

조직 회복탄력성

Topical Requirement

주제별 요건



The Institute of
Internal Auditors



번역

(사)한국감사협회

The Institute of Internal Auditors

Korea

조직 회복탄력성 주제별 요건

(Organizational Resilience Topical Requirement)

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

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

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

내부감사인은 국제내부감사표준에 부합하도록 주제별 요건을 적용해야 한다. 주제별 요건의 준수는 검증(assurance) 서비스에는 필수이며, 자문(advisory) 서비스에는 권장사항이다.

주제별 요건은 해당 주제가 다음에 해당할 때 적용된다:

- 내부감사 계획에 포함된 감사업무 주제
- 감사업무 수행 중 식별된 주제
- 최초 내부감사 계획에 포함되지 않은 요청된 감사업무 주제

모든 개별 요건이 모든 감사업무에 적용되는 것은 아니며, 일부 요건은 다른 접근 방식을 통해 충족될 수 있다. 특정 요건이 제외되거나 다른 규제 또는 계약상 요건에 의해 대체되는 경우, 또는 국제내부감사표준을 준수하는 절차의 이행을 통해 충족되는 경우, 그 근거를 문서화하고 보관해야 한다.

주제별 요건의 준수는 감사품질 평가 시 검토된다.

자세한 내용은 「조직 회복탄력성 주제별 요건 사용자 가이드」를 참조한다.

조직 회복탄력성

국제표준화기구(ISO)는 조직 회복탄력성을 "변화하는 환경에서 조직이 흡수하고 적응하는 능력"으로 정의한다(ISO 22316:2017). 이러한 정의가 명확한 지향점을 제시하지만, 실제로는 조직마다 변화와 중단을 예측하고, 이에 대응하며, 적응하고, 회복하는 방식이 매우 다양하다. 조직 회복탄력성은 전략적, 운영적, 기술적, 인적, 사회적, 재무적 영역을 포괄하기 때문에, 어떤 조직은 변화를 효과적으로 흡수할 수 있는 반면, 다른 조직은 이를 어려워하거나 불확실성에 직면하여 다른 접근 방식을 선택할 수도 있다.

조직 회복탄력성은 조직이 핵심 제품과 서비스를 제공하고, 이해관계자의 신뢰를 유지하며, 전략적 목표를 달성하는 능력을 심각하게 저해하거나 손상시킬 수 있는 리스크를 다루는 포괄적인 개념이다. 이러한 리스크는 돌발 사건(자연재해, 사이버 공격, 지정학적 갈등 등), 장기적 환경 압력(자원 부족, 공중보건 위기 등), 외부 환경의 변화(기술 변화로 인한 중단, 규제 환경의 변화, 그리고 평판의 저하 등)로 인해 발생할 수 있다.

이러한 리스크는 시간이 경과함에 따라 조직의 안정성과 적응 능력을 약화시키는 점진적인 변화나 서서히 누적되는 압박일 수도 있다. 이와 같은 점진적인 리스크는 일상적으로 간과되기 쉽다. 회복탄력성이 있는 조직은 성공을 위해 급격한 리스크와 감지하기 힘든 리스크를 모두 예측하고 이에 적응한다.

회복탄력성에 대한 위협을 증가시키는 고유 리스크 요인에는 고도로 복잡한 운영 구조, 글로벌화된 공급망, 중앙집중화된 인프라 또는 데이터 시스템, 제한적인 인력 가용성, 변동성이 높은 시장 환경, 핵심 제 3자 또는 특정 지역에 대한 높은 의존도가 포함된다. 고신뢰성 산업(High-Reliability Sectors)에 속하거나 강도 높은 규제 감독을 받는 조직은 공공에 미치는 영향과 규정 준수 의무로 인해 본질적으로 더 높은 리스크에 직면할 수 있다.

조직 회복탄력성 장애가 발생하기 전, 발생하는 동안, 그리고 발생한 후의 리스크 관리에 중점을 둔다. 내부감사인은 일반적으로 비즈니스 연속성 및 재해복구와 관련된 정보기술(IT) 프로세스 및 통제를 평가한다. 업무 연속성 계획(Business Continuity Plan, BCP)은 재해가 발생했을 때 조직이 핵심 기능을 유지하고 정상적인 운영 기능으로 복귀하기 위해 취하는 단계를 상세히 기술한다. 재해복구계획(DRP)이란 조직이 업무 중단을 초래하는 사건이 발생한 이후 정상적인 사업 운영을 재개할 수 있도록, IT 시스템·핵심 데이터·운영을 복구하는 방법을 기술한 계획을 말한다.

조직 회복탄력성은 이러한 두 계획을 모두 포함하며, 전략적 계획 수립, 전사적 리스크 관리, 효과적인 리더십과 문화, 조직 전반에 걸친 통제 프로세스가 필요하다. 조직 회복탄력성을 위한 강력한 통제 프로세스를 갖추는 것은 조직이 변화를 지속적으로 예측하고, 대비하며, 대응하고, 적응할 수 있을 뿐만 아니라, 생존하고 번영할 수 있도록 한다.

조직 회복탄력성 거버넌스, 리스크 관리, 통제 프로세스의 평가 및 검토

본 주제별 요건은 조직 회복탄력성의 거버넌스, 리스크 관리, 통제 프로세스의 설계 및 이행을 평가하기 위한 일관되고 포괄적인 접근방식을 제시한다. 이 요건은 조직 회복탄력성을 평가하기 위한 최소한의 기준을 제시한다.

거버넌스

요건

내부감사인은 조직 회복탄력성 거버넌스의 다음 측면들을 평가해야 한다:

- A. 회복탄력성을 다루는 공식적인 조직 전략이 경영진에 의해 수립되고, 이사회에 의해 채택 및 감독되며, 변화를 관리하고 운영을 지속하는 데 필요한 운영적, 기술적, 재무적 요소를 포함한다. 회복탄력성 목표가 조직의 전반적인 리스크 관리 접근 방식과 연계되어 있다.
- B. 회복탄력성 목표의 달성 현황이 검토를 위해 정기적으로 이사회에 보고된다. 이를 통해 회복탄력성이 핵심 사업 활동을 지원하는 데 필요한 자원 및 예산 고려사항을 포함하여, 전략적 감독, 장기 계획 프로세스, 승계 계획 및 조직 문화에 내재되도록 보장한다.
- C. 중요한 운영, 기술, 재무 프로세스에 대한 정책과 절차가 수립되며, 통제 환경을 강화하기 위해 필요에 따라 정기적으로 검토, 테스트, 업데이트된다.
- D. 조직 회복탄력성 목표를 감독하고 지원하기 위한 사고지휘체계(incident command structure, ICS)가 수립되어 운영된다. 이는 의사결정 체계, 커뮤니케이션 및 상향보고 프로토콜, 그리고 리더십 및 운영상의 역할과 책임을 포함한다.
- E. 회복탄력성의 성공에 필요한 역량을 정기적으로 검증하고, 회복탄력성 프로세스에서 중요한 역할을 수행하는 개인의 역량을 재평가하기 위한 프로세스가 수립된다.
- F. 조직 회복탄력성 목표의 달성을 위한 정보 및 보고 체계를 구축하는 과정에서 모든 관련 내부 및 외부 이해관계자가 식별되고, 우선순위가 정해지며, 참여하도록 보장하는 프로세스가 수립된다. 이해관계자에는 최고경영진, 운영(현업) 부서, 리스크 관리 부서, IT 부서, 공급망·조달 부서, 시설 관리 부서, 인사 부서, 재무 부서, 법무 부서, 검증 제공자(내부감사 포함), 컴플라이언스 부서, 홍보 부서, 핵심 공급업체, 고객, 규제기관 등이 포함될 수 있다.



리스크 관리

요건

내부감사인은 조직 회복탄력성 리스크 관리의 다음 측면들을 평가해야 한다:

- A.** 조직 회복탄력성과 관련된 리스크가 조직 전반에 걸쳐 정기적으로 식별, 평가, 관리된다. 회복탄력성 리스크가 조직의 전략적 목표와 매핑된다. 회복탄력성 리스크 관리 프로세스에는 핵심 프로세스에 대한 평가가 포함된다.
- B.** 조직 회복탄력성 리스크 관리에 대한 책무와 책임이 명확하게 정의된다. 지정된 담당자 또는 담당 조직이 조직 회복탄력성 리스크의 관리 상태를 정기적으로 모니터링하고 보고하도록 배정되어 있으며, 여기에는 리스크 완화에 필요한 자원과 조직 회복탄력성에 대해 새롭게 부상하는 위협의 식별이 포함된다
- C.** 조직 회복탄력성 리스크(새롭게 부각되거나 기존에 식별된)의 수준을 모니터링하고, 조직이 수립한 리스크 관리 지침 및 리스크 허용범위 또는 적용 가능한 법적·규제 요건에 따라 수용 불가능한 것으로 간주되는 수준에 도달한 리스크를 신속하게 상향보고하기 위한 프로세스가 수립된다. 조직 회복탄력성 리스크의 영향이 고려된다.
- D.** 경영진은 위기, 중단 및 비상사태 발생에 대응하고 이로부터 회복하기 위한 프로세스를 마련하고 정기적으로 테스트한다. 사고 대응 및 복구 프로세스에는 탐지, 우선순위 지정, 확산 방지, 복구, 사고 후 분석이 포함된다. 사고 대응 접근 방식에는 다양한 중단 사건에 대한 시나리오 분석 및 정기적인 스트레스 테스트가 포함된다.

통제 프로세스

요건

내부감사인은 조직 회복탄력성과 관련된 통제 프로세스의 다음 측면을 평가해야 한다:

- A.** 핵심 제 3 자 제공업체(공급업체 및 벤더)를 식별하고 필수 운영을 유지하는 데 필요한 최소 재고 수준을 결정하는 프로세스가 마련되어 있다. 해당 프로세스에는 대체 공급업체 목록을 최신 상태로 유지하는 것도 포함된다.
- B.** 운영에 핵심적인 데이터가 식별되고 분류되어 있다. 데이터 분류에는 데이터가 어디에 위치하는지, 누가 데이터 접근을 필요로 하는지, 어떻게 접근하는지, 그리고 비상사태 시 백업 및 복구가 가능한지 여부를 식별하는 것이 포함된다.
- C.** 정보보안 리스크(사이버 관련 리스크 포함)를 완화하고 위기, 중단, 비상사태 시 민감한 데이터를 보호하기 위한 핵심 IT 통제와 상시 모니터링 체계가 수립되어 있다. 통제 및 상시 모니터링에는 실시간 위협 인텔리전스 및 인가된 사용자로만 접근을 제한하는 것이 포함된다.
- D.** 핵심 IT 자산이 목록화되어 있다. 자산에는 위기, 중단, 비상사태 시 운영을 지원하는 데 필요한 하드웨어, 소프트웨어, 서비스가 포함된다.



- E. 비즈니스 연속성 계획과 재해복구 계획이 수립되어 있으며, 지정된 인력과 복구팀의 역할이 명확히 정의되어 있다. 해당 계획은 정기적으로 테스트되며(예: 모의훈련(tabletop exercise)), 개선 기회를 포함한 테스트 결과가 이사회와 최고경영진에게 보고된다.
- F. 위기, 운영 차질, 비상사태 시 근무 환경을 조정하기 위한 프로세스가 수립된다.
- G. 조직 회복탄력성에 영향을 미칠 수 있는 새로운 위협과 취약점을 지속적으로 모니터링하고 보고하기 위한 프로세스가 수립되어 있다. 해당 프로세스가 내부고발(whistleblowing) 또는 리스크 인텔리전스 수집 시스템을 포함하여, 조직 회복탄력성 운영을 개선할 수 있는 기회를 식별, 우선순위화, 이행하는 데 활용된다.
- H. 위기, 중단 및 비상사태 발생 시 준수해야 할 정책과 절차 및 취해야 할 조치를 임직원이 숙지할 수 있도록 조직 회복탄력성과 관련된 교육 및 훈련 프로세스가 수립되어 있다. 해당 프로세스에 중단 시나리오를 시뮬레이션하는 모의훈련이 포함되어 있다.
- I. 위기, 중단, 비상사태 시 필요한 운영적, 인적, 기술적, 재무적 자원이 예산에 반영되고 활용 가능하도록 보장하는 프로세스가 수립되어 있다. 조직 회복탄력성을 지원하는 데 필요한 재정적 자원이 정기적으로 분석되고 이사회에 보고된다.
- J. 위기, 중단, 비상사태가 발생한 후 이를 검토하고, 교훈 도출(lessons-learned) 프로세스를 통해 사후 검토 결과를 분석하며, 도출된 교훈을 향후 조직 회복탄력성 계획에 통합하는 것을 포함하는 프로세스가 수립되어 있다.

세계내부감사인협회(The Institute of Internal Auditors, IIA) 소개

세계내부감사인협회(IIA)는 전 세계적으로 265,000 이상의 회원을 보유하고 있으며, 200,000 개 이상의 국제공인내부감사사(CIA®) 자격을 부여한 비영리 국제 전문 협회입니다. 1941년에 설립된 IIA는 전 세계 내부감사 분야의 표준, 자격인증, 교육, 연구 및 기술 지침을 선도하는 기관으로 인정받고 있습니다. 자세한 내용은 theiia.org 에서 확인할 수 있습니다.

저작권

© 2026 세계내부감사인협회(IIA). 판권 소유. 복제를 원하시는 경우 copyright@theiia.org 로 문의하시기 바랍니다.

April 2026



The Institute of
Internal Auditors

Global Headquarters

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

