사이버 보안

Topical Requirement

주제별 요건 사용자 가이드

The Institute of
Internal Auditors

목차

주제별 요건 개요

국제내부감사직무수행체계(International Professional Practices Framework®)는 국제내부감사표준(Global Internal Audit Standards™), 주제별 요건(Topical Requirements), 그리고 국제지침(Global Guidance)으로 구성된다. 주제별 요건은 필수적인 실무 요건의 권위 있는 기준을 제공하는 국제내부감사표준과 함께 적용해야 한다. 본 가이드 전반에 걸쳐 더 자세한 정보가 필요할 때마다 국제내부감사기준을 참조하도록 안내하고 있다.

주제별 요건은 내부감사인이 주요 리스크 영역을 다루는 방식을 정형화하여, 내부감사직무의 품질과 일관성을 증진한다. 주제별 요건은 기준선을 설정하고 해당 요건과 관련된 검증 서비스를 수행하기 위한 적절한 기준을 제공한다. (표준 13.4 평가 기준). 주제별 요건의 준수는 검증 서비스에서는 필수적이며, 자문 서비스 평가 시는 권장사항이다. 주제별 요건은 감사 업무 수행 시 고려해야 할 모든 잠재적 측면을 다루기 위한 것이 아니라, 해당 주제에 대한 일관되고 신뢰할 수 있는 평가를 가능하게 하는 최소한의 요건을 제공하기 위한 것이다.

주제별 요건은 IIA의 3선 모델(Three Lines Model) 및 국제내부감사표준과 명확하게 연계된다. 거버넌스, 리스크 관리, 그리고 통제 프로세스는 주제별 요구사항의 주요 구성요소이다. 이는 표준 9.1 '거버넌스, 리스크 관리 및 통제 프로세스의 이해'와 일치한다. 3선 모델과 관련하여, 거버넌스는 이사회/지배기구와 연계되고, 리스크 관리는 제2선에 연계되며, 통제 또는 통제 프로세스는 제1선에 연계된다. 경영진이 제1선과 제2선을 모두 대표하지만, 내부감사부서는 독립적이고 객관적인 검증 제공자로서 제3선에 위치하며 이사회/지배기구에 보고한다(원칙 8 이사회의 감독).

적용 가능성, 리스크 및 전문가적 판단

내부감사부서는 주제별 요건이 존재하는 사안에 대해 감사업무를 수행하거나, 다른 감사업무 수행 중 주제별 요건의 일부가 식별되는 경우, 반드시 해당 요건을 준수해야 한다.

국제내부감사표준에 설명된 바와 같이, 리스크 평가는 최고감사책임자의 감사계획 수립에서 중요한 부분이다. 내부감사 계획에 포함할 감사업무를 결정하기 위해서는 조직의 전략, 목표 및 리스크를 최소 연 1회 평가해야 한다(표준 9.4 내부감사 계획). 개별 감사업무를 계획할 때, 내부감사인은 해당 업무와 관련된 리스크를 반드시 평가해야 한다(표준 13.2 감사업무 리스크 평가).

리스크 기반 내부감사 계획 수립 과정에서 특정 주제별 요건의 대상이 식별되어 감사계획에 포함된 경우, 감사업무 수행 시 주제별 요건 상의 요건들을 적용하여 대상을 평가한다. 또한, 내부감사인이 업무 수행 과정에서 주제별 요건과 관련된 요소가 식별되는 경우, 계획에 포함되었는지 여부와 상관없이 해당 감사업무의 일부로 주제별 요건의 적용가능성을 평가해야 한다. 마지막으로, 당초 내부감사 계획에 포함되지 않았으나 특정 주제를 포함하는 감사업무가 요청된 경우, 주제별 요건의 적용 가능성을 반드시 평가해야 한다.

전문가적 판단은 주제별 요건 적용에서 중요한 역할을 한다. 리스크 평가는 최고감사 책임자가 내부감사 계획에 어떤 업무를 포함할지 결정하는 데 핵심적인 역할을 한다. (표준 9.4 내부감사 계획). 또한 내부감사인은 전문가적 판단을 통해 각 업무에서 어떤 측면을 다룰 것인지 결정한다(표준 13.3 감사업무 목표 및 범위, 13.4 평가 기준, 13.6 감사업무 수행 프로그램). 부록 A "실무 적용 예시"는 내부감사인이 주제별 요건의 적용 여부를 판단하는 방식을 설명한다.

주제별 요건의 각 항목이 적용 가능한지 평가했다는 증거를 반드시 보관해야 한다. 여기에는 특정 요건을 제외했을 경우, 그 이유를 설명하는 근거도 포함된다. 주제별 요건의 준수 여부는 표준 14.6 감사업무 문서화에 설명된 대로 감사인의 전문가적 판단에 따라 문서화해야 한다.

사이버 보안 주제별 요건(Cybersecurity Topical Requirement)은 고려해야 할 통제 프로세스의 기준을 제시하지만, 사이버 리스크가 매우 크다고 평가한 조직은 추가적인 측면을 평가해야 할 수 있다.

최고감사책임자가 내부감사부서가 주제별 요건 대상에 대해 감사업무를 수행하는 데 필요한 지식을 갖추지 못했다고 판단하는 경우, 해당 감사업무를 아웃소싱 할 수 있다(표준 3.1 감사역량, 7.2 최고감사책임자의 자격, 10.2 인적자원 관리). 아웃소싱을 한다고 하여 주제별 요건 준수에 대한 내부감사부서의 책임이 면제되는 것은 아니다. 최고감사책임자는 규정 준수에 대한 최종적인 책임을 보유한다. 최고감사책임자는 또한 내부감사자원이 불충분하다고 판단하는 경우, 자원 부족의 영향과 해결방안에 대해 이사회에 보고해야 한다(표준 8.2 감사자원).

수행, 문서화 및 보고

내부감사인은 주제별 요건 적용 시 국제내부감사표준을 준수해야 하며, 영역 V: 내부감사 서비스 수행에 따라 업무를 수행해야 한다. 영역 V의 표준은 감사업무 계획 수립(원칙 13 효과적인 감사계획 수립), 감사업무 수행(원칙 14 감사업무 수행), 감사업무 결과 커뮤니케이션(원칙 15 감사결과 커뮤니케이션 및 조치계획 모니터링)에 대해 설명한다.

주제별 요건의 적용 범위는 감사인의 전문가적 판단에 따라 내부감사계획 또는 업무 수행 문서(working papers)에 문서화할 수 있다. 하나 또는 그 이상의 내부감사업무에서 요건을 다룰 수 있으며, 모든 요건이

적용되지 않을 수도 있다. 주제별 요건의 적용 가능성을 평가했다는 증거를 반드시 보관해야 한다. 이때 특정 요건을 제외했다면 그 이유를 설명하는 근거도 함께 포함해야 한다.

부록 C의 선택적 문서화 툴은 내부감사인이 수행하는 업무를 문서화하고 참조하는 데 사용할 수 있다.

품질 검증

국제내부감사표준에 따르면 최고감사책임자는 내부감사부서의 모든 측면을 포괄하는 감사품질 평가 및 개선 프로그램을 개발, 실행 및 유지해야 한다(표준 8.3 감사품질). 그 결과는 이사회 및 최고경영진을 대상으로 반드시 커뮤니케이션이 되어야 한다. 커뮤니케이션 시 내부감사부서가 국제내부감사표준을 준수하고 성과 목표를 달성했는지 보고해야 한다.

주제별 요건과의 적합성은 품질 평가 시 평가하게 된다. 내부감사인은 품질 검토를 준비하기 위해 부록 C에 제공된 툴을 사용할 수 있다.

사이버 보안

사이버 보안은 모든 조직의 다양한 기술적 측면과 관련된 광범위한 주제이다. 정보기술 외에도, 사이버 보안은 일반적으로 비즈니스 프로세스의 일부이므로, 내부감사인은 감사업무 계획, 범위 선정, 수행 시 사이버 관련 리스크를 평가해야 한다.

미국 상무부 산하 국립표준기술연구소(NIST)는 사이버 보안을 "사이버 공격으로부터 사이버 공간의 사용을 보호하거나 방어하는 능력"으로 정의한다. 사이버 보안 주제별 요건은 조직의 외부 경계에 중점을 둔다. 이 외부 경계는 허가 받지 않은 사용자와 악의적인 사이버 위협으로부터 오는 리스크를 줄이기 위해 조직이 보호하는 영역이다 . 사이버 보안은 포괄적인 정보보안의 일부이며, NIST에서는 "기밀성, 무결성 및 가용성을 제공하기 위해 무단 접근, 사용, 공개, 중단, 수정 또는 파괴로부터 정보 및 정보시스템을 보호하는 것"으로 정의한다.

사이버 보안 주제별 요건에 명시된 요건으로 다음 사항이 있다:

- 거버넌스 - 조직의 목표, 정책 및 절차를 지원하는 명확한 기본 사이버 보안 목표 및 전략
- 리스크 관리 - 사이버 리스크를 즉시 상향보고(escalation)하는 프로세스가 포함된 사이버 위협의 식별, 분석, 관리, 모니터링 프로세스
- 통제 - 사이버 리스크를 줄이기 위해 경영진이 수립하고 정기적으로 평가하는 통제 프로세스

고려사항

내부감사인은 사이버 보안 주제별 요건상의 요건을 평가할 때 다음 고려사항을 활용할 수 있다. 이 고려사항들은 요건들과 연계되어 있으며, 예시적인 성격을 가지고 있지만 반드시 따라야 하는 것은 아니다. 내부감사인들은 평가에 무엇을 포함할지 결정할 때 전문가적 판단에 따라야 한다

거버넌스 고려사항

내부감사인은 거버넌스 프로세스가 사이버 보안 목표에 어떻게 적용되는지 평가하기 위해 다음 사항을 검토할 수 있다:

A. 공식화되고 문서화된 사이버 보안 전략계획 및 목표. 이는 정보보안부서장(예: 최고정보보호책임자(CISO))이 제공한 사이버 보안 업데이트를 이사회가 주기적으로(일반적으로 분기마다) 검토했다는 증거이며, 이러한 증거로 다음 사항이 포함될 수 있다:
   - 전략적 목표의 달성 현황 모니터링
   - 사이버 보안 목표 및 목적을 지원하기 위한 예산 필요성
   - 개선조치 이행 현황을 포함한 리스크 및 내부통제 중점사항
   - 성과 측정을 위한 핵심성과지표(KPIs)
   - 사이버 보안 인력의 채용, 교육, 개발에 필요한 인적자원

B. 사이버 보안 프로세스 관리를 위한 정책, 절차 및 기타 관련 문서. 이 문서에는 다음 사항이 포함된다:
   - 최소 연 1회 검토 및 업데이트되는 정책. 이 정책은 새로운 사이버 리스크 발생 시 더 빈번한 검토와 업데이트가 필요할 수 있다.
   - 정책과 절차가 사이버 보안 운영 지원에 충분한지 판단하는 프로세스
   - 사이버 보안 프로세스 및 내부통제 강화를 위해 광범위하게 채택된 프레임워크(NIST, COBIT 등)

C. 사이버 보안 목표 달성을 지원하는 역할과 책임. 여기에는 사이버보안 부서가 조직 내에서 충분한 가시성을 가진 수준에 보고하여, 조직적 지원을 확보할 수 있는 구조가 포함된다
   - 사이버 보안 역할을 수행하는 인력의 지식, 기술 및 능력을 주기적으로 평가하는 프로세스

D. 최고경영진, 운영부서, 리스크관리부서, 인사부서, 법무부서, 컴플라이언스부서, 공급업체 등 관련 이해관계자와의 협업 증거. 협업에는 기존 및 신규 사이버 리스크와 이미 알려진 잠재적 취약점에 대한 커뮤니케이션이 포함된다. 커뮤니케이션의 증거로는 회의록, 보고서, 이메일 등이 포함될 수 있다.

리스크 관리 고려사항

내부감사인은 사이버 보안 목표에 대한 리스크 관리 프로세스 적용 방식을 평가하기 위해 다음 사항을 검토할 수 있다:

A. 조직의 사이버 보안 리스크 평가 및 관리 방식. 위협과 취약점에 대한 다음 사항을 포함한다:
   - 위협 및 취약점의 최초 식별 및 보고 방식
   - 조직 목표 달성에 미치는 리스크를 평가하는 분석 방법
   - 허용 가능한 수준으로 낮추기 위한 조치계획을 포함한 리스크 완화 방법
   - 위협이 완전히 해결될 때까지 지속적인 보고 계획을 포함한 모니터링 방식

B. 조직이 정보기술(IT), 전사적 리스크 관리(ERM), 인사, 법무, 컴플라이언스, 운영, 회계, 재무 등 다양한 기능 영역에서 사이버 보안 리스크 관리와 관련된 의견을 주기적으로 수집하는 방식. 이를 위해 여러 부서가 참여하는(Cross-functional)사이버보안팀 또는 IT 운영위원회를 활용할 수 있다.

C. 사이버 보안 리스크 관리에 대한 책임과 역할을 개인 또는 팀에 할당하는 방식
   - 책임자(들)는 주기적으로(분기별, 월별 또는 필요 시) 조직 전체에 사이버보안 리스크 현황을 지속적으로 커뮤니케이션해야 한다. 이때 리스크 완화 전략에 필요한 자원에 대한 정보도 포함될 수 있다.

D. 사이버 보안 위협 또는 리스크의 평가, 할당 및 우선순위 지정 방식을 포함한 상향보고(escalation) 프로세스. 검토에는 다음 사항을 식별하는 것이 포함될 수 있다:
   - 조직에서 정의한 리스크 수준(예: 높음, 보통, 낮음)과 각 리스크 수준에 대한 상세 설명 및 각 리스크별 상향보고 절차
   - 현재 식별된 사이버 보안 리스크 목록 및 각 리스크 사건의 완화 상태
   - 적용 법률, 규제 및 컴플라이언스 요건
   - 재무적 및 비재무적(예: 평판) 리스크 영향

E. 사이버 보안 리스크를 경영진과 직원에게 커뮤니케이션하는 방식. 다음 사항을 포함한다:
   - 최소 연 1회 직원 사이버 보안 교육(예: 조직의 인식을 테스트하고 추적하기 위한 불시 피싱 모의 훈련 실시)
   - 기존 사이버 보안 이슈의 개선 현황 업데이트 및 완료 예정일 안내

- 미준수 사항을 모니터링하고, 이사회 및 최고경영진에게 결과 업데이트 안내
- 조직의 리스크 성향 및 리스크 허용범위 변경 시 위협 재평가 절차

F. 조직이 운영하는 사건 대응 및 복구 프로세스. 다음 사항을 포함한다.

- 조직 운영의 변화를 반영하여 검토 및 갱신되는 문서화된 계획. 이 계획에는 다음 사항이 포함되어야 한다.
  - 사건 감지 및 보고 방법
  - 추가 피해 방지를 위해 사건을 억제하는 방법
  - 운영 재개를 위한 복구 및 대응 방법
  - 사고 분석을 통한 교훈 도출 및 유사 사고 재발 방지 방법
- 최소 연 1회 모의훈련(tabletop exercise) 실시 및 최고경영진 및 이해관계자에게 결과 보고. 훈련 결과에 따라 조치계획이 수립될 수 있음

통제 프로세스 고려사항

내부감사인은 사이버 보안 목표 관련 통제 프로세스의 적용 방식을 평가하기 위해 다음 사항을 검토할 수 있다:

A. 효과적인 사이버 보안 내부통제 환경 구축을 위한 경영진의 접근방식. 다음 사항을 포함한다:

- 조직의 리스크 평가 프로세스를 기반으로, 증가된 리스크를 완화하고 민감하고 중요한 데이터(개인정보 및 기밀 데이터 포함)를 보호하는 데 필요한 내부통제를 평가 및 구현
- 주요 사이버 보안 통제 유지에 필요한 자원 요건의 결정
- 통제 환경의 일부로 공급업체 기반 통제를 고려. 이는 비즈니스 관계를 시작하기 전과 유지기간 동안 공급업체의 서비스조직통제(SOC) 보고서를 검토하는 절차 포함
- 사이버 보안 통제가 리스크 완화 및 사이버 보안 목표 달성을 효과적으로 지원하는지 정기적인 테스트 수행
- 내부감사부서 또는 기타 검증 제공자가 수행한 평가(예: 모의 해킹 등)에서 발견된 내부통제 결함을 개선하거나 발견사항을 해결하기 위한 프로세스 수립

B. 조직의 사이버 보안 전문가 채용과 교육을 위한 인재 관리 프로세스. 조직이 사이버 보안 전문가의 역량을 강화하고 기술 지식을 지원하며, 새로운 이슈에 대한 인식 개선을 위한 기회를 식별하는 방식이 포함된다.

- 예: 교육 참여, 지식공유활동 참여, 사이버 관련 자격증 취득을 포함한 전문가 지속교육(CPE)

C. 일상적인 운영에 초점을 맞추어 새로운 사이버 보안 위협과 취약점을 지속적으로 식별, 우선순위 지정, 모니터링하고 보고하는 경영진의 프로세스. 인공지능 활용과 같은 신기술 관련 위협과 취약점 평가를 위한 프로세스 수립 여부 검토가 포함된다.

D. IT 자산의 전체 수명 주기 동안 IT 자산을 관리하고 보호하기 위해 수립된 경영진의 프로세스 및 통제에는 하드웨어, 소프트웨어, 공급업체 서비스의 선택, 사용, 유지보수. 폐기가 포함된다. 하드웨어에는 서버, 네트워크 장비(라우터, 방화벽 등), 데스크톱, 노트북, 휴대전화, 태블릿, 주변장치가 포함된다. 소프트웨어에는 운영체제(Windows 등), 전사적 자원 관리(ERP) 소프트웨어, 애플리케이션, 백신 프로그램 등이 포함된다. 하드웨어 및 소프트웨어 관련 고려사항으로 다음 사항이 포함될 수 있다:

- 조직의 암호화 사용, 바이러스 백신 소프트웨어, 모바일 장치 관리, 복잡한 비밀번호 요건, 인증을 위한 가상 사설망(VPN)/ 제로 트러스트 네트워킹(ZTN) 및 펌웨어의 주기적 업데이트
- 회사에서 발급한 하드웨어가 처음 배포될 때 적절한 보안 설정을 갖추고, 폐기 시에는 올바른 방법으로 처리되도록 보장하는 자산 관리 프로세스.
- 사용자 및 관리자 접근 제한, 암호화 사용 보장, 데이터베이스 백업 및 테스트, 강력한 네트워크 보안 통제를 포함한 데이터베이스 관련 통제
- 시스템 개발 수명 주기(SDLC)에서 사이버 보안 위협 및 취약점이 고려되는 방식
- 개발, 보안 및 운영(DevSecOps)팀이 소프트웨어 개발 프로세스에 사이버 보안을 포함하여 취약점을 사전에 식별하는 데 사용하는 접근 방식

E. 사이버 보안을 강화하기 위해 사용되는 프로세스. 이 프로세스는 다음을 포함한다:

- 사이버 보안 리스크 최소화를 위한 보안 설정 구성
- 모바일 장치 관리(이메일 및 애플리케이션 사용 포함)는 사이버 보안 리스크를 완화하고 사용자의 장치가 손상된 경우 원격으로 관리할 수 있도록 구성
- 저장된 데이터(하드 드라이브 저장 정보 등) 또는 전송 중인 데이터(이메일 등)에 암호화 사용
- 서버 및 소프트웨어(운영체제 등)에 대한 최신 보안 업데이트 적용
- 다중 인증(MFA, Multi-factor authentication), 정기적으로 갱신되는 복잡한 비밀번호가 설정된 고유 사용자 ID 사용 등 사용자 접근 관리
- 가용성 및 자원 활용도의 적정성 확인을 위한 모니터링 통제. 이를 통해 사이버 보안 이슈로 인한 성능 저하 가능성을 검토 및 분석이 가능
- 소프트웨어가 운영 환경으로 이전되기 전에 보안 취약점의 식별 및 해결을 위해 시스템 개발 수명 주기(SDLC)에서 사이버보안을 통합

F. 조직의 네트워크 경계를 보호하는 네트워크 관련 통제 방안들. 여기에는 조직이 다음과 같은 것들을 어떻게 활용하는지가 포함된다:
   - 네트워크 세분화
   - 방화벽
   - 사용자 접근 통제
   - 외부 및 내부 연결 제한
   - 상호 연결된 네트워크에서 사물 인터넷(IoT) 관련 보안 통제
   - 사이버 보안 공격을 예방, 탐지 및 복구하기 위한 침입 탐지/방지 시스템(IDS/IPS)

G. 이메일, 인터넷 브라우저, 화상 회의, 메시징(Zoom, MS Teams 등), 소셜 미디어, 클라우드, 파일 공유 프로토콜과 같은 서비스에 적용되는 엔드포인트(end point) 통신 보안 통제 방안. 이러한 통제에는 특정 파일 확장자(예: .exe 파일) 사용 제한 및 파일 공유를 위한 다중 인증(MFA)이 포함될 수 있다.

부록 A. 실무 적용 예시

다음 예시는 사이버 보안 주제별 요건이 적용될 수 있는 시나리오를 설명한다:

예시 1: 사이버 보안이 내부감사 계획에 포함된 내부감사업무로 식별된 경우

내부감사 부서가 리스크 기반 계획 수립 과정을 완료하고 내부감사 계획에 하나 이상의 사이버보안 관련 감사를 포함시킬 경우, 이러한 감사를 수행할 때는 반드시 주제별 요건을 적용해야 한다. 준수는 내부감사 계획의 하나 또는 여러 감사 업무에 걸쳐 이 요건들을 포함시킴으로써 달성할 수 있다

사이버 보안은 광범위한 주제이며, 주제별 요건의 모든 항목이 모든 감사업무에 적용되는 것은 아니다. 내부감사인이 전문가적 판단을 통해 사이버 보안 주제별 요건 중 일부가 해당 감사업무에 적용되지 않아 제외해야 한다고 판단하는 경우, 내부감사인은 반드시 이 요건을 제외하는 근거를 문서화하여 보관해야 한다. 예를 들어, 내부감사부서가 다양한 사이버 보안 감사 업무를 순환방식으로 수행하거나, 해당 감사업무에서 특정 리스크의 중요성이 낮다고 판단한 경우가 요건의 제외 근거가 될 수 있다.

예시 2: 사이버 보안에 중점을 두지 않은 감사업무 수행 중 사이버 보안 리스크가 식별된 경우

내부감사인은 사이버 보안과 직접적 관련이 없는 프로세스를 평가하는 과정에서 사이버 보안 리스크를 식별할 수 있다. 예를 들어, 내부감사인이 사이버 보안에 중점을 두지 않은 미지급금 처리 프로세스를 평가하는 감사업무를 수행할 때, 업무 계획 수립 시 사이버 보안 리스크를 감사범위로 식별하지 않을 수 있다. 그러나 초기 추적조사를 수행한 후, 내부감사인이 이러한 리스크가 감사범위에 포함되어야 한다고 판단할 수 있다, 예를 들어, 웹 기반의 초기 구매요청서 제출과 관련된 사이버 보안 리스크를 식별할 수 있다(표준 13.2 감사업무 리스크 평가).

관련 리스크가 식별되면 내부감사인은 사이버 보안 주제별 요건을 검토하고 적용 가능한 요건을 결정해야 한다. 이 예시에서는 사이버 보안 거버넌스 프로세스 또는 사이버 보안 리스크 관리 프로세스를 제외할 수 있다. 내부감사인은 사이버 보안 주제별 요건 중 적용을 제외한 요건이 있을 경우 그 근거를 감사조서에 문서화하고, 해당 문서를 보관해야 한다.

예시 3: 당초 내부감사계획에 포함되지 않았던 사이버 보안 감사업무가 요청된 경우

이사회, 경영진 또는 규제기관과 같은 이해관계자는 내부감사인에게 당초 감사계획에 포함되지 않은 사이버 보안 평가를 수행하도록 요청할 수 있다. 예를 들어, 조직이 사이버 공격의 표적이 된 경우, 이사회는 사이버 보안 통제 평가를 위한 내부감사 업무를 요청할 수 있다. 이러한 경우 주제별 요건을 적용하고 평가하며 모든 예외 사항을 문서화해야 한다.

부록 B. 프레임워크 매핑

조직은 COBIT 또는 NIST 등 리스크 관리 및 거버넌스 프레임워크(체계)를 활용하여 자체적인 사이버 보안 노력을 기울일 수 있다. 내부감사인은 이러한 프레임워크를 기반으로 감사 프로그램과 테스트 절차를 이미 개발했을 수 있다. 내부감사인은 적절한 감사 범위를 보장하기 위해 계획된 사이버 보안 통제 테스트를 주제별 요건과 조정해야 한다. 아래 표는 사이버 보안 주제별 요건을 일반적으로 사용되는 세 가지 프레임워크(NIST 사이버 보안 프레임워크 2.0, COBIT 2019, NIST 800-53)와 매핑한 것이다. 이러한 프레임워크들은 무료로 쉽게 이용할 수 있어 매핑 대상으로 선정되었다.

거버넌스 요건 (Governance Requirements)	프레임워크 참조		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
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.	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
B. 통제 환경 강화를 위한 사이버 보안 관련 정책 및 절차가 수립되고 정기적으로 업데이트된다.	GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; I-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11
C. 사이버 보안 목표를 지원하는 역할과 책임이 명확하게 설정되어 있으며, 해당 역할을 수행하는 인력의 지식, 기술 및 역량이 정기적으로 평가된다.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

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.	GV.OC-02; GV.RM-01; GV.RM-05; GV.RM-07; GV.OV-03; GV.SC-03	AC-1; CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02
리스크 관리 요건	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. 리스크 평가 및 관리 프로세스가 사이버 보안 위협이 조직의 전략적 목표 달성에 미치는 영향을 식별, 분석, 완화 및 모니터링하도록 운영되고 있다.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. 사이버 보안 리스크 관리가 조직 전반에서 수행되며, 정보 기술, 전사적 리스크 관리, 인사, 법무, 컴플라이언스, 운영, 공급망, 회계, 재무 등의 영역을 포함한다.	GV.RM-01; GV.RM-05; GV.RR-01; GV.RR-02; GV.OC-03; GV.SC-07	PM-29; AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
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.	GV.RR-01; GV.RR-02; GV.RR-03; GV.0V-01; GV.OV-02; GV.OV-03	PM-9; PM-29	EDM03; APO01; APO10; APO12

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.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. 경영진과 직원에게 사이버 보안 리스크에 대한 인식을 제고하기 위한 커뮤니케이션 프로세스가 수립되어 있으며, 경영진이 주기적으로 이슈, 격차, 결함 또는 통제 실패를 검토하고, 이를 적시에 보고하고 개선하는 프로세스가 운영된다.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. 조직은 사이버 보안 사고에 대한 체계적인 대응 및 복구 절차를 마련하고 있다. 이 절차는 사고 탐지, 피해 확산 방지, 시스템 복구, 사후 분석 단계를 포함하며, 그 효과성을 확인하기 위해 정기적으로 모의 훈련을 실시하고 있다	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07
통제 프로세스 요건	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. 조직의 시스템과 데이터의 기밀성, 무결성, 가용성을 보호하기 위한 내부통제와 공급업체 기반 통제가 수립되어 있으며, 이러한 통제가 조직의 사이버 보안 목표 달성을 촉진하고 문제를 적시에 해결되는지 평가한다.	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01

B. 사이버 보안 운영 관련 기술 역량을 개발 및 유지하기 위한 교육을 포함한 인재 관리 프로세스가 수립되어 있고, 주기적으로 검토된다.	pr.at-01; pr.at-02; gv.rr-03	AT-2; AT-3; IR-2; PM-14	APO07; DSS04
C. 새로운 사이버보안 위협 및 취약점을 지속적으로 모니터링하고 보고하는 프로세스가 수립되어 있으며, 사이버보안 운영을 개선하기 위한 기회가 효과적으로 식별, 우선순위가 지정되고 실행된다.	ID.RA-02, ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. 하드웨어, 소프트웨어, 공급업체 서비스를 포함한 모든 IT 자산의 생애주기 관리(선택, 사용, 유지보수, 폐기) 과정에서 사이버 보안이 효과적으로 반영되고 있다.	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9; CM-7; SC-49; SC-51; CM-2; SA-3; SA-10; SA-15; SA-17; SA-20; AU-6; IR-7	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06
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.	PR.PS-01; PR.PS-06; PR.DS-01; PR.DS-02; PR.PS-05; DE.CM-03	CM-6; SI-2; AC-3; CA-7; SA-4; AC-16; AC-18	BAI10; DSS05; DSS06.03; DSS01.03; MEA01
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.	pr.ir; de.cm-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02

G. 이메일, 인터넷 브라우저, 화상회의, 메시징, 소셜 미디어, 클라우드, 파일 공유 프로토콜과 같은 서비스와 관련하여 엔드포인트 통신 보안 통제가 수립되었다.	PR.DS-01; PR.DS-02; PR.DS-10; PR.IR	AC-2; AC-16; AU-10; CA-3; Si-8; Si-20; SC-8	BAI10

부록 C. 선택적 문서화 툴

내부감사인은 리스크 평가를 기반으로 주제별 요건의 적용 가능성을 판단할 때 전문가적 판단을 내리고, 특정 요건의 제외를 적절히 문서화해야 한다. 주제별 요건은 감사인의 전문가적 판단에 따라 내부감사계획 또는 감사업무 문서에 문서화할 수 있다. 하나 또는 그 이상의 내부감사업무를 통해 요건들을 다룰 수 있으며, 모든 요건이 항상 적용되는 것은 아니다. 아래 양식은 사이버 보안 주제별 요건의 준수 여부를 문서화하기 위한 한 가지 방법을 제시하지만, 이 양식을 반드시 사용해야 하는 것은 아니다.

사이버 보안 - 거버넌스

요건	실행 범위 또는 제외 근거	문서 참조
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 최고 경영진, 운영부서, 리스크관리부서, 인사부서, 법무부서, 컴플라이언스부서, 공급업체 등 관련 이해관계자와 논의 및 대응 협업이 이루어지는지 평가한다.		

사이버 보안 - 리스크 관리

요건	실행 범위 또는 제외 근거	문서 참조
A. 리스크 평가 및 관리 프로세스가 사이버 보안 위협이 조직의 전략적 목표 달성에 미치는 영향을 식별, 분석, 완화 및 모니터링하는지 평가한다.		
B. 사이버 보안 리스크 관리는 조직 전반에서 수행되며, 또한 정보 기술, 전사적 리스크 관리, 인사, 법무, 컴플라이언스, 운영, 공급망, 회계, 재무 등의 영역을 포함할 수도 있다.		
C. 사이버 보안 리스크 관리에 대한 책무성과 책임이 확립된다. 또한, 리스크를 완화하고 신규 사이버 보안 위협을 식별하는 데 필요한 자원을 포함하여, 사이버 보안 리스크가 어떻게 관리되고 있는지를 주기적으로 모니터링하고 보고할 개인 또는 팀이 지정되어 있다.		

요건	실행 범위 또는 제외 근거	문서 참조
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 직원에게 사이버 보안 리스크에 대한 인식을 제고하기 위한 커뮤니케이션 프로세스가 수립되어 있으며, 경영진이 주기적으로 이슈, 격차, 결함 또는 통제 실패를 검토하고, 이를 보고하고 개선하는 프로세스가 운영된다.		
F. 조직에 탐지, 피해확산 방지, 복구 및 사고 후 분석을 포함한 사이버 보안 사고 대응 및 복구 프로세스가 효과적으로 구현되어 있으며, 해당 프로세스가 정기적으로 테스트되고 있다.		

사이버 보안 - 통제 프로세스

요건	실행 범위 또는 제외 근거	문서 참조
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 교육을 포함한 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, 우선순위가 지정되고 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.		

요건	실행 범위 또는 제외 근거	문서 참조
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.		

내부감사기관 소개

국제 내부감사협회(IIA)는 전 세계 255,000명 이상의 회원을 보유하고 있으며 전 세계적으로 200,000명 이상의 공인 내부감사사(CIA®) 자격증을 수여한 국제 전문 협회이다. 1941년에 설립된 The IIA는 표준, 인증, 교육, 연구 및 기술 지침 분야에서 내부감사 업계의 리더로 전 세계적으로 인정받고 있다. 자세한 정보 www.theiia.org.

면책 조항

IIA는 정보 제공 및 교육 목적으로 이 문서를 발행한다. 이 자료는 특정 개별 상황에 대한 명확한 해답을 제공하기 위한 것이 아니므로 참고 자료로만 사용하시기 바랍니다. IIA는 특정 상황과 직접적으로 관련된 독립적인 전문가의 조언을 구할 것을 권장한다. IIA는 이 자료에 전적으로 의존하는 사람에 대해 어떠한 책임도 지지 않다.

저작권

2025년 2월

The Institute of Internal Auditors

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