사이버 보안

Topical Requirement

주제별 요건

The Institute of
Internal Auditors

사이버 보안 주제별 요건

국제내부감사직무수행체계(International Professional Practices Framework®)는 국제내부감사표준(Global Internal Audit Standards™), 주제별 요건(Topical Requirements), 그리고 국제지침(Global Guidance)으로 구성된다. 주제별 요건은 국제내부감사표준과 함께 사용되며, 필수적인 실무 요건을 정하는 권위 있는 기준을 제공한다.

주제별 요건은 특정 리스크 분야를 감사할 때 지켜야 할 최소한의 기준을 정함으로써, 내부감사인이 준수해야 할 최소 기준을 제시한다. 다만, 각 조직의 리스크 프로파일에 따라 내부감사인은 필요에 따라 해당 주제와 관련된 추가적인 요소를 고려해야 할 수도 있다.

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

내부감사인은 국제내부감사표준에 따라 주제별 요건을 적용해야 한다. 주제별 요건의 준수는 검증 서비스에 대해서는 필수 사항이며, 자문 서비스에 대해서는 권장사항이다.

주제별 요건은 주제가 다음에 해당할 때 적용된다:

A. 내부감사 계획에 포함된 감사 주제
B. 감사업무 수행 중 식별된 주제
C. 당초 내부감사 계획에 포함되지 않았으나 요청된 감사 주제

주제별 요건의 각 항목이 해당 감사에 적용 가능한지 평가했다는 증거를 문서화하고 보관해야 한다. 모든 요건이 각 감사에 동일하게 적용되는 것은 아니다. 만약 어떤 요건을 제외한다면, 그 근거를 문서화하여 보관해야 한다. 주제별 요건의 준수는 필수적이며, 이는 감사품질 평가 시 검토 대상이 된다.

자세한 내용은 사이버 보안 주제별 요건 사용자 가이드를 참조한다.

사이버 보안

미국 국립표준기술연구소(NIST)는 사이버 보안을 "사이버 공격으로부터 사이버 공간의 사용을 보호하거나 방어하는 능력"이라고 간결하게 정의한다. 사이버 보안은 전반적인 정보보안의 한 부분이다.

NIST는 정보보안을 "정보와 정보시스템의 기밀성, 무결성, 가용성을 보장하기 위해 허가 받지 않은 접근, 사용, 공개, 중단, 수정, 또는 파괴로부터 이를 보호하는 것"이라고 정의하고 있다.

사이버 보안은 전반적인 통제 환경을 강화하고 조직의 정보자산을 무단 접근, 중단, 변경 또는 파괴로부터 보호함으로써 리스크를 줄인다. 대부분의 조직에서 컴퓨터, 네트워크, 프로그램, 데이터 및 민감정보는 필수적인 요소이므로 사이버 공격은 종종 심각한 직·간접적인 결과를 초래할 수 있다.

사이버 보안 거버넌스, 리스크 관리 및 통제 프로세스 평가 및 검토

이 주제별 요건은 사이버 보안 거버넌스, 리스크 관리 및 통제 프로세스의 설계 및 구현을 평가하기 위한 일관되고 포괄적인 접근 방식을 제공한다. 이 요건은 조직 내 사이버 보안을 평가하기 위한 최소 기준을 제시한다.

거버넌스: 사이버 보안 거버넌스 평가 및 검토

요건:

내부감사인은 조직의 사이버 보안 거버넌스를 평가할 때 다음 사항을 반드시 검토해야 한다:

A. 공식적인 사이버 보안 전략과 목표가 수립되고 정기적으로 업데이트되며, 사이버 보안 전략 지원을 위한 자원 및 예산 고려사항을 포함한 사이버 보안 목표 달성 현황이 이사회에 정기적으로 보고되고 검토된다.

B. 통제 환경 강화를 위한 사이버 보안 관련 정책 및 절차가 수립되고 정기적으로 업데이트된다.

C. 사이버 보안 목표를 지원하는 역할과 책임이 명확하게 설정되어 있으며, 해당 역할을 수행하는 인력의 지식, 기술 및 역량이 정기적으로 평가된다.

D. 사이버 보안 환경에서 기존의 취약점과 새로운 위협을 파악하고 이에 대해 최고경영진, 운영부서, 리스크관리부서, 인사부서, 법무부서, 컴플라이언스부서, 공급업체 등 관련 이해관계자와 논의 및 대응을 위해 협업한다.

리스크 관리: 사이버 보안 리스크 관리 평가 및 검토

요건:

내부감사인은 조직의 사이버 보안 리스크 관리와 관련하여 다음 사항을 반드시 평가하여야 한다:

A. 리스크 평가 및 관리 프로세스가 사이버 보안 위협이 조직의 전략적 목표 달성에 미치는 영향을 식별, 분석, 완화 및 모니터링하도록 운영되고 있다.

B. 사이버 보안 리스크 관리가 조직 전반에서 수행되며, 정보 기술, 전사적 리스크 관리, 인사, 법무, 컴플라이언스, 운영, 공급망, 회계, 재무 등의 영역을 포함한다.

C. 사이버 보안 리스크 관리에 대한 책임과 역할이 명확하게 설정되어 있으며, 리스크를 완화하고 새로운 사이버 보안 위협을 식별하는 데 필요한 자원을 포함하여, 사이버 보안 리스크를 주기적으로 모니터링하고 보고하는 개인 또는 팀이 지정되어 있다.

D. 조직이 수립한 리스크 관리 지침 또는 관련 법률 및 규제 요건에 따라 수용할 수 없는 수준의 사이버 보안 리스크(신규 또는 기존 식별된 리스크)가 발생했을 때, 이를 신속하게 상향보고(escalation)하는 프로세스가 존재하고 효과적으로 운영된다. 또한, 사이버 보안 리스크의 재무적 및 비재무적(예: 평판 리스크) 영향이 고려된다.

E. 경영진과 직원들에게 사이버 보안 리스크에 대한 인식을 제고하기 위한 커뮤니케이션 프로세스가 수립되어 있으며, 경영진이 주기적으로 이슈, 격차, 결함 또는 통제 실패를 검토하여 적시에 보고하고 개선하는 프로세스가 운영된다.

F. 조직의 탐지, 봉쇄, 복구 및 사고 후 분석을 포함한 사이버 보안 사고 대응 및 복구 프로세스가 효과적으로 구현되어 있으며, 해당 프로세스가 정기적으로 테스트되고 있다.

통제: 사이버 보안 통제 프로세스 평가 및 검토

요건:

내부감사인은 조직의 사이버 보안 통제 프로세스와 관련하여 다음 사항을 반드시 평가하여야 한다:

A. 조직의 시스템과 데이터의 기밀성, 무결성, 가용성을 보호하기 위한 내부통제와 공급업체 기반 통제가 수립되어 있으며, 이러한 통제가 조직의 사이버 보안 목표 달성을 촉진하고 문제를 신속히 해결하는 방식으로 운영된다.

B. 사이버 보안 운영 관련 기술 역량을 개발 및 유지하기 위한 교육이 포함된 인재 관리 프로세스가 수립되고 주기적으로 검토된다.

C. 새로운 사이버보안 위협 및 취약점을 지속적으로 모니터링하고 보고하는 프로세스가 수립되어 있으며, 사이버보안 운영을 개선하기 위한 기회가 효과적으로 식별, 우선순위를 지정하고 실행된다.

D. 하드웨어, 소프트웨어, 공급업체 서비스를 포함한 모든 IT 자산의 생애주기 관리(선택, 사용, 유지보수, 폐기) 과정에서 사이버 보안이 효과적으로 반영되고 있다.

E. 보안 설정 구성, 최종 사용자 디바이스 관리, 암호화, 패치, 사용자 접근 관리, 가용성 및 성능 모니터링 등 사이버 보안 촉진을 위한 프로세스가 수립되어 있으며, 이를 효과적으로 운영하고 있는지 평가한다. 또한, 소프트웨어 개발(DevSecOps)에 사이버 보안 고려사항이 포함되어 있다.

F. 네트워크 접근 통제, 세분화, 방화벽 배치, 외부 네트워크 연결 제한, VPN, ZTNA, IoT 네트워크 통제, IDS/IPS 등의 네트워크 보안 통제가 수립되어 운영되고 있다.

G. 이메일, 인터넷 브라우저, 화상회의, 메시징, 소셜 미디어, 클라우드, 파일 공유 프로토콜 등의 서비스에 대한 엔드포인트 통신 보안 통제가 수립되어 있다.

세계내부감사인협회(IIA) 소개

세계내부감사인협회(IIA)는 전 세계적으로 255,000 이상의 회원을 보유하고 있으며, 200,000 개 이상의 국제공인내부감사사(CIA)® 자격을 부여한 비영리 국제 전문 협회이다. 1941 년에 설립된 IIA 는 전 세계 내부감사 분야의 표준, 자격인증, 교육, 연구 및 기술 지침을 선도하는 기관으로 인정받고 있다. 자세한 내용은 www.theiia.org 에서 확인할 수 있다.

저작권

The Institute of Internal Auditors

글로벌 본부
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
전화: +1-407-937-1111
팩스: +1-407-937-1101