을 던지는 것이 있다.
- 차이의 영향 또는 충격은 상태가 왜 문제의 원인이 될 수 있는지를 설명한다. 어떤 경우 영향은 객관적으로 정량화 할 수 있지만, 많은 경우 노출 정도는 검토대상활동 경영진의 정보와 함께 내부감사인이 전문가로서 정당한 주의를 행사하여 얻은 추정치이다. (원칙 4 전문가로서 정당한 주의 행사 참조)

내부감사인은 지적사항의 중대성을 판단하기 위해 최고감사책임자가 수립한 감사방법론을 사용한다. 내부감사인들은 기존 통제의 설계 적합성 및 효과성을 식별 및 평가한 다음, 잔여 리스크 수준 또는 통제가 존재함에도 불구하고 남아 있는 리스크를 결정한다.

내부감사인은 최고감사책임자가 수립한 감사방법론에 따라 지적사항에 등급을 부여함으로써 모든 내부감사업무의 일관성을 보장한다. 내부감사인은 지적사항 등급을 결정할 때 다음 사항을 고려해야 한다:

- 리스크의 충격/영향과 발생가능성
- 조직의 리스크 허용범위
- 최고감사책임자가 수립한 감사방법론
- 조직에 중요한 다른 추가적인 요소

감사지적사항 등급은 각 지적사항의 중대성을 설명하는 효과적인 커뮤니케이션의 수단이 될 수 있으며, 경영진이 조치 계획의 우선순위를 결정하는 데 도움이 될 수 있다. 등급의 예로 낮음, 보통, 높음, 심각이 있다.

최고 감사 책임자는 내부 감사인이 감사지적사항을 문서화하는 데 사용할 템플릿을 제공하여 다음과 같은 다양한 항목의 적절한 문서화를 보장할 수 있다:

- 기준
- 현재 상태
- 원인
- 영향
- 중대성 등급
- 지적사항을 해결하기 위한 권고사항 (표준 14.4 권고사항 및 조치 계획 참조)

지적사항은 검토대상활동의 경영진이 내부감사인의 평가 내용을 이해할 수 있도록 간단한 언어로 간결하게 작성해야 한다. 지적사항은 실제 상태와 기준 사이의 차이를 설명해야 하며 내부감사인의 평가 및 그 중대성에 대한 판단을 뒷받침하는 서면 증거와 연계되어야 한다.

적합성 증거

- 지적사항 평가에 사용된 기준을 설명하는 감사조서
- 기준, 상태, 근본 원인, 영향(리스크 또는 잠재적 노출) 및 각 지적사항의 중대성 등급을 열거한 감사조서
- 지적사항 분석의 기초로 사용된 중대성, 허용범위 및 비용-효익 분석의 요소를 설명하고 있는 감사조서나 기타 문서
- 관련 내부감사 규정, 템플릿(template) 및 지침
- 최종 감사업무 커뮤니케이션과 관련된 문서

국제내부감사표준 14.4 권고사항 및 조치 계획

요건

내부감사인은 반드시 권고사항을 형성해야 하고, 해당되는 경우 경영진의 조치계획을 구해야 한다.

권고사항은 다음과 같은 조치를 제안한다:

- 설정된 기준과 현상의 차이점을 해결함.
- 식별된 리스크를 경감함.
- 검토대상활동을 강화하거나 개선함.

내부감사인은 반드시 권고사항을 검토대상활동의 경영진과 논의해야 한다.

검증 감사의 경우, 내부감사인은 각 지적사항의 근본 원인을 해결하기 위한 경영진의 조치 계획을 반드시 확보해야 한다.

내부감사인과 경영진이 권고사항 및/또는 조치 계획에 대해 합의하지 못해 해결책을 수립할 수 없는 경우, 내부감사인은 최종 커뮤니케이션 내용에 반드시 의견 불일치의 이유와 양측의 입장이 모두 명시하여야 한다. (표준 13.1 감사업무 커뮤니케이션 참조)

시정 조치에 대한 권고사항 제시는 내부감사인의 의무이지만, 지적사항을 처리하기 위한 적절한 조치를 결정하고 조치계획을 이행하는 것은 경영진의 책임이다. (표준 15.1 최종 감사업무 커뮤니케이션 참조) 자문 업무에는 조치 계획이 필요하지 않다.

실행 및 적합성 증거를 위한 고려사항

실행

내부감사인은 감사업무 전반에 걸쳐 경영진과 상시적으로 커뮤니케이션을 해야 한다. (표준 13.1 감사업무 커뮤니케이션 참조) 내부감사인은 감사 수행과정 전반에 걸쳐 검토대상활동의 경영진과 지적사항 및 권고사항을 논의해야 한다. 감사보고서 등 최종 커뮤니케이션이 실시되기 전에 반드시 실시되어야 하는 감사종료단계 커뮤니케이션은 일반적으로 감사종료 회의와 같은 공식적 또는 구조적인(structured) 커뮤니케이션 기회이다. (표준 13.1 감사업무 커뮤니케이션 참조) 내부감사인은 최고감사책임자가 수립한 감사방법론을 사용하여 단계적으로 보고할 지적사항이 무엇인지를 결정해야 한다.

내부감사인은 검토대상활동의 변경을 실행하고 감독할 수 있는 충분한 권한이 있는 당사자에게 권고사항을 전달해야 한다. 최고감사책임자는 내부감사인이 적절한 당사자를 식별하는 데 도움이 되는 규정이나 지침을 만들 수 있다. 예를 들어, 내부감사 규정은 특정한 역할이나 계급(관리자급, 이사 또는 부사장 등)에게 내부감사 권고사항에 대한 조치 계획을 수립하도록 요구할 수 있다.

내부감사인은 지적사항을 해결하는 특정 시정 조치가 파악되면, 이를 권고사항에 포함하여 전달해야 한다. 또는 내부감사인이 경영진이 고려해야 할 몇 가지 방안을 제시할 수도 있다.

내부감사인은 경우에 따라 경영진이 방안을 연구하여 적절한 조치를 결정하도록 권고할 수 있다. 하나의 지적사항에 대해 권고되는 시정 조치가 여러 개 있을 수 있다.

내부감사인과 검토대상활동의 경영진이 감사 지적사항이나 권고사항에 대해 의견이 일치하지 않는 경우, 최고감사책임자는 해결을 용이하게 하기 위해 검토대상활동 경영진 보다 상위에 있는 경영진과 협력해야 한다. 표준 13.1 감사업무 커뮤니케이션의 요건에 따라, 내부감사인은 해결책을 수립할 수 없는 경우 감사보고서 등 최종 커뮤니케이션 내용에 양측의 입장을 기록하여 전달해야 한다. 또한, 각 당사자의 공식 의견을 커뮤니케이션의 부록으로 첨부할 수 있다. 부록으로 첨부되지 않은 경우, 요청이 있을 때 당사자의 완전한 의견이 제공되어야 한다.

내부감사인은 권고사항 및 조치 계획의 타당성과 합리성을 평가하고, 경영진과 논의해야 한다. 일반적으로 평가 및 논의에는 비용-효익 분석과 조치 계획이 조직의 리스크 허용범위에 따라 만족스럽게 리스크를 해결할 것인지에 대한 결정이 포함된다.

공공 부문

법규는 종종 공공 부문에서 근무하는 내부감사인에게 최종 커뮤니케이션 내용에 모든 경영진의 의견을 공개하도록 요구한다.

적합성 증거

- 기준, 상태, 영향, 근본 원인 및 권고사항이 포함된 각 지적사항에 대한 감사조서
- 관련 내부감사 규정, 절차, 템플릿(template) 및 지침
- 지적사항과 권고사항 및 조치 계획의 타당성에 대해 경영진과 논의했음을 입증하는 메모, 감사조서 또는 기타 문서
- 최종 커뮤니케이션과 관련된 문서

국제내부감사표준 14.5 감사 결론 도출

요건

내부감사인은 반드시 감사 결론을 도출해야 한다.

감사결론은 총괄적으로 봤을 때 감사지적사항의 전반적인 중대성에 대한 내부감사인의 판단이다. 결론에는 감사업무의 목표 및 범위와 관련된 감사 지적사항과 결과의 요약이 반드시 포함되어야 한다.

결론은 반드시 내부감사부서에서 수립된 방법론에 따라 도출되어야 한다.

감사결론을 토대로 내부감사인은 취합한 지적사항의 등급, 순위 또는 다른 중대성 지표를 발행해야 한다.

검증 감사의 경우 검토대상활동의 거버넌스, 리스크 관리 및/또는 통제 프로세스의 효과성에 대한 내부감사인의 판단이 반드시 결론에 포함되어야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

내부감사인은 검토대상활동에 대한 전반적인 감사 결론이나 요약에 결정하기 위해 개별 감사지적사항의 등급을 취합해야 한다. 최고감사책임자가 사전에 수립한 내부감사부서의 감사방법론은 통제의 효과성에 대해 합리적인 검증이 이루어졌는지 여부를 나타내는 척도를 제공한다. 예를 들어, 이러한 척도는 내부감사인의 평가에 근거하여 만족, 일부 만족, 개선이 필요한 수준 또는 불만족 수준으로 표시될 수 있다.

일반적으로 내부감사인은 감사업무 수행 시 감사등급평가 시스템을 포함하여, 감사의 시작 전에 최고감사책임자가 수립하고 최고경영진 및 이사회와 검토한 기준과 방법론을 사용한다. 이러한 등급평가 시스템은 조직의 전반적인 리스크 성향과 검토대상활동의 리스크 허용범위를 기반으로 해야 하며, 모든 내부감사 업무에 걸쳐 감사 결론 및 등급을 제시하기 위한 기반을 제공해야 한다. 감사 결론 및 등급평가에 대한 이해에 대해 합의가 있어야 감사업무 전체의 일관성이 확보된다.

감사결론은 검토대상 활동 및 조직 내에서 지적사항의 충격/영향에 관한 맥락을 추가로 제공할 수 있다. 예를 들어, 일부 지적사항은 미시적 수준에서 목표 달성 또는 리스크 관리에 중대한 영향을 미칠 수 있지만, 거시적 수준에서는 그렇지 않을 수 있다(예: 이중 결제 가능성을 관리하는데 실패한 것은 자회사에게는 중대할 수 있지만 그룹 전체로서는 아님). 내부감사인은 통제 수단이 경영진의 목표 달성에 대한 리스크를 얼마나 잘 관리하는지 고려해야 한다.

적합성 증거

전반적인 감사 결론의 근거와, 최고감사책임자의 등급평가제도와 감사업무의 일관성을 보여주는 감사조서

내부감사부서가 사용할 등급평가제도에 대해 최고감사책임자, 경영진 및 이사회가 일관됨을 보여주는 규정이나 회의록

국제내부감사표준 14.6 감사업무의 문서화

요건

내부감사인은 감사 지적사항, 권고사항 및 결론을 뒷받침하는 정보와 증거를 반드시 문서화해야 한다.

감사업무와 관련된 분석, 평가 및 보충 정보는 정보에 정통하고 신중한 내부감사인 또는 유사한 정보를 갖고 있는 유능한 사람이 감사업무를 반복했을 때, 동일한 지적사항, 권고사항 및 결론에 도달할 수 있도록 반드시 문서화해야 한다.

감사업무 문서에는 반드시 다음 사항이 포함되어야 한다:

- 감사일자 또는 기간
- 감사업무 수행 프로그램

- 감사업무 리스크 평가
- 감사업무의 목표 및 범위
- 절차 및 데이터 원천의 세부사항을 포함한 분석 설명
- 지적사항, 권고사항 및 결론
- 적절한 당사자와의 커뮤니케이션 증거
- 업무를 수행하고 감독한 개인의 이름이나 이니셜

내부감사인원은 감사업무 문서화의 정확성, 관련성 및 완전성을 반드시 검토해야 한다.

최고감사책임자 또는 지명된 자는 반드시 감사업무 문서화의 적정성을 검토하고 승인해야 한다.

내부감사인은 내부감사부서 및 조직의 규정과 절차뿐만 아니라 관련 법규에 따라 모든 감사업무 문서를 반드시 보관해야 한다.

실행 및 적합성 증거를 위한 고려사항

실행

감사조서를 통한 내부감사 업무의 문서화는 업무의 재수행을 가능하게 하고, 감사 결론 및 결과를 지원하는 방식으로 감사업무 정보를 구성하기 때문에 체계적이고 규율화된 감사 프로세스의 중요한 부분이다. 문서화는 개별 내부감사인을 감독하기 위한 기초를 제공하고, 최고감사책임자 및 다른 사람들이 내부감사부서의 업무 품질을 평가할 수 있도록 한다. 적절한 문서화는 내부감사부서의 표준 적합성을 입증하는 역할도 수행한다.

내부감사인은 수행한 감사 단계와 형식을 포함하여, 감사업무를 문서화하기 위해 최고감사책임자가 수립한 방법론을 사용해야 한다. 여기에는 감사조서를 작성하기 위한 템플릿(template) 또는 소프트웨어와 문서 보관 시스템이 포함될 수 있다. 감사조서는 감사 지적사항, 권고사항 및 결론을 결정하는 데 사용된 정보를 보여준다.

일반적으로 감사조서는 감사업무 수행 프로그램에서 정하고 있는 구조에 따라 구성되고, 관련 정보를 상호 참조한다. 최종 결과물은 완료된 감사절차, 확보된 감사정보, 형성한 감사결론, 도출된 권고사항 및 각 단계에 대한 논리적 근거를 집대성한 문서이다. 이 문서는 최고경영진, 이사회 및 검토대상활동의 경영진을 포함하여 이해관계자와 내부감사인 간의 커뮤니케이션을 위한 주요 자료들로 구성된다. 아마도 가장 중요한 것은 감사조서가 다른 내부감사인 또는 외부감사인과 같이 신중하고 정보에 입각한 유능한 사람이, 감사업무를 수행한 내부감사인이 도달한 것과 동일한 결론에 도달할 수 있도록 해주는 충분하고 관련 있는 정보를 포함하고 있다는 점이다.

감사조서의 기본 형식:

- 색인 또는 참조 번호
- 검토대상활동을 식별하는 제목 또는 표제
- 감사 일자 또는 기간
- 수행한 감사업무의 범위

- 데이터 확보 및 분석의 목적을 기술한 문서
- 감사계획 수립 문서
- 핵심 검토대상 프로세스에 대한 프로세스 지도(map), 업무흐름도(flow chart) 또는 설명
- 수행된 인터뷰 또는 발행된 설문조사의 요약
- 리스크 통제 매트릭스(Risk Control Matrix)
- 감사조서에 포함되어 있는 데이터의 출처
- 데이터를 분석하는 데 사용된 표본의 크기 및 선택 방법(테스트 접근방식)을 포함하여 평가 모집단에 대한 설명
- 수행된 테스트 및 분석의 세부사항
- 감사조서에 대한 상호 참조를 포함한 감사관찰사항에 대한 감사결론
- 제안된 후속감사 수행안
- 경영진의 대응방안이 포함된 감사보고서 등 최종 커뮤니케이션 내용
- 감사업무를 수행한 내부감사인의 성명
- 감사업무를 검토한 내부감사인의 이름과 검토 의견서

최고감사책임자는 감사조서 검토를 위한 방법론을 수립해야 한다. 최고감사책임자는 내부감사인이 감사업무 목표를 달성하고, 교육, 피드백(feedback) 및 코칭(coaching)을 받아 내부감사부서의 지속적인 발전과 성과 품질의 향상에 기여할 수 있도록 신뢰할 수 있는 프로세스를 수립해야 한다.

공공 부문

공공 부문에서 근무하는 내부감사인은 조직이 운영되는 사법관할권의 준거 법규가 감사조서 공개 요건에 어떤 영향을 미치거나 규정하는지 반드시 이해해야 한다. 일부 사법관할권에서는 내부감사인이 감사조서를 대중에 공개하는 것이 금지된 반면, 다른 사법관할권에서는 경영진이 보고서 초안을 받거나 최종 커뮤니케이션 내용이 공개되는 즉시 감사조서의 일부 또는 전부가 공개 대상이 될 수 있다.

적합성 증거

- 감사조서 및 감사업무 정보의 작성, 내용, 검토 및 보존을 위한 내부감사 방법론과 템플릿(template) 또는 소프트웨어
- 감사방법론에 따라 작성된 감사조서
- 감사조서 및 감독 규정 적합성을 검증하는 감사품질에 대한 내부평가 검토 결과

원칙 15 감사결론 커뮤니케이션 및 조치계획 모니터링

내부감사인은 감사 지적사항 및 결론을 적절한 당사자에게 커뮤니케이션을 실시하고, 경영진의 조치계획 이행 진척도를 모니터링한다.

내부감사인은 감사업무를 완료하고 지적사항, 권고사항, 결론 및 조치 계획에 대해 경영진과 커뮤니케이션을 실시한 다음 최종 커뮤니케이션 내용을 발행할 책임이 있다. 내부감사인은 합의된 조치의 이행 여부를 확인하기 위해 검토대상활동의 경영진과 계속 커뮤니케이션한다.

국제내부감사표준 15.1 최종 감사업무 커뮤니케이션

요건

개별 감사수행 시 내부감사인은 반드시 감사업무의 목표, 범위 및 결론을 포함하는 최종 커뮤니케이션을 실시해야 한다. 최종 커뮤니케이션 내용에는 감사 권고사항 및/또는 합의된 감사지적사항 조치계획도 포함되어야 한다.

검증 감사의 경우, 감사보고서 등 최종 커뮤니케이션 내용에는 다음도 포함되어야 한다.

- 지적사항과 등급, 순위 또는 기타 지적사항의 중대성을 표시하는 지표
- 감사범위 제한에 대한 설명(해당 시)

최종 커뮤니케이션 내용에는 지적사항에 대한 조치를 취할 책임이 있는 개인과 조치를 완료해야 하는 예정일을 반드시 명시해야 한다. 경영진이 최종 커뮤니케이션 실시전에 지적사항을 해결하기 위한 조치를 시작했거나 완료했음을 내부감사인이 알게 되면, 최종 커뮤니케이션 내용에 해당 완료된 조치내용을 반드시 언급해야 한다.

표준 11.2 효과적인 커뮤니케이션에 설명된 대로 감사보고서 등 최종 커뮤니케이션 내용은 반드시 정확하고 객관적이며 명확하고 간결하고 건설적이며 완전하고 시기적절해야 한다. 내부감사인은 최종 커뮤니케이션이 실시되기 전에 최고감사책임자 또는 지명된 자가 검토하고 승인했음을 반드시 보장해야 한다.

내부감사인은 감사보고서 등 최종 커뮤니케이션 내용을 공개하거나 전달하는 것과 관련하여 최고감사책임자가 수립한 규정 및 절차를 반드시 준수해야 한다. 최종 커뮤니케이션 내용을 뒷받침하는 감사조서는 반드시 보존되어야 하며, 외주 서비스 제공자가 감사업무를 수행하는 경우를 포함하여 조직 및 내부감사부서가 접근할 수 있어야 한다.

감사업무가 국제내부감사표준에 따라 수행된다는 기술은 내부감사인이 이 표준을 준수하였으며, 최신 감사품질 평가 및 개선 프로그램(QAIP)의 결과가 이 기술을 뒷받침하는 경우 감사보고서 등 최종 감사업무 커뮤니케이션 내용에 반드시 포함되어야 한다.

내부감사인은 감사업무가 이 표준에 따라 수행되지 않는 경우, 다음과 같은 부적합에 관한 세부내용을 반드시 공개해야 한다:

- 적합성을 미달한 표준

- 부적합 사유
- 감사 지적사항 및 결론에 부적합이 미치는 충격/영향

실행 및 적합성 증거를 위한 고려사항

실행

감사보고서 등 최종 감사업무 커뮤니케이션의 종류와 형식은 조직마다 다르지만, 일반적으로 최고감사책임자가 정한다. 최고감사책임자는 템플릿(template)과 절차를 제공할 수 있다.

최종 커뮤니케이션은 특정 커뮤니케이션 대상에 맞추어 형식, 내용 및 세부내용의 수준을 달리한 여러 버전(version)으로 실시될 수 있다. 최종 감사업무 커뮤니케이션 내용은 검토대상활동에 대해 얼마나 알고 있는지, 지적사항 및 결론이 그들에게 미치는 충격/영향, 정보사용 계획에 따라 구체적 대상에 맞춤화해야 한다.

보고서 형태로 발행될 때, 최종 커뮤니케이션에는 보통 다음 구성요소가 포함된다:

- 제목
- 목표(감사업무의 목적)
- 감사범위(활동, 업무의 성격과 범위, 감사범위의 제한)
- 감사실시 배경(검토대상활동에 대한 간략한 개요 또는 프로세스에 대한 설명)
- 인정(검토 중인 영역의 긍정적 측면 및/또는 협조에 대한 감사)
- 해당되는 경우 검토대상 영역 또는 프로세스 별로 그룹화된 개별 지적사항(중요성 순으로 나열):
 - 제목 및 참조
 - 관련 사례, 데이터, 분석, 표 또는 차트(chart)로 입증할 수 있는 사실의 기술(상태, 기준, 원인, 영향/리스크)
 - 지적사항의 중대성(등급, 순위 또는 지적사항의 중대성에 대한 기타 지표)
 - 권고사항 (지적사항에서 식별된 리스크를 경감하기 위한 시정 조치).
- 경영진의 조치 계획(시정 조치, 이행 담당자 및 완료 목표일)
- 감사 결론(종종 중대한 지적사항을 강조하는 감사업무 요약 평가)
- 감사업무 전체의 등급(감사 결론에 기반하여, 예를 들면 만족, 보통, 불만족, 통과 또는 실패 등급을 부여함.)
- 최종 감사커뮤니케이션 내용 배포 목록
- 국제내부감사표준 적합성에 관한 기술

최종 커뮤니케이션 내용 검토 대상에는 일반적으로 다음 사항이 포함된다:

- 수행하고 문서화한 업무가 감사업무의 목표, 범위 및 표준(적합성 주장 시)과 일치함. (표준 8.3 감사품질에 대한 외부평가 및 표준 12.1 감사품질에 대한 내부평가 참조)
- 감사 지적사항, 권고사항, 결론 및 조치 계획이 명확하게 기술되고 적절하고 신뢰할 수 있으며 충분한 정보로 뒷받침함. (표준 14.1 분석 및 평가를 위한 정보 수집 참조)
- 추가 설명 또는 기록이 필요한 영역이 언급되어 있음.
- 검토대상활동 조직과의 커뮤니케이션 요건이 충족됨.
- 필요한 모든 정보는 포함되고 불필요한 세부정보는 생략됨.

최고감사책임자 또는 지명된 자는 최종 감사업무 커뮤니케이션 내용의 배포 수단을 결정한다. 구두 발표는 일반적으로 디지털(digital) 또는 출력물 형태의 프레젠테이션 및/또는 서면 보고서로 보충된다.

내부감사인은 최종 감사업무 커뮤니케이션 내용을 배포하기 위해, 공공 부문과 같은 특정 부문이나 금융 서비스산업과 같은 특정 산업과 관련된 추가적인 법규를 준수해야 한다.

적합성 증거

- 서면으로 작성된 최종 커뮤니케이션
- 구두로 최종 커뮤니케이션을 실시하는 경우, 프레젠테이션 슬라이드 및/또는 회의록
- 최종 커뮤니케이션 내용에 대해 검토 및 승인이 이루어졌음을 보여주는 문서
- 검토대상활동 조직과 커뮤니케이션 할 요건이 충족되었음을 보여주는 기록

국제내부감사표준 15.2 경영진의 조치계획 이행 확인

요건

내부감사인은 경영진이 합의한 조치계획을 이행했는지 여부를 반드시 확인해야 한다.

내부감사인은 경영진이 감사 지적사항을 해결하기 위한 조치를 이행했는지 확인하기 위해 반드시 수립된 방법론을 준수해야 한다.

방법론에는 다음 사항이 포함된다:

- 조치 계획에 대한 진척상황 문의
- 후속 평가 및 분석의 수행
- 조치계획 이행 추적시스템에 조치계획의 진행상황을 업데이트(update)

내부감사인은 검토대상활동에서 발생한 변화로 인해 감사 지적사항 및 조치 계획이 더 이상 해당되지 않는 경우, 반드시 이를 통보하도록 경영진에게 요청해야 한다. 내부감사인은 경영진이 보고한 변화를 반드시 확인하고, 언제 변화가 발생했는지 파악해야 한다. 내부감사인이

지적사항이 유효하고 조치 계획이 여전히 필요하다고 생각하는 경우에는 반드시 이러한 정보를 문서화하여 최고감사책임자에게 알려야 한다.

내부감사인은 경영진이 정해진 완료일에 합의된 조치 계획을 이행하지 않은 경우, 경영진으로부터 그 이유에 대한 설명을 확인하여 문서화해야 한다. 내부감사인은 최고경영진이 조치를 취하지 않거나 조치 계획 이행 지연으로 인한 리스크를 수용했는지 판단할 책임이 있는 최고감사책임자와 반드시 이러한 문제를 논의해야 한다. (표준 11.5 리스크 수용에 대한 커뮤니케이션 참조)

실행 및 적합성 증거를 위한 고려사항

실행

최고감사책임자가 수립한 방법론은 내부감사인이 조치계획의 진척상황을 모니터링하고, 경영진이 조치 계획을 효과적으로 이행하도록 보장하는 방법을 설명한다.

내부감사인은 일반적으로 소프트웨어 프로그램, 스프레드시트(spreadsheet) 또는 시스템을 사용하여 조치 계획이 정해진 일정에 따라 이행되는지 추적한다. 또한, 추적 시스템은 조치가 미결 상태인지 또는 기한이 지났는지 표시하고, 내부감사인이 최고경영진 및 이사회와 커뮤니케이션할 수 있는 유용한 도구를 제공한다. 또한, 프로그램이나 시스템은 리스크 평가에서부터 조치 계획의 완료까지 업무흐름을 자동화할 수 있다. 예를 들어, 목표 완료일이 다가오는 조치에 대해 적절한 당사자에게 알리는 자동 이메일 발송이 업무 흐름에 포함될 수 있다.

내부감사인은 경영진의 조치계획 이행 상태를 추적하고, 내부감사 방법론에 설명된 대로 검토대상활동의 경영진, 이사회 및 최고감사책임자와 커뮤니케이션한다. 감사방법론은 미결된 조치계획에 대한 후속 처리 방법과 시기를 명시하고, 조치 계획이 지적사항을 효과적으로 해결하고 중대한 리스크를 경감했는지 확인하기 위해 후속 평가 및 분석을 수행할 시기를 결정할 수 있는 기준을 포함한다. 완료된 조치계획에 대한 후속 평가 및 분석은 리스크의 중대성에 따라 선별적으로 수행될 수 있다. 어떤 상황에서는 규제당국이 경영진의 조치 계획에 대한 보고를 요구할 수 있다.

내부감사인은 조치계획 진척상황에 대해 문의할 때, 조치가 아직 이행되지 않은 경우 경영진에게 그 이유를 설명하도록 요청해야 한다. 경영진이 대체 조치 계획을 결정하고 내부감사인이 이 계획이 만족스럽거나 원래의 조치 계획보다 낫다는 데 동의하면, 해당 대체 계획의 진척상황을 완료 시점까지 추적해야 한다.

공공 부문

일부 사법관할권에서는 내부감사인이 권고사항의 이행 상태에 대해 공개 보고서를 작성해야 할 수 있다.

적합성 증거

- 이전 감사 관찰사항, 관련 시정 조치계획 및 시정 상태, 그리고 이에 대한 내부감사인의 확인을 포함하는 예외사항 추적 시스템(예: 엑셀, 데이터베이스(database) 또는 기타 툴(tool))에 대한 반복적인 업데이트(update) 기록
- 최고경영진 및 이사회에 보고하기 위해 준비한 시정조치 상태 보고서

- 조치계획 이행 상태에 대해 이사회에 주기적으로 보고한 증거
- 조치계획 이행상태 보고서 공개 기록

