KAB-SR-PIMS

ISO 27701 개인정보보호경영시스템 인증스킴 요구사항

Issue 2

2026. 01. XX. 발행

2026. 01. XX. 시행

ISO/IEC 27706:2025

이 문서는 ISO 가 발행하고 IAF 가 승인한 ISO/IEC 27706:2025 Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of privacy information management systems 문서의 요구사항을 변경 없이 반영한 것으로, ISO 27701 개인정보보호경영시스템 인증서비스를 제공하는 인증기관이 준수하여야 할 인증스킴 요구사항이다.

KAB-SR-PIMS

ISO 27701 개인정보보호경영시스템 인증스킴 요구사항

목차

0 개요

이 문서는 **ISO/IEC 27701**에 따라 개인정보보호경영시스템 심사와 인증을 제공하는 기관에 대한 요구사항을 규정하고 있다.

이 문서는 또한 인정기관과 동등성평가사가 인증기관 인원의 적격성과 인증 프로세스에 관한 최소 요구사항을 효과적이고 일관성 있게 평가하도록 돕는데 목적이 있다.

1 적용범위

이 문서는 **KAB-R-MSCB**에 포함된 요구사항에 추가하여, **ISO/IEC 27701**에 따라 개인정보보호경영시스템(이하 PIMS)에 대한 심사와 인증을 제공하는 기관에 대한 요구사항을 규정하고 지침을 제공한다.

이 문서에 포함된 요구사항은 적격성과 신뢰성의 측면에서 PIMS 인증기관이 입증한다. 이 문서에 포함된 지침은 PIMS 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.

ISO/IEC 17000 적합성평가 – 용어 및 일반 원칙
KAB-R-MSCB 적합성평가 – 경영시스템 심사 및 인증을 제공하는 기관에 대한 요구사항 – 제 1 부: 요구사항
ISO/IEC 27701:2025 적합성평가 – 정보보안, 사이버보안 및 개인정보 보호 — 개인정보보호경영시스템 — 요구사항 및 지침

3 용어의 정의

이 문서의 목적에 따라 **ISO/IEC 17000, KAB-R-MSCB** 와 **ISO/IEC 27701** 에 주어진 것과 함께, 다음의 용어와 정의를 적용한다.

ISO 와 IEC 는 다음 주소에서 표준화에 사용하기 위한 용어 데이터베이스를 유지한다.

— ISO 온라인 검색 플랫폼: https://www .iso .org/obp
— IEC 전자사전: http://www. electropedia .org/

3.1 인증문서 (인증서)
Certification documents

클라이언트의 PIMS 가 경영시스템에서 요구하는 **ISO/IEC 27701** 및 모든 부속 문서에 적합함을 나타내는 문서

비고 1 이 정의는 인증문서라고 총칭되는 문서의 수를 제한하지 않는다.

[출처: ISO/IEC 27006-1:2024 3.1, 수정됨, "정보보안경영시스템"에 대한 인용이 "개인정보보호경영시스템"으로 변경되었고, **ISO/IEC 27001** 은 **ISO/IEC 27701** 로 변경됨]

3.2 개인정보 (PII)
Personally identifiable information PII

a) 어떤 정보와 연관된 자연인과 정보 간의 연결을 설정하는데 이용될 수 있는 정보 또는,
b) 자연인과 직접적 또는 간접적으로 연결되어 있거나 연결될 가능성이 있는 정보

비고 1 정의에서 말하는 "자연인"은 개인정보 주체를 지칭한다. 개인정보 주체가 식별 가능한지 여부를 결정하기 위하여, 해당 데이터를 보유한 프라이버시 이해당사자 또는 기타 어떠한 당사자에 의해서라도 개인정보 집합과 자연인 간의 연결을 설정하기 위하여 합리적으로 사용될 수 있는 모든 수단을 고려하여야 할 것이다.

[출처: ISO/IEC 29100:2024, 3.7]

3.3 개인정보 컨트롤러
PII controller

개인적인 목적으로 데이터를 이용하는 자연인을 제외하고 개인정보(3.2) 처리 목적과 방법을 결정하는 프라이버시 이해 당사자(또는 이해 당사자들)

비고 1 개인정보 컨트롤러는 때때로 다른 주체(예: 개인정보 프로세서(3.5))에게 자신을 대신해 개인정보를 처리(3.8)하도록 지시한다. 그럴 경우에도 처리에 대한 책임은 개인정보 컨트롤러에게 남아있다.

[출처: ISO/IEC 29100:2024, 3.8]]

3.4 개인정보 주체
PII principal

개인정보(3.2)가 관련되는 자연인

[출처: ISO/IEC 29100:2024, 3.9]

3.5 개인정보(PII) 프로세서
PII processor

개인정보 컨트롤러(3.3)의 지시에 따라서 개인정보(3.2)를 처리하는 프라이버시 이해 당사자

[출처: ISO/IEC 29100:2024, 3.10]

3.6 개인정보보호경영시스템 (PIMS)
Privacy information management system (PIMS)

개인정보 처리(3.8)에 의해 잠재적으로 영향을 받는 개인정보 보호를 다루는 경영시스템

[출처: ISO/IEC 27701:2025, 3.23]

3.7 프라이버시 영향 평가 (프라이버시 리스크 평가)
Privacy impact assessment (privacy risk assessment)

조직의 보다 광범위한 리스크 관리 프레임워크 내에서, 개인정보(3.2) 처리(processing)와 관련된 잠재적 프라이버시 영향의 처리(treatment)를 식별, 분석, 평가, 자문, 의사소통 및 계획하는 전반적인 프로세스

[출처: ISO/IEC 29100:2024, 3.18]

3.8 개인정보 처리
Processing of PII

개인정보(3.2)에 대해 행해지는 작업 또는 작업의 집합

비고 1 개인정보 처리 작업의 예는 개인정보의 수집, 저장, 변경, 검색, 참조, 공개, 익명화, 가명화, 배포 또는 가용화 조치, 삭제 또는 파기를 포함하며, 이에 국한되지 않는다.

[출처: ISO/IEC 29100:2024, 3.21]

3.9 적용성 보고서
Statement of applicability

모든 필수 통제항목과 통제항목의 포함 또는 제외에 대한 정당성을 문서화한 것

[출처: ISO/IEC 27701:2025, 3.25]

4 원칙

KAB-R-MSCB, 4 절의 원칙을 적용하여야 한다.

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.

5.2.2 이해상충

KAB-R-MSCB, 5.2.5의 요구사항과 더불어, 인증기관은 프라이버시, 데이터 보호(예: 외부 데이터보호책임자 제

공 또는 데이터 보호 점검의 형태) 또는 프라이버시 리스크 관리와 관련된 경영시스템에 대한 자문을 제공하여서는 안 된다.

인증기관은 자문으로 간주되지 않거나 잠재적인 이해상충을 가지지 않는 경우, 다음 활동을 수행할 수도 있을 것이다.

a) PIMS 와 관련하여 경영시스템 또는 심사와 관련된 교육훈련을 개최하거나 강사로 참여하는 경우, 인증기관이 공개적으로 이용 가능한 일반적인 정보만을 제공
b) 인증심사 및 사후관리 심사를 통한 부가적인 가치를 제공하는 행위. 예를 들어, 심사동안 개선의 기회가 명확해짐에 따라 이를 식별하는 것

5.3 배상책임 및 재정

KAB-R-MSCB, 5.3 의 요구사항을 적용하여야 한다.

6 조직구조 요구사항

KAB-R-MSCB, 6 절의 요구사항을 적용하여야 한다.

7 자원 요구사항

7.1 인원의 적격성

7.1.1 일반사항

KAB-R-MSCB, 7.1.1 의 요구사항을 적용하여야 한다.

7.1.2 적격성 기준의 결정

7.1.2.1 일반 사항

KAB-R-MSCB, 7.1.2 의 요구사항을 적용하여야 한다.

7.1.2.2 일반적 적격성 요구사항

인증기관은 **KAB-R-MSCB**, **표 A.1** 에 인용된 인증업무기능에 필요한 적격성 요구사항을 결정해야 한다.

인증기관은 PIMS 기술 분야와 관련하여 **부속서 C**의 요구사항들을 반영하여야 한다.

인증기관은 **ISO/IEC 27701**에 따라 심사팀의 정보보안에 대한 적격성 요구사항을 고려하여야 한다.

비고 KAB-SR-ISMS Issue 3.1의 **7.1.3**항은 정보보안에 대한 적격성 요구사항을 제공한다.

7.1.3 평가 프로세스

7.1.3.1 일반 사항

KAB-R-MSCB, 7.1.3 의 요구사항을 적용하여야 한다.

7.1.3.2 심사원 평가

인증기관은 다음을 통해 심사원이 필수 지식 및 경험을 보유함을 입증하여야 한다.

a) 인정된 PIMS 관련 자격사항
b) PIMS 교육 훈련과정 참여 및 개인 자격증 획득
c) 전문성 개발 기록의 최신화
d) 적격하고 권한을 부여받은 별도의 PIMS 심사원이 입회한 PIMS 심사

비고 프라이버시 관련 지식과 스킬에는 자격이 있는 별도의 PIMS 심사원의 감독하에 완료된 PIMS 심사의 이수 및 PIMS에 특정된 지식과 스킬을 포함할 수 있다.

7.1.3.3 심사원 선정

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

a) PIMS 심사원으로서 활동하기에 충분한 프라이버시 분야에서 근무한 업무경험
b) PIMS 심사 및 심사 관리와 관련한 교육을 이수하고, ISO/IEC 27701에 따라 심사 스킬을 입증
c) 지속적 전문성 개발을 통해 프라이버시 정보 관리와 심사에 대한 최신 지식 및 스킬 유지

7.1.3.4 기술전문가 선정

기술전문가를 선정하는 프로세스는 각 기술전문가에 대하여 다음 사항을 보장하여야 한다.

a) 기술전문가로서 활동하기에 충분한 프라이버시 분야에서 근무한 업무경험
b) 지속적 전문성 개발을 통한 프라이버시 정보 관리에 대한 최신 지식 및 스킬 유지

7.1.4 기타 고려 사항

KAB-R-MSCB, 7.1.4 의 요구사항을 적용하여야 한다.

7.2 인증 활동에 관련된 인원

KAB-R-MSCB. 7.2 의 요구사항을 적용하여야 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, 8.1 의 요구사항을 적용하여야 한다.

8.2 인증문서

8.2.1 일반사항

KAB-R-MSCB, 8.2 의 요구사항을 적용하여야 한다.

8.2.2 PIMS 인증문서

인증문서는 다음을 포함하여야 한다.

a) "개인정보보호경영시스템"이라는 문구
b) 인증범위 내 각 활동, 제품 또는 서비스에 대한 조직의 역할(즉, 조직이 개인정보 컨트롤러 또는 개인정보 프로세서 또는 둘 다로 활동하는지 여부)
c) 인증범위 내 각 활동, 제품 또는 서비스를 위해 데이터가 처리되는 개인정보 주체 (예: 직원, 고객)
d) 조직의 PIMS 에 대한 적용성 보고서의 해당 버전

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

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

8.3 인증에 대한 언급 및 마크의 사용

KAB-R-MSCB, 8.3 의 요구사항을 적용하여야 한다.

8.4 기밀준수

8.4.1 일반사항

KAB-R-MSCB, 8.4 의 요구사항을 용하여야 한다.

8.4.2 조직의 기록에 대한 접근

PIMS 관련 정보가(예를 들어 PIMS 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 PIMS 가 적절하게 심사될 수 있는지를 결정하여야 한다. 인증기관에서 확인된 기밀 정보 또는 민감한 정보에 대한 검토 없이는 PIMS 심사가 적절하지 않다고 결정되었다면, 인증기관은 클라이언트에게 적절한 접근 조치가 부여될 때까지 인증심사가 수행될 수 없음을 통지해야 한다.

8.5 인증기관과 클라이언트간의 정보 교환

KAB-R-MSCB, 8.5 의 요구사항을 적용하여야 한다.

9 프로세스 요구사항

9.1 인증 이전의 활동

9.1.1 신청

9.1.1.1 일반사항

KAB-R-MSCB, 9.1.1 의 요구사항을 적용하여야 한다.

9.1.1.2 신청 준비

인증기관은 **ISO/IEC 27701** 의 요구사항을 충족하는 PIMS 를 문서화하고 구현하지 않은 클라이언트의 신청을 수락하지 않아야 한다.

9.1.2 신청서 검토

KAB-R-MSCB, 9.1.2 의 요구사항을 적용하여야 한다.

9.1.3 심사 프로그램

9.1.3.1 일반사항

KAB-R-MSCB, 9.1.3 의 요구사항을 적용하여야 한다.

심사프로그램의 일부로 원격심사 방법이 고려되어야 할 것이다. 인증기관은 **ISO/IEC TS 17012** 를 참고할 수 있다.

9.1.3.2 PIMS 통제항목

PIMS 심사의 심사프로그램은 **ISO/IEC 27701, 6.1.3 b)** 와 **c)**에 따라 클라이언트가 결정한 통제항목을 반영하여야 한다.

9.1.4 심사시간 결정

9.1.4.1 일반사항

KAB-R-MSCB, 9.1.4 의 요구사항을 적용하여야 한다.

9.1.4.2 심사시간

인증기관은 최초인증, 사후관리 및 갱신인증을 포함한 ISO/IEC 27701 인증심사에 소요되는 심사시간을 결정하여야 한다.

인증기관은 심사시간을 결정하기 위해 부속서 A 를 사용하여야 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.

9.2.1.2 PIMS 인증범위 결정

인증기관은 ISO/IEC 27701 의 인증범위가 PIMS 의 범위에 정의된 대로 클라이언트 활동 범위 내에 포함됨을 보장하여야 한다.

인증기관은 개인정보 컨트롤러, 개인정보 프로세서 또는 그 둘 모두에 관한 클라이언트의 역할을 식별하여야 한다.

인증기관은 개인정보 처리가 클라이언트 PIMS 의 범위에 속하는지 검증하여야 한다. (ISO/IEC 27701:2025 4.3 참조)

인증기관은 클라이언트의 정보보안 및 프라이버시 리스크 평가와 리스크 처리가 클라이언트의 활동을 반영하고 PIMS 범위에 정의된 활동 영역까지 확장되도록 보장하여야 한다. 인증기관은 이것이 클라이언트의 PIMS 범위와 적용성 보고서에 반영된 것을 확인하여야 한다.

9.2.1.3 심사목적

심사 목적은 클라이언트가 프라이버시 리스크 평가를 기반으로 필수 통제항목을 식별함을 보장하는 것을 포함하여야 한다.

9.2.2 심사팀 선정 및 배정

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.

9.2.3.2 일반 고려사항

심사계획은 결정된 PIMS 통제항목을 반영하여야 한다.

9.3 최초인증

9.3.1 일반사항

KAB-R-MSCB, 9.3 의 요구사항을 적용하여야 한다.

9.3.2 최초인증심사

9.3.2.1 1 단계

이 단계 심사에서 인증기관은 **ISO/IEC 27701** 에서 요구하는 문서화를 포함하는 PIMS 의 설계문서를 획득하여야 한다.

최소한, 1 단계 심사 동안 다음의 정보가 클라이언트에 의해 제공되어야 한다.

a) 클라이언트가 다루는 PIMS 활동에 대한 일반 정보
b) **ISO/IEC 27701** 에 명시되고 요구되는 PIMS 문서 사본 및 필요한 경우 기타 관련 문서

인증기관은 클라이언트의 조직상황에서 PIMS 설계, (결정된 통제를 포함하는) 프라이버시 리스크 평가 및 처리, 프라이버시 방침 및 목표, 그리고 특히 클라이언트의 준비 상태에 대해 충분히 이해하여야 한다. 이는 2 단계 심사 계획에 사용되어야 한다.

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

비고 심사에 관여하지 않은 인증기관 소속 인원이 심사보고서를 검토하고, 2 단계 심사를 진행할지 여부를 결정하며, 2 단계 심사팀 구성원의 적격성을 확인하는 경우, 이는 관련된 리스크를 일정 수준 완화하는 하나의 방법이다. 다만, 동일한 목적을 달성하기 위하여 이미 다른 리스크 완화 조치가 마련되어 있을 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 작성하여야 한다. 2 단계의 목적은 PIMS 의 효과적 이행을 평가하는 것과 더불어 클라이언트가 자체 방침, 목표 및 절차를 준수하고 있음을 확인하는 것이다.

이를 위해, 심사는 클라이언트의 다음 사항에 중점을 두어야 한다.

a) 최고 경영층의 리더십과 프라이버시 목표에 대한 의지
b) 프라이버시 관련 리스크 평가. 심사는 해당 평가가 반복되는 경우 일관되고, 타당하며, 비교할 수 있는 결과를 도출함을 보장하여야 한다.
c) 프라이버시 리스크 평가와 리스크 처리 프로세스에 기반한 통제항목 선정
d) 프라이버시 목표에 대비하여 평가를 하는, 프라이버시 성과 및 PIMS 효과성
e) 선정된 통제항목, 적용성 보고서, 프라이버시 리스크평가 결과, 리스크 처리 프로세스 및 프라이버시 방침과 목표 간의 정합성
f) 내·외부 상황 및 관련 리스크를 고려한 통제항목 구현과 선언한 통제가 실제로 구현되고 전체적으로 효과적인지 여부를 결정하기 위한 프라이버시 프로세스 및 통제항목에 대한 조직의 모니터링, 측정 및 분석
g) 최고경영자의 결정과 프라이버시 방침 및 목표를 추적할 수 있음을 보장하기 위한 프로그램, 프로세스, 절차, 기록, 내부심사, PIMS 효과성 검토

9.4 심사 수행

9.4.1 일반사항

KAB-R-MSCB, 9.4 의 요구사항을 적용하여야 한다.

9.4.2 PIMS 심사의 특별요소

인증기관 심사팀은 다음 사항을 수행하여야 한다.

a) 프라이버시 관련 리스크 평가가 PIMS 인증범위 내에서 PIMS 운영과 관련이 있고 적절하다는 것을 클라이언트가 입증하도록 요구
b) 프라이버시 관련 리스크를 식별, 조사, 평가하기 위한 클라이언트의 절차와 이행의 결과가 클라이언트의 방침, 목표 및 세부목표와 일관성이 있는지를 확인

인증기관 심사팀은 프라이버시 리스크 평가 절차가 정상적으로 그리고 적절히 이행되었는지를 확인해야 한다.

9.4.3 심사보고서

9.4.3.1 KAB-R-MSCB 9.4.8 의 요구사항에 추가하여, 심사보고서는 다음의 정보나 참조사항을 제공해야 한다.

a) 클라이언트의 프라이버시 리스크 분석에 대한 인증심사의 설명
b) ISO/IEC 27701:2025 6.1.3 에서 요구하는 바와 같이 비교를 목적으로 조직이 사용하는 프라이버시 통제항목의 집합 전체
c) 클라이언트의 역할에 대한 설명 (예를 들어 개인정보 컨트롤러, 개인정보 프로세서 또는 그 둘 모두)

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

a) 중대한 심사 추적 및 활용된 심사기법
b) 적용성 보고서 버전에 대한 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 샘플에 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 PIMS 에 대한 신뢰를 주기 위하여 클라이언트에 의해 채택된 내부 조직 및 절차의 적절성을 고려하여야 한다.

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

9.5 인증결정

KAB-R-MSCB, 9.5 의 요구사항을 적용하여야 한다.

9.6 인증 유지

9.6.1 일반사항

KAB-R-MSCB, 9.6.1의 요구사항을 적용하여야 한다.

9.6.2 사후관리 활동

9.6.2.1 **KAB-R-MSCB, 9.6.2**의 요구사항을 적용하여야 한다.

9.6.2.2 사후관리 심사절차는 이 문서에서 기술하는 클라이언트에 대한 PIMS 인증심사 절차들의 부분집합이 되어야 한다. 사후관리 심사 프로그램은 최소한 다음 사항을 포함하여야 한다.

a) 프라이버시 리스크 평가, 통제 유지, PIMS 내부심사, 경영검토, 시정조치와 같은 PIMS 유지 요소
b) **ISO/IEC 27701** 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 PIMS의 효과성
b) 관련된 프라이버시 법규 및 규제사항 준수와 주기적 평가를 위한 절차의 기능
c) 결정된 통제항목의 변경 및 그 결과에 따른 적용성 보고서의 변경사항
d) 심사프로그램에 따른 통제항목의 구현 및 효과성

9.6.2.4 인증기관은 사후관리활동의 프로그램이 프라이버시 리스크와 관련된 이슈를 반영하도록 조정하여야 한다.

사후관리심사는 다른 경영시스템의 심사와 통합될 수도 있다. 심사보고서에는 각 경영시스템과 관련된 측면을 명시하여야 한다.

사후관리심사 동안 인증기관은 발생한 불만 및 이의제기에 대한 기록을 검토하여야 한다. 인증 요구사항의 불충족이나 부적합이 확인된 경우, 인증기관은 클라이언트가 자신의 PIMS 와 절차를 어떻게 조사하고 적절하게 시정조치를 취했는지를 확인하여야 한다.

사후관리 심사보고서에는 특히 이전에 발견된 부적합의 종결, 적용성 보고서의 버전, 이전 심사로부터의 주요 변화가 포함되어야 한다. 사후관리 심사보고서는 최소한 **9.6.2.2** 와 **9.6.2.3** 의 요구사항 전체를 포함하도록 작성되어야 한다.

9.7 이의제기

KAB-R-MSCB, 9.7의 요구사항을 적용하여야 한다.

9.8 불만

KAB-R-MSCB, 9.8의 요구사항을 적용하여야 한다.

9.9 클라이언트에 대한 기록

KAB-R-MSCB, 9.9의 요구사항을 적용하여야 한다.

10 인증기관 경영시스템 요구사항

10.1 선택사항

KAB-R-MSCB, 10.1 의 요구사항을 적용하여야 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) 심사시간

A.1 일반사항

이 **부속서**는 **KAB-R-MSCB 9.1.4**에 대한 추가 요구사항이며, PIMS 심사에 국한되어 있다. 이 **부속서**는 인증기관이 다양한 범위의 활동규모와 복잡성을 가지는 PIMS 운영 조직에 대한 심사를 수행할 때 필요한 심사시간을 결정하는 절차의 개발과 관련된 최소 요구사항 및 지침을 제공한다.

인증기관은 각 클라이언트와 인증된 PIMS 에 대한 최초인증, 사후관리 및 갱신심사에 소요되는 심사시간을 규정해야 한다. 심사계획단계 동안 이 **부속서**의 사용은 적절한 심사시간 결정을 일관된 접근 방법으로 유도한다. 추가로, 심사시간은 심사과정, 특히 1 단계에서 발견된 사항에 따라 조정될 수 있을 것이다. (예: PIMS 범위의 복잡성에 대한 평가의 차이, 또는 해당 인증범위의 추가된 사업장)

본 **부속서**는 다음과 같은 사항을 제시한다.

— 심사시간 계산에 사용되는 개념 **(A.2)**

— 각 심사단계에 대한 심사시간 결정 절차에 대한 요구사항 **(A.3, A.4, A.5, A.6, A.8)**

— 복수사업장 심사 관련 요구사항 **(A.7)**

— 범위확대를 위한 심사시간 요구사항 **(A.7)**

이 접근법의 기본 가정은 심사시간 결정을 위한 계산방법이 다음과 같아야 할 것이다.

a) 결정할 수 있는 증명된 특성만 고려함

b) 인증기관이 효율적으로 적용할 수 있을 만큼 간단함

c) 적절한 구별을 가능하게 할 만큼 복잡함

심사시간 결정은 **표 A.1**의 숫자를 근거로 한다. 심사시간을 결정할 때는 영향을 미치는 요인을 고려하여야 하며, 그에 따라 조정이 이루어져야 한다.

인증기관이 규정한 심사시간 결정을 위한 접근법은 PIMS 의 복잡성에 충분한지 확인하기 위하여 정기적으로 검토되어야 한다.

A.2 개념

A.2.1 조직의 관리하에 근무하는 인원의 수

인증범위 내 모든 교대조에 대하여 조직의 관리 하에 업무를 수행하는 총인원의 수가 심사시간을 결정하는 시작점이다.

비고 조직의 관리 하에 업무를 수행하는 인원은 (조직 소속 여부와 상관없이) 인증범위 내에서 PIMS 요구사항에 따라 업무를 수행하도록 요구되는 모든 인원을 포함한다.

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

인증범위 내에서 조직의 관리 하에 업무를 수행하는 인원의 높은 비율이 동일한 특정 활동을 수행하는 경우, **표 A.1**을 활용하는 것에 앞서 심사시간 산정을 위해 인원수를 감축하는 것이 허용된다.

인증기관은 **A.3.5**에서 제공된 요인을 사용하여야 하며, 인증범위 내에서의 인원 수 감축이 적용되는 방식을 결정하기 위하여 프라이버시 리스크와 관련된 활동의 영향을 고려하여야 한다. 반복 가능하고 회사별로 적용될 수 있는 통일성 있고 일관된 절차가 문서화되어야 한다.

A.2.2 심사일수

표 A.1에 언급된 "심사시간"은 심사에 소요되는 "심사일수"를 의미한다. 본 **부속서**는 1일 8시간을 근무시간으로 계산하는 것을 기본으로 한다. (약자 "**d**"로 표현)

A.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 필요성과 샘플링의 범위는 프라이버시 목표를 충족하는 데 있어 임시사업장에서 수행되는 활동의 리스크에 대한 평가에 기초하여야 할 것이다. 선정된 샘플 사업장은 활동의 규모와 유형, 진행 중인 프로젝트의 다양한 단계의 측면에서, 조직의 적격성 요구 및 서비스의 다양성을 대표하는 것이어야 할 것이다. 일반적인 샘플링은 **9.1.4**를 참조하여 수행한다.

A.3 최초심사를 위한 심사시간 결정 절차

A.3.1 일반사항

심사시간 계산은 문서화된 절차를 따라야 한다.

A.3.2 원격심사

조직과의 의사소통을 위하여 웹 기반 협력, 웹 미팅, 텔레컨퍼런스 및 전자적인 검증과 같은 원격심사 방법이 일부 또는 전체가 사용되는 경우, 이러한 활동은 심사계획에 명시되어야 하며(**9.2.3** 참조), 부분적으로 "현장심사시간"에 포함되는 것으로 간주될 수 있다.

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

A.3.3 심사시간 계산

표 A.1에 제시된 심사시간표는 최초심사일수의 평균에 대한 시작점을 나타낸다. 이 **부속서** 와 **부속서 B** 내

에서의 해당 일수는 최초심사(1 단계 및 2 단계)의 일수를 포함하며, 이는 경험적으로 조직의 통제 하에 있는 특정 인원수가 업무를 수행하는 PIMS 범위에 적절한 것으로 나타났다. 또한, 유사한 규모의 PIMS 범위라 하더라도 일부 범위는 다른 범위보다 더 많은 시간이 소요될 수 있다는 점도 경험적으로 확인되었다.

표 A.1은 심사계획에 사용되어야 하는 틀을 제공한다. 심사시간 산출의 시작점은 모든 교대조에 대하여 조직의 통제 하에 업무를 수행하는 총 인원을 기준으로 한다. 기본 심사시간을 조정하기 위해 각각의 요인의 비중을 추가하거나 줄이면서, 심사대상 PIMS 범위에 적용되는 중대한 요인에 근거하여 심사시간을 조정한다. **표 A.1**의 심사시간표는 적용되는 요인과 허용된 편차에 대한 제한을 반영하여 사용되어야 한다(**A.3.5** 및 **A.3.6** 참조). **표 A.1**에 사용된 용어는 **A.2**에서 설명한다. **부속서 B** 에서는 이 **부속서**의 계산법을 적용하는 예시를 보여준다.

표 A1 심사시간표

조직의 관리 하에 개인정보를 다루고 처리하는 업무를 수행하거나, 해당 데이터에 접근이 가능한 인원의 수	개인정보 컨트롤러 최초 심사시간 (심사일수)	개인정보 프로세서 최초 심사시간 (심사일수)	개인정보 프로세서 + 컨트롤러 최초심사시간 (심사일수)	가감요인	총 심사시간
1 ~ 10	4	3.5	6.5	A.3.5 참조	
11 ~ 15	4	3.5	6.5	A.3.5 참조	
16 ~ 25	5	4	6.5	A.3.5 참조	
26 ~ 45	5	4	7	A.3.5 참조	
46 ~ 65	6	4.5	8	A.3.5 참조	
66 ~ 85	6	4.5	9	A.3.5 참조	
86 ~ 125	7	5	10	A.3.5 참조	
126 ~ 175	7	5	11	A.3.5 참조	
176 ~ 275	8	5.5	12	A.3.5 참조	
276 ~ 425	8	6	12	A.3.5 참조	
426 ~ 625	9	6	14	A.3.5 참조	
626 ~ 875	10	7	15	A.3.5 참조	
876 ~ 1175	11	7	16	A.3.5 참조	
1176 ~ 1550	12	8	17	A.3.5 참조	
1551 ~ 2025	13	8	19	A.3.5 참조	
2026 ~ 2675	13	9	20	A.3.5 참조	
2676 ~ 3450	14	9	21	A.3.5 참조	
3451 ~ 4350	14	10	22	A.3.5 참조	
4351 ~ 5450	15	10	22	A.3.5 참조	
5451 ~ 6800	16	10	23	A.3.5 참조	
6801 ~ 8500	16	11	24	A.3.5 참조	
8501 ~ 10700	17	11	25	A.3.5 참조	
> 10700	위와 같이 증가	위와 같이 증가	위와 같이 증가	A.3.5 참조	

A.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

— PIMS 범위 내에서 조직의 정보처리 시설에 대한 접근 권한을 부여받지 못한 인원

— PIMS 범위 내에서 조직의 정보처리 시설에 대해 입증 가능하며 특정한 제한적 접근권한을 부여받은 인원

— 정보 공개를 제한하기 위하여 엄격한 제약조건(예: 개인 물품이나 기기의 작업공간 반입을 금지하는 조치)이 도입된 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, 이 값은 그 다음 정수로 올림 되어 심사기간 계산을 위해 사용된다. 이는 허용된 인원수에 대한 최대 감축이어야 한다.

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

이 절차를 적용하여 결정된 인원 수는 **표 A.1**의 출발점이다.

A.3.5 심사시간 조정 요인

심사시간표는 단독으로 사용되어서는 안 된다. 할당되는 심사시간은 PIMS의 복잡성 및 PIMS 심사에 필요한 노력과 관련된 요인을 고려하여야 한다. 요인은 다음을 포함하나, 이에 국한되지는 않는다.

a) 개인정보 처리 활동의 복잡성

b) **ISO/IEC 27701:2025**의 **부속서 A**와 **부속서 B**에 포함되나 이에 국한되지 않은, 적용된 통제항목의 수

c) 개인정보 처리 활동의 수

d) 처리되는 개인정보의 분류/범주

e) 운영되는 위치/지역/관할 구역의 수

f) 개인정보를 이전하는 범위

g) 개인정보 처리 또는 접근 권한이 있는 인원의 수

h) 개인정보의 양

i) 개인정보 데이터를 처리하는 플랫폼의 수

A.3.6 심사시간 편차의 제한

효과적인 심사가 수행되었음을 보장하고, 신뢰할 수 있는 비교 가능한 결과를 보장하기 위해 **표 A.1**에서의 심사시간을 30% 이상 축소할 수 없다. **표 A.1**과의 편차에 대한 적절한 사유는 확립되어야 하고 문서화되어야 한다.

A.3.7 현장심사시간

심사계획과 보고서 작성을 위해 산정된 시간이 일반적으로 **A.3.3, A.3.5** 및 **A.3.6**에 따라 산정된 총 현장 "심사 시간(물리/원격)"을 70% 미만으로 줄여서는 안 될 것이다. 심사계획 및/또는 보고서 작성에 시간이 추가로 요구되는 경우, 이는 현장 심사시간을 단축하는 정당한 사유가 되지 않아야 한다. 심사원의 이동시간은 이 심사시간 산정에 포함되지 않으며, 표에 제시된 심사시간에 추가된다.

비고 1 70%는 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 **A.3.2**. 참조) "현장" 심사에 대해서는 **KAB-R-MSCB 9.4.1** 또한 참조할 수 있다.

A.4 사후관리 심사시간

최초인증심사 주기에서, 사후관리에 소요되는 심사시간은 최초심사에 소요된 기간에 비례하여야 할 것이며, 매년 사후관리에 소요되는 총 시간은 최초인증심사에 소요된 시간의 약 1/3 정도가 되어야 할 것이다. 계획되어 있는 사후관리 시간은 심사시간에 영향을 미치는 변경사항을 반영하기 위하여 수시로 검토되어야 할 것이다. 사후관리를 위해 소요되는 시간은 PIMS의 변경 사항(예: 새로운 또는 변경된 프라이버시 통제항목, 프로세스 및 서비스)을 심사할 수 있도록 증가되어야 한다.

A.5 갱신심사시간

갱신심사 수행에 소요되는 총 시간은 **9.4.2** 및 **KAB-R-MSCB 9.6.3** 에 명시되어 있는 것과 같이 이전 심사 결과에 따라야 한다. 갱신심사에 소요되는 총 심사시간은 갱신심사 시점에서 동일한 조직에 대한 최초심사시간에 비례하여야 할 것이며, 최소한 2/3 이상이 되어야 할 것이다.

A.6 복수사업장 심사시간

일반적으로 현장심사에 대한 총 심사시간은 인원의 위치와 관계없이 조직의 관리 하에 업무를 수행하는 총 인원 수를 고려하여 산정되어야 한다.

또는, 문서화되어야 하는 정당한 이유가 있는 경우, 이 조항의 첫 번째 단락에 따라 정의된 심사시간보다 총 심사시간이 더 큰 경우에 한해서, 각각의 사업장 별로 산정한 심사시간을 더하는 것이 허용된다(즉, 총 심사시간은 모든 개별 사업장에 대한 심사시간의 합을 기반으로 한다). (적용 가능한 경우) 중앙사무소 또는 지역 사업장과 관련 없는 심사의 일부를 고려하여 단축할 수도 있다. 인증기관은 이와 같은 단축의 정당성에 대한 사유를 기록하여야 한다.

A.3.3, A.3.5, 그리고 이 조항에 명시된 절차에 따르는 범위에 대해 산정된 총 현장심사일수는 경영시스템, 사업장에서 수행되는 활동 및 식별된 리스크에 대한 사업장의 관련성에 근거하여 각 사업장 전반에 분배되어야 한다. 분배의 정당성은 인증기관에 의해 기록되어야 한다. 심사시간을 전체 심사시간과 비교하기 전에 단축이 적용되어야 한다.

A.7 범위확대를 위한 심사시간

PIMS 범위확대를 위한 심사시간은 다음과 같은 요인을 고려하여 산정되어야 한다.

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

인증기관은 범위확대에 대한 일관적인 접근방식을 제공하는 절차서를 보유하여야 한다. 신규 범위에 대한 최초심사의 경우, 그 시간은 **A.3.3, A.3.5**, 및 **A.3.6**을 활용한 기존 범위에 추가되는 인원 및 사업장의 수를 기반으로 산정되어야 한다.

심사시간은 클라이언트의 PIMS를 검토하기 위해 산정된 기간에 추가되어야 한다. 이 추가 시간은 최소한 다음과 같아야 한다.

— 범위확대 심사가 사후관리심사 또는 갱신심사와 함께 수행된다면, 0.5일(심사일수)

— 독립된 심사로 범위확대 심사가 수행되는 경우, 1일(심사일수)

부속서 B (참고) 심사시간 계산 방법

B.1 일반 사항

이 **부속서**는 심사시간 계산에 대한 공식을 개발하는 부가적인 가이드라인을 제시한다. **B.2** 에서는 심사시간 계산을 위해 기본적으로 사용될 수 있는 요인의 사례를 제시하고, **B.3** 에서는 심사시간 계산 예시를 제공한다.

B.2 심사시간 계산을 위한 요인의 분류

표 B.1 에서는 **A.3.5 a)**에서 **i)**까지 나열된 심사시간 계산을 위한 주요 요인의 분류 사례를 제시한다.

표 B.1- 심사시간 계산 요인의 분류

요인	심사시간 계산을 위한 분류		
	높음	중간	낮음
a) 개인정보의 분류	• 개인정보가 매우 민감한 것으로 간주됨 • 데이터보호영향평가(DPIA) 또는 유사한 프로세스가 요구됨 • 대량의 민감/특별 범주의 개인정보	• 개인정보에 은행 계좌 및 금융정보, 국가 식별번호(NI 번호) 취약계층이 포함됨 • 인적 자원 데이터와 같은 특별 범주의 일부 데이터를 포함한 다량의 정보 • 가명화 된 데이터 (원본 데이터로 복원 가능)	• 개인정보가 일반적임 • 일부 인적자원 관련 개인정보를 포함한 일반적인 회사 개인정보 • 암호화된 데이터 • 비식별화 된 데이터 (합리적인 수단으로 원본 데이터를 복원할 수 없음)
b) 개인정보의 이전	• 다양한 관할권 및 지역으로의 개인정보 이전	• 구속력 있는 기업 규칙 또는 다른 메커니즘을 통해 개인정보 이전이 통제됨	• 상호 관계 규칙이 운영되는 동일 관할권/지역 내에서의 개인정보 이전 • 개인정보 이전을 위한 암호화 사용
c) 처리의 복잡성	• 상업적 목적의 개인정보 프로파일링 • 데이터 마이닝 • 다수의 규정 및 법규	• 자체 목적을 위한 개인정보 프로파일링 • 일부 분야별 규정	• 일반적인 처리
d) 프로세스의 수	• 여러 다른 플랫폼 사용을 필요로 하는 다중 프로세스	• 동일한 플랫폼을 사용하는 다중 프로세스	• 동일한 플랫폼을 사용하는 1~2개의 단순 프로세스
e) 개인정보 처리 또는 접근 권한이 있는 인원의 수	• 인증범위와 관련된 조직 내 인원의 100%	• 인증범위와 관련된 조직 내 인원의 50%~70%	• 인증범위와 관련된 조직 내 인원의 25% 미만
f) 구현된 부속서 A의 통제항목의 수(A.1, A.2, A.3)	• 모든 통제항목이 구현됨	• 통제항목의 70%가 구현됨	• 통제항목의 30% 미만이 구현됨
g) 위치/지역/관할권의 수	• 다수의 지역/관할권에서 운영됨	• 동일 관할권 내 다수의 장소에서 운영됨	• 단일 장소

h) 개인정보 주체 데이터의 양 (기록)	• 10억 건을 초과하는 대용량 데이터	• 100만 건을 초과하는 중간 규모 데이터	• 10만 건 미만의 소량 데이터
i) 인증범위 내에서 개인정보를 처리하는 플랫폼의 수	• ≥ 10 조직 규모에 비해 많은 플랫폼을 사용하여 개인정보가 처리됨	• ≥ 5 평균적인 수의 플랫폼을 사용하여 개인정보가 처리됨	• < 5 소수의 플랫폼을 사용하여 개인정보가 처리됨

B.3 심사시간 계산 예시

다음 요인은 심사시간을 결정하기 위하여 사용될 수도 있다.

다음 예시는 심사시간을 계산하기 위하여 A.3.5에 제공된 요인을 사용할 수 있는 사례를 보여준다.

1단계 표 B.2의 개인정보 처리 리스크와 관련된 요인을 결정한다.

2단계 표 B.3의 표 B.3의 개인정보 운영 리스크와 관련된 요인을 결정한다.

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

4단계 심사시간 차트(표 A.1)를 적용한 일수를 3단계의 요인들과 곱한다. 복수사업장 샘플링이 사용된 경우, 산출된 심사일수는 복수사업장 샘플링을 실행하기 위해 요구되는 노력에 근거하여 증가된다.

이를 통해 나온 결과가 최종 심사일수이다.

표 B.2- 개인정보 처리 리스크

개인정보 처리 리스크	심사시간 계산을 위한 분류		
	높음	중간	낮음
개인 정보의 분류	— 개인정보가 매우 민감한 것으로 간주됨 — DPIA(데이터 보호 영향 평가) 또는 유사한 프로세스가 요구됨 — 대량의 민감 정보/특별 범주의 개인 정보	— 개인정보에 은행 계좌 및 금융 정보, 국가 식별정보(NI 번호), 취약계층이 포함됨 — 인적 자원 데이터와 같은 특별 범주의 일부 데이터를 포함한 다량의 정보 — 가명화 된 데이터 (원본 데이터로 복원 가능)	— 개인정보가 일반적임 — 일부 인적자원 관련 개인정보를 포함한 일반적인 회사 개인정보 — 암호화된 데이터 — 비식별화 된 데이터 (합리적인 수단으로 원본 데이터를 복원할 수 없음)
개인정보의 이전	다양한 관할권 및 지역으로의 개인정보 이전	구속력 있는 기업 규칙 또는 다른 메커니즘을 통해 개인정보 이전이 통제됨	— 상호 관계 규칙이 운영되는 동일 관할권/지역 내에서의 개인정보 이전 — 개인정보 이전을 위한 암호화 사용
처리의 복잡성	— 상업적 목적의 개인정보 프로파일링 — 데이터 마이닝 — 다수의 규정 및 법규 — 다수의 지역/관할권에서 운영됨 — 여러 다른 플랫폼 사용을 필요로 하는 다중 프로세스 — 자동화된 의사결정	— 자체 목적을 위한 개인정보 프로파일링 — 일부 분야별 규정 — 동일 관할권 내 다수의 장소에서 운영됨 — 동일 플랫폼을 사용하는 다중 프로세스	— 일반적인 처리 — 단일 장소 — 동일 플랫폼을 사용하는 1~2개의 단순 프로세스.

표 B.3- 운영 리스크

운영 리스크	심사시간 계산을 위한 분류		
	높음	중간	낮음
개인정보 처리 또는 접근 인원의 수	인증범위와 관련된 조직 내 인원의 100%	인증범위와 관련된 조직 내 인원의 50%~75%	인증범위와 관련된 조직 내 인원의 25% 미만
개인정보 주체 데이터의 양 기록의 수)	— 10억 건을 초과하는 대용량 데이터 — 다수의 데이터 세트	— 100만 건을 초과하는 중간 규모 데이터 — 소수의 데이터 세트	— 10만 건 미만의 소량 데이터; — 1~2개의 데이터 세트1-2
구현된 부속서 A의 통제항목의 수 (A.1, A.2, A.3)	모든 통제항목이 구현됨	통제항목의 70%가 구현됨	통제항목의 30% 미만이 구현됨

표 B.4- 심사시간에 영향을 미치는 요인

		개인정보 처리 리스크		
		낮음	중간	높음
개인정보 운영 리스크	높음	+5% ~ +20%	+10% ~ +50%	+20% ~ +100%
	중간	−5% ~ −10%	0%	+10% ~ +50%
	낮음	−10% ~ −30%	−5% ~ −10%	+5% ~ +20%

부속서 C (필수) 요구되는 지식과 스킬

C.1 일반사항

KAB-R-MSCB A.1 의 요구사항을 적용하여야 한다.

C.2 경영시스템 심사원과 심사팀의 적격성 요구사항

C.2.1 일반사항

KAB-R-MSCB A.2 의 요구사항을 적용하여야 한다.

C.2.2 PIMS 심사원과 심사팀의 적격성 요구사항

각 심사원은 다음의 지식을 보유하여야 한다.

a) ISO/IEC 27701
b) PIMS에서 사용하는 프라이버시 용어, 정의 및 개념
c) 개인정보의 식별, 관리 및 처리
d) 개인정보보호 중심 설계(privacy by design) 및 개인정보보호 기본 설정(privacy by default)
e) PIMS의 모니터링, 측정, 분석 및 평가
f) 프라이버시 정보 관리와 개인정보 처리와 관련된 리스크
g) 프라이버시 정보 관리의 정책 및 비즈니스 요구사항

총체적으로, 심사팀원들은 다음의 지식을 보유하여야 한다.

h) 프라이버시 정보 관리 및 개인정보 처리 관련 도구, 방법, 및 그 적용
i) 프라이버시 정보 리스크 평가, 프라이버시 영향 평가 및 관련 방법과 리스크 관리
j) PIMS에 적용 가능한 프로세스
k) 프라이버시와 관련되거나 프라이버시가 이슈가 되는 최신 기술
l) ISO/IEC 27701에 포함된 모든 통제항목 및 그 적용
m) 프라이버시 정보 관리 및/또는 개인정보 처리(예: 특정 분야 법률 및 지역 프라이버시 법률)에 적용되는 법적 요구사항
n) 업계 프라이버시 모범 사례 및 프라이버시 절차

C.3 심사보고서 검토 및 인증결정을 하는 인원을 위한 적격성 요구사항

C.3.1 일반사항

KAB-R-MSCB A.3의 요구사항을 적용한다. 추가로 다음의 요구사항과 지침을 적용한다.

C.3.2 PIMS 의 심사보고서 검토 및 인증결정을 하는 인원을 위한 적격성 요구사항

심사보고서를 검토하고 인증결정을 내리는 인원은 다음의 지식을 보유하여야 한다.

a) **ISO/IEC 27701**

b) 프라이버시 관련 법적 및 규제적 요구사항

c) 인증범위의 적절성 및 범위의 변경에 대한 검증이 가능하도록, **ISO/IEC 27701**의 개인정보 처리(예: 개인정보 컨트롤러 및 개인정보 프로세서 별 활동 또는 둘 다)에 대한 인증범위 요구사항

d) 프라이버시 정보 리스크 평가, 프라이버시 영향 평가 및 프라이버시 리스크 관리

e) PIMS에 적용 가능한 프로세스에 대한 일반적인 이해

C.4 요구되는 심사팀의 적격성 결정, 심사팀 선정 및 심사시간 결정을 위한 신청서 검토를 수행하는 인원에 대한 적격성 요구사항

KAB-R-MSCB A.3의 요구사항을 적용한다.

한국인정지원센터
Korea Accreditation Board

KAB-SR-PIMS

ISO 27701 개인정보보호경영시스템 인증스킴 요구사항

Issue 2