KAB-SR-ISMS

ISO 27001 정보보안경영시스템 인증스킴 요구사항

Issue 3.1

2024. 08. 28. 발행
2024. 08. 28. 시행

ISO/IEC 27006-1:2024

이 문서는 ISO가 발행하고 IAF가 승인한 ISO/IEC 27006-1:2024 Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 1: General 문서의 요구사항을 변경 없이 반영한 것으로, ISO 27001 정보보안경영시스템 인증서비스를 제공하는 인증기관이 준수하여야 할 인증스킴 요구사항이다.

KAB-SR-ISMS
ISO 27001 정보보안경영시스템 인증스킴 요구사항

목차

0 개요

KAB-R-MSCB 는 경영시스템 심사 및 인증을 제공하는 기관에 대한 요구사항 및 지침을 규정하고 있다. 이러한 기관이 ISO/IEC 27001 에 따른 정보보안경영시스템(ISMS)의 심사 및 인증을 목적으로 KAB-R-MSCB 에 적합함을 인정받으려면, KAB-R-MSCB 에 추가되는 요구사항과 지침이 필요하다. 이러한 사항들을 이 문서에서 제공한다.

이 문서는 ISMS에 대한 심사와 인증을 제공하는 기관에 대한 요구사항을 규정한다. 이 문서는 인증기관으로 칭해지는 이러한 기관에 대한 일반적인 요구사항을 제공한다. 이러한 요구사항에 대한 준수는 인증기관이 적격성을 갖추고, 일관되며, 공평한 방식으로 ISMS 인증을 운영함을 보장하여, 그 결과 국내 및 국제적 차원에서 이러한 기관에 대한 인정(recognition)과 인증의 수용을 촉진하도록 하는데 있다.

이 문서의 내용은 KAB-R-MSCB 의 구조를 따른다.

이 문서에서 다음과 같은 동사형태가 사용된다.
— “하여야 한다(shall)”는 요구사항을 의미한다.
— “하는 것이 좋다/하여야 할 것이다(should)”는 권고사항을 의미한다.
— “해도 된다(may)”는 허용을 의미한다.
— “할 수 있다(can)”는 가능성 또는 능력을 의미한다

1 적용범위

이 문서는 KAB-R-MSCB 에 포함된 요구사항에 추가하여, 정보보안경영시스템(ISMS)에 대한 심사 및 인증을 제공하는 기관에 대한 요구사항을 규정하고 지침을 제공한다.

이 문서에 포함된 요구사항은 적격성과 신뢰성의 측면에서 ISMS 인증기관이 입증한다. 이 문서에 포함된 지침은 ISMS 인증기관 요구사항에 대한 추가적인 해석을 제공한다.

비고 이 문서는 인정, 동등성평가 및 기타 심사프로세스의 기준문서로 활용할 수 있다.

2 인용표준

다음의 표준들은 그 내용의 일부 또는 전체가 이 문서의 필수 요구사항을 구성하는 방식으로 인용되었다. 발행연도가 표시된 표준은 해당 판이 적용된다. 발행연도가 표시되지 않은 표준(모든 수정사항 포함)은 최신판을 적용한다.

KAB-R-MSCB 적합성평가 – 경영시스템 심사 및 인증기관에 대한 요구사항 – 제 1 부: 요구사항
ISO/IEC 27001:2022 정보보안, 사이버보안 및 개인정보 보호 – 보안기술 – 정보보안경영시스템 – 요구사항

3 용어의 정의

이 문서의 목적에 따라 KAB-R-MSCB 와 ISO/IEC 27000 에 주어진 것과 함께, 다음의 용어와 정의를 적용한다.

3.1 인증문서(인증서)
Certification documents

클라이언트의 ISMS 가 시스템에서 요구하는 특정 ISMS 표준 및 모든 부속 문서에 적합함을 나타내는 문서

3.2 통제항목
Control

리스크를 유지 및/또는 수정하는 관리수단

비고 1 통제항목에는 리스크를 유지 및/또는 수정하는 모든 프로세스, 장치, 관행 또는 기타 조건 및/또는 행위를 포함하나 이에 한정되지 않는다.

비고 2 통제항목은 의도된 또는 추정된 수정 효과를 항상 발휘하지 않을 수도 있다.

[출처 : ISO/IEC 27002:2022, 3.1.8]

3.3 외부 상황
External context

조직이 자신의 목적을 달성하고자 하는 외부 환경

비고 1 외부 상황에는 다음이 포함될 수 있다.
- 국제, 국내, 지역 또는 현지 환경에 상관없이 문화적, 사회적, 정치적, 법적, 규제적, 재정적, 기술적, 경제적, 자연적, 경쟁적 환경
- 조직의 목적에 영향을 미치는 핵심 동인 및 동향
- 외부 이해관계자들과의 관계, 그리고 이들의 인식과 가치

[출처 : ISO/IEC 27000:2018, 3.22]

3.4 정보보안
Information security

정보의 기밀성, 무결성, 가용성을 보존하는 것

비고 1 이 밖에도 진본성, 책임추적성, 부인방지, 신뢰성을 비롯해 그 밖의 성질들이 포함될 수도 있다.

[출처 : ISO/IEC 27000:2018, 3.28]

3.5 정보보호 사건
Information security incident

기업 운영을 저해하고 정보보호를 위협할 확률이 상당한, 하나의 혹은 일련의 원치 않은 혹은 예기치 않은 정보보호 이벤트

[출처 : ISO/IEC 27000:2018, 3.31]

3.6 정보시스템
Information system

애플리케이션, 서비스, 정보기술 자산, 또는 그 밖의 정보처리 구성요소

[출처 : ISO/IEC 27000:2018, 3.35]

3.7 내부 상황
Internal context

조직이 자신의 목적을 달성하고자 하는 내부 환경

비고 1 내부 상황에는 다음이 포함될 수 있다.
- 지배구조, 조직의 구조, 역할 및 책임추적성
- 방침, 목적, 그리고 이를 달성하기 위해 시행하고 있는 전략
- 자원과 지식(예: 자본, 시간, 인력, 프로세스, 시스템, 기술)과 관련하여 알려진 능력들
- 정보시스템, 정보흐름, 의사결정 프로세스(공식적 및 비공식적)
- 내부 이해관계자들과의 관계, 그리고 이들의 인식과 가치
- 조직의 문화
- 조직이 채택한 표준, 가이드라인 및 모델
- 계약 관계의 형태와 범위

[출처 : ISO/IEC 27000:2018, 3.38]

3.8 경영시스템
Management system

방침과 목표를 수립하고 그 목표를 달성하기 위한 프로세스를 수립하기 위한, 상호 관련되거나 상호 작용하는 조직 요소의 집합

비고 1 경영시스템은 예를 들면, 품질경영, 재무경영 또는 환경경영 등, 단일 또는 다수의 분야를 다룰 수 있다.

비고 2 경영시스템 요소는 조직의 구조, 역할과 책임, 기획, 운영, 방침, 관행, 규칙, 신념, 목표, 그리고 이들 목표를 달성하기 위한 프로세스 등을 수립한다.

비고 3 경영시스템의 적용범위는 조직 전체, 조직의 특정한, 그리고 파악된 기능. 조직의 특정한, 그리고 파악된 부문, 또는 조직 그룹 전체에 있는 하나 또는 그 이상의 기능을 포함할 수 있다.

비고 4 이 용어와 정의는 **ISO/IEC Directives, Part1** 에 통합된 ISO 부록판의 **부속서 SL** 에 제시된 ISO 경영시스템 표준을 위한 공통 용어와 핵심 정의 중의 하나이다. 본래의 정의에서 **비고 1~비고 3** 이 변경되었다.

[출처 : ISO 9000:2015, 3.5.3]

3.9 조직
Organization

조직의 목표 달성에 대한 책임, 권한 및 관계가 있는 자체의 기능을 가진 사람 또는 사람의 집단

비고 1 조직의 개념은 다음을 포함하나 이에 국한되지 않는다.
개인사업자, 회사, 법인, 상사, 기업, 당국, 파트너십, 자선단체 또는 기구, 혹은 이들이 통합이든 아니든 공적이든 사적이든 이들의 일부 또는 조합

[출처 : ISO/IEC 27000:2018, 3.50]

3.10 리스크
Risk

불확실성이 목표에 미치는 영향

비고 1 영향이란 예상된 것에서 벗어난 것을 말한다. 긍정적 또는 부정적인 것일 수 있다.

비고 2 불확실성은 사건, 사건의 결과 또는 가능성에 대한 이해 또는 지식에 관련된 정보의 부족, 심지어 부분적으로 부족한 상태이다.

비고 3 위험은 잠재 이벤트(**ISO Guide 73:2009, 3.5.1.3**에서 정의됨)와 결과(**ISO Guide 73:2009, 3.6.1.3**에서 정의됨), 또는 이들의 조합으로 언급되는 경우가 많다.

비고 4 리스크는 흔히 (주변환경의 변화를 포함하는) 정보보호 이벤트의 결과와 이와 관련된 발생 가능성(**ISO Guide 73:2009, 3.6.1.1**에서 정의됨)의 조합으로 표현된다.

비고 5 정보보안 경영시스템의 맥락에서, 정보보안 리스크는 정보보안 목표에 대한 불확실성의 영향으로 표현될 수 있다.

비고 6 정보보호 리스크는 위협들이 정보 자산 또는 정보 자산들의 취약점을 악용하여 조직에 위해를 일으킬 잠재성과 관련되어 있다.

[출처 : ISO/IEC 27000:2018, 3.61]

3.11 리스크 분석
Risk analysis

리스크의 성격을 이해하고 리스크 수준을 결정하는 프로세스

비고 1 리스크 분석은 리스크 산정과 리스크 처리에 대한 의사결정의 기초가 된다.

비고 2 리스크 분석에는 리스크 추정이 포함된다.

[출처 : ISO/IEC 27000:2018, 3.63]

3.12 리스크 평가
Risk assessment

리스크 식별, 리스크 분석, 리스크 산정로 이루어진 전체 프로세스

[출처 : ISO/IEC 27000:2018, 3.64]

3.13 리스크 관리
Risk management

리크스에 관하여 조직이 지시하고 통제하는 협조 활동들

[출처 : ISO/IEC 27000:2018, 3.69]

3.14 리스크 처리
Risk treatment

리스크를 수정하는 프로세스

비고 1 리스크 처리에는 다음이 포함될 수 있다.
- 리스크를 일으키는 활동을 시작하지 않거나 지속하지 않기로 결정함으로써 리스크를 회피하는 것.
- 기회를 모색하기 위해 리스크를 받아들이거나 증가시키는 것.
- 리스크 근원을 제거하는 것.
- 가능성을 변화시키는 것.
- 결과를 변화시키는 것.
- 리스크를 다른 당사자(들)과 공유하는 것(계약, 위험재무을 포함한다).
- 정보에 따른 선택을 함으로써 리스크를 유지하는 것.

비고 2 부정적 결과를 다루는 리스크 처리는 “리스크 완화”, “리스크 제거”, “리스크 예방”, “리스크 축소”라고도 한다.

비고 3 리스크 처리는 새로운 리스크를 일으키거나 기존 리스크를 수정할 수 있다.

[출처 : ISO/IEC 27000:2018, 3.72]

3.15 규칙
Rule

완료되어야 할 것, 허용되는 것 또는 허용되지 않는 것에 대한 조직의 기대를 기술하는 용인된 원칙 또는 설명

[출처 : ISO/IEC 27002:2022, 3.1.32 – 수정됨. 비고 1 삭제]

4 원칙

KAB-R-MSCB, 4 절의 원칙을 적용한다.

5 일반 요구사항

5.1 법규 및 규제 요구사항

KAB-R-MSCB, 5.1 의 요구사항을 적용하여야 한다.

5.2 공평성 관리

5.2.1 일반사항

KAB-R-MSCB, 5.2 의 요구사항을 적용하여야 한다. 추가로 5.2.2 의 요구사항과 지침을 적용하여야 한다.

5.2.2 이해상충

인증기관은, 자문으로 간주되거나 잠재적인 이해상충을 가지지 않고, 인증심사 및 사후방문 활동을 통한 부가적인 가치를 제공하는 행위, 예를 들어, 심사시간 동안 개선의 기회가 명확한 경우, 특정한 해결책을 권고하지 않는 한도 내에서 개선사항의 식별·제공할 수도 있을 것이다.

인증기관은 클라이언트의 인증에 영향을 미치는 클라이언트의 내부적인 ISMS 에 대한 검토를 제공해서는 안 된다. 더욱이, 인증기관은 내부심사를 제공하는 기관 또는 기관들(모든 개인 포함)로부터 독립적이어야 한다.

5.3 배상책임 및 재정

KAB-R-MSCB, 5.3 의 요구사항을 적용하여야 한다.

6 조직구조 요구사항

KAB-R-MSCB, 6 절의 요구사항을 적용한다.

7 자원 요구사항

7.1 인원의 적격성

7.1.1 일반사항

KAB-R-MSCB, 7.1 의 요구사항을 적용하여야 한다. 추가로 7.1.2 및 7.1.3 의 요구사항과 지침을 적용하여야 한다.

7.1.2 일반적 적격성 요구사항

인증기관은 KAB-R-MSCB, 표 A.1 에 인용된 인증업무기능에 필요한 적격성 요구사항을 결정해야 한다. 인증기관은 인증기관이 결정한 ISMS 기술분야와 관련하여 KAB-R-MSCB 및 이 문서의 7.1.3 과 7.2.2 에 규정된 모든 요구사항들을 고려하여야 한다.

인증기관은 부속서 A 에서의 특정 기능에 요구되는 지식 및 스킬을 결정해야 한다.

적격성 요구사항을 포함하는 추가적인 특정 요구사항이 특정 표준(예: ISO/IEC 27006-2)에서 수립되었다면, 이를 적용하여야 한다.

7.1.3 적격성기준의 결정

7.1.3.1 ISMS 심사를 위한 적격성 요구사항

7.1.3.1.1 일반 요구사항

인증기관은 심사팀 멤버들이 최소한 다음의 지식을 적용하는 스킬을 보유함을 보장할 수 있도록, 심사팀 멤버들에 대한 적격성을 검증하기 위한 기준을 보유하여야 한다.

a) 정보보안
b) 심사대상활동에 대한 기술적 측면
c) 경영시스템
d) 심사원칙

비고 심사원칙에 대한 추가적 정보는 ISO 19011 에서 찾을 수 있다.

e) ISMS 모니터링, 측정, 분석 및 평가

a)부터 e)의 요구사항들은 심사팀을 구성하는 모든 심사원에게 적용된다. 그러나 b)는 심사팀을 구성하는 심사원들 간 공유할 수 있다.

심사팀 멤버들은 총체적으로 위 요구사항에 적절한 스킬을 보유하여야 하며, 이는 적용된 경험을 통해 입증될 수 있다.

심사팀 멤버들은 클라이언트의 ISMS 에 대한 보안사고의 징후를 적절한 ISMS 요소로 추적할 수 있는 적격성을 총체적으로 갖추고 있어야 한다. 개별 심사원은 정보보안의 모든 분야에 대한 완벽한 경험이 요구되지 않는다. 그러나 심사팀 전체적으로는 심사되는 ISMS 범위를 다루기 위해 적절한 적격성을 보유하여야 한다.

7.1.3.1.2 정보보안경영 용어, 원칙, 실행 및 기술

ISMS 심사팀의 개별 심사원은 다음의 지식을 보유해야 한다.

a) ISMS 특정 문서의 구조, 체계, 상호 연관성
b) 정보보안 리스크평가 및 리스크관리
c) ISMS 에 적용 가능한 프로세스

총체적으로, 심사팀은 다음의 지식을 보유해야 한다.

d) 정보보안경영과 관련된 도구, 방법, 기술 및 그 적용
e) 정보보안과 관련된 최신기술 또는 이슈사항

7.1.3.1.3 정보보안경영시스템 표준 및 참조문서

ISMS 심사팀의 각각의 심사원은 **ISO/IEC 27001** 의 모든 요구사항에 대한 지식을 보유하여야 한다.

총체적으로, 심사팀은 **ISO/IEC 27001 부속서 A** 에 포함된 모든 통제항목 및 구현에 대한 지식을 보유하여야 한다.

7.1.3.1.4 비즈니스경영 관행

ISMS 심사팀의 개별 심사원은 다음의 지식을 보유하여야 한다.

a) 산업 정보보안의 모범적 수행 및 정보보안 절차
b) 정보보안을 위한 방침 및 비즈니스 요구사항
c) 일반적 비즈니스경영 개념, 실행과 방침, 목표 및 결과 간의 상호 관련성
d) 경영프로세스 및 관련 용어

비고 이 프로세스들은 또한 인적자원 관리, 내·외부적 의사소통 및 기타 관련 지원 프로세스를 포함한다.

7.1.3.1.5 클라이언트 비즈니스 분야

ISMS 심사팀의 개별 심사원은 다음의 지식을 가지고 있어야 한다.

a) 특정 정보보안 분야, 지리적 및 지역 내에서의 법적 및 규제적 요구사항

비고 법적 및 규제적 요구사항에 대한 지식은 전문 법률 배경지식을 의미하지 않는다.

b) 비즈니스 분야와 관련된 정보보안 리스크
c) 클라이언트 비즈니스 분야와 관련된 일반적 용어, 프로세스 및 기술
d) 관련 비즈니스 분야 관행

기준 **a)**는 심사팀 간 공유될 수 있다.

7.1.3.1.6 클라이언트 제품, 프로세스 및 조직

총체적으로, ISMS 심사팀 멤버는 다음의 지식을 보유하여야 한다.

a) 아웃소싱을 포함하는 ISMS 의 개발, 이행 및 인증활동에 대하여 조직의 유형, 크기, 관리체계, 구조, 기능 및 관계가 미치는 영향
b) 폭 넓은 관점에서의 복합적 운영
c) 제품 또는 서비스에 대하여 적용 가능한 법적 및 규제적 요구사항

7.1.3.2 신청서 검토를 수행하기 위한 적격성 요구사항

7.1.3.2.1 클라이언트 비즈니스 분야

심사팀에 요구되는 적격성, 심사팀원 선정 및 심사시간 결정을 위해 신청서 검토를 수행하는 인원은 클라이언트 업무분야와 관련된 포괄적 용어, 프로세스, 기술 및 리스크에 대한 지식을 보유하여야 한다.

7.1.3.2.2 클라이언트의 제품, 프로세스 및 조직

심사팀에 요구되는 적격성, 심사팀원 선정 및 심사시간 결정을 위해 신청서 검토를 수행하는 인원은 외부에서 제공되는 기능을 포함하는 고객 제품, 프로세스, 조직 유형, 규모, 거버넌스, 구조, 기능 및 관계가 ISMS 의 개발과 실행 및 인증 활동에 미치는 영향에 대한 지식을 보유해야 한다.

7.1.3.3 심사보고서 검토 및 인증결정을 위한 적격성 요구사항

7.1.3.3.1 일반사항

심사보고서를 검토하고 인증결정을 수행하는 인원은 인증범위의 적절성뿐만 아니라, 인증범위 변경 및 이에 따른 심사의 효과성에 미치는 영향을 검증할 수 있는 지식, 특히 인터페이스 및 독립성, 식별의 지속적 유효성과 관련된 리스크를 검증할 수 있는 지식을 가져야 한다. 추가로, 심사보고서를 검토하고 인증을 결정하는 인원은 다음의 지식을 보유하여야 한다.

a) 일반적 경영시스템
b) 심사 프로세스 및 절차

7.1.3.3.2 정보보안경영 용어, 원칙, 실행 및 기술

심사보고서를 검토하고 인증을 결정하는 인원은 다음의 지식을 보유하여야 한다.

a) 7.1.3.1.2 a), b) 및 c)의 항목들
b) 정보보안 관련 법적 및 규제적 요구사항

7.1.3.3.3 클라이언트 비즈니스 분야

심사보고서를 검토하고 인증을 결정하는 인원은 관련 비즈니스 분야 관행과 관련된 일반적 용어 및 리스크에 대한 지식을 보유하여야 한다.

7.1.3.3.4 클라이언트 제품, 프로세스, 조직

심사보고서를 검토하고 인증을 결정하는 인원은 클라이언트 제품, 프로세스, 조직 유형, 규모, 관리체계, 구조, 기능 및 관계에 대한 지식을 보유하여야 한다.

7.2 인증 활동에 관련된 인원

7.2.1 일반사항

KAB-R-MSCB, 7.2 의 요구사항을 적용하여야 한다. 추가로 7.2.2 의 요구사항과 지침을 적용하여야 한다.

7.2.2 심사원 지식 및 경험의 입증

7.2.2.1 일반 고려사항

인증기관은 다음을 통해 심사원의 지식 및 경험을 실증하여야 한다.

a) 인정된 ISMS 의 특정 자격사항
b) 해당되는 경우, 심사원 등록

c) ISMS 교육 훈련과정 참여 및 관련 개인 자격증 취득
d) 전문성 개발 기록의 최신화
e) 다른 ISMS 심사원 입회를 통한 ISMS 심사

7.2.2.2 심사원 선정

7.1.3.1 의 요구사항에 추가하여, 심사원을 선정하는 프로세스는 각 심사원에 대하여 다음 사항을 보장하여야 한다.

a) 대학교육 수준에 상응하는 전문적 지식 및 교육훈련
b) ISMS 심사원으로 심사를 수행하기에 충분한, 정보기술 및 정보보안 분야에서 근무한 업무경험
c) ISMS 심사와 관련한 충분한 교육을 이수하고, **ISO/IEC 27001** 에 따라 심사 스킬을 입증. 심사경험은 최소한 1 회의 ISMS 최초 인증심사(1 단계와 2 단계) 또는 갱신심사 및 최소 1 회의 사후관리 심사에서 ISMS 평가자의 모니터링 하에 심사훈련(**KAB-R-MSCB**, **9.2.2.1.4** 참조)을 수행함으로써 얻어야 한다. 심사경험은 최근 5 년 동안 수행한 최소 10 일간의 ISMS 현장심사를 통해 얻어야 한다. 이 참여에는 문서검토와 리스크 평가, 평가 실행에 대한 검토 및 심사보고를 포함해야 한다.
d) 정보보안 및 심사에 대한 관련성 있는 최신 ISMS 지식 및 스킬 유지

비고 1 스킬 유지는 지속적 전문성 개발을 통해 입증될 수 있다.

비고 2 인증기관은 상기 요구사항과 증거를 일치시키기 위한 적격성 기준 목록이 필요하다

7.2.2.3 기술전문가 선정

기술 전문가를 선정하는 프로세스는 각 기술전문가에 대하여 다음 사항을 보장하여야 한다.

a) 대학교육 수준에 상응하는 전문적 지식 및 교육훈련
b) 기술 전문가로서 활동하기에 충분한, 정보기술 및 정보보안 분야에서 근무한 업무경험
c) 정보보안 및 심사에 대한 관련성 있는 최신 지식 및 스킬 유지

비고 스킬 유지는 지속적 전문성 개발을 통해 입증될 수 있다.

7.2.2.4 심사팀장 선정

7.2.2.2 에 추가로, 심사팀장 선정 기준은 해당 심사원에 대하여 적어도 3 회 이상 ISMS 심사의 모든 단계에 적극적으로 참여하였으며, 참여과정에는 최초 인증범위 결정 및 계획수립, 문서검토 및 리스크평가, 이행평가 및 공식 심사보고서 작성이 포함되어야 함을 보장하여야 한다.

7.3 개별 외부 심사원 및 외부 기술전문가의 활용

KAB-R-MSCB, 7.3 의 요구사항을 적용하여야 한다.

7.4 인원에 대한 기록

KAB-R-MSCB, 7.4 의 요구사항을 적용하여야 한다.

7.5 외주처리

KAB-R-MSCB, 7.5 의 요구사항을 적용하여야 한다.

8 정보 요구사항

8.1 공개 정보

KAB-R-MSCB, 8.1의 요구사항을 적용하여야 한다.

8.2 인증문서

8.2.1 일반사항

KAB-R-MSCB, 8.2 의 요구사항을 적용하여야 한다. 추가로 8.2.2 및 8.2.3 의 요구사항과 지침을 적용하여야 한다.

8.2.2 ISMS 인증문서

인증문서는 해당 권한이 있는 자의 서명이 있어야 한다. 인증서는 적용성 보고서의 해당 버전을 포함해야 한다.

비고 인증범위의 통제항목의 범위가 변경되지 않은 적용성 보고서 변경은 인증문서에 대한 업데이트를 요구하지 않는다.

인증범위 내의 조직의 활동 전체가 정해진 물리적 장소에서 수행되지 않는 경우, 인증문서는 조직의 활동이 원격으로 수행됨을 기술하여야 한다.

8.2.3 ISMS 인증문서 내의 타 표준의 참조

인증문서에서 국가 및 국제 표준은 다음의 조건 하에서만 참조할 수 있을 것이다.

a) 조직이 ISO/IEC 27001:2022, 6.1.3 c)에 따라 참조 통제가 부주의하게 누락되지 않았음을 알아내기 위해 참조 통제 출처에서 필요한 통제 전부를 비교함
b) 제외된 참조 통제에 대한 정당성이 ISO/IEC 27001:2022, 6.1.3 d)에 따라 적용성보고서에 기술됨

참조 통제 표준은 ISO/IEC 27001:2022 부속서 A 를 근거로 하거나, 정보보안 통제를 포함한 표준일 수 있다.

인증문서는 적용성보고서에 적용된 통제집합이 ISMS 통제의 추가 또는 제외에 대한 관련성을 언급하기 위해서만 사용되었고, 적합성평가를 위해 사용되지 않았음을 기술하여야 한다.

8.3 인증에 대한 언급 및 마크의 사용

KAB-R-MSCB, 8.3의 요구사항을 적용하여야 한다.

8.4 기밀성

8.4.1 KAB-R-MSCB, 8.4의 요구사항을 적용하여야 한다. 추가로 8.4.2의 요구사항과 지침을 적용하여야 한다.

8.4.2 조직의 기록에 대한 접근

ISMS 관련 정보가(예를 들어 ISMS 기록 또는 통제의 설계 및 효과성 관련 정보) 기밀 또는 민감한 정보를 포함하고 있어 심사팀 검토가 가능하지 않다면 인증심사 전에 인증기관은 이러한 사항을 보고하도록 클라이언트에게 요구하여야 한다. 인증기관은 이러한 기록의 부재 상태에서도 ISMS 가 적절하게 심사될 수 있는지를 결정하여야 한다. 인증기관에서 확인된 기밀 정보 또는 민감한 정보에 대한 검토 없이는 ISMS 심사가 적절하지 않다고 결정되었다면, 인증기관은 클라이언트에게 인증심사가 수행될 수 없음을 통지해야 한다.

8.5 인증기관과 클라이언트간의 정보 교환

KAB-R-MSCB, 8.5의 요구사항을 적용하여야 한다.

9 프로세스 요구사항

9.1 인증 이전의 활동

9.1.1 신청

9.1.1.1 일반사항

KAB-R-MSCB, 9.1.1의 요구사항을 적용하여야 한다. 추가로 **9.1.1.2**의 요구사항과 지침을 적용하여야 한다.

9.1.1.2 인증절차에 대한 고려사항

인증기관의 절차는 ISMS 이행에 대한 특정방법 또는 문서 및 기록에 대한 특정서식을 전제로 하여서는 안 된다. 인증절차는 클라이언트의 ISMS 가 **ISO/IEC 27001** 에 규정된 요구사항과 클라이언트의 방침 및 목표를 충족하고 있음을 확인하는데 초점을 맞추어야 한다.

비고 조직이 자체적으로 필요한 통제를 설계하고, 특정 출처에서 통제를 선정하는 것이 가능하다. 그러므로 필요한 통제가 **ISO/IEC 27001:2022 부속서 A** 에 명시되어 있는 통제항목에 명시되지 않음에도 불구하고, **ISO/IEC 27001** 인증을 받는 것이 가능하다.

9.1.2 신청서 검토

KAB-R-MSCB, 9.1.2의 요구사항을 적용하여야 한다.

9.1.3 심사 프로그램

9.1.3.1 일반사항

KAB-R-MSCB, 9.1.3 의 요구사항을 적용하여야 한다. 추가로 **9.1.3.2**, **9.1.3.3**, **9.1.3.4**, **9.1.3.5** 및 **9.1.3.6**의 요구사항과 지침을 적용하여야 한다.

9.1.3.2 일반 고려사항

ISMS 심사를 위한 심사 프로그램은 클라이언트가 결정한 정보보안 통제항목을 고려해야 한다.

비고 1 정보보안 통제항목은 **ISO/IEC 27001:2022 부속서 A** 및/또는 기타 적용가능한 표준을 출처로, 및/또는 자체 설계로 할 수 있다.

비고 2 심사에 관한 자세한 지침은 **ISO/IEC 27007** 참조

9.1.3.3 원격심사의 사용

원격심사 활동을 수행하고자 하는 인증기관은 클라이언트의 ISMS 심사에 적용될 수 있는 원격심사 활동("원격심사")의 수준을 결정하는 절차를 규정하여야 한다. 절차는 클라이언트에 대한 원격심사 사용과 관련한 리스크 분석을 포함하여야 하고, 다음의 요소를 고려하여야 한다.

a) 인증기관 및 클라이언트의 사용 가능한 기반구조(infrastructure)
b) 클라이언트가 운영하고 있는 분야
c) 최초심사부터 갱신심사까지 인증주기 동안의 심사 유형
d) 원격심사에 관여하는 인증기관 및 클라이언트 인원의 적격성
e) 기존에 입증된 클라이언트에 대한 원격심사 성과
f) 인증범위

리스크 분석은 원격심사 수행 전에 이루어져야 한다. 인증주기 동안의 원격심사 사용에 대한 분석 및 정당성은 문서화되어야 한다.

심사 프로세스의 효과성에 대한 수용 불가능한 리스크가 리스크 평가에서 식별된 경우 원격심사를 사용하여서는 안 된다.

리스크 평가는 지속적인 적절성을 보장하기 위하여 인증주기 동안 검토되어야 한다.

비고 클라이언트가 가상사업장을 운영하는 경우(예: 조직의 인원이 물리적 위치에 관계없이 프로세스를 수행하는 것을 허용하는 온라인 환경을 활용하여, 업무를 수행하고 서비스를 제공하는 위치), 원격심사 기술은 심사 계획의 적절한 부분이다.

9.1.3.4 최초심사를 위한 일반적 준비사항

인증기관은 클라이언트에게 내부심사 보고서 및 정보보안에 대한 독립적 검토 보고서에의 접근을 보장하기 위해 모든 필요사항을 갖추도록 요청해야 한다.

9.1.3.5 검토기간

인증기관은 적어도 인증범위를 포함하는 경영검토 및 ISMS 내부심사가 수행되었고, 효과적이며, 유지될 것을 입증하는 충분한 증거가 없다면 ISMS 를 인증해서는 안 된다.

9.1.3.6 ISMS 인증범위

심사팀은 적용 가능한 모든 인증 요구사항에 대해 규정된 인증범위를 포함한 클라이언트의 ISMS 를 심사해야 한다. 인증기관은 클라이언트가 ISMS 인증범위 내에서 **ISO/IEC 27001:2022, 4.3** 에 언급된 요구사항을 다루는지를 확인해봐야 한다.

인증기관은 클라이언트의 정보보안 리스크평가 및 리스크 처리가 클라이언트의 활동을 적절히 반영하고 인증범위에서 규정된 활동경계까지 확대되었음을 보장하여야 한다. 인증기관은 동 사항이 클라이언트의 ISMS 인증범위 및 적용성 보고서에 반영되었음을 확인하여야 한다. 인증기관은 인증범위당 최소 하나의 적용성 보고서가 있음을 확인해야 한다. 인증기관은 ISMS 범위 내에 완전히 포함되지 않은 서비스 또는 활동과의 인터페이스가 인증 대상의 ISMS 내에서 다루어 지고 클라이언트 정보보안 리스크평가에 포함됨을 보장하여야 한다. 이러한 상황의 예로는 타 조직과의 설비(예: IT 시스템, 데이터베이스 및 통신 시스템 또는 비즈니스 기능의 아웃소싱)의 공유가 있다.

9.1.4 심사시간 결정

9.1.4.1 일반사항

KAB-R-MSCB, 9.1.4의 요구사항을 적용하여야 한다. 추가로 **9.1.4.2**의 요구사항과 지침을 적용하여야 한다.

9.1.4.2 심사시간

심사시간 결정을 위해 인증기관은 **부속서 C**를 사용하여야 한다.

비고 심사시간 계산에 대한 추가적인 지침 및 사례는 **부속서 D**에서 제공한다.

9.1.5 복수사업장 샘플링

9.1.5.1 일반사항

KAB-R-MSCB, 9.1.5의 요구사항을 적용하여야 한다. 추가로 **9.1.5.2**의 요구사항과 지침을 적용하여야 한다.

9.1.5.2 복수사업장

9.1.5.2.1 클라이언트가 아래 **a)**부터 **c)**까지의 기준을 충족하는 다수의 사업장을 가지고 있을 경우, 인증기관은 복수사업장 인증심사를 위해 표본추출에 근거한 접근방법 사용을 고려해야 한다.

a) 모든 사업장이 동일한 ISMS 하에서 운영된다. 그러한 ISMS 는 본사에서 관리되고 심사되며, 본사의 경영검토를 필요로 한다.
b) 모든 사업장이 클라이언트의 내부 ISMS 심사 프로그램에 포함되어 있다.
c) 모든 사업장이 클라이언트의 ISMS 경영검토 프로그램에 포함되어 있다.

9.1.5.2.2 표본추출에 근거한 접근방법을 사용하고자 하는 인증기관은 다음을 보장하기 위한 절차를 보유하여야 한다.

a) 초기 계약검토에서 적절한 샘플링 수준을 결정하기 위해 최대한 사업장 간의 차이를 식별한다.
b) 다음 사항을 고려하여 인증기관은 전체 사업장 수를 대표할 수 있는 표본의 수를 추출한다.
   1) (적절한 경우) 중앙사무소 및 사업장에 대한 내부심사 결과
   2) 경영검토 결과
   3) 사업장 규모의 다양성
   4) 사업장 사업목적의 다양성
   5) 각 사업장들의 정보시스템 복잡성
   6) 업무실행의 다양성
   7) 수행활동의 다양성
   8) 통제항목의 설계 및 운영의 다양성
   9) 주요 정보시스템 또는 민감한 정보를 처리하는 정보시스템과의 잠재적 상호작용
   10) 상이한 법적 요구사항
   11) 지리 및 문화적 측면
   12) 사업장의 리스크 상황
   13) 특정 사업장의 정보보안사고
c) 대표적인 표본이 클라이언트의 ISMS 범위 내에 포함된 모든 사업장에서 선택되어야 한다. 이 선택은 상기 **b)**에서 기술된 사항뿐만 아니라 랜덤 요소를 반영하는 결정적 선택에 근거하여야 한다.
d) 인증기관은 중대한 리스크에 영향 받기 쉬운 ISMS 범위에 포함된 모든 사업장을 인증 전에 심사해야 한다.
e) 심사 프로그램은 상기 요구사항을 고려하여 설계되어야 하고, 3 년 내에 해당 ISMS 인증범위에 대한 대표적 표본을 다루어야 한다.
f) 단일 사업장에서 부적합이 발견되었을 경우, 시정조치 절차는 본사 및 인증서에 포함된 모든 사업장에 적용한다.

동일한 ISMS 가 모든 사업장에 적용되며 운영수준을 중앙에서 관리함을 보장하기 위해, 심사는 클라이언트의 활동을 다루어야 한다. 심사는 위에 기술된 모든 사항을 다루어야 한다.

9.1.6 복수의 경영시스템 표준

9.1.6.1 일반사항

KAB-R-MSCB, 9.1.6 의 요구사항을 적용하여야 한다. 추가로 **9.1.6.2** 및 **9.1.6.3** 의 요구사항과 지침을 적용하여야 한다.

9.1.6.2 ISMS 와 다른 경영시스템과 문서와의 통합

다른 시스템과의 적절한 상호작용과 함께 ISMS 가 명확히 식별된다면 인증기관은 통합된 문서(예: 정보보안, 품질, 보건안전 및 환경)를 수용할 수 있다.

9.1.6.3 통합경영시스템의 심사

ISMS 심사는 기타 경영시스템 심사와 통합될 수 있으며, 이러한 통합은 ISMS 인증을 위한 모든 요구사항에 심사가 적합하다는 것을 입증함으로써 가능하다. ISMS 에 중요한 모든 요소들은 심사보고서에 명확히 나타나야 하며, 쉽게 식별이 가능하여야 한다. 심사의 품질은 통합심사에 의해 부정적 영향을 받지 말아야 한다.

9.2 심사계획

9.2.1 심사 목적, 범위 및 기준의 결정

9.2.1.1 일반사항

KAB-R-MSCB, 9.2.1 의 요구사항을 적용하여야 한다. 추가로 **9.2.1.2** 및 **9.2.1.3** 의 요구사항과 지침을 적용하여야 한다.

9.2.1.2 심사 목적

심사 목적에는 다음이 포함되어야 한다.

a) 경영시스템의 효과성에 대한 결정
b) 클라이언트가 리스크 평가를 기반으로 필요한 통제항목을 식별함을 보장
c) 수립된 정보보안 목적을 달성하였음에 대한 결정

9.2.1.3 심사기준

클라이언트 ISMS 심사 기준에는 **ISO/IEC 27001** 을 포함하여야 한다.

9.2.2 심사팀 선정 및 배정

9.2.2.1 일반사항

KAB-R-MSCB, 9.2.2 의 요구사항을 적용하여야 한다.

9.2.3 심사계획

9.2.3.1 일반사항

KAB-R-MSCB, 9.2.3 의 요구사항을 적용하여야 한다. 추가로 **9.2.3.2** 및 **9.2.3.3** 의 요구사항과 지침을 적용하여야 한다.

9.2.3.2 일반 고려사항

ISMS 심사계획은 결정된 정보보안 통제항목을 고려해야 한다.

비고 인증기관은 심사대상 조직과 심사시기를 합의하여 조직의 전체 범위를 가장 잘 입증하는 것이 좋다. 여기에는 계절, 월, 일/날짜 및 해당되는 경우 교대 근무조 등에 대한 고려를 포함시킬 수 있다.

9.2.3.3 원격심사 기술

원격심사 기술의 목적은 심사 효과성 및 효율성을 증대하고, 심사프로세스의 완전성을 지원해야 할 것이다.

심사계획은 원격심사를 지원하는데 사용되는 장치를 언급하여야 한다.

9.3 최초인증

9.3.1 일반사항

KAB-R-MSCB, 9.3 의 요구사항을 적용하여야 한다. 추가로 **9.3.2** 의 요구사항과 지침을 적용하여야 한다.

9.3.2 최초인증심사

9.3.2.1 1단계

1 단계 심사에서 인증기관은 **ISO/IEC 27001** 에서 요구하는 문서화를 포함하는 ISMS 의 설계문서를 획득하여야 한다.
최소한, 1 단계 심사 동안 다음의 정보가 클라이언트에 의해 제공되어야 한다.

a) 클라이언트가 다루는 ISMS 및 활동에 대한 일반 정보
b) **ISO/IEC 27001** 에 명시되고 요구되는 ISMS 문서 사본 및 필요한 경우 기타 관련 문서

인증기관은 클라이언트의 조직상황에서 ISMS 설계, (결정된 통제를 포함하는) 리스크평가 및 처리, 정보보안방침 및 목표, 그리고 특히 클라이언트의 준비 상태에 대해 충분히 이해하여야 한다. 이는 2 단계 심사 계획에 사용되어야 한다.

1 단계 결과는 서면 보고서로 문서화 되어야 한다. 인증기관은 2 단계 심사 진행을 결정하기 전 1 단계 심사보고서를 검토해야 한다. 인증기관은 2 단계 심사팀원이 필요한 적격성을 갖추고 있음을 확인하여야 한다. 이에 대한 확인은 1 단계 심사를 수행했던 심사팀의 심사팀장에 의해 수행될 수 있다.

비고 보고서를 검토하는 심사에 관여하지 않으면서, 2 단계 심사에 대한 심사팀 멤버의 적격성을 결정하고 진행시킬 것을 결정하는 인원을 보유하는 것은 관련된 리스크를 완화하는 하나의 방법이다. 그러나 동일한 목표를 달성하기 위해 이미 다른 리스크 완화 조치가 마련되었을 수도 있다.

인증기관은 2 단계 심사동안 상세한 평가를 위해 필요할 수 있는 추가적인 유형의 정보 및 기록들을 고객에게 알려야 한다.

9.3.2.2 2 단계

1 단계 심사보고서의 문서화된 발견사항에 근거하여, 인증기관은 2 단계 심사를 수행하기 위한 심사계획을 작성한다. ISMS 의 효과적 이행에 대한 평가와 더불어 2 단계의 목적은 클라이언트가 자체 방침, 목표 및 절차를 준수하고 있음을 확인하는 것이다.

이를 위해, 심사는 클라이언트의 다음 사항에 중점을 두어야 한다.

a) 최고 경영층의 리더십, 정보보안 목표에 대한 의지
b) 리스크 관련 정보보안평가. 심사는 정보보안평가가 반복 수행 시 그 평가에서 나오는 일관성, 유효성 및 비교할 수 있는 결과를 도출함을 보장하여야 한다.
c) 정보보안 리스크평가 및 리스크 처리 프로세스에 기반한 통제항목 선정
d) 정보보안 목표에 대비하여 평가를 하는, 정보보안 성과 및 ISMS 효과성 검토
e) 결정된 통제항목 간의 유사성, 적용성 보고서와 정보보안 리스크평가 결과의 유사성, 리스크 처리 프로세스와 정보보안 정책 및 목적 간 유사성
f) 내·외부 상황 및 관련 리스크를 고려한 통제 구현(통제 심사에 대한 예는 **부속서 E** 참조)과 선언한 통제가 실제로 구현되고 전체적으로 효과적인지 여부의 결정하기 위한, 정보보안 프로세스 및 통제항목에 대한 조직의 모니터링, 측정과 분석
g) 경영자의 결정과 정보보안 방침 및 목표를 추적할 수 있음을 보장하기 위한 프로그램, 프로세스, 절차, 기록, 내부심사, ISMS 효과성 검토

9.4 심사 수행

9.4.1 일반사항

KAB-R-MSCB, 9.4의 요구사항을 적용하여야 한다. 추가로 **9.4.2** 및 **9.4.3**의 요구사항과 지침을 적용한다.

9.4.2 ISMS 심사의 특별요소

인증기관 심사팀은 다음 사항을 수행하여야 한다.

a) 정보보안 리스크 평가가 적절하고 ISMS 인증범위 내에서 ISMS 운영에 충분하다는 것을 클라이언트에게 입증하도록 요구
b) 정보보안 리스크의 식별, 시험 및 평가를 위한 클라이언트의 절차와 이행의 결과가 클라이언트의 방침, 목표 및 세부목표와 일관성이 있는지 여부를 확인

인증기관은 리스크평가 절차가 정상적으로 그리고 적절히 이행되었는지를 확인해야 한다.

9.4.3 심사보고서

9.4.3.1 심사보고서는 다음의 정보나 참조사항을 제공해야 한다.

a) 클라이언트의 정보보안 리스크 분석에 대한 인증심사의 설명
b) **ISO/IEC 27001:2022 6.1.3 c)**에서 요구하는 바와 같이 비교를 목적으로 조직이 사용하는 정보보안 통제항목의 집합 전체

9.4.3.2 심사보고서는 인증결정을 촉진하고 지원하기에 충분히 세부적이어야 하며, 다음 사항을 포함해야 한다.

a) 중대한 심사 추적 및 활용된 심사기법 (**9.1.1.2** 참조)
b) 적용성 보고서의 버전 인용, 그리고 해당되는 경우, 클라이언트의 이전 인증심사 결과와의 유용한 비교

완성된 질문지, 체크리스트, 관찰, 로그 또는 심사 노트는 전체 심사보고서의 일부일 수 있다. 이러한 방법이 사용된 경우, 이 문서는 인증결정을 지원할 증거로서 인증기관에 제출되어야 한다. 심사 중에 평가된 표본에 대한 정보는 심사보고서 또는 기타 인증문서에 포함되어야 한다.

원격심사 방법이 사용된 경우, 보고서는 심사수행에 있어 원격심사 방법이 사용된 정도와 심사목적 달성에 있어 원격심사 방법의 효과성을 명시하여야 한다.

조직의 활동이 규정된 물리적 위치에서 수행되지 않고, 그러므로 조직의 모든 활동이 원격으로 수행되는 경우, 심사보고서에는 조직의 모든 활동이 원격으로 수행됨을 기술하여야 한다.

보고서는 ISMS 에 대한 신뢰를 주기 위하여 클라이언트에 의해 채택된 내부 조직 및 절차를 적절하게 고려하여 작성되어야 한다.

심사보고서는 ISMS 요구사항 및 정보보안 통제항목의 이행 및 효과성과 관련하여 긍정적 측면뿐만 아니라 부정적인 측면을 포함하는 가장 중대한 관찰사항에 대한 요약을 포함하여야 한다.

9.5 인증결정

9.5.1 일반사항

KAB-R-MSCB, 9.5 의 요구사항을 적용하여야 한다. 추가로 **9.5.2** 의 요구사항과 지침을 적용하여야 한다.

9.5.2 인증결정

인증결정은 인증심사보고서에 제공된 심사팀의 인증권고에 근거하여야 한다.

경영검토 및 ISMS 내부심사가 수행되고, 효과적이며, 유지되는 것을 입증할 만한 충분한 증거가 있다면 클라이언트에게 인증이 승인된다.

9.6 인증 유지

9.6.1 일반사항

KAB-R-MSCB, 9.6.1 의 요구사항을 적용하여야 한다.

9.6.2 사후관리 활동

9.6.2.1 **KAB-R-MSCB, 9.6.2** 의 요구사항을 적용하여야 한다. 추가로 **9.6.2.2, 9.6.2.3** 및 **9.6.2.4** 의 요구사항과 지침을 적용한다.

9.6.2.2 사후관리심사절차는 이 문서에서 기술하는 클라이언트의 ISMS 인증심사와 관련 절차들의 부분집합이 되어야 한다.

사후관리의 목적은 승인된 ISMS 가 이행되고, 클라이언트의 운영 관행 상 변경에 따라 발생된 ISMS 변경사항의 영향을 고려하며, 인증 요구사항을 지속적으로 준수하는지를 확인하기 위해 검증하는 것이다. 사후관리 프로그램은 최소한 다음 사항을 포함하여야 한다.

a) 정보보안 리스크평가, 통제 유지, ISMS 내부심사, 경영검토와 시정조치 및 예방조치와 같은 ISMS 유지 요소
b) **ISO/IEC 27001** 및 인증을 위해 요구되는 기타 문서에 요구되는 외부 이해관계자와의 의사소통 사항

9.6.2.3 인증기관은 사후관리심사 시 최소한 다음 사항을 검토하여야 한다.
a) 클라이언트의 정보보안 방침의 목표를 달성하기 위한 ISMS 의 효과성
b) 관련된 정보보안 법규 및 규제사항 준수에 대한 주기적 평가 및 검토를 위한 절차의 기능

c) 결정된 통제항목의 변경 및 그 결과에 따른 적용성보고서의 변경들
d) 심사프로그램에 따른 통제항목의 구현 및 효과성

9.6.2.4 리스크 및 영향에 관련된 인증기관 클라이언트의 정보보안 이슈를 반영하기 위해, 사후관리 활동 프로그램을 채택하고, 해당 프로그램을 정당화 할 수 있어야 한다.

사후관리 심사는 다른 경영체제의 심사와 통합될 수도 있다. 심사 보고서에는 각 경영체제와 관련된 측면을 명시하여야 한다.

사후관리 심사 동안, 인증기관은 발생된 불만 및 이의제기에 대한 기록을 확인하여야 한다. 인증 요구사항에 대한 부적합 또는 실패가 확인된 경우, 인증기관은 클라이언트가 자신의 ISMS 및 절차를 조사하고 적절하게 시정조치를 취했음을 확인하여야 한다.

사후관리 보고서에서는 특히, 이전에 발견된 부적합 및 적용성 보고서에 대한 명확한 정보와 이전 심사로부터의 중요 변화가 포함되어야 한다. 사후관리 보고는 최소한 9.6.2.2 와 9.6.2.3 의 요구사항 전체를 포함하여 작성되어야 한다.

9.6.3 갱신인증

9.6.3.1 일반사항

KAB-R-MSCB, 9.6.3 의 요구사항을 적용하여야 한다. 추가로 9.6.3.2 의 요구사항과 지침을 적용하여야 한다.

9.6.3.2 갱신심사

갱신심사절차는 이 문서에서 기술하는 클라이언트의 ISMS 에 대한 최초인증심사와 관련된 절차들의 부분집합이 되어야 한다.

시정조치 이행을 위해 허용된 기간은 부적합의 심각성 및 관련된 정보보안 리스크와 일관되어야 한다.

9.6.4 특별심사

KAB-R-MSCB, 9.6.4 의 요구사항을 적용하여야 한다.

9.6.5 인증의 정지, 취소, 또는 인증범위 축소

KAB-R-MSCB, 9.6.5 의 요구사항을 적용하여야 한다.

9.7 이의제기

KAB-R-MSCB, 9.7 의 요구사항을 적용하여야 한다.

9.8 불만

9.8.1 일반사항

KAB-R-MSCB, 9.8 의 요구사항을 적용하여야 한다.

9.8.2 불만

불만은 가능한 부적합에 관한 잠재적 사고 및 암시를 의미한다.

9.9 클라이언트에 대한 기록

KAB-R-MSCB, 9.9 의 요구사항을 적용하여야 한다.

10 인증기관 경영시스템 요구사항

10.1 경영시스템에 대한 선택사항

10.1.1 일반사항

KAB-R-MSCB, 10.1 의 요구사항을 적용하여야 한다. 추가로 10.1.2 의 요구사항과 지침을 적용하여야 한다.

10.1.2 ISMS 실행

인증기관이 ISO/IEC 27001 에 따라 ISMS 를 실행할 것을 권고 한다.

10.2 선택사항 A: 일반적인 경영시스템 요구사항

KAB-R-MSCB, 10.2 의 요구사항을 적용하여야 한다.

10.3 선택사항 B: ISO 9001 에 따른 경영시스템 요구사항

KAB-R-MSCB, 10.3 의 요구사항을 적용하여야 한다.

부속서 A (필수) 정보보안경영시스템 심사 및 인증을 위한 지식과 스킬

A.1 개요

표 A.1 에는 **KAB-R-MSCB** 에 추가하여, 특정 인증업무기능에 대하여 인증기관이 규정해야하는 지식 및 기술이 명시되어 있다. "○"는 인증기관이 지식 및 스킬의 기준과 깊이를 규정해야 함을 의미한다. **표 A.1** 에 명시되어 있는 지식 및 기술은 **7**절에 더욱 자세하게 설명되어 있으며, **표 A.1**의 괄호 안에 상호참조가 되어 있다.

표 A.1 ISMS 심사 및 인증을 위한 지식 및 스킬

지식 및 스킬	인증업무기능		
	요구되는 심사팀 적격성 결정, 심사팀 구성원 선정, 심사시간 결정을 위한 신청서 검토 수행	심사 보고서 검토 및 인증결정	심사 및 심사팀 통솔
정보보안경영 용어, 원칙, 관행 및 기술		○ (7.1.3.3.2 참조)	○ (7.1.3.1.2 참조)
정보보안경영시스템 표준/참조문서			○ (7.1.3.1.3 참조)
비즈니스경영 관행			○ (7.1.3.1.4 참조)
클라이언트의 비즈니스 분야	○ (7.1.3.2.1 참조)	○ (7.1.3.3.3 참조)	○ (7.1.3.1.5 참조)
클라이언트의 제품, 프로세스 및 조직	○ (7.1.3.2.2 참조)	○ (7.1.3.3.4 참조)	○ (7.1.3.1.6 참조)

비고 추가 적격성 고려사항은 **부속서 B**에 명시됨

부속서 B (참고) 추가 적격성 고려사항

B.1 일반 적격성 고려사항

심사원의 지식 및 경험을 입증할 수 있는 방법에는 여러 가지가 있다. 예를 들어, 지식과 경험은 공인된 자격으로 평가될 수 있다. 요구되는 지식과 경험을 평가하기 위해 자격인증 스킴에 등록된 기록 등이 또한 사용될 수 있다. 심사팀에 대하여 요구되는 적격성 수준은 조직의 산업/기술적 분야 및 ISMS 의 복잡성에 반영하여 설정되어야 할 것이다.

B.2 특정지식 및 경험 고려사항

B.2.1 ISMS 관련 대표적 지식

7.1.3 의 요구사항에 추가하여 다음 사항이 고려되어야 한다. 심사원들은 다음에 대한 심사와 ISMS 대상에 대한 지식 및 이해를 보유하여야 할 것이다.

— 심사프로그램 및 계획
— 심사유형 및 방법
— 심사 리스크
— 정보보안 프로세스 분석
— 지속적 개선
— 정보보안에 대한 내부심사

심사원들은 다음 규제 요구사항에 대한 지식 및 이해를 보유하여야 할 것이다.

— 지적재산권
— 조직 기록물의 내용, 보호 및 유지
— 데이터 보호 및 프라이버시
— 암호화 통제에 관한 규제사항
— 전자 상거래
— 전자 및 디지털 서명
— 업무현장 관찰
— 정보통신 도청 및 데이터 감시(예: 전자메일)
— 컴퓨터(시스템) 부정이용
— 전자적 증거 수집
— 모의해킹
— 국제 및 국내 분야별 특정 요구사항(예: 은행)

특정 분야에 대하여, 지식 및 이해가 특정 표준(예: **ISO/IEC 27006-2**)으로부터 설정하는 것이 가능하다.

부속서 C (필수) 심사시간

C.1 일반사항

이 부속서는 KAB-R-MSCB, 9.1.4 에 대한 부가적인 요구사항이며, 인증기관이 다양한 범위의 활동규모와 복잡성을 가지는 ISMS 범위에 대한 인증에 필요한 심사시간을 결정하는 절차의 개발에 관련된 최소 요구사항 및 지침을 제공한다.

인증기관은 최초심사, 사후심사 또는 갱신심사와 관련된 모든 활동을 착수할 수 있는 충분한 시간을 심사원이 확보할 수 있도록 하여야 한다. 심사시간 전체에 대한 계산에는 심사보고서 작성을 위한 충분한 시간을 포함하여야 한다.

인증기관은 각 클라이언트 및 인증된 ISMS 에 대한 최초인증, 사후관리 및 갱신심사에 소요되는 심사시간을 규정해야 한다. 심사기획단계 동안 이 부속서의 사용은 적절한 심사시간 결정을 일관된 접근 방법으로 유도한다. 추가로, 심사시간은 심사과정, 특히 1 단계에서 발견된 사항에 따라 조정될 수 있을 것이다(예: ISMS 범위의 복잡성에 대한 평가의 차이, 또는 해당 범위의 추가 사업장).

본 부속서는 다음과 같은 사항을 제시한다.

— 심사시간 계산에 사용되는 개념(C.2)
— 각 심사단계에 대한 최초심사시간 결정 절차에 대한 요구사항 (C.3)
— 사후관리심사(C.4) 및 갱신심사(C.5) 심사시간에 대한 요구사항
— 복수사업장 심사 관련 요구사항(C.6)
— 범위확대를 위한 심사시간 요구사항(C.7)

본 부속서의 적용을 나타내는 심사시간 계산 예시는 부속서 D 에서 참조할 수 있다.

심사시간 결정을 위한 계산방법인 본 부속서의 접근방법의 기본적인 가정은 다음과 같아야 할 것이다.

a) 객관적으로 평가될 수 있는 증명된 특성만 고려
b) 인증기관이 적용하고, 비교가능하고 재현이 가능한 유효한 결과를 달성에 충분히 간단함
c) 특성 값에서의 변동이 결과적으로 산정될 심사시간에서의 비교할만한 변화를 야기하도록 충분히 정교하여야 한다.

심사시간 결정은 아래 표 C.1 의 숫자를 근거로 하며 수정에 영향을 미치는 요인들을 고려해야 한다.

인증기관이 규정한 심사기간 결정을 위한 이 접근법이 ISMS 의 복잡성에 대하여 충분한지 검증하기 위하여 정기적으로 검토되어야 한다.

C.2 개념

C.2.1 조직의 관리 하에 근무하는 인원의 수

인증범위 내 모든 교대조에서, 조직의 관리 하에 업무를 수행하는 총 인원의 수가 심사시간을 결정하는 시작점이다.

비고 조직의 관리 하에 근무하는 개인은 (조직에 소속 여부와 상관없이) 인증범위 내에서 ISMS 요구사항에 따라 업무를 수행하도록 요구되는 모든 인원을 포함하여야 한다.

조직의 관리 하에서 파트타임으로 업무를 수행하는 인원은 조직의 관리 하에서 업무를 수행하는 상근직원과 비교한 근무시간의 수에 비례적으로 조직의 관리 하에서 업무를 수행하는 인원들의 수에 포함된다. 이러한 결정은 상근직원과 비교한 근무시간에 따라 결정하여야 한다.

인증범위에 포함되는 조직의 관리 하에 근무하는 인원의 높은 비율이 특정한 동일 활동을 수행할 때, **표 C.1**을 활용하기에 앞서, 인원 수에 대한 감축이 심사시간 산정을 위해 허용된다. 인증기관은 **C.3.4** 에서 제공된 요인을 사용하여야 하며, 인증범위 내에서의 인원 수 감축이 적용되는 방식을 결정하기 위하여 정보보안 리스크와 관련된 활동의 영향을 고려하여야 한다. 반복가능하고 회사별로 적용될 수 있는 통일성 있고 일관된 절차가 문서화되어야 한다.

C.2.2 심사일수

표 C.1 의 심사시간은 심사에 소요되는 심사일수로 표현된다. 본 부속서는 1 일 8 시간 근무시간으로 계산하는 것을 기본으로 한다. (약자 “d”로 표현)

C.2.3 임시사업장

인증범위에 포함되는 임시사업장은 인증문서에 명시된 사업장 이외의 장소로서, 정해진 기간 동안 인증범위에 속하는 활동이 실행되는 장소를 가리킨다. 이러한 임시사업장은 대규모 프로젝트 관리 사업장에서부터 소규모 서비스/설치 사업장에 이르기까지 다양할 것이다. 이러한 사업장을 방문해야 하는 필요성 및 샘플링의 범위는 정보보안 목적을 충족하는데 있어 임시사업장에서 수행되는 활동의 리스크에 대한 평가에 기초하여야 할 것이다. 선정된 샘플 사업장은 활동의 규모 및 유형, 진행 중인 프로젝트의 다양한 단계의 측면에서, 조직의 적격성 요구 및 서비스의 다양성을 대표하는 것이어야 한다. 일반적인 샘플링은 **9.1.5.2**를 참조하여 수행한다.

C.3 최초심사를 위한 심사시간 결정 절차

C.3.1 일반사항

인증기관은 심사시간 계산을 위한 문서화된 절차를 보유하고 준수하여야 한다.

C.3.2 원격심사방법

조직과의 의사소통을 위하여 웹 기반 협력, 웹 미팅, 원격 회의 및/또는 전자적인 검증과 같은 원격심사방법이 사용되는 경우, 이러한 활동은 심사계획에 명시되어야 할 것이며(**9.2.3** 참조), 부분적으로 총 “현장심사시간”에 포함되는 현장심사활동으로 간주될 수 있다.

비고 현장심사시간은 개별 사업장 별로 배정된 현장심사시간을 나타낸다. 원거리 사업장에 대한 전자방식의 심사는 해당 심사가 조직의 사업장에서 직접 실시되었다고 하더라도 원격심사로 간주된다.

C.3.3 심사시간 계산

표 C.1 에 제시된 심사시간표는 최초심사시간의 평균에 대한 출발점을 나타낸다(본 부속서 및 **부속서 D** 내에서는, 이하 해당시간은 최초심사 단계(1 단계 및 2 단계) 포함). 이러한 경험은 ISMS 범위와 함께 조직의 통제 하에서 일하는 인원수에 적절한 것으로 보인다. 또한 유사한 규모의 ISMS 범위에 대해서 심사시간이 더 필요하거나 덜 필요할 수 있음을 나타내었다.

아래 심사시간표는 심사계획에 사용되어야 하는 틀을 제공한다. 심사시간 산출의 출발점은 모든 교대조에 대하여 조직의 통제 하에 업무를 수행하는 총 인원을 기준으로 한다. 기본 심사시간을 조정하기 위해 각각의 요인의 비중을 추가하거나 줄이면서, 심사대상 ISMS 범위에 적용되는 중대한 요인에 근거하여 심사시간을 조정한다. **표 C.1** 의 심사시간표는 적용되는 요인과 허용된 편차에 대한 제한을 고려하여 사용되어야

한다(C.3.5 및 C.3.6 참조). 이 표(표 C.1)에 사용된 용어는 C.2 에서 설명한다. 부속서 D 에서는 이 부속서의 계산법이 적용되는 예시를 보여준다.

C.3.4 인원에 대한 초기값 설정

인증기관은 특정한 동일 활동을 수행하는 많은 수의 인원과 관련한 정보를 클라이언트에 요청하여야 한다.

— 활동에 관여하는 인원의 수
— 활동 또는 프로세스의 유형

특정한 동일 활동을 수행하고, 산정의 기초로 활용되는 인원 수를 감축할 수 있는 요인의 예시는 다음을 포함한다.

— 해당 직무를 수행하기 위하여 정보에 대한 읽기전용 권한(read-only access)만을 부여받은 인원
— ISMS 범위 내에서 조직의 정보처리 시설에 대한 접근 권한을 부여받지 못한 인원
— ISMS 범위 내에서 조직의 정보처리 시설에 대한 입증 가능한 특정의 제한적 접근권한을 부여받은 인원
— 정보 공개를 제한하기 위하여 엄격한 제약조건(예: 개인 물품이나 기기를 작업공간 반입을 금지하는 조치)이 이행되는 곳에서 활동을 수행하는 인원

동일 활동을 수행하는 인원 수를 감축하는 것은 과업과 관련된 활동의 리스크에 기반하여 이루어져야 한다. 동일 활동 각각에 대한 인원 수의 제곱근이 유효종업원 수를 결정하기 위해 사용될 수도 있을 것이며, 이는 심사기간 산정을 위해 사용되고 그 다음 정수로 반올림한 값이다. 이는 허용된 인원 수에 대한 최대 감축이여야 한다.

과업의 성질, 법적 요구사항 및 개인이 접근할 수 있는 정보의 중요도는 감축을 제한할 수 있다.

이 절차를 적용하여 결정된 인원 수는 표 C.1 의 출발점이다.

비고 표는 KAB-AR-MD5 와 동일하게 구조화되었다.

C.3.5 심사시간 조정 요인

표 C.1 은 단독으로 사용되어서는 안 된다. 할당되는 심사시간은 ISMS 의 복잡성과 관련된 다음의 요인과 복잡성에 따라 ISMS 심사에 필요한 노력을 고려해야 한다.

a) ISMS 의 복잡성(예: 정보의 중요성, ISMS 의 리스크 상황 등)
b) ISMS 범위 내에서 수행된 사업의 유형
c) 이전에 입증된 ISMS 성과
d) ISMS 의 다양한 요소의 이행에 활용되는 기술의 정도 및 다양성 (예: 상이한 IT 플랫폼의 수, 분리된 네트워크의 수)
e) ISMS 범위 내에서 사용된 외주업체 및 제 3 자 협약의 범위
f) 정보시스템 개발 범위
g) 사업장 수 및 재난 복구(DR) 사업장의 수
h) 1 단계 심사 이후, 인증기관은 통제항목의 수와 복잡성
i) 사후관리 및 갱신심사: KAB-R-MSCB, 8.5.3 에 따른 ISMS 관련 변화의 정도 및 범주

표 C.1 심사시간표

조직의 관리 하에 업무를 수행하는 개인의 수	QMS 최초심사시간 (심사일)	EMS 최초심사시간 (심사일)	ISMS 최초심사시간 (심사일)	가감요인	총 심사시간
1 ~ 10	1.5 ~ 2	2.5 ~ 3	5	C.3.5 참조	
11 ~ 15	2.5	3.5	6	C.3.5 참조	
16 ~ 25	3	4.5	7	C.3.5 참조	
26 ~ 45	4	5.5	8.5	C.3.5 참조	
46 ~ 65	5	6	10	C.3.5 참조	
66 ~ 85	6	7	11	C.3.5 참조	
86 ~ 125	7	8	12	C.3.5 참조	
126 ~ 175	8	9	13	C.3.5 참조	
176 ~ 275	9	10	14	C.3.5 참조	
276 ~ 425	10	11	15	C.3.5 참조	
426 ~ 625	11	12	16.5	C.3.5 참조	
626 ~ 875	12	13	17.5	C.3.5 참조	
876 ~ 1175	13	15	18.5	C.3.5 참조	
1176 ~ 1550	14	16	19.5	C.3.5 참조	
1551 ~ 2025	15	17	21	C.3.5 참조	
2026 ~ 2675	16	18	22	C.3.5 참조	
2676 ~ 3450	17	19	23	C.3.5 참조	
3451 ~ 4350	18	20	24	C.3.5 참조	
4351 ~ 5450	19	21	25	C.3.5 참조	
5451 ~ 6800	20	23	26	C.3.5 참조	
6801 ~ 8500	21	25	27	C.3.5 참조	
8501 ~ 10700	22	27	28	C.3.5 참조	
> 10700	위와 같이 증가	위와 같이 증가	위와 같이 증가	C.3.5 참조	

부속서 D에 심사시간 계산 시 고려해야 할 요인들의 예시가 제공된다.

심사시간 증가가 요구되는 요인의 예시는 다음과 같다.

— ISMS 범위 내 2개 이상의 건물이나 장소가 포함되는 복잡한 프로세스의 관리
— 2개 이상의 언어를 사용하는 직원(통역사를 필요로 하거나, 심사원들이 개별적으로 심사하는데 장애가 되는 언어) 또는 2개 이상의 언어로 제공되는 문서
— 인증대상이 되는 경영시스템을 보유한 상설 사업장의 활동을 확인하기 위해 임시사업장 방문이 요구되는 활동(하단의 목록 참조)
— ISMS에 적용되는 표준 및 규제사항이 많은 경우

심사시간 단축이 허용될 수 있는 요인의 예는 다음과 같다.

— 리스크가 없거나/낮은 프로세스
— 프로세스가 단일 활동에 관련된 경우(예: 서비스에 국한)
— 조직에 대한 사전 지식(예를 들어, 동일한 인증기관에서 이미 다른 표준 인증을 받은 경우)
— 인증에 대한 신청 조직의 준비 정도(예: 이미 다른 제 3자 제도에 의해 인증이나 인정(recognition)을 받음)

— 경영시스템의 성숙도

클라이언트 또는 인증조직이 임시사업장에서 자사의 제품(들) 또는 서비스(들)을 제공하는 경우에는 이러한 임시사업장에 대한 평가를 심사 및 사후관리 프로그램에 포함시키는 것이 중요하다.

위의 요인에 대해 심사시간을 조정할 수 있다. 심사시간 증가 또는 감축에 필요한 요인은 서로에 의해 상쇄될 수 있다. 심사시간 표에 주어진 기간에 대한 조정이 있는 모든 경우, 이를 정당화하는 충분한 증거 및 기록을 유지해야 한다.

C.3.6 심사시간 편차의 제한

효과적 심사가 수행되었음을 보장하고, 신뢰할 수 있는 비교 가능한 결과를 보장하기 위해 해당 표에서의 심사시간을 30% 이상 축소할 수 없다.

편차에 대한 적절한 사유는 확립되어야 하고 문서화되어야 한다.

C.3.7 현장심사시간

심사계획과 보고서 작성을 위해 계산된 시간이 일반적으로 **C.3.3**, **C.3.4** 및 **C.3.5** 에 따라 산정된 총 현장 "심사시간"을 70% 미만으로 줄여서는 안 될 것이다. 심사계획과 보고서 작성에 요구되는 추가 시간이 현장 심사시간을 줄이는 명분이 되어서는 안 될 것이다. 심사원 이동시간은 이러한 계산에 포함되지 않으며, 심사시간표에서 참조된 심사시간에 추가된다. 심사계획 및/또는 보고서 작성에 시간이 추가로 요구되는 경우, 이는 현장 심사시간을 단축하는 정당한 사유가 될 수 없다. 심사원의 이동 시간은 이 계산에 포함되지 않으며, 상기 표에 제시된 심사시간에 추가한다.

비고 1 70%는 ISMS 심사원의 경험에 근거한 요소이다.

비고 2 용어 "물리/원격"은 (클라이언트의 물리적 장소 또는 전자적 장소에 대한) "현장"심사가 물리적으로 또는 원격으로 수행될 수 있음을 뜻한다. (**9.2.3** 및 **C.3.2** 참조) "현장"심사에 대해서는 **KAB-R-MSCB 9.4.1** 또한 참조할 수 있다.

C.4 사후관리심사시간

최초심사주기에서, 사후관리에 소요되는 심사시간은 최초심사에 소요된 기간에 비례하며, 매년 사후관리에 소요된 총 기간은 최초심사에 소요된 기간의 약 1/3 정도이다. 계획되어 있는 사후관리 기간은 심사시간에 영향을 미치는 변경사항이나 시스템의 성숙도 등을 고려하여 때때로 검토되어야 한다. 사후관리를 위해 소요되는 시간은 ISMS 의 변경사항(예: 새로운 사항 또는 변경된 정보보안 통제항목, 프로세스 및 제품)을 심사하기 위해 증가되어야 한다.

C.5 갱신심사시간

갱신심사 수행에 소요되는 총 시간은 **9.4.3** 및 **KAB-R-MSCB, 9.6.3** 에 명시되어 있는 이전 심사 결과에 따른다. 갱신심사에 소요되는 총 시간은 동일한 조직에 대한 최초심사시간에 비례하여야 하며, 동일한 조직에 대한 최초심사시간의 약 2/3 가 되어야 한다.

C.6 복수사업장 심사시간

일반적으로 현장심사에 대한 총 심사시간은 인원의 위치와 관계없이 조직의 관리 하에 근무하는 총 인원수를 고려하여 계산되어야 한다.

또는, 문서화되어야 하는 정당화된 이유에 대해서는, 이 조항의 첫 번째 단락에 따라 정의된 심사시간보다 총 심사시간이 더 큰 경우에 한해서, 각각의 사업장 별로 계산한 심사시간을 더하는 것이 허용된다. 본사 또는 지역 사업장과 관련 없는 심사의 일부를 고려하여 단축할 수도 있다. 인증기관은 이 같은 시간 단축의 정당성에 대한 사유를 기록해야 한다.

C.3.3 및 **C.3.4** 에 명시된 절차에 따르는 범위에 대해 계산된 총 현장심사일수는 경영시스템, 사업장에서 수행되는 활동 및 파악된 위험에 대한 사업장의 관련성에 근거하여 분배되어야 한다. 분배의 정당성은 인증기관에 의해 기록되어야 한다.

심사시간을 전체 심사시간과 비교하기 전, 감축이 적용되어야 한다.

C.7 범위확대를 위한 심사시간

ISMS 범위확대를 위한 심사시간은 다음과 같은 요인을 고려하여 계산되어야 한다.

a) 확대의 유형
b) 현행 인증의 활동/활동들
c) 활동/활동들이 수행되는 장소의 수
d) 활동/활동들과 관련된 정보보안 리스크
e) 확대와 관련된 통제항목의 수
f) 새로운 범위에 대하여 조직의 관리 하에서 근무하는 인원의 수
g) 확대 범위를 ISMS 로 통합하는 것을 검토하는데 요구되는 시간

인증기관은 범위확대에 대한 일관적인 접근방식을 제공하는 절차서를 보유하여야 한다.

신규범위에 대한 최초심사의 경우, 심사시간은 **C.3.3**, **C.3.4** 및 **C.3.4** 를 활용한 기존 범위에 추가되는 인원 및 사업장의 수를 기반으로 계산되어야 한다.

심사시간은 클라이언트의 ISMS 를 검토하기 위해 계산된 기간에 추가되어야 한다. 이 추가시간은 최소한 다음과 같아야 한다.

1) 범위확대 심사가 사후관리심사 또는 갱신심사와 함께 수행된다면, 0.5 일(MD)
2) 독립된 심사로 범위확대 심사가 수행되는 경우, 1 일(MD)

부속서 D (참고) 심사시간 계산방법

D.1 일반사항

이 부속서는 심사시간의 계산에 대한 공식을 개발하는 부가적인 가이드라인을 제시한다. D.2 에서는 심사시간 계산을 위해 기본적으로 사용될 수 있는 요인을 분류하는 사례를 제시하고, D.3 에서는 심사시간 계산의 예시를 제공한다.

비고 이 부속서의 개념은 C.3.4 에 기술된 바와 같이 특정 동일 활동을 수행하는 인원에 대한 모든 감축이 적용된 후에 시작한다.

D.2 심사시간 계산을 위한 요인의 분류

표 D.1 에서는 C.3.5, a)에서 i)까지 나열된 심사시간 계산을 위한 주요요인의 분류사례를 제시한다. 이 분류는 인증기관이 9.1.4.2 에 따라 심사시간 계산 방법을 이끌어 도출하는데 사용할 수 있다.

표 D.1 심사시간 계산 요인의 분류

요인 (C.3.5 참조)	심사수행에 미치는 영향		
	심사수행 감소	일반적인 심사수행	심사수행 증가
a) ISMS의 복잡성 • 정보보안 요구사항[기밀준수, 무결성, 가용성(CIA)] • 중요 자산의 수 • 절차 및 서비스 수	• 덜 민감하거나 덜 비밀인 정보, 낮은 가용성 요구사항 • 적은 중요 자산(CIA측면) • 적은 인터페이스 및 적은 비즈니스 단위가 포함된 하나의 비즈니스 프로세스	• 더 높은 가용성 요구사항 또는 일부 민감한/비밀 정보 • 약간의 중요 자산 • 약간의 인터페이스 및 비즈니스 유닛이 포함된 2-3개의 단순 비즈니스 과정	• 더 높은 규모의 민감 또는 기밀 정보(예: 건강, 개인 신원 정보, 보험, 은행) 또는 높은 가용성 요구사항 • 다수의 중요 자산 • 다수의 인터페이스 및 비즈니스 유닛이 포함된 세 개 이상의 복합적 절차
b) ISMS 범위에서 수행되는 비즈니스 유형	• 규제 요구사항이 없는 리스크가 낮은 비즈니스	• 높은 규제 요구사항	• 제한된 규제 요구사항(만) 있는 높은 리스크의 비즈니스
c) 사전에 입증된 ISMS 수행	• 최근 인증된 내용 • 인증 받지는 않았으나 여러 심사에 걸쳐 충분히 수행되고 문서화된 내부심사, 경영검토, 효율적 지속 개선 시스템을 포함한 개선 주기에 대해 수행된 ISMS	• 최근의 사후관리 심사 • 인증 받지 않았으나 부분적으로 수행된 ISMS: 일부 경영시스템 도구가 이용가능하며 수행됨; 일부 지속적 개선 과정이 마련되어 있으나 일부만 문서화됨	• 인증 및 최근 심사 없음 • ISMS가 처음이며 완전히 확립되지 않음(예: 경영시스템 특정 통제 메커니즘 부족, 지속적 개선 과정 미흡, 임시 프로세스 수행)
d) ISMS의 다양한 구성의 수행에 활용되는 기술 범위 및 다양성(예: 각 IT 플랫폼의 수, 분리된 네트워크의 수)	• 낮은 다양성으로 고도로 표준화된 환경 (적은 수의 IT 플랫폼, 서버, 운영 시스템, 데이터베이스, 네트워크 등)	• 표준화되었으나 다양한 IT 플랫폼, 서비스, 운영 시스템, 데이터베이스, 네트워크	• IT의 고도의 다양성 및 복잡성(다양한 네트워크 분리, 서버 유형 또는 데이터베이스, 핵심 어플리케이션 수)

요인 (C.3.5 참조)	심사수행에 미치는 영향		
	심사수행 감소	일반적인 심사수행	심사수행 증가
e) ISMS 범위 내에서 사용되는 외주업체 및 제 3자 협약 범위	• 제조자에게 아웃소싱하지 않고 의존도가 낮거나, • 잘 정의되고 관리되며, 모니터링되는 아웃소싱 협약 • 관련된 독립적 보증 보고서가 이용가능함	• 부분적으로 관리된 아웃소싱 협약들	• 아웃소싱에 대한 높은 의존도 또는 중요한 비즈니스 활동에 큰 영향을 미치는 공급자, 또는 • 알려지지 않은 아웃소싱 규모 또는 범위, 또는 • 일부 관리되지 않은 아웃소싱 협약
f) 정보시스템 개발 범위	• 인하우스 시스템 개발 없음 • 표준 소프트웨어 플랫폼 사용	• 복잡한 구성/매개변수화를 갖춘 표준 소프트웨어 플랫폼 사용 • (고도화된) 커스터마이즈 소프트웨어 • 일부 개발 활동(인하우스 또는 아웃소싱)	• 중요한 비즈니스 목표를 위해 진행 중인 프로젝트에 대한 내부 소프트웨어 개발 활동범위
g) 사업장 수 및 재난복구(DR) 사업장 수	• 요구사항 가용성이 낮고 대체 DR 사업장이 하나이거나 없음	• 요구사항 가용성이 중간이거나 높고 대체 DR 사업장이 하나이거나 없음	• 요구사항 가용성이 높음(예: 24시간) • 다수의 DR 사업장 • 다수의 데이터 센터
h) 통제항목의 수 및 복잡성	• 포함되지 않은 일부 공통 통제항목 영역을 포함하여, 통제항목의 수가 통상적인 것보다 적음	• 통제항목의 대표적인 수와 복잡성	• 자세하고 복잡한 통제항목의 수가 통상적인 것보다 많음. 예: 네트워킹 프로토콜 또는 암호해독에 관련된 다수의 통제항목
i) 사후관리 및 갱신심사에 대해: KAB-R-MSCB, 8.5.3 따라 ISMS와 관련된 변경사항 규모와 범위	• 마지막 갱신심사 이후 변경 없음	• ISMS 범주 또는 사후관리에서의 약간의 변화. 예를 들어, 일부 정책, 문서 등 • 상기 언급된 사항에서의 약간의 변화	• ISMS 범주 또는 사후관리에서의 주요 변화. 예를 들어, 새로운 프로세스, 새로운 비즈니스 단위, 지역, 리스크 평가 관리 방법, 정책, 문서, 리스크 처리 • 상기 언급된 사항에서의 주요 변화

D.3 심사시간 계산 예시

다음 예시는 심사시간을 계산하기 위하여 **C.3** 에 제공된 요인을 사용하는 사례를 보여준다. 아래 예시에서 심사시간 계산은 다음과 같이 사용된다.

1단계 비즈니스와 조직과 관련된 요인 결정(IT 이외)

표 D.2 에 제시된 각 항목에 대한 적절한 등급을 결정하고 그 결과를 합산한다.

2단계 IT 환경 관련 요인의 결정

표 D.3 의 각 항목에 적절한 등급을 결정하고, 그 결과를 합산한다.

3단계 상기 1 단계 및 2 단계 결과를 근거로 **표 D.4** 에서 적절한 항목을 선택하여 심사시간에 미치는 요인들의 영향을 식별한다.

4단계 최종 결론

심사시간 차트(**표 C.1**)를 적용한 일수를 3 단계의 요인들과 곱한다. 복수사업장 샘플링이 사용된 경우, 산출된 심사시간은 복수사업장 샘플링을 실행하기 위해 요구되는 노력에 근거하여 증가된다.

이를 통해 나온 결과가 최종 심사시간이다.

표 D.2 사업 및 조직 관련 요인 (IT 이외)

항목	등급
비즈니스 유형 및 규제 요구사항	1. 비핵심 사업부문 및 비규제 부문의 조직 업무* 2. 핵심사업부문에서 조직이 보유한 고객* 3. 핵심사업부문에서의 조직 업무*
프로세스 및 과업	1. 적은 수의 제품 및 서비스에 대한 표준 프로세스 2. 다수의 제품 및 서비스에 대한 표준이지만 반복적이지 않은 과정 3. 복잡한 과정, 다수의 제품 및 서비스, 인증범위를 포함한 다수의 사업 단위(ISMS가 매우 복잡한 과정 또는 상대적으로 많거나 특수한 활동 포함)
경영시스템 구축 수준	1. ISMS가 이미 잘 구축되었고 그리고/또는 다른 경영시스템이 갖춰져 있음 2. 다른 경영시스템의 일부 요소는 수행되고 일부는 그렇지 않음 3. 어떠한 경영시스템도 수행되지 않음, ISMS 가 신규이며 구축되어 있지 않음
* 핵심(ciritical)사업부문은 국가에 매우 부정적 영향을 미칠 수 있는 건강, 보안, 경제, 이미지, 정부의 능력에 리스크를 야기할 가능성이 있는 중요 공공서비스에 영향을 미치는 부문을 일컫는다.	

표 D.3 IT 환경 관련 요인들

항목	등급
IT 인프라 복잡성	1. 약간 또는 고도로 표준화된 IT 플랫폼, 서버, 운영 시스템, 데이터베이스, 네트워크 등 IT 인프라 복잡성 2. 일부 다른 IT 플랫폼, 서버, 운영 시스템, 데이터베이스, 네트워크 3. 여러 다른 IT 플랫폼, 서버, 운영 시스템, 데이터베이스, 네트워크
클라우드 서비스를 포함한 아웃소싱 및 공급자 의존성	1. 아웃소싱 또는 공급자에게 거의 또는 전혀 의존하지 않음 2. 일부 관련된 아웃소싱 또는 공급자에 의존하는 일부 중요한 사업 3. 아웃소싱 및 공급자에 대한 높은 의존성, 대부분 중요 사업 활동에 영향을 미침
정보시스템 개발	1. 인하우스 시스템/어플리케이션 개발이 전혀 없거나 매우 제한됨 2. 일부 중요 사업을 제안하기 위한 일부 인하우스 또는 아웃소싱 시스템/어플리케이션 개발 3. 중요한 사업 목표를 위한 광범위한 인하우스 또는 아웃소싱 시스템/어플리케이션 개발

표 D.4 심사시간에 영향을 미치는 요인

		IT 복잡성		
		낮음(3~4)	중간(5~6)	높음(7~9)
비즈니스 복잡성	높음(7~9)	+ 5 % ~ + 20 %	+ 10 % ~ + 50 %	+ 20 % ~ + 100 %
	중간(5~6)	- 5 % ~ - 10 %	0 %	+ 10 % ~ + 50 %
	낮음(3~4)	- 10 % ~ - 30 %	- 5 % ~ - 10 %	+ 5 % ~ + 20 %

사례 1

심사대상 조직의 직원은 700명이므로, **표C.1**에 따르면 최초심사에 17.5일이 필요하다. 해당 조직은 핵심(critical) 사업 부문에서 업무를 수행하지 않으며, 고도로 표준화되고 반복적인 업무를 수행하며, 최근 ISMS를 확립하였다. **표 D.2**에 따르면 이는 1+3+1=5 일의 비즈니스 및 조직 관련 요인을 생성한다. 조직은 아주 적은 수의 IT 플랫폼 및 데이터베이스를 보유하고 있으며, 광범위하게 외주처리를 활용하고 있다. 소프트웨어 개발은 조직 내 또는 외주처리를 통해서도 이루어지지 않는다. **표 D.3** 에 의하면 이는 1+3+1=5 일의 IT 환경 관련 요인을 생성한다. **표 D.4**에 따라 심사시간은 조정되지 않는다.

사례 2

앞 사례와 같은 조직이되, 다양한 경영시스템이 운영 중이며, ISMS 가 잘 확립된 경우, **표 D.4** 에 따른 계산을 1+1+1=3 로 변경한다. **표 D.4** 에 의하면 심사시간이 5%에서 10% 감축되게 된다. 즉 심사시간이 1 일에서 1.5 일까지 줄어들어 총 16 에서 16.5 일이 된다.

부속서 E (참고) ISO/IEC 27001:2022 부속서 A 통제항목의 구현을 위한 검토지침

E.1 목적

(적용성 보고서에 따라) ISMS 클라이언트에 의해 필수적으로 결정된 통제항목의 구현은 **9.3.2.2 f)**의 요구사항에 따라 최초심사의 2 단계심사 시 검토되어야 하며, 사후관리 또는 갱신심사 시에도 검토되어야 한다. 이는 통제항목이 구현되고 효과적인지, 통제항목이 기술된 정보보안 목적에 부합하는지를 결정하는 것을 목적으로 한다.

심사원이 조직을 방문하기 전까지 인증기관이 조직의 필요한 통제항목이 무엇인지를 아는 것, 또는 **ISO/IEC 27001:2022 부속서 A**와 동일한 통제항목 문구를 활용하여 통제항목이 기술되었는지를 아는 것은 일반적이지는 않다. 또한, 인증기관은 정보보안 통제항목 간의 관계 또는 정보보안 통제항목과 조직의 프로세스 간의 관계도 알 수 없다. 그러므로, 최초심사에서 개별 통제항목을 심사하는 데 제한이 있는 반면, 그 이후의 심사에서 조직이 적용하고 있는 조직의 프로세스 및 리스크 처리 계획의 맥락에서의 통제항목 심사에 대한 더 효과적인 접근법을 선택할 수 있다.

그럼에도 불구하고, 인증기관은 조직이 **ISO/IEC 27001:2022 부속서 A**에서의 통제항목과 조직이 필요로 하는 통제항목에 대한 비교를 요구해야 함을 인지하고, 조직의 필요한 통제항목과 **ISO/IEC 27001:2022 부속서 A**의 통제항목 간 관계가 존재함을 인지한다. **표 E.1** 에서 제공된 지침은 **ISO/IEC 27001:2022 부속서 A**에서의 통제항목과의 관계를 고려하여 클라이언트에 의해 결정된 필요한 통제항목을 다루는 심사계획을 개발할 때 인증기관을 지원하는 것을 목적으로 한다.

E.2 표 E.1 의 사용방법

E.2.1 일반사항

표 E.1 은 필요한 통제항목들의 검토를 위한 예시 지침을 제공한다. 해당 표는 **ISO/IEC 27001:2022 부속서 A**에 나열된 항목들을 활용하지만, 심사원은 통제항목의 효과성을 입증하기 위한 심사증거 수집 시, **표 E.1**에서 제공된 지침을 해석하는데 있어 표준에서의 통제항목들과 조직의 필요한 통제항목들 간의 관계를 활용하여야 할 것이다.

비고 **표 E.1**는 **ISO/IEC 27001:2022 부속서 A**에 나타난 사항과 관련 없는 통제검토는 안내하지 않는다.

대부분의 통제항목들은 예를 들어, 클라이언트의 통제항목, 프로세스 또는 절차의 문서화에 대한 검토, 인터뷰 또는 관찰을 통하여 증거로 사용할 수 있는 조직의 측면을 포함한다.

많은 통제항목이 클라이언트 조직이 수립한 규칙을 기반으로 한다. 이러한 규칙은 특정 주제에 대한 방침, 프로세스 또는 절차에 대한 요구사항 또는 인원에게 전달되는 규칙의 기타 유형의 형태가 될 수 있다. **표 E.1** 은 “규칙”이라는 일반적인 용어를 클라이언트 조직의 경영자에 의해 설정된 이러한 요구사항이나 기대를 명시하기 위해 사용한다.

많은 통제항목들이 예를 들어, 통제 활동의 결과에 대한 샘플을 검토하는 샘플링을 통해 시험될 수 있다.

E.2.2 "시스템시험" 영역

ISO/IEC 27001:2022 부속서 A 의 많은 통제항목들은 (특정 시스템 설정, 기술의 구성 또는 기능성을 통한) 기술적 통제에 의해 구현된다. 기술적 통제항목의 성과에 대한 증거는 시스템 시험을 통해 또는 전문심사 또는 보고 도구의 활용을 통해 보통 수집될 수 있다. "시스템시험"은 정보시스템에 대한 직접적인 검토를 의미한다. 심사원은 시스템 설정 및 구성을 검토하거나 또는 시험도구의 결과를 평가할 수 있다. 클라이언트가 심사원에게 알려진 도구를 사용하고 있다면, 이는 심사를 지원하는데 사용될 수 있거나 또는 심사원이 클라이언트에 의해 실행된 평가결과를 검토할 수도 있다.

표 E.1 의 "시스템시험" 영역은 기술적 통제검토를 위한 지침을 제공한다.

— 공란 : ISMS 심사에서 보통 적용이 불가능하거나 필요하지 않은 시스템시험을 의미
— 가능: 시스템시험 통제구현을 위한 평가에 보통 적절하나 통상적으로 ISMS 심사에 필요한 것은 아님
— 권고: 시스템시험이 통상적으로 ISMS 심사에 필요함

E.2.3 "육안검사" 영역

ISO/IEC 27001:2022 부속서 A 의 기타 통제항목은 이러한 통제항목의 구현 및 효과성 평가 시 현장에서의 "육안검사"를 통해 검토될 수 있다. 관련문서에 대한 검토나 인터뷰만으로는 충분치 않으므로, 심사원은 통제가 구현되는 장소에서 검증해야 할 필요가 있다.

비고 현장에서의 육안검사는 또한 원격 검사 기술(예: 현장에서 인원이 실시간 비디오를 심사원에게 제공)을 활용하여 수행될 수도 있다.

표 E.1 의 "육안검사" 영역은 통제항목의 물리적 증거를 검토하는 지침을 제공한다.

— 공란 : ISMS 심사에서 보통 적용이 불가능하거나 필요하지 않은 육안검사를 의미
— 가능: 육안검사가 통제구현을 위한 평가에 보통 적절하나 통상적으로 ISMS 심사에 필요한 것은 아님
— 권고: 육안검사가 통상적으로 ISMS 심사에 필요함

E.2.4 통제항목의 설계 및 구현에 대한 가능한 증거

"통제항목의 설계 및 구현에 대한 가능한 증거" 영역은 심사원이 **ISO/IEC 27001:2022 8.3**(리스크 처리 계획에 필요한 요구사항 및 그렇게 함으로써 필요한 통제항목)에 대한 적합성을 평가하도록 지원할 수 있는 증거에 대한 지침을 제공한다. 이 영역의 많은 다양한 요점들은 요구사항이 아니며, 전체 목록을 구성하는 것도 아니다. **ISO/IEC 27001:2022 부속서 A** 의 통제항목 문구에서 도출된 것으로 조직이 필요한 통제항목에 반드시 적합한 것은 아니다. 이 경우, 다른 형태의 증거가 활용되는 것이 좋다. 조직의 적용성보고서 및 관련 ISMS 문서화는 조직의 필요한 통제항목의 명세로서 활용되는 것이 좋다. 조직의 적용성보고서는 필요한 통제항목, 통제항목을 구현하는 것과 상관없이 통제항목을 포함한 것에 대한 정당성, 그리고 **ISO/IEC 27001:2022 부속서 A** 에서 제외된 모든 통제항목에 대한 정당성을 포함한다.

표 E.1 통제항목의 평가

ISO/IEC 27001:2022, 부속서A[a]에서의 통제항목	시스템 시험	육안 검사	통제항목의 설계 및 구현에 대한 가능한 증거
5 조직적 통제항목			
5.1 정보보안 방침			- 정보보안 방침 - 조직에 의해 필요하다고 판단된 경우, 정보보안 특정 주제에 대한 방침 - 관련 인원 및 이해관계자에게 방침 배포
5.2 정보보안 역할 및 책임			- 정보보안의 실행, 운영 및 관리를 위하여 분배된 역할 및 책임
5.3 의무의 구분			- 상충되는 의무 또는 책임을 식별하고 상응하는 분리 규칙 식별
5.4 경영책임			- 정보보안 목표, 방침, 절차 등에 대한 경영기술 및 지원 - 인원의 정보보안에 책임을 지는 개인에 대한 모니터링
5.5 권한에 대한 접근			- 관련 권한에 대한 규정된 연락망 - 사건 보고 규칙 - 관련 권한 간의 정보흐름의 내용
5.6 특정 목적 집단과의 접촉			- 특정 목적 집단, 기타 포럼 또는 연합체에 대한 멤버쉽 또는 연락망 (예: 컴퓨터 비상사태 대응 팀(CERTs), 사이버보안 업체) - 이러한 조직 내에서 논의될 수 있는 사항에 대한 규칙 - 이러한 조직 간의 정보흐름의 내용
5.7 위협 인텔리전스			- 관련된 위협 인텔리전스 수집에 대한 접근법 - 조직과 관련된 위협 인텔리전스 분석 및 분석 내용을 적절한 집단에 배포
5.8 프로젝트 관리에서의 정보보안			- 요구사항 정의, 시험에서의 프로젝트 수명주기 동안 프로젝트 관리에서 수립된 정보보안 - 프로젝트의 샘플로, 식별된 정보보안 리스크 및 그에 상응하는 리스크 처리
5.9 인벤토리 및 기타 관련 자산	가능		- ISMS에 의해 보유되는 정보 및 기타 관련 자산의 인벤토리 - 인벤토리 목록 내에서 보유되고 있는 소유권 - 자산에 대한 소유자 책임 규칙, 즉 분류
5.10 허용 가능한 정보 및 기타 관련 자산 사용			- 정보 및 기타 관련 자산의 허용 가능한 사용에 대한 문서화된 규칙 - 정보 및 기타 관련 자산을 처리하는 절차
5.11 자산 반환			- 조직의 자산 반환에 대한 규칙, 예: 고용, 계약 또는 협약 변경 또는 종료에 대한 체크리스트 - 문서화된 반환기록의 샘플
5.12 정보 분류			- (예를 들어, 특정 주제에 대한 방침에서의) 정보분류에 대한 규칙 및 스킴 - 분류되는 것이 좋은 다양한 출처에서의 정보 샘플
5.13 정보의 표시		가능	- 정보 및 기타 관련 자산에 대한 표시 규칙 - 특정 유형의 정보 및 기타 관련 자산에 대한 표시 절차
5.14 정보 전환	가능		- (예를 들어, 특정 주제에 대한 방침에서의) 정보 전환 규칙 -물리적, 전자적 또는 구두 전환을 포괄하여, ISMS에서 식별된 정보 전환 및 그에 상응하는 규칙, 절차 또는 협약 유즈 케이스(use case)에 대한 정의

ISO/IEC 27001:2022, 부속서A[a]에서의 통제항목	시스템 시험	육안 검사	통제항목의 설계 및 구현에 대한 가능한 증거
			- 실행된 정보전환 절차 또는 협약의 샘플
5.15 접근 통제	가능		- (예를 들어, 특정 주제에 대한 방침에서 접근 통제와 관련하여) 정보 및 기타 관련 자산에 대한 물리적 및 논리적 접근 관리에 대한 규칙 - 위의 규칙에 따라 적합성이 확인된, 정보 및 기타 관련 자산에 대한 높은 리크스의 물리적 또는 논리적 접근에 대한 접근 권한의 (샘플) 추출
5.16 신원 관리			- 수명주기 동안의 개인 또는 인간이 아닌 존재에 부여한 신원을 관리하는 절차
5.17 인증 정보	권고		- 인증정보의 배분 및 관리에 대한 프로세스 설명 - 인증을 위해 활용되는 정보를 적절하게 처리하기 위한 사용자 설명서 - 비밀번호가 사용되는 경우, 비밀번호 관리 시스템의 보안 환경 (예: 길이, 복잡도, 순환)
5.18 접근 권한	권고		- (예를 들어, 특정 주제에 대한 (물리적 및 논리적) 접근권한과 관련하여) 접근 관리에 대한 규칙 - 접근권한 부여, 갱신 또는 해지에 대한 설명 - 접근 권한에 대한 정기 검토의 규칙 및 프로세스 - 신원의 샘플에 부여된 접근 권한 - 접근 권한에 대해 수행된 검토 결과
5.19 공급자 관계 정보보안			- (예를 들어, 특정 주제에 대한 공급자의 제품과 서비스 사용 관련 방침에서) 공급자 관계에서의 정보보안 리스크를 관리하는 규칙 - 관계의 수명주기 동안 공급자 관계에서의 정보보안을 관리하는 프로세스 또는 절차 - 공급자 평가의 결과(예: 정보 및 통신기술 기반구조 요소, 서비스) - (예를 들어, 공급자 관계 샘플에 대한) 수립된 정보보안 요구사항에 대한 적합성 모니터링 결과
5.20 공급자와 협약 시 정보보안 언급			- 공급자 관계의 유형과 관련된, 외부 집단과의 협약 등록 - 관련 정보보안 요구사항 및 서비스 수준 계약(SLA)을 포함한 공급자 협약(샘플)
5.21 정보통신기술(ICT) 공급망에서의 정보보안 관리			- ICT 제품 또는 서비스 획득에 있어 정보보안을 다루는 규칙 - 정보보안 리스크 관리에서의 ICT 공급망 (ICT 공급망 정보보안 리스크 관리 관행) - 수행된 리스크 분석의 결과. 예: 특정 ICT 공급망의 샘플에 대한 통제항목 완화
5.22 공급자 서비스 모니터링, 검토 및 변경사항 관리			- 공급자 정보보안 관행 및 서비스 전달에서의 변경사항 관리 프로세스 - (예를 들어, 서비스 보고서 및 공급자 감사를 통한) 공급자 정보보안 관행에 대한 정기 모니터링, 검토, 평가 - 조치계획(action plans)을 포함한 모니터링 및 검토 활동의 결과
5.23 클라우드 서비스 사용에 대한 정보보안			- (예를 들어, 특정 주제에 대한 클라우스 서비스 사용 관련 방침에서) 클라우드 서비스에서의 정보보안 리스크 관리 규칙 - 조직에서 사용하는 클라우드 서비스의 목록

ISO/IEC 27001:2022, 부속서A[a]에서의 통제항목	시스템 시험	육안 검사	통제항목의 설계 및 구현에 대한 가능한 증거
			- 클라우드 서비스 사용과 관련된 정보보안 리스크 관리 프로세스 - 클라우드 서비스 협약이 조직의 기밀성, 완전성, 가용성, 정보 처리 요구사항을 다루지 않는다면, 조직의 데이터, 서비스 가용성에 대한 구체적인 조항
5.24 정보보안사고 관리 계획 및 대비			- 정보보안사고를 다루기 위한 프로세스, 계획, 역할 및 책임 - 정보보안 이벤트에 대한 절차 보고 및 이러한 보고에 대한 예시
5.25 정보보안 이벤트에 대한 평가 및 결정			- 정보보안 이벤트 평가 기준 - 정보보안 사건에 대한 분류 및 우선순위 스킴
5.26 정보보안사고에 대한 대응			- 정보보안사고 대응에 대한 절차 - 사고 및 해당 사고에 대한 대응의 기록
5.27 정보보안사고에 대한 시사점			- 유형, 규모 및 발생 비용을 포함하여, 발생한 정보보안사고의 기록 - 정보보안사고 분석을 통한 시사점. 예: 사고관리 계획의 보완, 관리 및 인식 활동의 개선
5.28 증거 수집			- 정보보안사고와 관련된 증거를 다루는 절차. 예: 식별, 수집, 획득 및 보존
5.29 중단된 상태 동안의 정보보안			- 중단된 상태 동안의 적절한 정보보안 수준을 유지하기 위한 계획 - 정보보안 요구사항을 비즈니스 연속성 경영시스템 계획 및 프로세스에 포함
5.30 비즈니스연속성을 위한 ICT 준비도			- 비즈니스 영향 분석에서 도출된 ICT 지속성 요구사항 - ICT 지속성 계획 - ICT 지속성 정기시험 결과
5.31 법적, 규제적 및 계약 요구사항			- 조직의 정보보안에 영향을 미칠 수 있는, 조직이 사업을 수행하는 또는 제품 및 서비스를 사용하는 관련 국가의 목록 - 정보보안과 관련한, 특히 모든 형태의 암호 사용과 관련한, 법적, 규제적 또는 계약 요구사항을 포함하여 식별된 외부 요구사항
5.32 지적재산권			- (예를 들어, 특정 주제에 대한 방침에서) 지적재산권 관리를 위한 규칙 - 문서 저작권, 디자인 권리, 상표, 특허 및 소스 코드 라이선스 및 해당 인벤토리를 다루는 절차
5.33 기록물 보호	권고		- (예를 들어, 특정 주제에 대한 방침에서) 적용가능한 법, 규제 및 계약 요구사항과 연관된 기록관리 규칙 - 기록의 관리 연속성, 보유 및 폐기를 다루는, 저장 관련 절차 - 기록관리 요구사항(예: 보존, 보유)를 가능하도록 하는 데이터 저장 시스템의 구성
5.34 개인 정보(PII)의 프라이버시 및 보호			- (예를 들어, 특정 주제에 대한 방침에서) 개인 정보(PII)를 다루는 규칙 - 개인 정보의 프라이버시 및 보호에 영향을 미칠 수 있는, 조직이 사업을 수행하는 또는 제품 및 서비스를 사용하는 관련 국가의 목록

ISO/IEC 27001:2022, 부속서A[a]에서의 통제항목	시스템 시험	육안 검사	통제항목의 설계 및 구현에 대한 가능한 증거
			- 개인 정보의 프라이버시 및 보호에 대한 법적, 규제적 또는 계약 요구사항을 포함하여 식별된 외부 요구사항 - 적절한 기술적 및 조직적 조치를 통해 요구사항이 충족됨을 보여주는 개인 정보를 다루는 데 책임이 있는 집단이 수행한 분석
5.35 정보보안의 독립적 검토			- 정보보안의 독립적 검토 수행 계획 - 독립적 검토 결과(샘플)를 최고 경영자에게 보고 - 조직의 정보보안 관리 접근법이 부적절하다고 발견된 경우에 취해진 시정조치
5.36 정보보안 정책, 규제 및 표준의 준거			- 정보보안 정책, 특정 주제에 대한 방침, 규칙 및 표준에 대한 조직의 준수를 검토하는 계획 - 이러한 검토(샘플)의 결과 및 취해진 시정조치
5.37 문서화된 운영 절차			- 정보보안과 관련된, 정보처리 시설에 대한 운영 절차
6 인원관리			
6.1 조사(screening)			- 적용가능한 법, 규제 및 윤리를 고려하여, 신원조사에 대한 규칙 및 프로세스 - 적용 가능한 경우, 신규 입사자 및 기존 인원의 샘플(예: 승진, 민감한 직무 프로필)에 대하여 수행된 신원 조회
6.2 고용조건			- 정보보안 책임(예: 행동강령)과 관련한 일반적인 고용조건 또는 일반적인 규칙 - 인원에 의한 정보보안과 관련된 고용조건의 수용 - 주요 역할(예: 민감 정보 접근권한 또는 시스템에 대한 특권 보유)을 수행하는 인원에 의해 동의된 특정 정보보안 책임의 샘플
6.3 정보보안 인식, 학력 및 교육훈련			- 중요한 특정 그룹을 대상으로한 특정 주제에 대한 정보보안 인식, 학력 및 교육훈련 - 수행된 정보보안 교육훈련에 대한 참여자 목록 - 기대되는 행동에 대하여, 참여자 샘플의 인터뷰 답변
6.4 징계 프로세스			- 인원 및 기타 관련 이해관계자에게 전달된 것과 같은 공식적인 징계 프로세스
6.5 고용 종료 및 변경 이후의 책임			- 퇴사 이후 또는 고용의 변경 이후에 유효한 특정 역할 및 직무에 대하여, 인원에 의한 서면 수락
6.6 기밀준수 또는 비공개 협약			- 인원 및 기타 관련 이해관계자가 서명한 기밀준수 협약
6.7 원격 근무	가능		- (예를 들어, 특정 주제에 대한 방침에서) 원격 근무 규칙 - 물리적 조치 및 통신 보안 조치에 대한 샘플 - 원격으로 사용할 수 있는 보안 정보처리 장치 설계(예: "개인 기기를 활용하는 것" (BYOD), 노트북)
6.8 정보보안 이벤트 보고			- 인원에 의해 식별될 수 있는 정보보안 이벤트를 보고하는 구조 - 정보보안 이벤트 보고에 대한 인식 제고를 위한 설명 또는 의사소통
7 물리적 관리			
7.1 물리적 보안 경계		가능	- 보안 영역 설계 및 물리적 경계의 영향력에 대한 규칙 - 물리적 보안 경계 및 각각의 관련 위치에 대한 보안 영역 설계
7.2 물리적 출입	가능	권고	- 보안 영역으로의 출입 지점에 대한 (물리적 또는 전자적) 접근권한 승인 시스템

ISO/IEC 27001:2022, 부속서A[a]에서의 통제항목	시스템 시험	육안 검사	통제항목의 설계 및 구현에 대한 가능한 증거
			- 인원 및 방문자의 출입 추적에 대한 접근권한 기록 - 해당 프로세스 설명에 맞는 배달 및 적재 영역의 물리적 설계
7.3 사무실, 공간 및 시설의 보안		가능	- 처리된 민감 정보를 보호하기 위한 사무소 및 시설에 대한 물리적 보안 설계 및 이행
7.4 물리적 보안 모니터링	가능	가능	- 미승인된 물리적 접근을 감지하기 위한 물리적 사후관리 시스템의 설계 - 모니터링 시스템의 보호 - 물리적 사후관리 시스템 운영으로 생성된 기록
7.5 물리적 및 환경적 위협에 대한 보호		권고	- 물리적 및 환경적 위협에 대한 리스크 평가 결과 - 물리적 및 환경적 위협에 대하여 적절한 보호조치의 설계
7.6 보안 영역에서의 작업		가능	-(구체적인 보안 조치를 기술하는) 보안 영역에서의 근무 규칙 - 보안 영역에 대하여 이행된 보안 조치
7.7 청결한 책상 및 청결한 화면		권고	- (예를 들어, 특정 주제에 대한 방침에서) 청결한 책상 및 청결한 화면에 대한 규칙 - 청결한 책상 및 청결한 화면 상태에 대한 불시(임의) 점검
7.8 장비위치 및 보호		가능	- 장비 위치 및 보호에 대한 규칙 - 장비 위치 및 보호에 대한 불시(임의)점검
7.9 사업장 외 자산의 보안			- 조직 사업장 밖 자산 활용에 대한 규칙(예: "개인 기기 지참" 가이드라인) - 조직 사업장 밖 자산을 활용하는 인원에 대해 수행한 인터뷰 또는 설문조사 결과
7.10 저장 매체	가능		- (예를 들어, 특정 주제에 대한 방침에서) 삭제 가능한 저장 매체 사용에 대한 규칙 - 이동식 저장 매체에서 이동식 저장 매체로의 정보 전송(예 : 암호화 포함)을 제한하거나 보호하기 위한 장치의 구성 - 안전한 폐기를 위한 프로세스 및 폐기 프로세스로부터의 기록
7.11 보조 유틸리티		권고	- 특히, 데이터 센터에서, 설치된 유틸리티 보호 조치(예: 온도, 전기 공급, 물) - 전기, 물, 가스 또는 기타 유틸리티를 차단하는 비상사태 조항
7.12 케이블류 보안		가능	- 케이블류의 물리적 라우팅 및 보호
7.13 장비 유지			- 각종 장비의 유지보수 절차 - 장비 유지보수 기록
7.14 장비의 보안 처리 또는 재사용	가능	가능	- 저장 수단을 포함하는 장비의 처리 또는 재사용에 대한 규칙 - 정보 또는 장비의 물리적 또는 논리적 파괴에 대한 기록
8 기술적 통제항목			
8.1 사용자 엔드 포인트 기기	가능		- (예를 들어, 특정 주제에 대한 방침에서) 사용자 엔드포인트 기기에 대한 보안 설정 및 처리에 대한 규칙 - 사용자 엔드포인트 기기 보호를 위한 보안 요구사항 및 절차를 다루는 최종 사용자 인식 활동 - 적용 가능한 경우, 개인기기(BYOD)에 대한 분리 및 보호에 대한 규칙

ISO/IEC 27001:2022, 부속서A[a]에서의 통제항목	시스템 시험	육안 검사	통제항목의 설계 및 구현에 대한 가능한 증거
			- 원격으로 사용할 수 있는 기기를 처리하는 보안 정보의 설계 (예: 개인기기 지참, 노트북)
8.2 특권	가능		- (예를 들어, 특정 주제에 대한 방침에서) 제한된 분배, 사용 및 모니터링 에 대한 규칙 - 특권 관리를 위한 승인 및 검토 프로세스
8.3 정보 접근 제한	권고		- (예를 들어, 특정 주제에 대한 방침에서) 정보 및 기타 관련 재산에 대한 접근 제한 규칙 - 정보의 수명 주기 (예: 생성, 처리, 저장, 전달, 폐기) 동안, 민감 정보에 대한 접근을 보호하는 접근관리 기술 및 프로세스
8.4 소스코드에 대한 접근	권고		- 소스코드, 개발도구 및 소프트웨어 라이브러리에 대한 읽기 및 쓰기 접근(엑세스) 관리 절차
8.5 보안 인증	권고		- (예를 들어, 특정 주제에 대한 방침에서) 접근 관리에 대한 인증 기술 및 절차에 대한 규칙 - 시스템 또는 애플리케이션에서 로그인 절차에 대한 리스크 기반 결정 및 그에 상응하는 이행 - 중요 정보시스템에 대한 강력 또는 다중 인증의 사용
8.6 용량 관리	가능		- 예상되는 최신의 용량 요구사항 - 자원 활용의 측정 (예: 정보처리 시설, 인적자원, 사무소 및 기타 시설) - 충분한 용량 제공 또는 용량감소 요구사항에 대한 절차
8.7 악성 소프트웨어로부터의 보호	권고		- 악성 소프트웨어로부터의 보호에 대한 규칙 - 자산의 위험에 기반한 적용 범위와 이에 상응하는 악성소프트웨어(말웨어) 탐지 소프트웨어의 구성(설정) - 악성 소프트웨어로부터 정보 및 기타 자원을 보호하는 기타 절차 및 조치 - 악성 소프트웨어에 대한 최종 사용자 인식 활동
8.8 기술적 취약점 관리	권고		- 활용하는 정보시스템의 기술적 취약점에 대한 정보의 수집 및 관리 -(정기적으로 수행된) 취약점 스캔의 결과 또는 침투 테스트의 결과 - 기술적 취약점에 대한 조직의 노출 및 계획된 완화 조치에 대해 수행된 평가 - 소프트웨어 업데이트 프로세스를 통한 가장 최신의 승인된 패치 및 어플리케이션 업데이트의 설치 보장
8.9 형상 관리	권고		- 보안 구성, 하드웨어, 소프트웨어, 서비스 및 네트워크를 포함한 구성에 대한 규칙 - 구성의 관리, 실행 또는 적용, 모니터링 및 검토에 대한 프로세스 - 하드웨어, 소프트웨어, 서비스 및 네트워크(예: 경화)의 보안구성에 대한 표준 양식
8.10 정보 삭제			- (예를 들어, 특정 주제와 관련된 데이터 보존 방침에 따라) 정보 시스템, 기기 또는 기타 저장 수단에 저장된 정보의 시기적절한 삭제에 대한 규칙 - 시스템, 어플리케이션 및 서비스 상의 민감 정보를 안전하게 삭제하는 절차 - 제 3자가 조직의 정보를 저장하는 경우, 정보 삭제에 대한 조항을 포함한 제 3자 계약

ISO/IEC 27001:2022, 부속서A[a]에서의 통제항목	시스템 시험	육안 검사	통제항목의 설계 및 구현에 대한 가능한 증거
8.11 데이터 마스킹			- (예를 들어, 특정 주제에 대한 접근 권한 방침에 따라) 데이터 마스킹에 대한 규칙 - 민감 정보(예: 개인정보(PII) 보호가 데이터 마스킹, 가명화, 익명화와 같은 기술을 요구하는 경우를 결정하기 위해 수행된 분석의 결과 - 데이터 마스킹, 가명화 또는 익명화에 사용된 기술
8.12 데이터 유출 예방	가능		- 민감 정보를 처리, 저장 또는 전달하는 시스템, 네트워크 및 기타 기기에 적용되는 데이터 유출 예방 조치에 대한 규칙 - 유출로부터의 보호를 요구하는 식별된 정보 - 모니터링을 포함하여 유출을 예방하는 조치를 보유하고 있는 식별된 유출 채널 - 데이터 손실 예방 시스템에 대한 구성
8.13 정보 백업	권고		- (예를 들어, 특정 주제에 대한 방침에서 백업과 관련하여) 정보, 소프트웨어 및 시스템 백업에 대한 규칙 - 조직의 수립된 비즈니스 요구사항을 기반으로 한, 백업 계획 - 백업의 시기적절하고 올바른 시행을 모니터링하고, 실패를 다루기 위한 운영 절차 - 정기적인 주기로 수행된 백업 복원 테스트
8.14 정보처리 시설의 중복성			- 비즈니스 서비스 및 정보 시스템의 가용성에 대하여 식별된 요구사항 - 적절한 중복성을 제공하는 상위 요구사항을 포함하는 시스템의 아키텍처 - 수행된 시스템 대체 작동 테스트의 결과
8.15 로깅(logging)	권고		- (예를 들어, 특정 주제와 관련된 기록 방침에서) 로그 생성 목적, 수집되는 데이터 및 로그 데이터 처리를 위한 로그별 요구사항에 대한 규칙 - 보안관련 로그 목록 및 미승인 조작에 대한 보호조치 - (예를 들어, 정상이 아닌 활동 또는 비정상 행위를 식별하기 위하여) 로그 이벤트의 정기적 분석 및 해석을 수행하는 절차 - 로그 시스템 구성
8.16 모니터링 활동	가능		- 이상행위에 대한 네트워크, 시스템 및 어플리케이션(응용프로그램) 모니터링 규칙 - 정상 행위에 대해 수립된 베이스라인과 경고를 트리거하기 위해 도출된 기준 - 규정된 보존 기간 동안 보유된 모니터링 로그 - 이상행동을 식별하기 위해 수행된 분석의 결과
8.17 클락 동기화	가능		- 조직이 사용하는 기준 시간 출처의 목록 - 클락 동기화 방법 및 시차 처리
8.18 특권을 가진 유틸리티 프로그램의 사용	가능		- 시스템 및 어플리케이션 제어를 우선할 수 있는 사용된 유틸리티 프로그램 목록 - 이러한 유틸리티 프로그램을 제한하고 엄격하게 제어하기 위해 사용되는 프로세스, 절차 및 기타 방법
8.19 운영 시스템 상의 소프트웨어 설치	가능		- 버전과 함께, 설치된 소프트웨어 인벤토리를 포함하여 운영 시스템 상의 소프트웨어 설치를 관리하는데 사용되는 절차 및 조치

ISO/IEC 27001:2022, 부속서A[a]에서의 통제항목	시스템 시험	육안 검사	통제항목의 설계 및 구현에 대한 가능한 증거
			- 사용자가 설치할 수 있는 소프트웨어 종류에 대한 규칙 - 교육을 받은 관리자 이외의 인원이 소프트웨어를 설치하기 위한 제한사항
8.20 네트워크 보안	권고		- 미승인 접근으로부터 네트워크 상의 정보보안을 보장하고, 연결된 서비스를 보호하는 규칙 - 네트워크 상 정보 및 정보처리 시설의 보호를 위해 실행된 조치 및 보안 특성 (예: 구성 템플릿, 암호 통제항목 구성, 게이트웨이 규칙 집합, 네트워크 장비 구성 샘플) - 네트워크 구성 문서화 (도식, 구성 파일, 구분) - 네트워크와의 인증 시스템 연결에 대한 규칙
8.21 네트워크 서비스 보안			- 네트워크 및 네트워크 서비스 안전 사용에 대한 규칙 - 보안 메커니즘 및 서비스 수준에 사용된 네트워크 및 네트워크 서비스에 대한 목록 - 네트워크 서비스 제공자로부터 획득한 보증
8.22 네트워크 분리			- 네트워크 도메인 분리에 관한 규칙(예 : 신뢰수준, 중요도 및 민감도)과 엑세스 제어에 대한 특정 주제별 정책에 따른 규칙 - 네트워크 토폴로지(무선 포함)와 목적 및 규칙에 대한 설명이 포함된 구역 분리 - 네트워크 도메인의 보안 경계의 정의 - 방화벽 규칙뿐만 아니라 네트워크 도메인 보안 경계를 관리하는 프로세스
8.23 웹 필터링	가능		- 바람직하지 않거나 부적절한 웹사이트에 대한 모든 제한을 포함하여, 온라인 출처의 안전하고 적절한 사용에 대한 규칙 - 외부 웹사이트의 악의적인 내용에 대한 노출을 줄이기 위하여 실행된 조치 (예: 필터링 규칙) - 온라인 출처의 안전하고 적절한 사용에 대하여 모든 인원에게 전달된 인식 및 교육훈련 활동
8.24 암호 사용	권고		- (예를 들어, 특정 주제에 대한 암호 관련 방침에서) 수용 가능한 암호 및 키 관리를 포함하여, 암호의 효과적인 사용에 대한 규칙 - 조직이 사용하고 있는 암호 기술의 목록 - 암호 키의 생성, 저장, 보관, 복원, 배포, 폐기 및 파괴를 포함한 키의 관리를 위한 표준 및 방법
8.25 안전한 개발 생명주기	가능		- 정보보안이 안전한 개발 생명주기 내에 설계되고 실행됨을 보장하기 위한 안전한 소프트웨어 개발의 규칙 - 개발, 테스트, 생산 환경 간 구분 - 전체 소프트웨어 개발 동안 정보보안 요구사항을 적절하게 보장하는 보안 프로세스 및 체크 포인트 - 소프트웨어 개발이 외주처리된 경우, 정보보안 요구사항의 적절한 처리에 대해 얻은 보증
8.26 어플리케이션 보안 요구사항			- 구체적인 리스크 평가를 기반으로 어플리케이션 보안 요구사항을 규정하는 프로세스 - 특정 정보보안 요구사항을 명시하는 어플리케이션 리스크 평가 수행 - 어플리케이션의 최근 개발/실행, 특히 거래 서비스, 전자 주문 및 결제 어플리케이션 샘플에 대해 식별된 요구사항

ISO/IEC 27001:2022, 부속서A[a]에서의 통제항목	시스템 시험	육안 검사	통제항목의 설계 및 구현에 대한 가능한 증거
8.27 보안 시스템 구성 및 공학 원칙			- 개발 수명주기 내에서 정보 시스템이 보안 설계, 실행 및 운영됨을 보장하기 위해 수립된 아키텍처 및 보안 공학 원칙 - 소프트웨어 개발 시 보안공학 원칙을 통합 - 위의 공학 원칙 사용을 확인하는, 어플리케이션 별 보안 실행의 샘플 - 적용 가능한 경우, 외주처리된 개발에 대한 계약서 상에 삽입된 안전한 공학 원칙
8.28 보안 코딩	가능		- 신규 개발 및 재활용 시나리오에 둘 다 사용되는 보안 코드 원칙에 대한 규칙 - 계획 단계, 코딩 전, 코딩 동안, 검토 및 유지보수 동안에의 보안 코딩 원칙 적용을 보장하는 프로세스 - 코드 스캐닝 기술을 포함하여, 최근 개발 활동의 샘플에 대한 구체적인 보안 코딩 원칙의 적용 - 접근 제한을 포함하여, 코드에 대한 보호 메커니즘
8.29 개발 및 수용에서의 보안 테스트	권고		- 정보보안 요구사항이 어플리케이션 또는 코드가 생산 환경에서 사용되었을 때 충족하는지를 검증하기 위한 보안 테스트의 규칙 - 보안 테스트에 실제 사용되는 요구사항 집합의 샘플과 해당 시험 결과 - 자동화된 테스트 장치(예: 코드 분석 장치, 취약점 스캐너, 기능 테스트)로부터의 결과 및 후속조치
8.30 외주처리된 개발			- 조직에 의해 요구되는 정보보안 조치가 외주처리된 시스템 개발에서 어떻게 실행되어야 하는지에 대한 규칙 - 외주처리된 시스템 개발과 관련한 활동의 지시, 모니터링 및 검토하기 위해 수행된 절차 - 기대에 부합함을 보장하는 공급업체에 대한 모니터링 또는 검토 결과
8.31 개발, 테스트 및 생산 환경의 구분	가능		- 다른 개발 환경에 대한 구체적인 요구사항을 포함하여, 생산, 테스트 및 개발 환경 간 구분 수준에 대한 규칙 - 개발, 테스트 및 생산 환경 간 구분 - 테스트 및 생산 환경의 보호 (예: 민감 생산 정보가 활용되지 않음을 보장하면서, 접근 제한, 네트워크 분리)
8.32 변경 관리	권고		- 정보보안을 관리하기 위한 변경 관리 규칙 - 변경 관리 절차 (예: 문서화, 사양, 테스트, 품질관리, 관리된 실행) - 변경사항이 어떻게 테스트, 승인 및 사용되는지를 보여주는 발생된 변경의 샘플
8.33 테스트 정보	가능		- 테스트 정보의 적절한 선정, 사용, 보호 및 관리에 대한 규칙 - 테스트 목적으로 사용하는 동안 운영 정보의 보호 절차 (예: 마스킹) - 테스트 환경에서 정보를 삭제한 샘플
8.34 심사 테스트 동안의 정보 시스템 보호	가능		- 심사 테스트 또는 운영 시스템 평가를 포함하는 기타 보증 활동의 요청 목록 - 수행된 심사 테스트 및 이러한 테스트가 승인되고 수행된 샘플
a 이 영역에서 인용된 수는 ISO/IEC 27011:2022 부속서 A의 통제항목 번호와 일치한다.			

이 페이지는 제본을 위해 의도적으로 삽입된 페이지임.
This page remains blank for editorial purpose.

한국인정지원센터
Korea Accreditation Board

KAB-SR-ISMS

ISO 27001 정보보안경영시스템 인증스킴 요구사항

Issue 3.1