



세계내부감사인협회 (IIA) 3 선 모델

3 선 방어 모델 개정본

목차

서론.....	1
3 선 모델의 원칙.....	2
원칙 1: 거버넌스.....	2
원칙 2: 지배 기구의 역할.....	2
원칙 3: 경영진과 제 1 선 및 제 2 선의 역할.....	3
원칙 4: 제 3 선의 역할.....	3
원칙 5: 제 3 선의 독립성.....	3
원칙 6: 가치의 창출과 보호.....	4
3 선 모델의 핵심 역할.....	5
지배 기구.....	5
경영진.....	5
내부 감사.....	Error! Bookmark not defined.
외부의 보증 제공자.....	6
주요 역할 간의 관계.....	7
지배 기구와 경영진 (제 1 선 및 제 2 선 역할)의 관계.....	7
경영진 (제 1 선 및 제 2 선 역할)과 내부 감사의 관계.....	7
내부 감사와 지배 기구의 관계.....	8
전체적인 관계.....	8
3 선 모델의 적용.....	9
구조, 역할 및 책임.....	9
감시와 보증.....	10
조율과 방향 일치.....	10

서론

조직은 불확실성, 복잡성, 상호 연결성 및 불안정성이 증가하고 있는 세상에서 **운영되는 인간 활동의 유기체**이다. 조직에는 다양하고, 가변적이며, 때로 경쟁적인 이해관계를 갖고 있는 여러 이해당사자가 존재하는 경우가 흔하다. 이해당사자는 지배 기구에 조직을 감시하도록 위임하는데, 지배 기구는 다시 경영진에게 자원과 권한을 위임하여 리스크 관리를 포함하는 적절한 조치를 취하도록 한다.

이러한 이유 등으로, 조직에는 강력한 거버넌스 및 리스크 관리를 뒷받침하는 가운데 목표 달성을 가능하게 하는 효과적인 구조와 프로세스가 필요하다. 지배 기구는 경영진으로부터 활동, 성과, 전망에 대한 보고를 받기 때문에 지배 기구와 경영진은 내부 감사가 제반 사항에 대해 독립적이고 객관적인 보증 및 조언을 제공하고, 혁신과 개선을 촉진하고 장려할 것을 기대한다. 지배 기구는 궁극적으로 거버넌스의 책임을 지는데 거버넌스는 경영진 및 내부 감사는 물론, 지배 기구의 조치 및 행위를 통해 달성된다.

3 선 모델은 목표 달성에 필요한 최선의 지원을 얻을 수 있고, 강력한 거버넌스 및 리스크 관리를 촉진하는 구조와 프로세스를 조직이 식별하도록 돕는다. 이 모델은 모든 조직에 적용되며 다음을 통해 최적화된다:

- 원칙 기반의 접근법 채택 및 조직의 목표와 상황에 맞게 모델 변용
- 리스크 관리가 “방어”의 사안 및 가치의 보호는 물론, 목표 달성과 가치 창출에 기여하는 바에 집중
- 3 선 모델 및 3 선 간의 관계가 대표하는 역할과 책임을 명확하게 이해
- 조직의 활동 및 목표가 이해당사자가 우선시하는 이익과 일치되어 있음을 보장하는 조치 이행.

핵심 용어

조직 - 공동의 목적을 위해 노력하는 사람, 수행하는 활동, 투입되는 자원으로 구성된 그룹.

이해당사자 - 조직이 그 이익을 위해 봉사하거나 이익에 영향을 미치는 그룹 및 개인.

지배 기구 - 조직의 성공을 위해 이해당사자에게 책임이 있는 개인.

경영진 - 조직의 클라이언트에게 제품 및/또는 서비스를 제공할 임무를 맡은 개인, 팀, 지원 부서.

내부 감사 - 거버넌스 및 리스크 관리 (내부 통제 포함)의 적정성과 효과성에 대한 보증과 통찰력을 제공하기 위해 경영진으로부터 독립적으로 운영되는 개인.

3 선 모델 - 구 (舊) 3 선 방어 모델.

내부 통제 - 목표 달성에 대해 합리적인 확신을 제공하기 위해 고안된 프로세스.

3 선 모델의 원칙

원칙 1: 거버넌스

조직의 거버넌스를 위해서는 다음을 가능케 하는 적절한 구조 및 프로세스가 필요하다:

- 청렴성, 리더십 및 투명성을 통해 지배 기구가 이해당사자에게 지니는 조직 감시의 **책임성**
- 리스크에 기반한 의사 결정 및 자원 이용을 통해 조직의 목표를 달성하기 위해 경영진이 취하는 **조치** (리스크 관리 포함)
- 철저한 조사와 통찰력 있는 커뮤니케이션을 통해 명료성과 확신을 제공하고, 지속적인 개선을 촉진 및 장려하기 위해 독립적인 내부 감사 기능이 제공하는 **보증과 조언**.

핵심 용어

리스크에 기반한 의사 결정 - 분석, 기획, 조치, 모니터링 및 리뷰를 포함하며 불확실성이 목표에 미치는 잠재적 영향을 고려하는 프로세스.

보증 - 독립성 있는 확인 및 확신.

원칙 2: 지배 기구의 역할

지배 기구는 다음을 보장한다:

- 효과적인 거버넌스를 위해, 적절한 구조 및 프로세스가 마련되어 있음
- 조직의 목표 및 활동이 이해당사자가 우선시하는 이익과 일치되어 있음.

지배 기구는:

- 법규 및 윤리적 기대치가 충족됨을 보장하는 가운데, 경영진에게 자원을 제공하고 책임을 위임하여 조직의 목표를 달성토록 한다.
- 독립적이며, 객관성 있고 유능한 내부 감사 기능을 설치하고 감시하여 목표 달성의 진척에 대해 명료성과 확신을 제공하도록 한다.

원칙 3: 경영진과 제 1 선 및 제 2 선 역할

조직의 목표를 달성해야 하는 경영진의 책임은 제 1 선 및 제 2 선 역할로 구성된다.¹ *제 1 선 역할*은 조직의 클라이언트에게 제품 및/또는 서비스를 전달하는 것과 가장 직접적으로 일치되어 있으며, 지원 부문의 역할을 포함한다.² *제 2 선 역할*은 리스크 관리를 지원한다.

제 1 선 및 제 2 선 역할은 혼합되거나 분리될 수 있다. 제 2 선 역할 중 일부는 전문가에게 맡겨, 제 1 선 역할을 담당하는 이들을 보완하는 전문성, 지원, 모니터링 및 도전과제를 제공하게 할 수도 있다. 제 2 선 역할은 법규 준수, 허용되는 윤리적 행위, 내부 통제, 정보 기술 보안, 지속가능성 및 품질 보증과 같은 리스크 관리의 구체적인 목표에 집중할 수 있다. 또는, 전사적 리스크 관리 (ERM)와 같이 보다 광범위한 리스크 관리 책임까지 포괄할 수 있다. 어찌되었건, 리스크 관리의 책임은 제 1 선의 역할이자 경영의 범위에 포함된다.

원칙 4: 제 3 선의 역할

내부 감사는 거버넌스와 리스크 관리의 적정성 및 효과성에 대해 독립적이고 객관적인 보증과 조언을 제공한다.³ 체계적이며 규율이 존재하는 프로세스, 전문성 및 통찰력을 적절하게 활용하여 이를 달성한다. 내부 감사 지적사항을 경영진과 지배 기구에 보고하여 지속적인 개선을 촉진 및 장려한다. 그 과정에서, 내외부의 다른 보증 제공자들의 소견을 고려할 수도 있다.

원칙 5: 제 3 선의 독립성

경영의 책임으로부터 독립적인 내부 감사는 객관성, 권위 및 공신력을 유지하는데 필수적이다. 독립성은 다음을 통해 확보된다: 지배 기구에 대한 책임성, 업무 완수에 필요한 인력, 자원 및 데이터에 대한 제한 없는 액세스, 감사 서비스의 기획과 이행에 있어 간섭이나 편향으로부터의 자유.

1. “제 1 선”, “제 2 선”, “제 3 선”이라는 용어는 친숙함을 위해 원 모델의 용어를 그대로 유지한 것이다. 그러나, “선”이라는 용어는 구성 요소라기보다는 차별화된 역할을 효과적으로 가리키기 위해 사용되었다. 논리적으로, 지배 기구의 역할도 “선”을 구성하지만 혼란을 방지하기 위해 이 규칙은 도입되지 않았다. 순서 (제 1 선, 제 2 선, 제 3 선)는 순차적인 운영을 의미하지 않으며, 모든 역할은 동시에 가능하다.

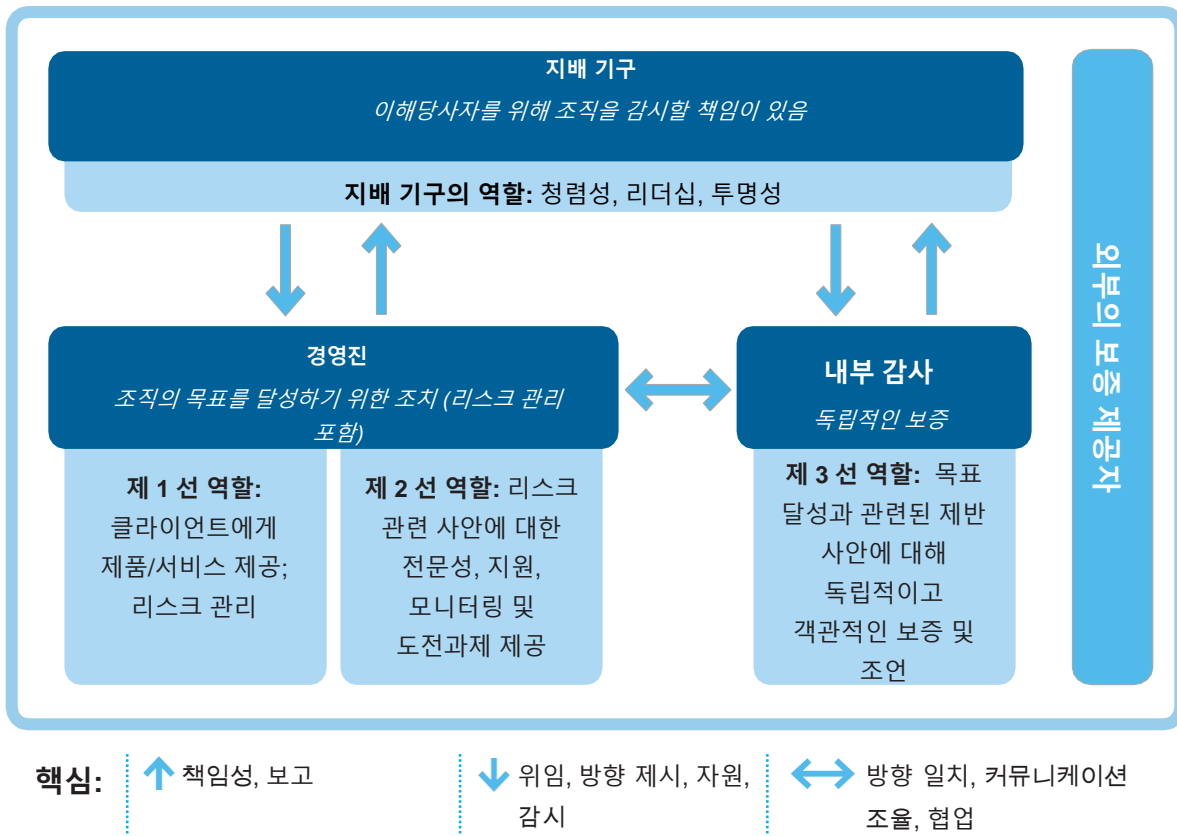
2. 일부는 지원 부문 (HR, 총무 및 건물 관리 등)의 역할을 제 2 선이라고 생각한다. 명료성을 위해, 3 선 모델에서는 *제 1 선 역할*이 “일선 부서” 및 “후선 부서” 활동을 모두 포함하고, *제 2 선 역할*은 리스크 관련 사안에 초점을 맞춘 보완적 활동을 구성한다고 여감을 밝힌다.

3. 일부 조직에서는 다른 제 3 선 역할도 식별된다. 예: 감시, 검사, 조사, 평가 및 시정. 이들은 내부 감사 기능의 일부이거나 개별적으로 기능할 수 있다.

원칙 6: 가치의 창출과 보호

집합적으로 기능하는 모든 역할은 각자의 역할 및 이해당사자가 우선시하는 이익과 일치할 때 가치의 창출과 보호에 기여한다. 활동의 방향 일치는 커뮤니케이션, 협력 및 협업을 통해 달성된다. 이는 리스크 기반 의사 결정을 위해 필요한 정보의 신뢰도, 통일성 및 투명성을 보장한다.

IIA 의 3 선 모델



3 선 모델의 핵심 역할

조직의 책임 분배 방식은 모두 다르다. 그러나, 다음의 상위 역할은 3 선 모델의 원칙을 강조하고 있다.

지배 기구

- 이해당사자를 위해 조직 감시의 책임을 진다.
- 이해당사자와 소통하여 이들의 이익을 모니터링하고 목표 달성에 대해 투명하게 커뮤니케이션한다.
- 윤리적 행위 및 책임성을 장려하는 문화를 함양한다.
- 필요 시 보조 위원회를 포함하여, 거버넌스를 위한 구조 및 프로세스를 수립한다
- 조직의 목표 달성을 위해 경영진에 책임을 위임하고 자원을 제공한다.
- 조직의 리스크 성향을 결정하고 리스크 관리 (내부 통제 포함) 상태를 감시한다.
- 법규 및 윤리적 기대치의 준수 상태를 지속적으로 감시한다.
- 독립적이며 객관성 있고 유능한 내부 감사 기능을 설치하고 감시한다.

경영진

제1 선의 역할

- 조직의 목표 달성을 위해 조치 (리스크 관리 포함) 및 자원 사용을 주도하고 방향을 제시한다.
 - 조직의 목표와 연계된 계획, 실적 및 예상 결과와 리스크에 대해 지배 기구와 지속적으로 대화하고, 보고한다.
 - 운영 및 리스크의 관리 (내부 통제 포함)를 위해 적절한 구조 및 프로세스를 수립하고 유지한다.
 - 법규 및 윤리적 기대치의 준수를 보장한다.
-

제2 선의 역할

- 다음을 포함하여 리스크 관리와 관련된 보완적 전문성, 지원, 모니터링 및 도전과제를 제공한다:
 - 프로세스, 시스템 및 조직 차원에서 리스크 관리 관행 (내부 통제 포함)의 수립, 구현, 지속적인 개선.
 - 법규 및 허용되는 윤리적 행위 준수, 내부 통제, 정보 기술 보안, 지속가능성, 품질 보증과 같은 리스크 관리의 목표 달성.
- 리스크 관리 (내부 통제 포함)의 적정성 및 효과성에 대해 분석하고 보고한다.

내부 감사

- 지배 기구에 대해 일차적인 책임이 있으며, 경영 책임으로부터 독립성을 유지한다.
- 조직의 목표 달성을 뒷받침하고 지속적인 개선을 촉진 및 장려하기 위해 경영진과 지배 기구에게 거버넌스 및 리스크 관리 (내부 통제 포함)의 적정성과 효과성에 대해 독립적, 객관적 보증과 조언을 전달한다.
- 지배 기구에 독립성 및 객관성의 훼손을 보고하고 필요 시 보호장치를 구현한다.

외부의 보증 제공자

- 다음을 위해 추가적인 보증을 제공한다:
 - 이해당사자의 이익을 보호하기 위해 존재하는 법적, 규제적 기대치 충족.
 - 내부의 보증 제공을 보완하기 위해 경영진 및 지배 기구의 요구사항을 충족.

주요 역할 간의 관계

지배 기구와 경영진 (제 1 선 및 제 2 선 역할)의 관계

통상적으로 지배 기구는 비전, 미션, 가치 및 조직의 리스크 성향을 정의함으로써 조직의 방향을 정한다. 그리고 경영진에게 필요한 자원과 함께, 조직의 목표 달성 책임을 위임한다. 지배 기구는 경영진으로부터 리스크 및 리스크 관리에 대한 보고는 물론 계획, 실적, 예상 결과에 대해 보고를 받는다.

핵심 용어

최고 경영 책임자 (CEO) - 조직에서 경영을 책임지는 가장 높은 직위의 개인.

지배 기구와 경영진 간의 역할이 겹치거나 분리되는 정도는 조직마다 다르다. 지배 기구는 조직의 전략적 운영에 대해 다소 “직접 개입 (hands on)”할 수 있다. 지배 기구나 경영진이 전략 계획 수립을 주도할 수도 있고, 공동의 과제가 될 수도 있다. 일부 사법권에서는, 최고 경영자 (CEO)가 지배 기구의 멤버일 수도 있으며 지배 기구 의장을 맡을 수도 있다. 어떤 경우이건, 경영진과 지배 기구 사이에는 원활한 커뮤니케이션이 필요하다. CEO는 통상적으로 이러한 커뮤니케이션의 구심점인데, 다른 최고 관리자가 지배 기구와의 빈번한 상호작용을 담당할 수도 있다. 조직은 최고 리스크 책임자 (CRO) 및 최고 준법 감시인 (CCO)과 같은 제 2 선 역할의 리더가 지배 기구에 직접 보고하기를 희망하거나, 규제당국에서 그를 요구할 수도 있다. 이는 3 선 모델의 원칙과 전적으로 일치한다.

경영진 (제 1 선 및 제 2 선 역할)과 내부 감사의 관계

경영진으로부터 독립적인 내부 감사는 감사 기획과 감사 업무 수행에 있어 방해 및 편향으로부터 자유로우며, 필요한 인력, 자원, 정보에 대해 제한 없는 액세스를 누림을 보장한다. 내부 감사는 지배 기구에게 책임이 있다. 그러나, 독립성이 단절을 의미하지는 않는다. 내부 감사의 업무가 조직의 전략적, 운영적 니즈와 일치하며 유관함을 보장하기 위해, 내부 감사와 경영진 간의 상호작용은 반드시 정기적으로 실시되어야 한다. 모든 활동을 통해 내부 감사는 조직에 대한 지식과 이해를 축적하고, 이는 신뢰받는 자문인이자 전략적 파트너로서

내부 감사가 전달하는 보증 및 조언에 기여한다. 불필요한 중복, 중첩 또는 차이가 없음을 보장하기 위해, 경영진의 제 1 선 및 제 2 선 역할과 내부 감사 간에 협업과 커뮤니케이션이 필요하다.

내부 감사와 지배 기구의 관계

내부 감사는 지배 기구에게 책임이 있으며, 지배 기구의 “눈과 귀”라고 묘사되기도 한다.

지배 기구는 내부 감사를 감시할 책임이 있는데, 그러기 위해서는 독립적인 내부 감사 기능의 설치 (최고 감사 책임자 (CAE)의 임면 포함) 보장, CAE의 일차적 보고선으로 기능⁴, 감사 계획의 승인 및 자원 할당, CAE의 보고 수신 및

보고 내용 고려, 지배 기구에 대한 CAE의 자유로운 액세스 보장 (경영진이 배척하지 않는 회동 포함)이 필요하다.

핵심 용어

최고 감사 책임자 (CAE) - 조직에서 내부 감사 서비스에 대한 책임이 있는 가장 높은 개인. 내부 감사 부서장 (HOIA) 또는 유사한 직책으로도 알려짐.

전체적인 관계

지배 기구, 경영진 및 내부 감사는 소임이 명백히 다르지만, 모든 활동은 조직의 목표와 일치되어야 한다. 성공적인 일치를 위해서는 정기적, 효과적인 조율, 협업 및 커뮤니케이션이 기본이다.

4. 행정상의 목적으로 CAE는 적절한 고위 경영진에게 보고할 수도 있다.

모델의 적용

구조, 역할 및 책임

3 선 모델은 조직의 목표 및 상황에 맞게 변용될 때 **가장 효과적이다**. 조직의 구조와 역할 분장은 경영진 및 지배 기구의 결정 사항이다. 지배 기구는 위원회를 발족시켜 감사, 리스크, 재무, 기획 및 보상과 같은 특정 영역에 대해 추가적인 감시를 제공하도록 할 수 있다. 조직의 규모와 복잡도가 증가함에 따라, 경영진 내에는 기능적 및 위계적 구조와 업무의 전문화가 발생하기 마련이다.

부문, 팀, 심지어 개인이 제 1 선 및 제 2 선 역할을 모두 포함하는 책임을 맡을 수도 있다. 그러나 제 2 선 역할이 지배 기구에 대해 일차적으로 책임을 지고 보고하도록 함으로써, 제 2 선 업무의 방향 제시와 감시가 제 1 선 역할 담당자 (및 가장 직위가 높은 경영진)로부터 어느 정도의 독립성을 확보하도록 설계될 수도 있다. 3 선 모델은 경영진과 지배 기구 간에 필요한 수만큼 보고선을 허용한다. 일부 조직 (특히 규제가 가장 심한 금융 기관)에서는, 충분한 독립성을 보장하기 위해 그러한 구조를 갖추는 것이 법정 요건이다. 이러한 상황에서조차, 리스크 관리의 책임은 제 1 선 역할을 맡은 경영진에게 있다.

제 2 선 역할은 리스크 관리와 관련된 사안에 대한 모니터링, 조언, 가이드스, 테스트, 분석 및 보고를 포함한다. 이들이 제 1 선 역할을 하는 이들에게 지원 및 도전과제를 제공하고 경영진이 의사를 결정하고 조치를 내리는데 필수적인 한, 제 2 선 역할은 경영진의 책임 중 일부이며 보고선 및 책임성과 무관하게 경영진으로부터 완전히 독립되어 있지 못하다.

제 3 선 역할의 두드러진 특징은 경영진으로부터의 독립성이다. 3 선 모델의 원칙은 내부 감사 독립성의 중요성과 그 성격을 설명하고 있으며, 내부 감사를 다른 부문으로부터 구별하고 보증과 조언이라는 독특한 가치를 가능하게 한다. 내부 감사의 독립성은 경영진 책임 (리스크 관리 포함)의 일부인 의사결정을 내리거나 조치를 취하지 않고, 내부 감사가 현재 또는 과거에 담당했던 활동에 대해 보증을 제공하지 않으므로써 지켜진다. 예를 들어, 일부 조직은 CAE 에게 준법 감시나 ERM 과 같이 유사한 능력을 활용할 수 있는 활동에

대해 추가적인 의사결정 책임을 맡도록 요구하고 있다. 그러한 상황에서, 내부 감사는 해당 활동이나 그 결과에 대해 독립성을 잃게 된다. 따라서 그러한 영역과 관련된 독립적이며 객관적인 보증 및 조언을 지배 기구가 구할 때에는 적격인 제삼자가 제공하도록 해야 한다.

감시 및 보증

이해당사자에게 책임이 있는 조직의 목표 달성과 감시를 위해, 지배 기구는 경영진 (제 1 선 및 제 2 선 역할 담당자로 구성), 내부 감사, 그리고 다른 이들의 보고에 의존한다. 경영진은 직접 경험과 전문성을 이용함으로써 계획, 실적, 전망과 리스크 및 리스크 관리에 대해 가치 있는 보증 (증명이라고도 칭함)을 제공한다. 제 2 선 역할 담당자는 리스크 관련 사안에 대해 추가적인 보증을 제공한다. 내부 감사의 독립성 때문에, 내부 감사가 제공하는 보증은 보고선과 무관하게 제 1 선 및 제 2 선 역할 담당자들이 지배 기구에게 제공할 수 있는 수준을 넘어 최고 수준의 객관성 및 확신을 제공한다. 외부 기관이 추가적인 보증을 제공할 수도 있다.

조율과 방향 일치

효과적인 거버넌스를 위해서는 협력, 협업 및 커뮤니케이션을 통한 견조한 활동 방향 일치는 물론 적절한 책임 분장이 필요하다. 지배 기구는 내부 감사를 통해 거버넌스 구조 및 프로세스가 적절하게 설계되고 의도한 대로 운영되고 있다는 확인을 구한다.

세계내부감사인협회 소개

세계내부감사인협회 (IIA)는 세계적으로 널리 인정받는 표준과 가이드를 주창 및 교육하고, 자격인증을 제공하는 내부 감사직 종사자들의 단체이다. 1941년에 설립된 이래 오늘날 170여개국에서 200,000명 이상의 회원들을 위해 봉사하고 있다. 협회의 글로벌 본부는 미국 플로리다주의 레이크 메리 (Lake Mary)에 위치하고 있다. 보다 자세한 내용은 협회 웹사이트 참조 (www.globaliia.org)

주의

IIA는 정보 및 교육 목적으로 본 문서를 출간하였다. 본 자료는 특정한 개별 상황에 결정적인 답을 제공하지 않으며, 가이드로 사용될 뿐이다. IIA는 특정 상황과 직접적으로 연관된 내용에 대해서는 제삼자의 전문가적 조언을 구할 것을 권고한다. IIA는 본 자료에만 의존하는 이에 대해 어떠한 책임도 지지 않음을 밝힌다.

저작권

Copyright © 2020 The Institute of Internal Auditors, Inc. All rights reserved. 복제 허가는 다음 웹사이트로 연락하기 바람: copyright@theiia.org.

2020년 7월



Global

Global Headquarters

The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 149
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org