

〈ISO 27001 정보보안경영시스템 인증스킴 요구사항(KAB-SR-ISMS) 신규조문 대비표〉

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
0. 개요 KAB-R-MSCB는 경영시스템 심사 및 인증을 수행하는 기관에 대한 기준을 규정하고 있다. 이러한 기관이 ISO/IEC 27001:2013에 따른 정보보안경영시스템(ISMS)의 심사 및 인증을 목적으로 KAB-R-MSCB에 적합함을 인정받으려면, KAB-R-MSCB에 추가되는 요구사항과 지침이 필요하다. 이러한 사항들을 이 문서에서 제공한다.	0. 개요 KAB-R-MSCB는 경영시스템 심사 및 인증을 제공하는 기관에 대한 <u>요구사항 및 지침</u> 을 규정하고 있다. 이러한 기관이 ISO/IEC 27001에 따른 정보보안경영시스템(ISMS)의 심사 및 인증을 목적으로 KAB-R-MSCB에 적합함을 인정받으려면, KAB-R-MSCB에 추가되는 요구사항과 지침이 중요하다. 이러한 사항들을 이 문서에서 제공한다.	- 영문 표현 변경에 따른 번역 수정 - 참조표준 변경 - 영문 표현 변경에 따른 번역 수정
<신 설>	이 문서는 ISMS에 대한 심사와 인증을 제공하는 기관에 대한 <u>요구사항</u> 을 규정한다. 이 문서는 인증기관으로 칭해지는 이러한 기관에 대한 일반적인 <u>요구사항</u> 을 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.	- 문서 기능의 명확화
이 문서의 내용은 KAB-R-MSCB의 구조를 따르고 있으며, KAB-R-MSCB를 ISMS 인증에 적용하기 위한 ISMS에 특화된 <u>요구사항과 지침</u> 은 “IS” 로 표기되어 있다.	이 문서의 내용은 KAB-R-MSCB의 <u>구조</u> 를 따른다.	- ISMS에 특화된 요구사항 및 지침에 대한 내용 삭제
이 문서에서 “~하여야 한다(shall)” 로 표기된 것은 KAB-R-MSCB와 ISO/IEC 27001을 반영한 의무사항이다. “~하여야 할 것이다(should)” 로 표기된 것은 권고를 의미한다.	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.	- 서술 방식 변경 및 may, can의 추가
이 문서의 우선적인 목적은 KAB가 인증기관을 평가할 때 활용하여야 하는 표준을 보다 효과적이고 일관성 있게 적용할 수 있도록 하는 데 있다.	<삭 제>	- 문서의 우선적 목적 부분 삭제
이 문서 전체에서 “경영시스템” 과 “시	<삭 제>	- “경영시스템” 용

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
스텝”은 같은 용어로 사용된다. 경영시스템의 용어정의는 ISO 9000:2005에서 찾을 수 있다. 이 문서에서 사용하는 경영시스템을 IT시스템과 같은 다른 유형의 시스템과 혼동하여서는 안 될 것이다.		어 설명 삭제
1. 적용범위	1. 적용범위	
이 문서는 KAB-R-MSCB와 ISO/IEC 27001에 포함된 요구사항에 추가하여, 정보보안경영시스템(ISMS)에 대한 심사 및 인증을 제공하는 기관에 대한 요구사항을 규정하고 지침을 제공한다. 이 문서의 우선적인 목적은 ISMS 인증을 제공하는 인증기관의 인정을 지원하는 것이다.	이 문서는 KAB-R-MSCB에 포함된 요구사항에 추가하여, 정보보안경영시스템(ISMS)에 대한 심사 및 인증을 제공하는 기관에 대한 요구사항을 규정하고 지침을 제공한다. <삭 제>	- ISO/IEC 27001 삭제 - 문서의 목적 삭제
이 문서에 포함된 요구사항은 적격성과 신뢰성의 측면에서 ISMS 인증기관이 입증할 필요가 있으며, 이 문서에 포함된 지침은 ISMS 인증기관 요구사항에 대한 추가적인 해석을 제공한다.	이 문서에 포함된 요구사항은 적격성과 신뢰성의 측면에서 ISMS 인증기관이 입증한다. 이 문서에 포함된 지침은 ISMS 인증기관 요구사항에 대한 추가적인 해석을 제공한다.	- 영문 표현 변경에 따른 번역 수정
2 인용표준	2 인용표준	
다음의 표준들은 그 내용의 일부 또는 전체가 이 문서의 필수 요구사항을 구성하는 방식으로 인용되었으며 반드시 활용되어야 한다.	다음의 표준들은 그 내용의 일부 또는 전체가 이 문서의 필수 요구사항을 구성하는 방식으로 인용되었다.	- 영문 표현 변경에 따른 번역 수정
KAB-R-MSCB 적합성평가 - 경영시스템 심사 및 인증기관에 대한 요구사항 - 제1부: 요구사항 ISO/IEC 27000 정보보안 - 보안기술 - 정보보안경영시스템 - 개요 및 용어 ISO/IEC 27001:2013 정보보안 - 보안기술 - 정보보안경영시스템 - 요구사항	KAB-R-MSCB 적합성평가 - 경영시스템 심사 및 인증기관에 대한 요구사항 - 제1부: 요구사항 <삭 제> ISO/IEC 27001:2022 정보보안, 사이버보안 및 개인정보 보호 - 정보보안경영시스템 - 요구사항	- 인용표준 삭제 - 인용표준 최신본 반영
3 용어의 정의	3 용어의 정의	
<신 설>	3.2 통제항목 / Control	
<신 설>	리스크를 유지 및/또는 수정하는 관리수단	
<신 설>	비고 1 통제항목에는 리스크를 유지 및/또는 조정하는 모든 프로세스, 장치, 관행 또는 기타 조건 및/또는 행위를 포함하나 이에 한정되지 않는다.	
<신 설>	비고 2 통제항목은 의도된 또는 추정된	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
	완화 효과를 항상 발휘하지 않을 수도 있다. [출처 : ISO/IEC 27002:2022, 3.1.8]	
<신 설>	3.3 외부 상황 / External context	
<신 설>	조직이 자신의 목적을 달성하고자 하는 외부 환경	
<신 설>	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]	
<신 설>	3.4 정보보안 / Information security	
<신 설>	정보의 기밀성, 무결성, 가용성을 보존하는 것	
<신 설>	비고 1 이 밖에도 진본성, 책임추적성, 부인방지, 신뢰성을 비롯해 그 밖의 성질들이 포함될 수도 있다. [출처 : ISO/IEC 27000:2018, 3.28]	
<신 설>	3.5 정보보호 사건 / Information security incident	
<신 설>	기업 운영을 저해하고 정보보호를 위협할 확률이 상당한, 하나의 혹은 일련의 원치 않은 혹은 예기치 않은 정보보호 이벤트 [출처 : ISO/IEC 27000:2018, 3.31]	
<신 설>	3.6 정보 시스템 / Information system	
<신 설>	애플리케이션, 서비스, 정보기술 자산, 또는 그 밖의 정보처리 구성요소 [출처 : ISO/IEC 27000:2018, 3.35]	
<신 설>	3.7 내부 상황 / internal context	
<신 설>	조직이 자신의 목적을 달성하고자 하는 내부 환경	
<신 설>	비고 1 내부 상황에는 다음이 포함될 수 있다.	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
	<ul style="list-style-type: none"> — 지배구조, 조직의 구조, 역할 및 책임 추적성 — 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 <p>[출처 : ISO/IEC 27000:2018, 3.38]</p>	
<신 설>	3.8 경영시스템 / Management system	
<신 설>	방침과 목표를 수립하고 그 목표를 달성하기 위한 프로세스를 수립하기 위한, 상호 관련되거나 상호 작용하는 조직 요소의 집합	
<신 설>	비고 1 경영시스템은 예를 들면, 품질경영, 재무경영 또는 환경경영 등, 단일 또는 다수의 분야를 다룰 수 있다.	
<신 설>	비고 2 경영시스템 요소는 조직의 구조, 역할과 책임, 기획, 운영, 방침, 관행, 규칙, 신념, 목표, 그리고 이들 목표를 달성하기 위한 프로세스 등을 수립한다.	
<신 설>	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.	
<신 설>	비고 4 이 용어와 정의는 ISO/IEC Directives, Part1에 통합된 ISO 부록판의 부속서 SL에 제시된 ISO 경영시스템 표준을 위한 공통 용어와 핵심 정의 중의 하나이다. 본래의 정의에서 비고 1~비고 3이 변경되었다. <p>[출처 : ISO 9001:2015, 3.5.3]</p>	
<신 설>	3.9 조직 / Organization	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
<신 설>	조직의 목표 달성에 대한 책임, 권한 및 관계가 있는 자체의 기능을 가진 사람 또는 사람의 집단	
<신 설>	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]	
<신 설>	3.10 리스크 / Risk	
<신 설>	불확실성이 목표에 미치는 영향	
<신 설>	비고 1 영향이란 예상된 것에서 벗어난 것을 말한다. 긍정적 또는 부정적인 것일 수 있다.	
<신 설>	비고 2 불확실성은 사건, 사건의 결과 또는 가능성에 대한 이해 또는 지식에 관련된 정보의 부족, 심지어 부분적으로 부족한 상태이다.	
<신 설>	비고 3 위험은 잠재 이벤트(ISO Guide 73:2009, 3.5.1.3에서 정의됨)와 결과(ISO Guide 73:2009, 3.6.1.3에서 정의됨), 또는 이들의 조합으로 언급되는 경우가 많다.	
<신 설>	비고 4 리스크는 흔히 (주변환경의 변화를 포함하는) 정보보호 이벤트의 결과와 이와 관련된 발생 가능성(ISO Guide 73:2009, 3.6.1.1에서 정의됨)의 조합으로 표현된다.	
<신 설>	비고 5 정보보안 경영시스템의 맥락에서, 정보보안 리스크는 정보보안 목표에 대한 불확실성의 영향으로 표현될 수 있다.	
<신 설>	비고 6 정보보호 리스크는 위협들이 정보 자산 또는 정보 자산들의 취약점을 악용하여 조직에 피해를 일으킬 잠재성과 관련되어 있다. [출처 : ISO/IEC 27000:2018, 3.61]	
<신 설>	3.11 리스크 분석 / Risk analysis	
<신 설>	리스크의 성격을 이해하고 리스크 수준을 결정하는 프로세스	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
<신 설>	비고 1 리스크 분석은 리스크 산정과 리스크 처리에 대한 의사결정의 기초가 된다.	
<신 설>	비고 2 리스크 분석에는 리스크 추정이 포함된다. [출처 : ISO/IEC 27000:2018, 3.63]	
<신 설>	3.12 리스크 평가 / Risk assessment	
<신 설>	리스크 식별, 리스크 분석, 리스크 산정으로 이루어진 전체 프로세스 [출처 : ISO/IEC 27000:2018, 3.64]	
<신 설>	3.13 리스크 관리 / Risk management	
<신 설>	리스크에 관하여 조직이 지시하고 통제하는 협조 활동들 [출처 : ISO/IEC 27000:2018, 3.69]	
<신 설>	3.14 리스크 처리 / Risk treatment	
<신 설>	리스크를 수정하는 프로세스	
<신 설>	비고 1 리스크 처리에는 다음이 포함될 수 있다. — 리스크를 일으키는 활동을 시작하지 않거나 지속하지 않기도 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, 위험재무를 포함한다). — 정보에 따른 선택을 함으로써 리스크를 유지하는 것.	
<신 설>	비고 2 부정적 결과를 다루는 리스크 처리는 “리스크 완화”, “리스크 제거”, “리스크 예방”, “리스크 축소” 라고도 한다.	
<신 설>	비고 3 리스크 처리는 새로운 리스크를 일으키거나 기존 리스크를 완화시킬 수 있다. [출처 : ISO/IEC 27000:2018, 3.72]	
<신 설>	3.15 규칙 / Rule	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
<신 설>	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]	
5.2 공정성 관리	5.2 공정성 관리	
<신 설>	5.2.1 일반사항	- 조항 제목 신설
KAB-R-MSCB, 5.2의 요구사항을 적용한다. 추가로 다음의 요구사항과 지침을 적용한다.	KAB-R-MSCB, 5.2의 요구사항을 적용하여야 한다. 추가로 5.2.2의 요구사항과 지침을 적용하여야 한다.	- 5.2 및 5.2.2 적용 의무화 (“shall”로 변경, 이하 동일)
5.2.1 IS 5.2 이해상충	5.2.2 이해상충	- 조항번호 및 조항제목 변경
<p>인증기관은 자문으로 간주되지 않거나 잠재적인 이해상충을 가지지 않는 경우, 다음 활동을 수행해도 된다.</p> <p>a) 정보보안경영, 관련 경영시스템 또는 심사와 관련된 교육훈련을 개최하거나 강사로 참여하는 경우, 인증기관의 활동은 공개적으로 이용가능한 일반적인 정보 및 조건의 제공으로 제한하여야 한다. 즉, 아래 b)에 기술된 요구사항에 위반하는 회사의 특정 권고사항을 제공하지 않아야 할 것이다.</p> <p>b) 인증심사표준의 요구사항에 대한 인증기관의 해설을 기술한 정보를 이용 가능하게 하거나 요구 시 정보의 게시(9.1.3.6 참조)</p> <p>c) 오로지 인증심사의 준비상태를 결정할 목적으로 수행되는 심사 전 활동. 단 이들 활동은 이 조항을 위반하는 조언 또는 권고를 초래하지 않아야 하며, 인증기관은 그러한 활동들이 이 요구사항들을 위반하지 않고, 인증심사 기간 단축을 정당화하기 위해 사용하지 되지 않음을 확인할 수 있어야 한다.</p> <p>d) 인정범위에 속하지 않는 표준이나 규정에 근거한 제2자와 제3자의 심사수행</p> <p>e) 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·제공</p>	<p><삭 제></p> <p>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</p>	<p>- 수행할 수 있는 활동의 삭제</p> <p>- 영문 표현 변경에 따른 번역 수정</p>

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
	해결책을 권고하지 않는 한도 내에서 개선사항의 식별·제공 할 수도 있을 것이다.	
7 자원 요구사항	7 자원 요구사항	
7.1 인원의 적격성	7.1 인원의 적격성	
<신 설>	7.1.1 일반사항	- 조항 제목 신설
KAB-R-MSCB, 7.1의 요구사항을 적용한다. 추가로 다음의 요구사항과 지침을 적용한다.	KAB-R-MSCB, 7.1의 요구사항을 적용하여야 한다. 추가로 7.1.2 및 7.1.3의 요구사항과 지침을 적용하여야 한다.	- 7.1, 7.1.2 및 7.1.3 적용 의무화
7.1.1 일반 고려사항	<삭 제>	
7.1.1.1 일반적 적격성 요구사항	7.1.2 일반적 적격성 요구사항	- 조항 번호 변경
인증기관이 심사하는 클라이언트의 ISMS와 관련된 기술적, 법적 및 규제적 사항에 대한 지식을 가지고 있음을 보장하여야 한다.	<삭 제>	- 적격성 요구사항 삭제
인증기관은 KAB-R-MSCB, 표 A.1에 인용된 인증업무기능에 필요한 적격성 요구사항을 결정해야 한다. 인증기관은 인증기관이 결정한 ISMS 기술분야와 관련하여 KAB-R-MSCB, 7.1.2 및 이 문서의 7.2.1에 규정된 모든 요구사항들을 고려하여야 한다.	인증기관은 KAB-R-MSCB, 표 A.1에 인용된 인증업무기능에 필요한 적격성 요구사항을 결정해야 한다. 인증기관은 인증기관이 결정한 ISMS 기술분야와 관련하여 KAB-R-MSCB, 7.1.2 및 이 문서의 7.2.2에 규정된 모든 요구사항들을 고려하여야 한다.	- 참조 조항 변경
비고 부속서 A에서 특정 인증업무기능과 관련된 인원에 대한 적격성 요구사항에 대한 요약を提供한다.	<삭 제>	- 비고 삭제
<신 설>	인증기관은 부속서 A에서의 특정 기능에 요구되는 지식 및 스킬을 결정해야 한다.	- 부속서를 통한 적격성 요구사항 구체화
<신 설>	적격성 요구사항을 포함하는 추가적인 특정 요구사항이 특정 표준(예: ISO/IEC 27006-2)에서 수립되었다면, 이를 적용하여야 한다.	- 특정 표준에서 요구하는 적격성 요구사항의 반영
7.1.2 IS 7.1.2 적격성기준의 결정	7.1.3 적격성기준의 결정	- 조항번호 및 조항 제목 변경
7.1.2.1 ISMS 심사를 위한 적격성 요구사항	7.1.3.1 ISMS 심사를 위한 적격성 요구사항	- 조항번호 변경
7.1.2.1.1 일반 요구사항	7.1.3.1.1 일반 요구사항	- 조항번호 변경
인증기관은 최소한 다음사항을 보장할 수	인증기관은 심사팀 멤버들이 최소한 다음	- 적격성을 검증하는

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
있도록, 심사팀 멤버들에 대한 경험, 특정 훈련 또는 요약된 정보(프로필)를 검증하기 위한 기준을 보유하여야 한다.	의 지식을 적용하는 스킬을 보유함을 보장할 수 있도록, 심사팀 멤버들의 적격성을 검증하기 위한 기준을 보유하여야 한다.	기준을 보유하는 것으로 요구사항 변경
a) 정보보안에 대한 지식 b) 심사활동에 대한 기술적 지식 c) 경영시스템에 대한 지식 d) 심사원칙에 대한 지식 비고 심사원칙에 대한 추가적 정보는 ISO 19011에서 찾을 수 있다. e) ISMS 모니터링, 측정, 분석 및 평가에 대한 지식	a) 정보보안 b) 심사대상 활동에 대한 기술적 측면 c) 경영시스템 d) 심사원칙 비고 심사원칙에 대한 추가적 정보는 ISO 19011에서 찾을 수 있다. e) ISMS 모니터링, 측정, 분석 및 평가	- “지식” 삭제 - 의미 명확화 및 원문 표현 변경에 따른 번역 수정
<신 설>	심사팀 멤버들은 총체적으로 위 요구사항에 적절한 스킬을 보유하여야 하며, 이는 적용된 경험을 통해 입증될 수 있다.	- 요구사항 신설
심사팀은 클라이언트의 ISMS에 대한 보안사고의 징후를 적절한 ISMS 요소로 추적할 수 있는 적격성을 갖추고 있어야 한다.	심사팀 멤버들은 클라이언트의 ISMS에 대한(ISMS에서 발생한) (정보)보안사고의 징후를 적절한 ISMS 요소(ISMS의 적절한 요소)로 추적할 수 있는 적격성을 총체적으로 갖추고 있어야 한다.	- 원문 표현 변경에 따른 번역 수정
심사팀은 상기 사항에 대한 적절한 업무 경험을 보유하고 각 항목에 대해 실질적으로 적용할 수 있어야 한다. 이것은 심사원에 대하여 정보보안의 모든 분야에 대한 완벽한 경험을 요구하는 것을 의미하는 것은 아니다. 그러나 심사팀 전체적으로는 심사되는 ISMS 범위를 다루기 위해 충분한 이해와 경험을 보유하여야 한다).	<삭 제> 개별 심사원은 정보보안의 모든 분야에 대한 완벽한 경험이 요구되지 않는다. 그러나 심사팀 전체적으로는 심사되는 ISMS 범위를 다루기 위해 적절한 적격성을 보유하여야 한다.	- 의미 명확화 - 용어 변경
7.1.2.1.2 정보보안경영 용어, 원칙, 실행 및 기술	7.1.3.1.2 정보보안경영 용어, 원칙, 실행 및 기술	- 조항번호 변경
전반적으로, 심사팀의 모든 멤버들은 다음의 지식을 보유해야 한다.	ISMS 심사팀의 각각의 심사원은 다음의 지식을 보유해야 한다.	- 대상 변경
a) (생략) b) 정보보안경영과 관련된 도구, 방법, 기술 및 그 적용 c) 정보보안 리스크평가 및 리스크관리	a) (현행과 같음) b) 정보보안 리스크평가 및 리스크관리 c) ISMS에 적용 가능한 프로세스	- 현행 c)에서 이동 - 현행 d)에서 이동
<신 설>	총체적으로, 심사팀은 다음의 지식을 보	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
d) ISMS에 적용 가능한 프로세스 e) (생략)	유해야 한다. d) 정보보안경영과 관련된 도구, 방법, 기술 및 그 적용 e) (현행과 같음)	- b)에서 이동
모든 심사원들은 a), c) 및 d)를 충족해야 한다.	<삭 제>	- 요구사항 삭제
7.1.2.1.3 정보보안경영시스템 표준 및 참조문서	7.1.3.1.3 정보보안경영시스템 표준 및 참조문서	- 조항번호 변경
ISMS 심사에 포함된 심사원들은 다음의 지식을 보유하여야 한다. a) ISO/IEC 27001의 모든 요구사항	ISMS 심사팀의 각각의 심사원은 ISO/IEC 27001의 모든 요구사항에 대한 지식을 보유하여야 한다.	- 자구 수정
전반적으로, 심사팀의 모든 멤버는 다음의 지식을 보유하여야 한다. b) 다음과 같이 분류되는 ISO/IEC 27002에 포함된 모든 통제항목 및 실행(특정 분야 표준에 필수적이라고 결정된 경우) 1) 정보보안 방침 2) 정보보안 조직 3) 인적자원 보안 4) 자산 관리 5) 접근권한 통제 6) 암호 해독 7) 물리적 및 환경적 보안 8) IT 서비스를 포함한 운영 보안 9) 네트워크 보안관리 및 정보전달을 포함한 의사소통 보안 10) 시스템 도입, 개발 및 유지 11) 아웃소싱 서비스를 포함하는 공급자 관계 12) 정보보안사고 관리 13) 중복성을 포함하는 비즈니스연속성 경영에 대한 정보보안 측면 14) 정보보안 검토를 포함하는 준수사항	총체적으로, 심사팀은 ISO/IEC 27001:2022 부속서 A에 포함된 모든 통제항목 및 구현에 대한 지식을 보유하여야 한다. <삭 제>	- 참조표준 변경 및 자구 수정 - 개별 통제항목 삭제
7.1.2.1.4 비즈니스경영 관행	7.1.3.1.4 비즈니스경영 관행	- 조항번호 변경
ISMS 심사에 관련된 심사원은 다음의 지식을 보유하여야 한다. a)~d) (생략) 비고 (생략)	ISMS 심사팀의 개별 심사원은 다음의 지식을 보유하여야 한다. a)~d) (현행과 같음) 비고 (현행과 같음)	- 자구수정
7.1.2.1.5 클라이언트 비즈니스 분야	7.1.3.1.5 클라이언트 비즈니스 분야	- 조항번호 변경

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
ISMS 심사에 관련된 심사원은 다음의 지식을 보유하여야 한다. a)~d) (생략) 기준 a)는 심사팀 간 공유될 수 있다.	ISMS 심사팀의 개별 심사원은 다음의 지식을 보유하여야 한다. a)~d) (현행과 같음) (현행과 같음)	- 자구수정
7.1.2.1.6 클라이언트 제품, 프로세스 및 조직	7.1.3.1.6 클라이언트 제품, 프로세스 및 조직	
전반적으로, ISMS 심사에 관련된 심사원은 다음의 지식을 보유하여야 한다. a)~c) (생략)	총체적으로, ISMS 심사팀 멤버는 다음의 지식을 보유하여야 한다. a)~c) (현행과 같음)	- 자구 수정
7.1.2.2 ISMS 심사팀장에 대한 적격성 요구사항	<삭 제>	- 심사팀장 적격성 요구사항 삭제
7.1.2.1의 요구사항에 추가하여, 심사팀은 다음의 요구사항을 충족해야 하며, 이는 지도 및 감독 하에 수행되는 심사에서 실증되어야 한다. a) 인증심사 프로세스 및 심사팀 관리를 위한 지식 및 스킬 b) 구술 또는 서면으로 이루어지는 효율적 의사소통 능력	<삭 제>	
7.1.2.3 신청서 검토를 수행하기 위한 적격성 요구사항	7.1.3.2 신청서 검토를 수행하기 위한 적격성 요구사항	- 조항번호 변경
7.1.2.3.1 정보보안경영시스템 표준 및 표준문서	<삭 제>	- 적격성 요구사항 삭제
심사팀에 요구되는 적격성, 심사팀원 선정 및 심사시간 결정을 위해 신청서 검토를 수행하는 인원은 다음의 지식을 보유하여야 한다. a) 인증프로세스에 사용되는 관련 ISMS 기준 및 기타 참조 문서	<삭 제>	- 적격성 요구사항 삭제
7.1.2.3.2 클라이언트 비즈니스 분야	7.1.3.2.1 클라이언트 비즈니스 분야	- 조항번호 변경
심사팀에 요구되는 적격성, 심사팀원 선정 및 심사시간 결정을 위해 신청서 검토를 수행하는 인원은 다음의 지식을 보유하여야 한다. a) 클라이언트 업무분야와 관련된 포괄적 용어, 프로세스, 기술 및 리스크	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.	- 서술 방식 변경
7.1.2.3.3 클라이언트의 제품, 프로세스 및 조직	7.1.3.2.2 클라이언트의 제품, 프로세스 및 조직	- 조항번호 변경
심사팀에 요구되는 적격성, 심사팀원 선정 및 심사시간 결정을 위해 신청서 검토	심사팀에 요구되는 적격성, 심사팀원 선정 및 심사시간 결정을 위해 신청서 검토	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
<p>를 수행하는 인원은 <u>다음의</u> 지식을 보유하여야 한다.</p> <p>a) 아웃소싱 기능을 포함하는 ISMS의 개발 및 이행과 인증활동에 관련된 클라이언트의 제품, 프로세스, 조직 유형, 규모, 관리체계, 구조, 기능 및 관계</p>	<p>를 수행하는 인원은 <u>외부에서</u> 제공되는 기능을 포함하는 <u>고객 제품, 프로세스, 조직 유형, 규모, 거버넌스, 구조, 기능 및 관계가 ISMS의 개발과 실행 및 인증 활동에 미치는 영향에 대한</u> 지식을 보유해야 한다.</p>	- 서술 방식 변경 및 자구 수정
7.1.2.4 심사보고서 검토 및 인증결정을 위한 적격성 요구사항	7.1.3.3 심사보고서 검토 및 인증결정을 위한 적격성 요구사항	- 조항번호 변경
7.1.2.4.1 일반사항	7.1.3.3.1 일반사항	- 조항번호 변경
<p>심사보고서를 검토하고 ...<u>(중략)</u>... 지식을 가져야 한다. 추가로, 심사보고서를 검토하고 인증을 결정하는 인원은 다음의 지식을 보유하여야 한다.</p> <p>a) 일반적 경영시스템 b) 심사 프로세스 및 절차 c) 심사원칙, 실행 및 기술</p>	<p>심사보고서를 검토하고 ...<u>(중략)</u>... 지식을 가져야 한다. 추가로, 심사보고서를 검토하고 인증을 결정하는 인원은 다음의 지식을 보유하여야 한다.</p> <p>a) 일반적 경영시스템 b) 심사 프로세스 및 절차 <삭 제></p>	- 요구사항 삭제
7.1.2.4.2 정보보안경영 용어, 원칙, 실행 및 기술	7.1.3.3.2 정보보안경영 용어, 원칙, 관행 및 기술	- 조항번호 변경 - 번역 수정
<p>심사보고서를 검토하고 인증을 결정하는 인원은 다음의 지식을 보유하여야 한다.</p> <p>a) 7.1.2.1.2 a), c) 및 d)의 항목들 b) 정보보안 관련 법적 및 규제적 요구사항</p>	<p>심사보고서를 검토하고 인증을 결정하는 인원은 다음의 지식을 보유하여야 한다.</p> <p>a) 7.1.3.1.2 a), c) 및 d)의 항목들 b) 정보보안 관련 법적 및 규제적 요구사항</p>	- 참조 조항 변경
7.1.2.4.3 정보보안경영시스템 표준 및 참조 문서	<삭 제>	
<p>심사보고서를 검토하고 인증을 결정하는 인원은 다음의 지식을 보유하여야 한다.</p> <p>a) 관련된 ISMS 표준 및 인증 프로세스에 사용되는 기타 참조 문서</p>	<삭 제>	
7.1.2.4.4 클라이언트 비즈니스 분야	7.1.3.3.3 클라이언트 비즈니스 분야	- 조항번호 변경
<p>심사보고서를 검토하고 인증을 결정하는 인원은 <u>다음의</u> 지식을 보유하여야 한다.</p> <p>a) <u>관련 비즈니스 분야 관행과 관련된 일반적 용어 및 리스크</u></p>	<p>심사보고서를 검토하고 인증을 결정하는 인원은 <u>관련 비즈니스 분야 관행과 관련된 일반적 용어 및 리스크에 대한</u> 지식을 보유하여야 한다.</p>	- 서술 방식 변경
7.1.2.4.5 클라이언트 제품, 프로세스, 조직	7.1.3.3.4 클라이언트 제품, 프로세스, 조직	- 조항번호 변경
<p>심사보고서를 검토하고 인증을 결정하는 인원은 다음의 지식을 보유하여야 한다.</p> <p>a) 클라이언트 제품, 프로세스, 조직 유형, 규모, 관리체계, 구조, 기능 및 관계</p>	<p>심사보고서를 검토하고 인증을 결정하는 인원은 <u>클라이언트 제품, 프로세스, 조직 유형, 규모, 관리체계, 구조, 기능 및 관계에 대한</u> 지식을 보유하여야 한다.</p>	- 서술 방식 변경

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
7.2 인증 활동에 관련된 인원	7.2 인증 활동에 관련된 인원	
<신 설>	7.2.1 일반사항	- 조항 신설
KAB-R-MSCB, 7.2의 요구사항을 적용한다. 추가로 다음의 요구사항과 지침을 적용한다.	KAB-R-MSCB, 7.2의 요구사항을 적용하여야 한다. 추가로 7.2.2의 요구사항과 지침을 적용한다.	- 7.2 및 7.2.2 적용의 의무화
7.2.1 IS 7.2 심사원 지식 및 경험의 입증	7.2.2 심사원 지식 및 경험의 입증	- 조항번호 변경 및 자구수정
<신 설>	7.2.2.1 일반 고려사항	- 조항 신설
인증기관은 다음을 통해 <u>심사원의</u> 지식 및 경험을 실증하여야 한다.	인증기관은 다음 사항의 각각을 통해 <u>개별 심사원의</u> 지식 및 경험을 실증하여야 한다.	- 의미 명확화
a)~e) (생략)	a)~e) (현행과 같음)	
7.2.1.1 심사원 선정	7.2.2.2 심사원 선정	- 조항번호 변경
7.1.2.1의 요구사항에 추가하여, 심사원을 선정하는 기준은 각 심사원에 대하여 다음 사항을 보장하여야 한다.	7.1.3.1의 요구사항에 추가하여, 심사원을 선정하는 프로세스는 각 심사원에 대하여 다음 사항을 보장하여야 한다.	- 참조 조항 변경 - 영문 표현 변경에 따른 번역 수정
a) (생략) b) <u>정보기술분야에서 최소 4년 이상 상근 직원으로 근무한 업무경험을 가져야 하며, 이 중 최소 2년은 정보보안과 관련된 역할 또는 기능 수행</u> c) <u>ISMS 심사 및 심사 관리를 포함하는 적어도 5일의 교육과정에 대한 성공적 수료</u> d) <u>ISMS 심사원으로 심사를 수행하기 전 ISMS 심사경험을 보유. 심사경험은 최소한 1회의 ISMS 최초 인증심사(1단계와 2단계) 또는 갱신심사 및 최소 1회의 사후관리 심사에서 ISMS 평가자의 모니터링 하에 심사훈련(KAB-R-MSCB, 9.2.2.1.4 참조)을 수행함으로써 얻어야 한다. 이 참여에는 문서검토와 리스크 평가, 평가 실행에 대한 검토 및 심사보고를 포함해야 한다.</u>	a) (현행과 같음) b) <u>ISMS 심사원으로 심사를 수행하기에 충분한, 정보기술 및 정보보안 분야에서 근무한 업무경험</u> c) <u>ISMS 심사와 관련한 충분한 교육을 이수하고, ISO/IEC 27001에 따라 심사 스킬을 입증. 심사경험은 최소한 1회의 ISMS 최초 인증심사(1단계와 2단계) 또는 갱신심사 및 최소 1회의 사후관리 심사에서 ISMS 평가자의 모니터링 하에 심사훈련(KAB-R-MSCB, 9.2.2.1.4 참조)을 수행함으로써 얻어야 한다. 심사경험은 최근 5년 동안 수행한 최소 10일간의 ISMS 현장심사를 통해 얻어야 한다. 이 참여에는 문서검토와 리스크 평가, 평가 실행에 대한 검토 및 심사보고를 포함해야 한다.</u> <삭 제>	- 업무경험에서 최소 기한의 삭제 - 요구사항 c) 및 d) 통합

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
<p>다. 심사경험은 최근 5년 동안 수행한 최소 10일간의 ISMS 현장심사를 통해 얻어야 한다. 이 참여에는 문서검토와 위협평가, 실행평가 및 심사보고를 포함해야 한다.</p> <p>e) 최근의 심사경험을 가지고 있어야 한다(관련성이 있는 현재의 업무).</p> <p>f) <u>지속적 전문성 개발을 통해 정보보안 및 심사에 대한 최신 지식 및 스킬을 유지하여야 한다.</u></p> <p>g) ISO/IEC 27001에 따른 ISMS 심사 적격성 보유</p>	<p><삭 제></p> <p>d) <u>정보보안 및 심사에 대한 관련성 있는 최신 지식 및 스킬 유지</u></p> <p><삭 제></p>	<ul style="list-style-type: none"> - 최근의 심사경험에 대한 요구사항 삭제 - 지속적 전문성 개발 내용은 비고로 이동 - 적격성 요구사항 삭제
<신 설>	비고 1 스킬 유지는 지속적 전문성 개발을 통해 입증될 수 있다.	- 비고 신설
<신 설>	비고 2 인증기관은 상기 요구사항과 증거를 일치시키기 위한 적격성 기준 목록이 필요하다	- 비고 신설
<신 설>	7.2.2.3 기술전문가 선정	- 기술전문가 선정 프로세스 신설
<신 설>	기술 전문가를 선정하는 프로세스는 각 심사원에 대하여 다음 사항을 보장하여야 한다.	
<신 설>	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	
<신 설>	비고 스킬 유지는 지속적 전문성 개발을 통해 입증될 수 있다.	
7.2.1.2 심사팀장 선정	7.2.2.4 심사팀장 선정	- 조항번호 변경
7.1.2.2 및 7.2.1.1에 추가로, 심사팀 리더 선정 기준은 해당 심사원에 대하여 다음 사항을 보장하여야 한다. a) 적어도 3회 이상 ISMS 심사의 모든 단계에 적극적으로 참여하였으며, 참여과정에는 최초 인증범위 결정 및 계획수립, 문서검토 및 리스크평가, 이행평가 및 공식 심사보고서 작성이 포함되어야 한다.	7.1.2.2에 추가로, 심사팀 리더 선정 기준은 해당 심사원에 대하여 적어도 3회 이상 ISMS 심사의 모든 단계에 적극적으로 참여하였으며, 참여과정에는 최초 인증범위 결정 및 계획수립, 문서검토 및 리스크평가와 이행에 대한 검토 및 공식 심사보고서 작성이 포함되어야 함을 보장하여야 한다.	<ul style="list-style-type: none"> - 조항번호 변경 - 서술 방식 변경 및 자구 수정

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
7.3 개별 외부 심사원 및 외부 기술전문가의 활용	7.3 개별 외부 심사원 및 외부 기술전문가의 활용	
KAB-R-MSCB, 7.3의 요구사항을 적용한다. 추가로 다음의 요구사항과 지침을 적용한다.	KAB-R-MSCB, 7.3의 요구사항을 적용하여야 한다. <삭 제>	- 7.3 적용 의무화 및 추가 요구사항 삭제
7.3.1 IS 7.3 심사팀의 일부로써 외부 심사원 또는 외부 기술전문가 활용	<삭 제>	- 요구사항 삭제
기술전문가는 심사원의 감독 하에 업무를 수행해야 한다. 기술전문가에 대한 최소 요구사항은 7.2.1.1에 기술되어 있다.	<삭 제>	- 요구사항 삭제
7.4 인원에 대한 기록	7.4 인원에 대한 기록	
KAB-R-MSCB, 7.4의 요구사항을 적용한다.	KAB-R-MSCB, 7.4의 요구사항을 적용하여야 한다.	- 7.4 적용 의무화
7.5 외주처리	7.5 외주처리	
KAB-R-MSCB, 7.5의 요구사항을 적용한다.	KAB-R-MSCB, 7.5의 요구사항을 적용하여야 한다.	- 7.5 적용 의무화
8 정보 요구사항	8 정보 요구사항	
8.1 공개 정보	8.1 공개 정보	
KAB-R-MSCB, 8.1의 요구사항을 적용한다.	KAB-R-MSCB, 8.1의 요구사항을 적용한다.	- 8.1 적용 의무화
8.2 인증문서	8.2 인증문서	
<신 설>	8.2.1 일반사항	- 조항제목 신설
KAB-R-MSCB, 8.2의 요구사항을 적용한다. 추가로 다음의 요구사항과 지침을 적용한다.	KAB-R-MSCB, 8.2의 요구사항을 적용하여야 한다. 추가로 8.2.2 및 8.2.3의 요구사항과 지침을 적용하여야 한다.	- 8.2, 8.2.2 및 8.2.3 적용 의무화
8.2.1 IS 8.2 ISMS 인증문서	8.2.2 ISMS 인증문서	- 조항번호 변경 및 자구 수정
인증문서에는 ISO/IEC 27001:2013 6.1.3 d) 항에 의거하여 조직의 적용성보고서에서 필요하다고 결정된 통제에 대한 통제집합의 출처로서 국가와 국제표준을 참조할 수 있다. 인증문서에 표기되는 참조내용은 해당 인증이 아닌 적용성보고서에 적용되는 통제에 대한 통제집합의 출처임을 명확하게 명시해야 한다.	<삭 제>	
<신 설>	인증범위 내의 조직의 활동 전체가 정해진 물리적 장소에서 수행되지 않는 경우,	- 원격 활동에 대한 인증서 기술 방법

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
	인증문서는 조직의 활동이 원격으로 수행됨을 기술하여야 한다.	명시
<신 설>	8.2.3 ISMS 인증문서 내의 타 표준의 참조	- 요구사항 신설
<신 설>	인증문서에서 국가 및 국제 표준은 다음의 조건 하에서만 참조할 수 있을 것이다.	- 요구사항 신설
<신 설>	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	- 요구사항 신설
<신 설>	참조 통제 표준은 ISO/IEC 27001:2022 부속서 1를 근거로 하거나, 정보보안 통제를 포함한 표준일 수 있다.	- 요구사항 신설
<신 설>	인증문서는 적용성보고서에 적용된 통제 집합이 ISMS 통제의 추가 또는 제외에 대한 관련성을 언급하기 위해서만 사용되었고, 적합성평가를 위해 사용되지 않았음을 기술하여야 한다.	
8.3 인증에 대한 언급 및 마크 사용	8.3 인증에 대한 언급 및 마크 사용	
KAB-R-MSCB, 8.3의 요구사항을 <u>적용</u> 한다.	KAB-R-MSCB, 8.3의 요구사항을 <u>적용</u> 하여야 한다.	- 8.3 적용 의무화
8.4 기밀성	8.4 기밀성	
<신 설>	8.4.1 일반사항	- 조항 제목 신설
KAB-R-MSCB, 8.4의 요구사항을 <u>적용</u> 한다. 추가로 <u>다음의</u> 요구사항과 지침을 <u>적용</u> 한다.	KAB-R-MSCB, 8.4의 요구사항을 <u>적용</u> 하여야 한다. 추가로 <u>8.4.2의</u> 요구사항과 지침을 <u>적용</u> 하여야 한다.	- 8.4 및 8.4.2 적용 의무화
8.4.1 IS 8.4 조직의 기록에 대한 접근	8.4.2 조직의 기록에 대한 접근	- 조항번호 변경 및 자구 수정
8.5 인증기관과 클라이언트간의 정보 교환	8.5 인증기관과 클라이언트간의 정보 교환	
KAB-R-MSCB, 8.5의 요구사항을 <u>적용</u> 한다.	KAB-R-MSCB, 8.5의 요구사항을 <u>적용</u> 하여야 한다.	- 8.5 적용 의무화
9 프로세스 요구사항	9 프로세스 요구사항	
9.1 인증 이전의 활동	9.1 인증 이전의 활동	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
9.1.1 신청	9.1.1 신청	
<신 설>	9.1.1.1 일반사항	- 조항 제목 신설
KAB-R-MSCB, 9.1.1의 요구사항을 <u>적용</u> 한다. 추가로 <u>다음의</u> 요구사항과 지침을 <u>적용</u> 한다.	KAB-R-MSCB, 9.1.1의 요구사항을 <u>적용</u> 하여야 한다. 추가로 <u>9.1.1.2의</u> 요구사항과 지침을 <u>적용</u> 하여야 한다.	- 9.1.1 및 9.1.1.2 적용 의무화
9.1.1.1 IS 9.1.1 신청 준비	9.1.1.2 인증절차에 대한 고려사항	- 조항번호 변경 및 제목 변경
인증기관은 클라이언트에게 ISO/IEC 27001 및 인증을 위해 요구되는 기타 문서에 적합하게 문서화 되고 이행되는 ISMS 보유하도록 요구하여야 한다.	<삭 제>	
<신 설>	인증기관의 절차는 ISMS 이행에 대한 특정방법 또는 문서 및 기록에 대한 특정서식을 전제로 하여서는 안 된다. 인증절차는 클라이언트의 ISMS가 ISO/IEC 27001에 규정된 요구사항과 클라이언트의 방침 및 목표를 충족하고 있음을 확인함에 초점을 맞추어야 한다.	- 현행 9.1.3.2에서 이동
<신 설>	비고 조직이 자체적으로 필요한 통제를 설계하고, 특정 출처에서 통제를 선정하는 것이 가능하다. 그러므로 필요한 통제가 ISO/IEC 27001:2022 부속서 A에 명시되어 있는 통제항목에 명시되지 않음에도 불구하고, ISO/IEC 27001 인증을 받는 것이 가능하다.	
9.1.2 신청서 검토	9.1.2 신청서 검토	
KAB-R-MSCB, 9.1.2의 요구사항을 <u>적용</u> 한다.	KAB-R-MSCB, 9.1.2의 요구사항을 <u>적용</u> 하여야 한다.	- 9.1.2 적용 의무화
9.1.3 심사 프로그램	9.1.3 심사 프로그램	
<신 설>	9.1.3.1. 일반사항	- 조항 제목 신설
KAB-R-MSCB, 9.1.3의 요구사항을 <u>적용</u> 한다. 추가로 <u>다음의</u> 요구사항과 지침을 <u>적용</u> 한다.	KAB-R-MSCB, 9.1.3의 요구사항을 <u>적용</u> 하여야 한다. 추가로 <u>9.1.3.2, 9.1.3.3, 9.1.3.4, 9.1.3.5 및 9.1.3.6의</u> 요구사항과 지침을 <u>적용</u> 하여야 한다.	- 9.1.3, 9.1.3.2, 9.1.3.3, 9.1.3.4, 9.1.3.5 및 9.1.3.6 적용 의무화
9.1.3. IS 9.1.3 일반사항	9.1.3.2 일반 고려사항	- 조항 번호 및 조항 제목 변경
ISMS 심사를 위한 심사 <u>프로그램</u> 은 결정된 정보보안 통제항목을 고려해야 한다.	ISMS 심사를 위한 심사 <u>프로그램</u> 은 클라이언트가 결정한 정보보안 통제항목을 고	- 자구 수정

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
	려해야 한다.	
<신 설>	비고 1 정보보안 통제항목은 ISO/IEC 27001:2022 부속서 A 및/또는 기타 적용 가능한 표준을 출처로, 및/또는 자체 설계로 할 수 있다.	- 비고 신설
9.1.3.2 IS 9.1.3 심사기법	<삭 제>	
인증기관의 절차는 ISMS 이행에 대한 특정방법 또는 문서 및 기록에 대한 특정서식을 전제로 하여서는 안 된다. 인증절차는 클라이언트의 ISMS가 ISO/IEC 27001에 규정된 요구사항과 클라이언트의 방침 및 목표를 충족하고 있다는 설정에 초점을 맞추어야 한다.	<삭 제>	- 개정(안) 9.1.1.2로 이동
비고 (생략)	비고 2 (현행과 같음)	- 비고 번호 변경
<신 설>	9.1.3.3 원격심사의 사용	- 원격심사 요구사항 신설
<신 설>	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.	
<신 설>	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	
<신 설>	<u>리스크 분석은 원격심사 수행 전에 이루어져야 한다. 인증주기 동안의 원격심사 사용에 대한 분석 및 정당성은 문서화되어야 한다.</u>	
<신 설>	심사 프로세스의 효과성에 대한 수용 불가능한 리스크가 리스크 평가에서 식별된 경우 원격심사를 사용하여서는 안 된다.	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
<신 설>	리스크 평가는 지속적인 적절성을 보장하기 위하여 인증주기 동안 검토되어야 한다.	
<신 설>	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.	
9.1.3.3 IS 9.1.3 최초심사를 위한 일반적 준비사항	9.1.3.4 최초심사를 위한 일반적 준비사항	- 조항번호 변경 및 자구수정
인증기관은 클라이언트에게 내부심사 보고서 및 정보보안에 대한 독립적 검토 보고서에 접근할 수 있는 모든 필요사항을 갖추도록 요청해야 한다. 최소한 다음의 정보는 1단계 심사시간 동안 클라이언트에 의해 제공되어야 한다. a) ISMS에 대한 일반적 정보 및 해당 정보를 다루는 활동 b) ISO/IEC 27001에 규정된 요구되는 ISMS 문서 및 요구되는 경우, 관련 문서의 사본	인증기관은 클라이언트에게 내부심사 보고서 및 정보보안에 대한 독립적 검토 보고서에의 접근을 보장하기 위해 모든 필요사항을 갖추도록 요청해야 한다. <삭제>	- 의미 명확화
9.1.3.4 IS 9.1.3 검토기간	9.1.3.5 검토기간	- 조항번호 변경 및 자구수정
인증기관은 적어도 인증범위를 포함하는 <u>최소한 1회의 경영검토 및 1회의 ISMS 내부심사를 통하여 ISMS가 운영되지 않았다면 ISMS를 인증해서는 안 된다.</u>	인증기관은 인증범위를 포함하는 <u>경영검토 및 ISMS 내부심사가 수행되었고, 효과적이며, 유지될 것을 입증하는 충분한 증거가 없다면 ISMS를 인증해서는 안 된다.</u>	- 단순 횡수에서 효과성을 강조
9.1.3.5 IS 9.1.3 인증범위	9.1.3.6 ISMS 인증범위	- 조항번호 변경 및 자구 수정
심사팀은 적용 가능한 모든 인증 요구사항에 대해 규정된 인증범위를 포함한 클라이언트의 ISMS를 심사해야 한다. 인증기관은 클라이언트가 ISMS 인증범위 내에서 ISO/IEC 27001, 4.3에 언급된 요구사항을 다루는지를 확인해봐야 한다.	심사팀은 적용 가능한 모든 인증 요구사항에 대해 규정된 인증범위를 포함한 클라이언트의 ISMS를 심사해야 한다. 인증기관은 클라이언트가 ISMS 인증범위 내에서 ISO/IEC 27001:2022, 4.3에 언급된 요구사항을 다루는지를 확인해봐야 한다.	- 최신 인용 표준 적용
인증기관은 클라이언트의 정보보안 리스크평가 및 리스크관리가 클라이언트의 활동에 포함(반영)되고 클라이언트의 활동범위가 인증범위에서 정의하는 것과 같이	인증기관은 클라이언트의 정보보안 리스크평가 및 리스크관리가 클라이언트의 활동을 적절히 반영하고 인증범위에서 규정된 활동경계까지 확대되었음을 보장하여	- 번역 수정

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
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.	야 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.	
9.1.3.6 IS 9.1.3 인증심사기준	<삭 제>	- 요구사항 삭제
심사대상인 클라이언트 ISMS에 대한 기준은 ISO/IEC 27001이어야 한다. 수행되고 있는 기능과 관련된 인증을 위해서 다른 문서가 요구될 수 있다.	<삭 제>	- 요구사항 삭제
9.1.4 심사시간 결정	9.1.4 심사시간 결정	
<신 설>	9.1.4.1 일반사항	- 조항 제목 신설
KAB-R-MSCB, 9.1.4의 요구사항을 적용한다. 추가로 다음의 요구사항과 지침을 적용한다.	KAB-R-MSCB, 9.1.4의 요구사항을 적용하여야 한다. 추가로 9.1.4.2의 요구사항과 지침을 적용하여야 한다.	- 9.1.4 및 9.1.4.2 적용 의무화
9.1.4.1 IS 9.1.4 심사시간	9.1.4.2 심사시간	- 조항번호 변경 및 자구수정
인증기관은 최초심사, 사후관리 심사 또는 갱신심사와 관련된 모든 활동을 수행하기 위한 충분한 시간을 심사원에게 허락하여야 한다. 전체 심사시간 계산은 심사보고서 작성을 위한 충분한 시간이 포함하여야 한다.	<삭 제>	
심사시간 결정을 위해 인증기관은 <u>부속서 B</u> 를 사용하여야 한다.	심사시간 결정을 위해 인증기관은 <u>부속서 C</u> 를 사용하여야 한다.	- 부속서 번호 변경
비고 심사시간 계산에 대한 추가적인 지침 및 사례는 <u>부속서 C</u> 에서 제공한다.	비고 심사시간 계산에 대한 추가적인 지침 및 사례는 <u>부속서 D</u> 에서 제공한다.	- 부속서 번호 변경
9.1.5 복수사업장 샘플링	9.1.5 복수사업장 샘플링	
<신 설>	9.1.5.1 일반사항	- 조항 제목 신설
KAB-R-MSCB, 9.1.5의 요구사항을 적용한다. 추가로 다음의 요구사항과 지침을 적	KAB-R-MSCB, 9.1.5의 요구사항을 적용하여야 한다. 추가로 9.1.5.2의 요구사항과	- 9.1.5 및 9.1.5.2 적용 의무화

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
용한다.	지침을 적용한다.	
9.1.5.1 IS 9.1.5 복수사업장	9.1.5.2 복수사업장	- 조항번호 변경 및 자구수정
9.1.5.1.1 클라이언트가 …(중략)… 접근방 법 사용을 고려해야 한다. a)~c) (생략)	9.1.5.2.1 (현행과 같음)	- 조항번호 변경
9.1.5.1.2 표본추출에 근거한 접근방법을 …(중략)… 절차를 보유하여야 한다.	9.1.5.2.2 (현행과 같음)	
a) 초기 계약검토를 식별하기 위하여 사 업장 간의 적절한 레벨의 표본이 결정되 어야 한다.	a) 초기 계약검토에서 적절한 샘플링 수 준을 결정하기 위해 최대한 사업장 간의 차이를 식별한다.	- 번역 수정
b) 다음 사항을 고려하여 인증기관은 전 체 사업장 수를 대표할 수 있는 표본의 수를 추출한다. 1) <u>본사</u> 및 사업장에 대한 내부심사 결과 2) ~ 5) (생략) 6) 업무실행의 다양성 7) ~ 13) (생략)	b) 다음 사항을 고려하여 인증기관은 전 체 사업장 수를 대표할 수 있는 표본의 수를 추출한다. 1) (적절한 경우) <u>중앙사무소</u> 및 사업 장에 대한 내부심사 결과 2)~5) (현행과 같음) 6) 업무관행의 다양성 7) ~ 13) (현행과 같음)	- 영문 표현 변경에 따른 번역 수정 - 번역 수정
c)~e) (생략)	c)~e) (현행과 같음)	
f) <u>본사</u> 또는 <u>단일</u> 사업장에서 부적합이 발견되었을 경우, 시정조치 절차는 <u>본사</u> 및 인증서에 포함된 모든 사업장에 적용 한다.	f) <u>단일</u> 사업장에서 부적합이 발견되었을 경우, 시정조치 절차는 인증서에 포함된 모든 사업장에 적용한다.	- “본사” 삭제
동일한 ISMS가 모든 사업장에 적용되며 운영수준을 중앙에서 관리함을 보장하기 위해, 심사는 <u>클라이언트 본사의</u> 활동을 다루어야 한다. 심사는 위에 기술된 모든 사항을 다루어야 한다.	동일한 ISMS가 모든 사업장에 적용되며 운영수준을 중앙에서 관리함을 보장하기 위해, 심사는 <u>클라이언트의</u> 활동을 다루 어야 한다. 심사는 위에 기술된 모든 사 항을 다루어야 한다.	- “본사” 삭제
9.1.6 복수의 경영시스템 표준	9.1.6 복수의 경영시스템 표준	
<신 설>	9.1.6.1 일반사항	
KAB-R-MSCB, 9.1.6의 요구사항을 적용한 다. 추가로 다음의 요구사항과 지침을 적 용한다.	KAB-R-MSCB, 9.1.6의 요구사항을 적용하 여야 한다. 추가로 9.1.6.2 및 9.1.6.3의 요 구사항과 지침을 적용한다.	- 9.1.6, 9.1.6.2 및 9.1.6.3 적용 의무 화
9.1.6.1 IS 9.1.6 다른 경영시스템과 ISMS 문서와의 통합 (생략)	9.1.6.2 ISMS와 다른 경영시스템 문서와의 통합 (현행과 같음)	- 조항번호 변경 및 자구 수정
9.1.6.2 IS 9.1.6 통합경영시스템의 심사	9.1.6.3 통합경영시스템의 심사	- 조항번호 변경 및

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
		자구 수정
(생략)	(현행과 같음)	
9.2 심사계획	9.2 심사계획	
<신 설>	9.2.1.1 일반사항	- 조항제목 신설
KAB-R-MSCB, 9.2.1의 요구사항을 적용한다. 추가로 다음의 요구사항과 지침을 적용한다.	KAB-R-MSCB, 9.2.1의 요구사항을 적용하여야 한다. 추가로 9.2.1.2 및 9.2.1.3의 요구사항과 지침을 적용하여야 한다.	- 9.2.1, 9.2.1.2 및 9.2.1.3 적용 의무화
9.2.1.1 IS 9.2.1 심사 목적	9.2.1.2 심사 목적	- 조항번호 변경 및 자구 수정
클라이언트가 리스크평가를 기반으로 적용 가능한 통제항목을 이행하고 수립된 정보보안 목적을 달성하였음을 보장하기 위해 경영시스템의 효과성에 대한 결정이 심사 목적에 포함되어야 한다.	심사 목적에는 다음이 포함되어야 한다. a) 경영시스템의 효과성에 대한 결정 b) 클라이언트가 리스크평가를 기반으로 필요한 통제항목을 식별함을 보장 c) 수립된 정보보안 목적을 달성하였음에 대한 결정	- 서술방식 변경 및 자구 수정
<신 설>	9.2.1.3 심사기준	- 심사기준 요구사항 신설
<신 설>	클라이언트 ISMS 심사 기준에는 ISO/IEC 27001을 포함하여야 한다.	- 심사기준 요구사항 신설
9.2.2 심사팀 선정 및 배정	9.2.2 심사팀 선정 및 배정	
<신 설>	9.2.2.1 일반사항	
KAB-R-MSCB, 9.2.2의 요구사항을 적용한다. 추가로 다음의 요구사항과 지침을 적용한다.	KAB-R-MSCB, 9.2.2의 요구사항을 적용하여야 한다. <삭 제>	- 9.2.2 적용 의무화
9.2.1.1 IS 9.2.2 심사팀	<삭 제>	- 요구사항 삭제
심사팀은 공식적으로 임명되어야 하며 적절한 작업 문서가 제공되어야 한다. 심사팀에게 주어지는 임무는 명확하게 정의되고 클라이언트에게 알려져야 한다. 심사팀은 7.1.2.1 기준을 모두 충족한 한 사람의 개인으로 구성할 수 있다.	<삭 제>	- 요구사항 삭제
9.2.1.2 IS 9.2.2 심사팀 적격성	<삭 제>	- 요구사항 삭제
7.1.2에 기술된 요구사항이 적용된다. 사후관리 및 특별 심사활동에 관해서는 사전에 계획된 사후관리 활동 및 특별 심사활동과 관련된 요구사항만 적용된다. 특정 인증심사를 위해 심사팀을 선정하고 관리하는 경우 인증기관은 각 임무에 관	<삭 제>	- 요구사항 삭제

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
<p>런된 적격성이 적절함을 보장해야 한다. 심사팀은 다음과 같은 사항을 따라야 한다.</p> <p>a) 인증을 위한 ISMS 범위 내의 특정활동과 관련된 절차 및 잠재적 정보보안 리스크에 대한 적절한 기술적 지식을 가져야 한다(기술전문가가 이러한 기능을 수행할 수 있다).</p> <p>b) 제품 및 서비스 정보보안 관리 조직 내에서 주어진 ISMS 범위 및 맥락을 신뢰할 수 있는 ISMS를 수행하기 위해 클라이언트에 대하여 충분히 이해해야 한다.</p> <p>c) 클라이언트의 ISMS에 적용 가능한 법적 및 규제적 요구사항에 대해 적절히 이해해야 한다.</p> <p>비고 적절한 이해가 전문적 법률지식을 의미하지는 않는다.</p>		
9.2.3 심사계획	9.2.3 심사계획	
<신 설>	9.2.3.1 일반사항	
KAB-R-MSCB, 9.2.3의 요구사항을 <u>적용한다</u> . 추가로 <u>다음의</u> 요구사항과 지침을 <u>적용하여야 한다</u> .	KAB-R-MSCB, 9.2.3의 요구사항을 <u>적용하여야 한다</u> . 추가로 <u>9.2.3.2 및 9.2.3.3의</u> 요구사항과 지침을 <u>적용하여야 한다</u> .	- 9.2.3, 9.2.3.2 및 9.2.3.3 적용 의무화
9.2.3.1 IS 9.2.3 일반사항	9.2.3.2 일반 고려사항	- 조항번호 변경 및 자구수정
<신 설>	비고 인증기관은 심사대상 조직과 심사시기를 합의하여 조직의 전체 범위를 가장 잘 입증하는 것이 좋다. 여기에는 계절, 월, 일/날짜 및 해당되는 경우 교대 근무 조 등에 대한 고려를 포함시킬 수 있다.	- 비고 신설 (현행 9.2.3.3에서 이동)
9.2.3.2 IS 9.2.3 네트워크를 이용한 심사 기법	<삭 제>	
심사계획에서는 심사시간 동안 활용될 네트워크를 이용한 심사기법을 적절히 파악하여야 한다. 네트워크를 이용한 심사기법은 전화 회의, 웹 미팅, 웹 기반의 양방향 의사소통, ISMS 문서 또는 ISMS 프로세스에 대한 원격 전자 접근 등을 포함할 수 있다. 이와 같은 기술의 중점은 심사의 효과성 및 효율성을 높여야 할 것이고, 심사 절차에 대한 무결성을 지원해야 할 것이다.	<삭 제>	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
<신 설>	9.2.3.3 원격심사 기술	- 원격심사 기술 요구 사항 신설
<신 설>	원격심사 기술의 목적은 심사 효과성 및 효율성을 증대하고, 심사프로세스의 완전성을 지원해야 할 것이다.	- 원격심사 기술 요구 사항 신설
<신 설>	심사계획은 원격심사를 지원하는데 사용되는 장치를 언급하여야 한다.	- 원격심사 기술 요구 사항 신설
9.2.3.3 IS 9.2.3 심사시기	<삭 제>	
인증기관은 조직의 전체 범위를 최상으로 입증할 수 있는 심사시기에 대해 조직과 합의해야 한다. 여기에는 계절, 월, 일/날짜 및 해당되는 경우 교대 근무조 등에 대한 고려를 포함시킬 수 있다.	<삭 제>	- 개정(안) 9.2.3.2 비고로 이동)
9.3 최초인증	9.3 최초인증	
<신 설>	9.3.1 일반사항	
KAB-R-MSCB, 9.3의 요구사항을 적용한다. 추가로 다음의 요구사항과 지침을 적용한다.	KAB-R-MSCB, 9.3의 요구사항을 적용하여야 한다. 추가로 9.3.2의 요구사항과 지침을 적용하여야 한다.	- 9.3 및 9.3.2 의무 적용화
9.3.1 IS 9.3.1 최초인증심사	9.3.2 최초인증심사	- 조항번호 변경 및 자구수정
9.3.1.1 IS 9.3.1.1 1단계	9.3.2.1 1단계	- 조항번호 변경 및 자구수정
1단계 심사에서 인증기관은 ISO/IEC 27001에서 요구하는 문서화를 포함하는 ISMS의 설계문서를 획득하여야 한다.	(현행과 같음)	
<신 설>	최소한, 1단계 심사 동안 다음의 정보가 클라이언트에 의해 제공되어야 한다.	- 파악되어야 할 최소 정보 명확화
<신 설>	a) 클라이언트가 다루는 ISMS 및 활동에 대한 일반 정보 b) ISO/IEC 27001에 명시되고 요구되는 ISMS 문서 사본 및 필요한 경우 기타 관련 문서	- 파악되어야 할 최소 정보 명확화
인증기관은 클라이언트의 조직, 리스크평가 및 대응(결정된 관리방안을 포함하는), 정보보안방침 및 목표, 그리고 특히 클라이언트의 심사 준비상태의 맥락에서 ISMS 설계에 대해 충분히 이해하여야 한다. 이를 통해 2단계 심사 계획이 가능하다.	인증기관은 클라이언트의 조직상황에서 ISMS 설계, (결정된 통제를 포함하는) 리스크평가 및 처리, 정보보안방침 및 목표, 그리고 특히 클라이언트의 준비 상태에 대해 충분히 이해하여야 한다. 이는 2단계 심사 계획에 사용되어야 한다.	- 번역 수정 - 2단계 심사 계획 시 1단계 심사 결과 사용의 의무화

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
1단계 결과는 서면 보고서로 문서화 되어야 한다. 인증기관은 2단계 심사 진행을 결정하기 전 1단계 심사보고서를 검토해야 하고 2단계 심사팀원이 필요한 적격성을 갖추고 있는지 확인하여야 한다. 적격성 및 적절성에 대한 확인은 1단계 심사를 이끌었던 심사원에 의해 수행될 수 있다.	1단계 결과는 서면 보고서로 문서화 되어야 한다. 인증기관은 2단계 심사 진행을 결정하기 전 1단계 심사보고서를 검토해야 한다. 인증기관은 2단계 심사팀원이 필요한 적격성을 갖추고 있음을 확인하여야 한다. 이에 대한 확인은 1단계 심사를 수행했던 심사팀의 심사팀장에 의해 수행될 수 있다.	- 자구 수정 - 적격성 확인을 심사팀장이 수행할 수 있도록 허용
비고 독립적 검토(예, 심사에 포함되지 않은 인증기관 인원에 의한)는 2단계를 누구와 함께 진행할 것인지 결정할 때 관련된 위험을 완화하는 하나의 방법이다. 그러나 동일한 목표를 달성하기 위해 이미 다른 위험완화 조치가 마련되었을 수도 있다.	비고 보고서를 검토하는 심사에 포함되지 않고, 2단계 심사에 대한 심사팀 멤버의 적격성을 결정하고 진행시킬 것을 결정하는 인원을 보유하는 것은 관련된 위험을 완화하는 하나의 방법이다. 그러나 동일한 목표를 달성하기 위해 이미 다른 위험완화 조치가 마련되었을 수도 있다.	- 영문 변경에 따른 번역 수정
<신 설>	인증기관은 2단계 심사동안 상세한 평가를 위해 필요할 수 있는 추가적인 유형의 정보 및 기록들을 고객에게 알려야 한다)	- 번역 누락에 따른 추가 번역
9.3.1.2 IS 9.3.1.2 2단계	9.3.2.2 2단계	- 조항번호 변경 및 자구수정
9.3.1.2.1 1단계 심사보고서의 문서화된 발견사항에 근거하여, 인증기관은 2단계 심사를 수행하기 위한 심사계획을 작성한다. ISMS의 효과적 이행에 대한 평가와 더불어 2단계의 목적은 다음과 같다. a) 클라이언트가 자체 방침, 목표 및 절차를 준수하고 있음을 확인	1단계 심사보고서의 문서화된 발견사항에 근거하여, 인증기관은 2단계 심사를 수행하기 위한 심사계획을 작성한다. ISMS의 효과적 이행에 대한 평가와 더불어 2단계의 목적은 클라이언트가 자체 방침, 목표 및 절차를 준수하고 있음을 확인하는 것이다.	- 조항번호 삭제 - 서술 방식 변경
9.3.1.2.2 이를 위해, 심사는 클라이언트의 다음 사항에 중점을 두어야 한다.	이를 위해, 심사는 클라이언트의 다음 사항에 중점을 두어야 한다.	- 조항번호 삭제
a) 최고 경영층의 리더십, 정보보안 방침 및 정보보안 목표에 대한 의지 b) ISO/IEC 27001에 제시된 문서 요구사항 c) 리스크 관련 정보보안평가 및 반복 수행 시 그 평가에서 나오는 일관성, 유효성 및 비교할 수 있는 결과 d) 정보보안 리스크평가 및 리스크관리 프로세스에 기반한 통제목적 및 통제항목 선정 e) 정보보안 수행 및 ISMS 효과성 검토,	a) 최고 경영층의 리더십, 정보보안 목표에 대한 의지 b) <삭 제> 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 리스크처리 프로세스에 기반한 통제항목 선정 d) 정보보안 목표에 대비하여 평가를 하	- “정보보안 방침” 삭제 - 조항번호 변경 및 자구수정 - 번역수정 및 “통제 목적” 삭제

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
<p><u>정보보안 목표에 대한 평가</u></p> <p>f) 결정된 통제항목 간의 유사성, 적용성 보고서와 정보보안 리스크평가 결과의 유사성, 리스크처리 프로세스와 정보보안 정책 및 목적 간 유사성</p> <p>g) 통제항목의 이행(부속서 D 참조), 내·외부 상황 및 관련 리스크, 조직의 모니터링, 정보보안 프로세스 및 통제항목의 측정과 분석, 통제항목에 대한 이행성 및 효과성과 제시된 정보보안 목표를 만족하는지 결정하는 것</p> <p>h) 경영자의 결정과 정보보안 방침 및 목표를 추적할 수 있음을 보장하기 위한 프로그램, 프로세스, 절차, 기록, 내부심사, ISMS 효과성 검토</p>	<p>는, 정보보안 수행 및 ISMS 효과성</p> <p>e) 결정된 통제항목 간의 유사성, 적용성 보고서와 정보보안 리스크평가 결과의 유사성, 리스크처리 프로세스와 정보보안 정책 및 목적 간 유사성</p> <p>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</p> <p>g) 경영자의 결정과 정보보안 방침 및 목표를 추적할 수 있음을 보장하기 위한 프로그램, 프로세스, 절차, 기록, 내부심사, ISMS 효과성 검토</p>	<p>- 의미 명확화</p> <p>- 조항번호 변경</p> <p>- 부속서명 변경 및 의미 명확화</p> <p>- 조항번호 변경</p>
9.4 심사 수행	9.4 심사 수행	
(없음)	9.4.1 일반사항	- 조항제목 신설
KAB-R-MSCB, 9.4의 요구사항을 적용한다. 추가로 다음의 요구사항과 지침을 적용한다.	KAB-R-MSCB, 9.4의 요구사항을 적용하여야 한다. 추가로 9.4.2 및 9.4.3의 요구사항과 지침을 적용하여야 한다.	- 9.4, 9.4.2 및 9.4.3 적용 의무화
9.4.1 IS 9.4 일반사항	<삭 제>	
<p>인증기관은 다음에 대한 문서화된 절차를 보유해야 한다.</p> <p>a) 경영체제 인증기관 인정기준(KAB-R-MSCB)의 조항에 따른 클라이언트의 ISMS에 대한 최초 인증심사</p> <p>b) 경영체제 인증기관 인정기준(KAB-R-MSCB)에 따라 클라이언트의 ISMS이 관련 요구사항에 대한 적합성을 지속적으로 유지하고 클라이언트가 모든 부적합사항에 대하여 시기적절하게 시정조치를 실시한 것을 검증하고 기록하는 주기적 사후 및 갱신심사</p>	<삭 제>	
9.4.2 IS 9.4 ISMS 심사의 특별요소	9.4.2 ISMS 심사의 특별요소	- 조항제목 자구 수정
<p>심사팀으로 대표되는 인증기관은 다음 사항을 수행하여야 한다.</p> <p>a) 리스크와 관련된 정보보안 평가가 적절하고 ISMS 인증범위 내에서 ISMS 운영에 충분하다는 것을 클라이언트에게 입증하도록 요구</p>	<p>인증기관 심사팀은 다음 사항을 수행하여야 한다.</p> <p>a) 정보보안 리스크 평가가 적절하고 ISMS 인증범위 내에서 ISMS 운영에 충분하다는 것을 클라이언트에게 입증하도록 요구</p>	<p>- 번역 수정</p> <p>- 번역 수정</p>

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
b) <u>리스크와 관련된 정보보안의 식별</u> , 시험 및 평가를 위한 클라이언트의 절차와 이행의 결과가 클라이언트의 방침, 목표 및 세부목표와 일관성이 있는지 여부를 확인 (이하 생략)	b) <u>정보보안 리스크의 식별</u> , 시험 및 평가를 위한 클라이언트의 절차와 이행의 결과가 클라이언트의 방침, 목표 및 세부목표와 일관성이 있는지 여부를 확인 (현행과 같음)	- 번역 수정
9.4.3 IS 9.4 심사보고서	9.4.3 심사보고서	- 조항제목 자구 수정
9.4.3.1 KAB-R-MSCB 9.4.8 보고서에 대한 요구사항에 추가하여, 심사보고서는 다음의 정보나 참조사항을 제공해야 한다.	9.4.3.1 심사보고서는 다음의 정보나 참조사항을 제공해야 한다.	- 참조 요구사항 삭제
a) 문서검토에 대한 요약사항을 포함한 심사의 설명 b) 클라이언트의 정보보안 리스크 분석에 대한 인증심사의 설명 c) 심사계획의 변경사항(예: 예정된 활동에 대하여 늘어난 또는 단축된 시간) d) ISMS 범위 <신 설>	<삭 제> a) 클라이언트의 정보보안 리스크 분석에 대한 인증심사의 설명 <삭 제> <삭 제> 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.	9.4.3.2 심사보고서는 인증결정을 촉진하고 지원하기에 충분히 세부적이어야 하며, 다음 사항을 포함해야 한다.	
a) 중대한 심사 추적 및 활용된 심사기법 (9.1.3.2 참조) b) 긍정적(예: 주목할 만한 특징), 부정적(예: 잠재적인 부적합) 면을 포함한 관찰 사항 c) <u>부적합에 대한 명확한 진술, 적용성 보고서의 버전 인용, 그리고 적용 가능한 경우, 클라이언트의 이전 인증심사 결과와의 유용한 비교를 포함하여, 인증 요구사항에 대한 클라이언트의 ISMS 적합성에 대한 의견</u>	a) 중대한 심사 추적 및 활용된 심사기법 (9.1.1.2 참조) <삭 제> b) <u>적용성 보고서의 버전 인용, 그리고 적용 가능한 경우, 클라이언트의 이전 인증심사 결과와의 유용한 비교</u> <삭 제>	- 참조 조항 변경 - 조항번호 변경 및 일부 내용 삭제
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. <u>심사기간에</u> 평가된 표본에 대한 정보는 심사보고서 또는 기타 인증문서에 포함되어야 한다.	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. <u>심사 중에</u> 평가된 표본에 대한 정보는 심사보고서 또는 기타 인증문서에 포함되어야 한다.	- 번역 수정

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
<신 설>	원격심사 방법이 사용된 경우, 보고서는 심사수행에 있어 원격심사 방법이 사용된 정도와 심사목적 달성에 있어 원격심사 방법의 효과성을 명시하여야 한다.	- 원격심사 관련 요구 사항 신설
<신 설>	조직의 활동이 규정된 물리적 위치에서 수행되지 않고, 그러므로 조직의 모든 활동이 원격으로 수행되는 경우, 심사보고서에는 조직의 모든 활동이 원격으로 수행됨을 기술하여야 한다.	- 원격심사 관련 요구 사항 신설
보고서는 ISMS에 대한 신뢰를 주기 위하여 클라이언트에 의해 채택된 내부 조직 및 절차를 적절하게 고려하여 작성되어야 한다.	(현행과 같음)	
KAB-R-MSCB, 9.4.8의 요구사항에 추가하여, 그 보고서에는 다음 사항이 포함되어야 한다. a) ISMS 요구사항 및 IS 통제항목의 이행 및 효과성과 관련하여 긍정적 측면뿐만 아니라 부정적인 측면을 포함하는 가장 중대한 관찰사항에 대한 요약 b) 클라이언트의 ISMS에 대한 인증여부와 관련된 심사팀의 권고사항 및 이 권고사항을 뒷받침 하는 정보	<삭 제> 심사보고서는 ISMS 요구사항 및 IS 통제항목의 이행 및 효과성과 관련하여 긍정적 측면뿐만 아니라 부정적인 측면을 포함하는 가장 중대한 관찰사항에 대한 요약을 포함하여야 한다. <삭 제>	- 보고서에 포함되어야 할 사항 일부 삭제 - 조항번호 삭제 - 세부 조항 삭제
9.5 인증결정	9.5 인증결정	
<신 설>	9.5.1 일반사항	
KAB-R-MSCB, 9.5의 요구사항을 적용한다. 추가로 다음의 요구사항과 지침을 적용한다.	KAB-R-MSCB, 9.5의 요구사항을 적용하여야 한다. 추가로 9.5.2의 요구사항과 지침을 적용하여야 한다.	- 9.5 및 9.5.2 적용 의무화
9.5.1 IS 9.5 인증결정	9.5.2 인증결정	- 조항번호 변경 및 자구 수정
인증결정은 KAB-R-MSCB 요구사항에 추가로 인증심사보고서에 제공된 심사팀의 인증권고에 근거하여야 한다 (삭제) (9.4.3 참조).	인증결정은 인증심사보고서에 제공된 심사팀의 인증권고에 근거하여야 한다.	- 참조문서 및 참조조항 삭제
인증허용을 결정하는 개인 또는 위원회는 일반적으로 심사팀의 부정적 권고를 뒤집을 수 없다. 그러한 상황이 발생하였을 경우, 인증기관은 권고에 대한 반복결정 근거를 문서화하고 정당화하여야 한다.	<삭 제>	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
경영검토 및 ISMS 내부심사가 수행되고, 효과적이며, 유지되는 것을 입증할 만한 충분한 증거가 있다면 클라이언트에게 인증이 승인된다.	경영검토 및 ISMS 내부심사가 수행되고, 효과적이며, 유지되는 것을 입증할 만한 충분한 증거가 있다면 클라이언트에게 인증이 승인된다.	
9.6 인증 유지	9.6 인증 유지	
9.6.1 일반사항	9.6.1 일반사항	
KAB-R-MSCB, 9.6.1의 요구사항을 적용한다. 추가로 다음의 요구사항과 지침을 적용한다.	KAB-R-MSCB, 9.6.1의 요구사항을 적용하여야 한다. <삭 제>	- 9.6.1 적용 의무화
9.6.2 사후관리 활동	9.6.2 사후관리 활동	
KAB-R-MSCB, 9.6.2의 요구사항을 적용한다. 추가로 다음의 요구사항과 지침을 적용한다.	9.6.2.1 KAB-R-MSCB, 9.6.2의 요구사항을 적용하여야 한다. 추가로 9.6.2.2, 9.6.2.3 및 9.6.2.4의 요구사항과 지침을 적용한다.	- 조항번호 신설 및 9.6.2, 9.6.2.2, 9.6.2.3, 9.6.2.4 적용 의무화
9.6.2.1 IS 9.6.2 사후관리심사	<삭 제>	- 조항제목 삭제
9.6.2.1.1 사후관리심사절차는 이 문서에서 기술하는 클라이언트의 ISMS 인증심사와 관련 사항들과 일관되어야 한다.	9.6.2.2 사후관리심사절차는 이 문서에서 기술하는 클라이언트의 ISMS 인증심사와 관련 절차들의 부분집합이 되어야 한다.	- 조항번호 변경 - 영문 표현 변경에 따른 번역 수정
사후관리의 목적은 승인된 ISMS가 이행되고, 클라이언트의 운영 상 변경에 따라 발생된 시스템 변경사항의 영향을 고려하며, 인증 요구사항을 지속적으로 준수하는지를 확인하기 위해 검증하는 것이다. 사후관리 프로그램은 최소한 다음 사항을 포함하여야 한다.	사후관리의 목적은 승인된 ISMS가 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.	- 자구 수정
a) 정보보안 리스크평가, 통제 유지, ISMS 내부심사, 경영검토와 시정조치 및 예방조치와 같은 시스템 유지 요소 b) ISMS 표준인 ISO/IEC 27001 및 인증을 위해 요구되는 기타 문서에 요구되는 외부 이해관계자와의 의사소통 사항 c) 문서화된 시스템의 변경사항 d) 변경을 필요로 하는 분야 e) 선정된 ISO/IEC 27001 요구사항 f) 적절하게 선정된 다른 분야	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 <삭 제> <삭 제> <삭 제> <삭 제>	- 자구 수정 - 자구 수정 - 요구사항 삭제 - 요구사항 삭제 - 요구사항 삭제 - 요구사항 삭제
9.6.2.1.2 인증기관은 사후관리 시 최소한 다음 사항을 검토하여야 한다. a) (생략) b) 관련된 정보보안 법규 및 규제사항을	9.6.2.3 인증기관은 사후관리심사 시 최소한 다음 사항을 검토하여야 한다. a) (현행과 같음) b) 관련된 정보보안 법규 및 규제사항 준	- 조항번호 변경 및 자구수정 - 번역 수정

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
<p>주기적으로 평가 및 준수를 검토하기 위한 절차의 기능</p> <p>c) 결정된 통제항목의 변경, <u>적용성보고서 변경 결과</u></p> <p>d) 심사프로그램에 따른 통제항목의 이행 및 효과성</p>	<p>수에 대한 주기적 평가 및 검토를 위한 절차의 기능</p> <p>c) 결정된 통제항목의 변경 및 그 결과에 따른 <u>적용성보고서의 변경들</u></p> <p>d) 심사프로그램에 따른 통제항목의 <u>구현</u> 및 효과성</p>	<p>- 번역 수정</p> <p>- 번역 수정</p>
<p>9.6.2.1.3 인증기관 클라이언트의 정보보안 이슈와 관련된 리스크 및 영향에 대한 사후관리 프로그램을 채택하고, 해당 프로그램을 정당화 할 수 있어야 한다.</p>	<p>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.</p>	<p>- 조항번호 변경 및 자구수정</p>
<p>사후관리 심사는 다른 경영체제의 심사와 통합될 수도 있다. 그 보고서에는 각 경영체제와 관련된 측면을 명시하여야 한다.</p>	<p>사후관리 심사는 다른 경영체제의 심사와 통합될 수도 있다. 심사 보고서에는 각 경영체제와 관련된 측면을 명시하여야 한다.</p>	<p>- 자구수정</p>
<p>사후관리 심사시간 동안, 인증기관은 발생한 불만에 대한 기록을 확인하여야 한다. 인증 요구사항에 대한 부적합 또는 실패가 확인된 경우, 클라이언트는 자신의 ISMS 및 절차를 조사하고 적절하게 시정조치를 취하여야 한다</p>	<p>사후관리 <u>심사</u> 동안, 인증기관은 발생한 불만 및 이의제기에 대한 기록을 확인하여야 한다. 인증 요구사항에 대한 부적합 또는 실패가 확인된 경우, <u>인증기관은</u> 클라이언트가 자신의 ISMS 및 절차를 조사하고 적절하게 시정조치를 <u>취했음을 확인</u>하여야 한다.</p>	<p>- 번역 수정</p> <p>- 번역 수정</p> <p>- 확인 주체의 명확화</p>
<p>사후관리 보고서에서는 특히, 이전에 발견된 부적합 및 적용성 보고서에 대한 명확한 정보와 이전 심사로부터의 중요 변화가 포함되어야 한다. 사후관리 보고는 최소한 위 9.6.2.1.1와 9.6.2.1.2의 요구사항 전체를 포함하여 작성되어야 한다.</p>	<p>사후관리 보고서에서는 특히, 이전에 발견된 부적합 및 적용성 보고서에 대한 명확한 정보와 이전 심사로부터의 중요 변화가 포함되어야 한다. 사후관리 보고는 최소한 9.6.2.2와 9.6.2.3의 요구사항 전체를 포함하여 작성되어야 한다.</p>	<p>- 참조 조항 변경</p>
<p>9.6.3 갱신인증</p>	<p>9.6.3 갱신인증</p>	
<p><신 설></p>	<p>9.6.3.1 일반사항</p>	
<p>KAB-R-MSCB, 9.6.3의 요구사항을 적용한다. 추가로 다음의 요구사항과 지침을 적용한다.</p>	<p>KAB-R-MSCB, 9.6.3의 요구사항을 적용하여야 한다. 추가로 9.6.3.2의 요구사항과 지침을 적용하여야 한다.</p>	<p>- 9.6.3 및 9.6.3.2 적용 의무화</p>
<p>9.6.3.1 IS 9.6.3 갱신심사</p>	<p>9.6.3.2 갱신심사</p>	<p>- 조항번호 변경 및 자구수정</p>
<p>갱신심사절차는 이 문서에서 기술하는 클라이언트의 ISMS에 대한 최초인증심사와 관련된 사항들과 일관되어야 한다.</p>	<p>갱신심사절차는 이 문서에서 기술하는 클라이언트의 ISMS에 대한 최초인증심사와 관련된 <u>절차들의 부분집합이</u> 되어야 한다.</p>	<p>- 영문 표현 변경에 따른 번역 수정</p>
<p>9.6.4 특별심사</p>	<p>9.6.4 특별심사</p>	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
KAB-R-MSCB, 9.6.4의 요구사항을 <u>적용한다</u> . 추가로 다음의 요구사항과 지침을 적용한다.	KAB-R-MSCB, 9.6.4의 요구사항을 <u>적용하여야 한다</u> . <삭 제>	- 9.6.4 적용 의무화
9.6.4.1 IS 9.6.4 특별심사 사례	<삭 제>	- 특별심사 사례 삭제
사후관리 활동에서 클라이언트가 인증된 ISMS에 대해 중대한 시스템 변경을 하였거나, 인증에 영향을 받을 수 있는 기타 변경이 이루어진 경우, 이 조항을 적용할 수 있다.	<삭 제>	- 특별심사 사례 삭제
9.6.5 인증의 정지, 취소, 또는 인증범위 축소	9.6.5 인증의 정지, 취소, 또는 인증범위 축소	
KAB-R-MSCB, 9.6.5의 요구사항을 <u>적용한다</u> .	KAB-R-MSCB, 9.6.5의 요구사항을 <u>적용하여야 한다</u> .	- 9.6.5 적용 의무화
9.7 이의제기	9.7 이의제기	
KAB-R-MSCB, 9.7의 요구사항을 <u>적용한다</u> .	KAB-R-MSCB, 9.7의 요구사항을 <u>적용하여야 한다</u> .	- 9.7 적용 의무화
9.8 불만	9.8 불만	
<신 설>	9.8.1 일반사항	- 조항제목 신설
KAB-R-MSCB, 9.8의 요구사항을 <u>적용한다</u> . 추가로 다음의 요구사항과 지침을 적용한다.	KAB-R-MSCB, 9.8의 요구사항을 <u>적용하여야 한다</u> . <삭 제>	- 9.8 적용 의무화
9.8.1 IS 9.8 불만	9.8.2 불만	- 조항번호 변경 및 자구수정
불만은 가능한 부적합에 관한 잠재적 사고 및 암시를 의미한다.	(현행과 같음)	
9.9 클라이언트에 대한 기록	9.9 클라이언트에 대한 기록	
KAB-R-MSCB, 9.9의 요구사항을 <u>적용한다</u> .	KAB-R-MSCB, 9.9의 요구사항을 <u>적용하여야 한다</u> .	- 9.9 적용 의무화
10 인증기관 경영시스템 요구사항	10 인증기관 경영시스템 요구사항	
10.1 경영시스템에 대한 선택사항	10.1 경영시스템에 대한 선택사항	
<신 설>	10.1.1 일반사항	
KAB-R-MSCB, 10.1의 요구사항을 <u>적용한다</u> . 추가로 다음의 요구사항과 지침을 적용한다.	KAB-R-MSCB, 10.1의 요구사항을 <u>적용하여야 한다</u> . 추가로 10.1.2의 요구사항과 지침을 <u>적용하여야 한다</u> .	- 10.1 및 10.1.2 적용 의무화
10.1.1 IS 10.1 ISMS 실행	10.1.2 ISMS 실행	- 조항번호 변경 및 자구수정

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
(생략)	(현행과 같음)	
10.2 선택사항 A: 일반적인 경영시스템 요구사항	10.2 선택사항 A: 일반적인 경영시스템 요구사항	
KAB-R-MSCB, 10.2의 요구사항을 적용한다.	KAB-R-MSCB, 10.2의 요구사항을 적용하여야 한다.	- 10.2 적용 의무화
10.3 선택사항 B: ISO 9001에 따른 경영시스템 요구사항	10.3 선택사항 B: ISO 9001에 따른 경영시스템 요구사항	
KAB-R-MSCB, 10.3의 요구사항을 적용한다.	KAB-R-MSCB, 10.3의 요구사항을 적용하여야 한다.	- 10.3 적용 의무화
부속서 A (참고) 정보보안경영시스템 심사 및 인증을 위한 지식과 스킬	부속서 A (필수) 정보보안경영시스템 심사 및 인증을 위한 지식과 스킬	- 부속서 A 의무화
A.1 개요	A.1 개요	
<p>표 A.1은 ISMS 심사 및 인증에 필요한 지식 및 숙련도/기량에 대한 요약을 제공하나, 오직 특정 인증기능에 대한 지식 및 스킬만 다루기 때문에 참고용으로 제공된다. 각 기능에 대한 적격성 요구사항은 이 국제표준 본문에 언급되어 있으며, 이 표는 구체적인 요구사항에 대한 참고사항을 제공한다.</p> <p><신 설></p>	<p><삭 제></p> <p>표 A.1 에는 KAB-R-MSCB에 추가하여, 특정 인증업무기능에 대하여 인증기관이 규정해야하는 지식 및 기술이 명시되어 있다. “○” 는 인증기관이 지식 및 스킬의 기준과 깊이를 규정해야 함을 의미한다. 표 A.1에 명시되어 있는 지식 및 기술은 7항에 더욱 자세하게 설명되어 있으며, 표 A.1의 괄호 안에 상호참조가 되어 있다.</p>	- 표 설명 신설
표 A.1 ISMS 심사 및 인증을 위한 지식	표 A.1 ISMS 심사 및 인증을 위한 지식 및 스킬	- 영문 표현 변경에 따른 번역 수정
(표 생략)	(표 생략)	- 표의 현행/개정(안)은 [별표 1] 참조
<신 설>	비고 추가 적격성 고려사항은 부속서 B에 명시됨	
<신 설>	부속서 B (참고) 추가 적격성 고려사항	- 추가 적격성 고려사항에 대한 부속서 신설

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
A.2 일반 적격성 고려사항	B.1 일반 적격성 고려사항	- 부속서 이동에 따른 조항제목 변경(이하 동일)
심사원의 지식 및 경험을 증명할 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 ISMS의 복잡성에 따라 설정되어야 할 것이다.	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 ISMS의 복잡성을 반영하여 설정되어야 할 것이다.	- 자구 수정 - 자구 수정
A.3 특정지식 및 경험 고려사항	B.2 특정지식 및 경험 고려사항	
A.3.1 ISMS 관련 대표적 지식	B.2.1 ISMS 관련 대표적 지식	
7.1.2의 요구사항에 추가하여 다음 사항이 고려되어야 한다. 심사원들은 다음에 대한 심사와 ISMS 대상에 대한 지식 및 이해를 보유하여야 할 것이다. (이하 생략)	7.1.3의 요구사항에 추가하여 다음 사항이 고려되어야 한다. 심사원들은 다음에 대한 심사와 ISMS 대상에 대한 지식 및 이해를 보유하여야 할 것이다. (현행과 동일)	- 참조조항 변경
<신 설>	특정 분야에 대하여, 지식 및 이해가 특정 표준(예: ISO/IEC 27006-2)으로부터 설정하는 것이 가능하다.	- 특정 표준에 의한 지식/이해 설정 허용
부속서 B (필수) 심사시간	부속서 C (필수) 심사시간	- 부속서 번호 변경
B.1 개요	C.1 일반사항	- 조항번호 및 제목 변경
이 부속서는 KAB-R-MSCB, 9.1에 대한 부가적인 요구사항이며, 인증기관이 다양한 범위의 활동규모와 복잡성을 가지는 조직에 대한 심사를 수행할 때 필요한 심사시간을 결정하는 절차의 개발에 관련된 최소 요구사항 및 지침을 제공한다.	이 부속서는 KAB-R-MSCB, 9.1.4에 대한 부가적인 요구사항이며, 인증기관이 다양한 범위의 활동규모와 복잡성을 가지는 ISMS 범위에 대한 인증에 필요한 심사시간을 결정하는 절차의 개발에 관련된 최소 요구사항 및 지침을 제공한다.	- 번역 수정
<신 설>	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.	- 충분한 심사시간 확보에 대한 사항 신설
인증기관은 각 클라이언트 및 인증된 ISMS에 대한 최초인증, 사후관리 및 갱신 심사에 소요되는 심사시간을 규정해야 한다	인증기관은 각 클라이언트 및 인증된 ISMS에 대한 최초인증, 사후관리 및 갱신 심사에 소요되는 심사시간을 규정해야 한다	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
다. <u>심사기획단계에서</u> 이 부속서의 사용은 적절한 심사시간 결정을 일관된 접근 방법으로 유도한다. 추가로, 심사시간은 심사과정, 특히 1단계에서 발견된 사항에 따라 조정될 수 있을 것이다(예: ISMS 범위의 복잡성에 대한 평가의 차이, 또는 해당 범위의 추가 사업장).	다. <u>심사계획단계 동안</u> 이 부속서의 사용은 적절한 심사시간 결정을 일관된 접근 방법으로 유도한다. 추가로, 심사시간은 심사과정, 특히 1단계에서 발견된 사항에 따라 조정될 수 있을 것이다(예: ISMS 범위의 복잡성에 대한 평가의 차이, 또는 해당 범위의 추가 사업장).	- 자구 수정
본 부속서는 다음과 같은 사항을 제시한다.	본 부속서는 다음과 같은 사항을 제시한다.	
<ul style="list-style-type: none"> - 심사시간 계산에 사용되는 개념(B.2) - 각 심사단계에 대한 <u>심사시간 결정 절차</u>에 대한 요구사항 (B.3에서 B.5까지) (없음) - 복수사업장 심사 관련 요구사항(B.6) (없음) 	<ul style="list-style-type: none"> - 심사시간 계산에 사용되는 개념(C.2) - 각 심사단계에 대한 <u>최초심사 결정 절차</u>에 대한 요구사항 (C.3) - (신설) <u>사후관리심사(C.4) 및 갱신심사(C.5) 심사시간에 대한 요구사항</u> - 복수사업장 심사 관련 요구사항(C.6) - (신설) <u>범위확대를 위한 심사시간 요구사항(C.7)</u> 	<ul style="list-style-type: none"> - 참조조항 변경 - 참조조항 변경 및 의미 명확화 - 사후 및 갱신심사 요구사항 신설 - 참조조항 변경 - 범위확대 요구사항 신설
<u>부속서 B의 적용을 나타내는</u> 심사시간 계산 예시는 <u>부속서 C에서</u> 참조할 수 있다.	<u>본 부속서의 적용을 나타내는</u> 심사시간 계산 예시는 <u>부속서 D에서</u> 참조할 수 있다.	- 참조문서 번호 변경
심사시간 결정을 위한 계산방법에 대한 <u>이 접근방법의 기본적인 가정</u> 은 다음과 같아야 할 것이다.	심사시간 결정을 위한 계산방법에 대한 <u>본 부속서의 접근방법에 대한 기본적인 가정</u> 은 다음과 같아야 할 것이다.	- 자구 수정
a) <u>결정할 수 있는 증명된</u> 특성만 고려 b) 인증기관이 <u>효율적으로 적용할 수 있도록 충분히 쉬워야 한다.</u> c) <u>충분히 구분할 수 있는 복잡성</u>	a) <u>객관적으로 평가될 수 있는</u> 특성만 고려 b) 인증기관이 <u>적용하고, 비교가능하고 재현이 가능한 유효한 결과를 달성하기에 충분히 간단함</u> c) <u>특성 값에서의 변동이 결과적으로 산정될 심사시간에서의 비교할만한 변화를 야기하도록 충분히 정교하여야 한다.</u>	<ul style="list-style-type: none"> - 영문표현 변경에 따른 번역 변경 - 영문표현 변경에 따른 번역 변경 - 영문표현 변경에 따른 번역 변경
심사시간 결정은 <u>아래 표 B.1의 숫자</u> 를 근거로 하며 수정에 영향을 미치는 요인들을 고려해야 한다.	심사시간 결정은 <u>표 C.1의 숫자</u> 를 근거로 하며 수정에 영향을 미치는 요인들을 고려해야 한다.	- 참조 표 번호 변경
<신 설>	<u>인증기관이 규정한 심사기간 결정을 위한 이 접근법이 ISMS의 복잡성에 대하여 충분한지 검증하기 위하여 정기적으로 검토되어야 한다.</u>	- 요구사항 신설
<u>B.2 개념</u>	<u>C.2 개념</u>	- 조항번호 변경
<u>B.2.1 조직의 관리 하에 근무하는 인원의</u>	<u>C.2.1 조직의 관리 하에 근무하는 인원의</u>	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
수	수	
비고 “조직의 관리 하에 근무하는 개인”은 KAB-R-MSCB에 나오는 인원을 뜻한다.	비고 조직의 관리 하에 근무하는 개인은 (조직에 소속 여부와 상관없이) 인증범위 내에서 ISMS 요구사항에 따라 업무를 수행하도록 요구되는 모든 인원을 포함하여야 한다.	- 의미 명확화
<신 설>	인증범위에 포함되는 조직의 관리 하에 근무하는 인원의 높은 비율이 특정한 동일 활동을 수행할 때, 표 C.1을 활용하기에 앞서, 인원 수에 대한 감축이 심사시간 산정을 위해 허용된다. 인증기관은 C.3.4에서 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.	
B.2.2 심사일수	C.2.2 심사일수	- 조항번호 변경
표 B.1의 “심사시간”은 심사에 소요되는 “심사일수”로 표현된다. 부속서B에 따른 계산은 1일 8시간 근무시간을 기본으로 한다.	표 C.1의 심사시간은 심사에 소요되는 심사일수로 표현된다. 본 부속서는 1일 8시간 근무시간으로 계산하는 것을 기본으로 한다. (약자 “d”로 표현)	- 참조 표 번호 변경 및 자구 수정 - 자구수정
B.2.3 임시사업장	C.2.3 임시사업장	- 조항번호 변경
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 임시사업장에서 발생한 부적합으로 인해 제품 또는 서비스가 IS 목적을 충족시키는 데 실패할 리스크에 대한 평가에 기초하여야 할 것이다. 선정된 샘플 사업장은 활동의 규모 및 유형, 진행 중인 프로젝트의 다양한 단계를 고려하여, 조직의 적격성 요구 및 서비스의 다양성을 대표하는 것이어야 한다. 일반적인 샘플링은 9.1.5.1을 참조하여 수행한다.	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 9.1.5.2를 참조하여 수행한다.	- 의미 명확화 - 영문 표현 변경에 따른 번역 수정 - 영문 표현 변경에 따른 번역 수정 - 참조조항 변경
B.3 최초심사를 위한 심사시간 결정 절차	C.3 최초심사를 위한 심사시간 결정 절차	- 조항번호 변경

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
B.3.1 일반사항	C.3.1 일반사항	- 조항번호 변경
심사시간 계산은 문서화된 절차를 따라야 한다.	인증기관은 심사시간 계산을 위한 문서화된 절차를 보유하고 준수하여야 한다.	- 영문표현 변경에 따른 번역 수정
B.3.2 원격심사	C.3.2 심사수행을 위한 원격의 방법	- 조항번호 변경
조직과의 의사소통을 위하여 웹 기반 협력, 웹 미팅, 원격 회의 및/또는 전자적인 검증과 같은 원격심사기법이 사용되는 경우, 이러한 활동은 심사계획에 명시되어야 할 것이며(9.2.3 참조), 부분적으로 총 “현장심사시간”에 포함되는 현장심사활동으로 간주될 수 있다.	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.	- 영문표현 변경에 따른 번역 수정
심사계획의 수립 시, 원격심사활동이 계획된 현장심사시간의 30%를 초과하는 경우, 인증기관은 실행 전에 해당 심사계획의 정당성을 입증해야 하며 인정기관으로부터 명확한 승인을 받아야 한다.	<삭 제>	- 요구사항 삭제
B.3.3 심사시간 계산	C.3.3 심사시간 계산	- 조항번호 변경
아래 제시된 심사시간표는 최초심사시간의 평균에 대한 출발점을 나타낸다(이하 해당시간은 최초심사 단계(1단계 및 2단계) 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.	표 C.1에 제시된 심사시간표는 최초심사시간의 평균에 대한 출발점을 나타낸다(본 부속서 및 부속서 D 내에서는, 이하 해당시간은 최초심사 단계(1단계 및 2단계) 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.	- 참조 표 번호 변경 - 범위 명확화
아래 심사시간표는 심사계획을 위해 모든 교대조에 대하여 조직의 관리 하에 업무를 수행하는 총 인원을 근거로 심사시간 산출의 출발점을 파악하며, 심사대상 ISMS 범위에 적용되는 중대한 요인에 근거하여 심사시간을 조정하고, 기본 심사시간을 조정하기 위해 각각의 요인의 비중을 추가하거나 줄여야 하는 틀을 제공한다. 이 표에 사용된 용어는 B.2에서 설명하며, 부속서 C에서는 그 예시를 보여준다.	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.1의 심사시간표는 적용되는 요인과 허용된 편차에 대한 제한을 고려하여 사용되어야 한다. 이 표(표 C.1)에 사용된 용어는 C.2에서 설명한다. 부속서 D에서는 이 부속서의 계산법이 적용되는 예시를 보여준다.	- 서술방식의 변경 및 참조 조항/표 번호 변경

현행(Issue No.2, 2020.12.03.)				개정(안) (Issue No.3, 2024.06.20.)				개정 사유	
<신 설>				C.3.4 인원에 대한 초기값 결정					
<신 설>				인증기관은 특정한 동일 활동을 수행하는 많은 수의 인원과 관련한 정보를 클라이언트로에 요청하여야 한다. - 활동에 관여하는 인원의 수 - 활동 또는 프로세스의 유형				- 인원 수 결정을 위한 요구사항 신설	
<신 설>				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 작업의 작업공간 반입을 금지하는 조치)이 이행되는 곳에서 활동을 수행하는 인원				- 인원 수 결정을 위한 요구사항 신설	
<신 설>				동일 활동을 수행하는 인원 수를 감축하는 것은 과업과 관련된 활동의 리스크에 기반하여 이루어져야 한다. 동일 활동 각각에 대한 인원 수의 제공근이 유효종업원 수를 결정하기 위해 사용될 수도 있을 것이며, 이는 심사기간 산정을 위해 사용되고 그 다음 정수로 반올림한 값이다. 이는 허용된 인원 수에 대한 최대 감축이어야 한다.				- 인원 수 결정을 위한 요구사항 신설	
<신 설>				과업의 성질, 법적 요구사항 및 개인이 접근할 수 있는 정보의 중요도는 감축을 제한할 수 있다.				- 인원 수 결정을 위한 요구사항 신설	
<신 설>				이 절차를 적용하여 결정된 인원 수는 표 C.1의 출발점이다.				- 인원 수 결정을 위한 요구사항 신설	
<신 설>				비고 표는 IAF MD5와 동일하게 구조화되었다.				- 인원 수 결정을 위한 요구사항 신설	
표 B.1 심사시간표				표 C.1 심사시간표				- 표 번호 변경	
조직의 관 (생략) 가감요인 (생략)				조직의 관 (생략) 가감요인 (생략)				- 가감요인 참조 조항	

현행(Issue No.2, 2020.12.03.)				개정(안) (Issue No.3, 2024.06.20.)				개정 사유
리 하에 업무를 수 행하는 개 인의 수				리 하에 업무를 수 행하는 개 인의 수				변경(표 전체)
	1 ~ 10	(생략)	B.3.4 참조		1 ~ 10	(생략)	C.3.5 참조	
	(중략)				(중략)			
	> 10700	(생략)	B.3.4 참조		> 10700	(생략)	C.3.5 참조	
B.4.3 심사시간 조정 요인				C.3.5 심사시간 조정 요인				- 조항번호 변경
심사시간 표는 단독으로 사용되어서는 안 된다. 할당되는 심사시간은 ISMS의 복잡성과 관련된 다음의 요인과 복잡성에 따라 ISMS 심사에 필요한 노력을 고려해야 한다.				표 C.1은 단독으로 사용되어서는 안 된다. 할당되는 심사시간은 ISMS의 복잡성과 관련된 다음의 요인과 복잡성에 따라 ISMS 심사에 필요한 노력을 고려해야 한다.				- 표 번호 명시
a) ISMS의 복잡성(예: 정보의 중요성, ISMS의 리스크 상황 등) b) ISMS 범위 내에서 수행된 사업의 유형 c) 이전에 입증된 ISMS 성과 d) ISMS의 다양한 요소의 이행에 활용되는 기술의 정도 및 다양성				a) (현행과 같음) b) (현행과 같음) c) (현행과 같음) d) ISMS의 다양한 요소의 이행에 활용되는 기술의 정도 및 다양성 (예: 상이한 IT 플랫폼의 수, 분리된 네트워크의 수)				- 예시 추가
e) ISMS 범위 내에서 사용된 외주업체 및 제 3자의 범위 f) 정보시스템 개발 범위 g) 사업장 수 및 재난 복구(DR) 사업장의 수 〈신 설〉				e) ISMS 범위 내에서 사용된 외주업체 및 제 3자 협약의 범위 f) (현행과 같음) g) (현행과 같음) h) 1단계 심사 이후, 인증기관은 통제항목의 수와 복잡성				- 번역 수정 - 요구사항 신설
h) 사후관리 및 갱신심사: KAB-R-MSCB, 8.5.3에 따른 ISMS 관련 변화의 정도 및 범주				i) 사후관리 및 갱신심사: KAB-R-MSCB, 8.5.3에 따른 ISMS 관련 변화의 정도 및 범주				- 조항 변경
부속서 C에 심사시간 계산 시 고려해야 할 요인들의 예시가 제공된다.				부속서 D에 심사시간 계산 시 고려해야 할 요인들의 예시가 제공된다.				- 참조조항 변경
심사시간 증가가 요구되는 추가적인 요인의 예시는 다음과 같다.				심사시간 증가가 요구되는 요인의 예시는 다음과 같다.				- 자구 수정
- ISMS 범위 내 2개 이상의 건물이나 장소가 포함되는 복잡한 지리적 위치(및 이에 따른 이동) (이하 생략)				- ISMS 범위 내 2개 이상의 건물이나 장소가 포함되는 복잡한 프로세스의 관리 (현행과 같음)				- 자구 수정 및 번역 오류 수정
심사시간 단축이 허용될 수 있는 요인의 예는 다음과 같다.				심사시간 단축이 허용될 수 있는 요인의 예는 다음과 같다.				

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
<ul style="list-style-type: none"> - 리스크가 없거나/낮은 <u>제품/프로세스</u> - 프로세스가 단일 활동에 관련된 경우 (예: 서비스에 국한) - 조직의 관리 하에 동일한 단순 작업을 하는 개인의 비율이 높을 경우 - 조직에 대한 사전 지식(예를 들어, 동일한 인증기관에 대해 이미 다른 표준 인증을 받은 경우) - 인증에 대한 신청 조직의 준비 정도 (예: 이미 다른 제 3자 제도에 의해 인증이나 <u>인정</u>을 받음) - 경영시스템의 성숙도 	<ul style="list-style-type: none"> - 리스크가 없거나/낮은 <u>프로세스</u> - (현행과 같음) <삭 제> - (현행과 같음) - 인증에 대한 신청 조직의 준비 정도 (예: 이미 다른 제 3자 제도에 의해 인증이나 <u>인정(recognition)</u>을 받음) - (현행과 같음) 	<ul style="list-style-type: none"> - 제품 삭제 - 심사시간 단축 허용 요인 삭제 - 의미 명확화
<p><u>인증신청조직</u> 또는 인증조직이 임시사업장에서 자사의 제품(들) 또는 서비스(들)을 제공하는 경우에는 이러한 임시사업장에 대한 평가를 심사 및 사후관리 프로그램에 포함시키는 것이 중요하다.</p>	<p>클라이언트 또는 인증조직이 임시사업장에서 자사의 제품(들) 또는 서비스(들)을 제공하는 경우에는 이러한 임시사업장에 대한 평가를 심사 및 사후관리 프로그램에 포함시키는 것이 중요하다.</p>	<ul style="list-style-type: none"> - 영문표현 변경에 따른 용어 수정
<p><u>효과적인 심사를 위해 위의 요인들이 고려되어야 하며 그 요인들로 인한 조정은 심사시간의 가감을 정당화 하여야 한다. 심사시간 연장요인은 단축요인에 의해 상쇄될 수 있다. 심사시간 표에 주어진 기간에 대한 조정이 있는 모든 경우, 이를 정당화하는 충분한 증거 및 기록을 유지해야 한다.</u></p>	<p><u>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.</u></p>	
<p>B.3.5 심사시간 편차의 제한</p>	<p>C.3.6 심사시간 편차의 제한</p>	<ul style="list-style-type: none"> - 조항번호 변경
<p><u>효율적</u> 심사가 수행되었음을 보장하고, 신뢰할 수 있는 비교 가능한 결과를 보장하기 위해 해당 표에서의 심사시간을 30% 이상 축소할 수 없다.</p>	<p><u>효과적</u> 심사가 수행되었음을 보장하고, 신뢰할 수 있는 비교 가능한 결과를 보장하기 위해 해당 표에서의 심사시간을 30% 이상 축소할 수 없다.</p>	<ul style="list-style-type: none"> - 번역 수정
<p>편차에 대한 적절한 사유는 <u>확증</u>되어야 하고 문서화되어야 한다.</p>	<p>편차에 대한 적절한 사유는 <u>확립</u>되어야 하고 문서화되어야 한다.</p>	<ul style="list-style-type: none"> - 번역 수정
<p>B.3.6 현장심사시간</p>	<p>C.3.7 현장심사시간</p>	<ul style="list-style-type: none"> - 조항번호 변경
<p>심사계획과 보고서 작성을 위해 계산된 시간이 일반적으로 B.3.3 과 B.3.4 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.</p>	<p>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.</p>	<ul style="list-style-type: none"> - 참조조항 변경

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
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.	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 70%는 ISMS 심사원의 경험에 근거한 요소이다.	비고 1 (현행과 같음)	- 비고 번호 신설
<신 설>	비고 2 용어 “물리/원격”은 (클라이언트의 물리적 장소 또는 전자적 장소에 대한) “현장” 심사가 물리적으로 또는 원격적으로 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.	- 비고 신설
B.4 사후관리심사시간	C.4 사후관리심사시간	- 조항번호 변경
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 수시로 검토되어야 한다. 사후관리를 위해 소요되는 시간은 ISMS의 변경사항(예: 새로운 사항 또는 변경된 통제항목)을 심사하기 위해 증가되어야 한다.	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 ISMS의 변경사항(예: 새로운 사항 또는 변경된 정보보안 통제항목, 프로세스 및 제품)을 심사하기 위해 증가되어야 한다.	- 영문 표현 변경에 따른 번역 수정 - 의미 명확화
B.5 갱신심사시간	C.5 갱신심사시간	
갱신심사 수행에 소요되는 총 시간은 9.4.3 및 KAB-R-MSCB, 9.6.3에 명시되어 있는 이전 심사 결과에 따른다. 갱신심사에 소요되는 총 시간은 동일한 조직에 대한 <u>최소 심사시간</u> 에 비례하여야 하며, 동일한 조직에 대한 최초심사시간의 약 2/3가 되어야 한다.	갱신심사 수행에 소요되는 총 시간은 9.4.3 및 KAB-R-MSCB, 9.6.3에 명시되어 있는 이전 심사 결과에 따른다. 갱신심사에 소요되는 총 시간은 동일한 조직에 대한 <u>최초심사시간</u> 에 비례하여야 하며, 동일한 조직에 대한 최초심사시간의 약 2/3가 되어야 한다.	- 번역 오류 수정
B.6 복수사업장 심사	C.6 복수사업장 심사	
<신 설>	일반적으로 현장심사에 대한 총 심사시간은 인원의 위치와 관계없이 조직의 관리하에 근무하는 총 인원수를 고려하여 계산되어야 한다.	- 요구사항 신설
<신 설>	또는, 문서화되어야 하는 정당화된 이유	- 요구사항 신설

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
	에 대해서는, 이 조항의 첫 번째 단락에 따라 정의된 심사시간보다 총 심사시간이 더 큰 경우에 한해서, 각각의 사업장 별로 계산한 심사시간을 더하는 것이 허용된다. (현행의 마지막 단락에서 이동) 본사 또는 지역 사업장과 관련 없는 심사의 일부를 고려하여 단축할 수도 있다. 인증기관은 이 같은 시간 단축의 정당성에 대한 사유를 기록해야 한다.	
B.3.3에 명시된 절차에 따르는 범위에 대해 계산된 총 현장심사일수는 경영시스템 및 파악된 위험에 대한 사업장의 관련성에 근거하여 분배되어야 한다. 분배의 정당성은 인증기관에 의해 기록되어야 한다.	C.3.3 및 C.3.4에 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.	- 참조조항 변경 - 고려 요인 추가
본사 또는 지역 사업장과 관련 없는 심사의 일부를 고려하여 단축할 수도 있다. 인증기관은 이 같은 시간 단축의 정당성에 대한 사유를 기록해야 한다.	<삭 제>	- 개정(안)의 첫 번째 단락으로 이동
최초심사와 사후심사에서 소요된 총 시간은 중앙 사무소 및 각 사업장에서 소모된 시간의 합이며, 모든 작업이 단일 사업장(예: 한 회사의 직원들이 모두 같은 사업장에서 근무하는 경우)에서 수행되는 경우에 운영의 규모와 복잡성에 대해 계산된 시간보다 작게 산정할 수 없다.	<삭 제>	- 요구사항 신설
<신 설>	심사시간을 전체 심사시간과 비교하기 전, 감축이 적용되어야 한다.	
<신 설>	C.7 범위확대를 위한 심사시간	- 요구사항 신설
<신 설>	ISMS 범위확대를 위한 심사시간은 다음과 같은 요인을 고려하여 계산되어야 한다.	- 요구사항 신설
<신 설>	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	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
	g) 확대 범위를 ISMS로 통합하는 것을 검토하는데 요구되는 시간	
<신 설>	인증기관은 범위확대에 대한 일관적인 접근을 제공하는 절차서를 보유하여야 한다.	
<신 설>	신규범위에 대한 최초심사의 경우, 심사시간은 C.3.3, C.3.4 및 C.3.4를 활용한 기존 범위에 추가되는 인원 및 사업장의 수를 기반으로 계산되어야 한다.	
<신 설>	심사시간은 클라이언트의 ISMS를 검토하기 위해 계산된 기간에 추가되어야 한다. 이 추가시간은 최소한 다음과 같아야 한다.	
<신 설>	1) 범위확대 심사가 사후관리심사 또는 갱신심사와 함께 수행된다면, 0.5일(MD) 2) 독립된 심사로 범위확대 심사가 수행되는 경우, 1일(MD)	
부속서 C (참고) 심사기간 계산방법	부속서 D (참고) 심사기간 계산방법	- 조항번호 변경
C.1 일반사항	D.1 일반사항	
이 부속서는 심사시간의 계산에 대한 공식을 <u>이끌어내는</u> 부가적인 가이드라인을 제시한다. C.2에서는 심사시간 계산을 위해 기본적으로 사용될 수 있는 요인을 분류하는 사례를 제시하고, C.3에서는 심사시간 계산의 예시를 제공한다.	이 부속서는 심사시간의 계산에 대한 공식을 <u>개발하는</u> 부가적인 가이드라인을 제시한다. D.2에서는 심사시간 계산을 위해 기본적으로 사용될 수 있는 요인을 분류하는 사례를 제시하고, D.3에서는 심사시간 계산의 예시를 제공한다.	- 영문표현 변경에 따른 번역 수정 - 참조조항 변경
<신 설>	비고 이 부속서의 개념은 C.3.4에 기술된 바와 같이 특정 동일 활동을 수행하는 인원에 대한 모든 감축이 적용된 후에 시작한다.	
C.2 심사시간 계산을 위한 요인의 분류	D.2 심사시간 계산을 위한 요인의 분류	- 조항번호 변경
표 C.1에서는 B.3.4, a)에서 h)까지 나열된 심사시간 계산을 위한 주요요인의 분류사례를 제시한다. 이 분류는 인증기관이 9.1.4.1에 따라 심사시간 계산 방법을 이끌어 도출하는데 사용할 수 있다.	표 D.1에서는 C.3.5, a)에서 i)까지 나열된 심사시간 계산을 위한 주요요인의 분류사례를 제시한다. 이 분류는 인증기관이 9.1.4.2에 따라 심사시간 계산 방법을 이끌어 도출하는데 사용할 수 있다.	- 참조조항 변경
표 C.1 심사시간 계산 요인의 분류	표 D.1 심사시간 계산 요인의 분류	- 표 번호 변경
(표 생략)	(표 생략)	- 표의 현행/개정(안)은 [별표 2] 참조
C.3 심사시간 계산 예시	D.3 심사시간 계산 예시	- 조항번호 변경

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유																
다음 예시는 심사시간을 계산하기 위하여 B.3에 제공된 요인을 사용하는 사례를 보여준다. 아래 예시에서 심사시간 계산은 다음과 같이 사용된다.	다음 예시는 심사시간을 계산하기 위하여 C.3에 제공된 요인을 사용하는 사례를 보여준다. 아래 예시에서 심사시간 계산은 다음과 같이 사용된다.	- 참조조항 변경																
1단계 비즈니스와 조직과 관련된 요인 결정(IT 이외)	1단계 비즈니스와 조직과 관련된 요인 결정(IT 이외)																	
표 C.2에 제시된 각 항목에 대한 적절한 등급을 결정하고 그 결과를 합산한다.	표 D.2에 제시된 각 항목에 대한 적절한 등급을 결정하고 그 결과를 합산한다.	- 참조 표 번호 변경																
2단계 IT 환경 관련 요인의 결정	2단계 IT 환경 관련 요인의 결정																	
표 C.3의 각 항목에 적절한 등급을 결정하고, 그 결과를 합산한다.	표 D.3의 각 항목에 적절한 등급을 결정하고, 그 결과를 합산한다.	- 참조 표 번호 변경																
3단계 상기 1단계 및 2단계 결과를 근거로 표 C.4에서 적절한 항목을 선택하여 심사시간에 미치는 요인들의 영향을 식별한다	3단계 상기 1단계 및 2단계 결과를 근거로 표 D.4에서 적절한 항목을 선택하여 심사시간에 미치는 요인들의 영향을 식별한다	- 참조 표 번호 변경																
4단계 최종 결론	4단계 최종 결론																	
심사시간 차트(표 B.1)를 적용한 일수를 3단계의 요인들과 곱한다. 복수사업장 샘플링이 사용된 경우, 산출된 심사시간은 복수사업장 샘플링을 실행하기 위해 요구되는 노력에 근거하여 증가된다.	심사시간 차트(표 C.1)를 적용한 일수를 3단계의 요인들과 곱한다. 복수사업장 샘플링이 사용된 경우, 산출된 심사시간은 복수사업장 샘플링을 실행하기 위해 요구되는 노력에 근거하여 증가된다.	- 참조 표 번호 변경																
표 C.2 사업 및 조직 관련 요인 (IT 이외)	표 D.2 사업 및 조직 관련 요인 (IT 이외)	- 표 번호 변경																
<table><tr><th>항목</th><th>등급</th></tr><tr><td>비즈니스 유형 및 규제 요구 사항</td><td>(생략)</td></tr><tr><td>프로세스 및 과업</td><td>1. 표준 및 반복 작업, 동일한 과업을 수행하는 조직의 관리 하에서 일하는 다수의 개인, 적은 수의 제품 및 서비스에 대한 표준 프로세스 2. (생략) 3. (생략)</td></tr><tr><td>경영 시스템 구축 수준</td><td>(생략)</td></tr></table> <p>*핵심사업부문은 국가에 매우 부정적 영향을 미칠 수 있는 건강, 보안, 경제, 이미지, 정부의 능력에 리스크를 야기할 가능성이 있는 중요 공공서비스에 영향을 미치는 부문을 일컫</p>	항목	등급	비즈니스 유형 및 규제 요구 사항	(생략)	프로세스 및 과업	1. 표준 및 반복 작업, 동일한 과업을 수행하는 조직의 관리 하에서 일하는 다수의 개인, 적은 수의 제품 및 서비스에 대한 표준 프로세스 2. (생략) 3. (생략)	경영 시스템 구축 수준	(생략)	<table><tr><th>항목</th><th>등급</th></tr><tr><td>비즈니스 유형 및 규제 요구 사항</td><td>(생략)</td></tr><tr><td>프로세스 및 과업</td><td>1. 적은 수의 제품 또는 서비스에 대한 표준 프로세스 2. (생략) 3. (생략)</td></tr><tr><td>경영 시스템 구축 수준</td><td>(생략)</td></tr></table> <p>*핵심(critical)사업부문은 국가에 매우 부정적 영향을 미칠 수 있는 건강, 보안, 경제, 이미지, 정부의 능력에 리스크를 야기할 가능성이 있는 중요 공공서비스에 영향을 미치는 부문</p>	항목	등급	비즈니스 유형 및 규제 요구 사항	(생략)	프로세스 및 과업	1. 적은 수의 제품 또는 서비스에 대한 표준 프로세스 2. (생략) 3. (생략)	경영 시스템 구축 수준	(생략)	- 생략된 부분 현행과 같음 (표 전체 적용) - 반복 작업, 동일 과업 수행에 대한 내용 삭제
항목	등급																	
비즈니스 유형 및 규제 요구 사항	(생략)																	
프로세스 및 과업	1. 표준 및 반복 작업, 동일한 과업을 수행하는 조직의 관리 하에서 일하는 다수의 개인, 적은 수의 제품 및 서비스에 대한 표준 프로세스 2. (생략) 3. (생략)																	
경영 시스템 구축 수준	(생략)																	
항목	등급																	
비즈니스 유형 및 규제 요구 사항	(생략)																	
프로세스 및 과업	1. 적은 수의 제품 또는 서비스에 대한 표준 프로세스 2. (생략) 3. (생략)																	
경영 시스템 구축 수준	(생략)																	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
는다.	을 일컫는다.	
표 C.3 IT 환경 관련 요인들 (표 생략)	표 D.3 IT 환경 관련 요인들 (현행과 같음)	- 표 번호 변경
표 C.4 심사시간에 영향을 미치는 요인 (표 생략)	표 D.4 심사시간에 영향을 미치는 요인 (현행과 같음)	- 표 번호 변경
사례 1 심사대상 조직의 직원은 700명이므로, 표 B.1에 따르면 최초심사에 17.5일이 필요하다. 해당 조직은 <u>중요</u> 사업 부문에서 업무를 수행하지 않으며, 고도로 표준화되고 반복적인 업무를 수행하며, 최근 ISMS를 확립하였다. 표 C.2에 따르면 이는 1+3+1=5일의 비즈니스 및 조직 관련 요인을 생성한다. 조직 및 아웃소싱에서의 개발은 없다. 표 C.3에 의하면 이는 1+3+1=5 일의 IT 환경 관련 요인을 생성한다. 표 C.4에 따라 심사시간은 조정되지 않는다.	사례 1 심사대상 조직의 직원은 700명이므로, 표 C.1에 따르면 최초심사에 17.5일이 필요하다. 해당 조직은 <u>핵심(critical)</u> 사업 부문에서 업무를 수행하지 않으며, 고도로 표준화되고 반복적인 업무를 수행하며, 최근 ISMS를 확립하였다. 표 D.2에 따르면 이는 1+3+1=5일의 비즈니스 및 조직 관련 요인을 생성한다. 조직은 <u>아주 적은 수의 IT플랫폼 및 데이터베이스를 보유하고 있으며, 광범위하게 외주처리를 활용하고 있다. 소프트웨어 개발은 조직 내 또는 외주처리를 통해서도 이루어지지 않는다.</u> 표 D.3에 의하면 이는 1+3+1=5 일의 IT 환경 관련 요인을 생성한다. 표 D.4에 따라 심사시간은 조정되지 않는다.	- 참조 표 변경 - 번역 수정 - 참조 표 변경 - 의미 명확화 - 참조 표 변경 - 참조 표 변경
사례 2 앞 사례와 같은 조직이되, 다양한 경영시스템이 운영 중이며, ISMS가 잘 확립된 경우이다. 이 경우 표 C.2에 따른 계산을 1+1+1=3로 변경한다. 표 C.4에 의하면 심사시간이 5%에서 10% 감축되게 된다. 즉 심사시간이 1일에서 1.5일까지 줄어들어 총 16에서 16.5일이 된다.	사례 2 앞 사례와 같은 조직이되, 다양한 경영시스템이 운영 중이며, ISMS가 잘 확립된 경우, 표 D.2에 따른 계산을 1+1+1=3로 변경한다. 표 D.4에 의하면 심사시간이 5%에서 10% 감축되게 된다. 즉 심사시간이 1일에서 1.5일까지 줄어들어 총 16에서 16.5일이 된다.	- 자구수정 및 참조 표 변경
부속서 D (참고) ISO/IEC 27001:2013 부속서의 실행을 위한 검토지침	부속서 E (참고) ISO/IEC 27001:2022 부속서의 실행을 위한 검토지침	- 조항 번호 변경
D.1 목적 (적용성 보고서에 따라) ISMS 클라이언트에 의해 필수적으로 결정된 통제항목의 실행은 최초심사의 2단계심사 시 검토되어야 하며, 사후관리 또는 갱신심사 시에도 검토되어야 한다 (삭제) [9.3.1.2.2 g)참조].	E.1 목적 (적용성 보고서에 따라) ISMS 클라이언트에 의해 필수적으로 결정된 통제항목의 구현은 (신설) 9.3.2.2 f)의 요구사항에 따라 최초심사의 2단계심사 시 검토되어야 하며, 사후관리 또는 갱신심사 시에도 검토되어야 한다. (신설) 이는 통제항목이 구현되고 효과적인지, 통제항목이 기술된	- 조항 번호 변경 - 참조조항 명확화 - 목적 신설

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
	정보보안 목적에 부합하는지를 결정하는 것을 목적으로 한다.	
<p>인증기관에서 수집한 심사증거는 통제항목이 효과적인지에 대한 결론을 이끌어낼 수 있을 정도로 충분하여야 한다. 통제를 실행하기 위한 방법은, 예를 들어 클라이언트의 절차 또는 정책으로 규정되어야 한다.</p> <p><신 설></p>	<p><삭 제></p> <p>심사원이 조직을 방문하기 전까지 인증기관이 조직의 필요한 통제항목이 무엇인지를 아는 것, 또는 ISO/IEC 27001:2022 부속서 A와 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.</p>	- 내용 명확화
<신 설>	그럼에도 불구하고, 인증기관은 조직이 ISO/IEC 27001:2022 부속서에서의 통제항목과 조직이 필요로 하는 통제항목에 대한 비교를 요구해야 함을 인지하고, 조직의 필요한 통제항목과 ISO/IEC 27001:2022 부속서의 통제항목 간 관계가 존재함을 인지한다. 표 E.1에서 제공된 지침은 ISO/IEC 27001:2022 부속서에서의 통제항목과의 관계를 고려하여 클라이언트에 의해 결정된 필요한 통제항목을 다루는 심사계획을 개발할 때 인증기관을 지원하는 것을 목적으로 한다.	- 지침의 목적 명확화
D.1.1 심사증거	<삭 제>	- 심사증거 관련 내용 삭제
<p>우수한 품질의 심사증거는 심사원의 관찰 (예: 잠겨져 있어야 할 문이 잠겨져 있는지, 기밀 준수 서약서에 서약을 했는지, 자산등록이 존재하는지, 포함된 자산이 유지되는지, 수립된 시스템이 적절한지</p>	<삭 제>	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
등)로부터 수립된다. 증거는 통제(출력물)에 대한 접근 권리가 정확하게 공식적으로 부여된 자에게 주어짐, 사고 해결 기록, 프로세스가 정확하게 공식적으로 권한이 부여된 자에게 주어짐, 경영검토(또는 다른) 의사록 등). 증거는 심사원에 의한 통제항목에 대한 직접적인 시험(또는 재성과) 결과가 될 수 있다. 예를 들어, 통제항목에 의해 금지된 임무수행을 시도, 악성코드 예방을 위한 소프트웨어가 설치되고 기계가 최신화 되며, 승인된 접근권한(권한 검토 후) 등이 있다. 증거는 프로세스 및 통제항목에 대해 조직의 관리 하에 업무를 수행하는 개인과의 인터뷰를 통해 수집되며, 실제로 정확한지의 여부를 위해 수집된다.		
D.2 표D.1의 사용방법	E.2 표E.1의 사용방법	- 조항번호 및 제목 변경
D.2.1 일반사항	E.2.1 일반사항	- 조항번호 변경
표 D.1은 ISO/IEC 27001:2013 부속서 A에 나열된 항목들의 수행검토를 위한 안내와 최초심사 및 후속 심사를 수행하는 동안의 심사증거 수집에 대해 안내한다. <u>해당 표는 ISO/IEC 27001:2013 부속서 A에 나타난 사항 외의 통제검토는 안내하지 않는다.</u>	표 E.1은 필요한 통제항목들의 검토를 위한 예시 지침을 제공한다. 해당 표는 ISO/IEC 27001:2022 부속서 A에 나열된 항목들을 활용하지만, 심사원은 통제항목의 효과성을 입증하기 위한 심사증거 수집 시, 표 E.1에서 제공된 지침을 해석하는데 있어 표준에서의 통제항목들과 조직의 필요한 통제항목들 간의 관계를 활용하여야 할 것이다.	- 참조 표 변경 - 표 활용 방법의 명확화 - 삭제된 부분 비고로 이동
<신 설>	비고 표 E.1은 ISO/IEC 27001:2022 부속서 A에 나타난 사항과 관련 없는 통제검토는 안내하지 않는다.	- 현행의 첫 단락에서 이동
<신 설>	대부분의 통제항목들은 예를 들어, 클라이언트의 통제항목, 프로세스 또는 절차의 문서화에 대한 검토, 인터뷰 또는 관찰을 통하여 증거로 사용할 수 있는 조직의 측면을 포함한다.	- 증거 수집의 예시 명시
<신 설>	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.1은 “규칙”이라는 일반적인	

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
	용어를 클라이언트 조직의 경영자에 의해 설정된 이러한 요구사항이나 기대를 명시하기 위해 사용한다.	
<신 설>	많은 통제항목들이 예를 들어, 통제 활동의 결과에 대한 샘플을 검토하는 것을 통한 샘플링을 통해 시험될 수 있다.	
D.2.2 “조직의 통제” 및 “기술적 통제” 영역	<삭 제>	- 해당 내용이 개정(안) 표 E.1의 통제항목으로 삽입됨
“○”로 표기된 영역은 조직의 통제 또는 기술적 통제를 나타낸다. 이중 몇 통제항목은 조직적 및 기술적 통제항목 모두에 해당하며, 그러한 통제항목은 양쪽에 모두 기입된다.	<삭 제>	- 해당 내용이 개정(안) 표 E.1의 통제항목으로 삽입됨
조직의 통제항목의 성과는 통제항목, 인터뷰, 관찰 및 물리적 검사의 성과기록에 대한 검토를 통해 수집될 수 있다. 기술적 통제 성과의 증거는 시스템검사(아래참고) 또는 특정 심사/보고 기법의 사용을 통해 수집될 수 있다.	<삭 제>	- 해당 내용이 개정(안) 표 E.1의 통제항목으로 삽입됨
D.2.3 “시스템검사” 영역	E.2.2 “시스템시험” 영역	- 조항번호 변경 및 자구수정
“시스템검사”는 정보시스템에 대한 직접적인 검토 수립된 시스템에 대한 검토 또는 형상 검토를 의미한다. 심사원의 질문은 시스템 제어 장치 또는 시험기법 평가에 의해 응답될 수 있다. 만일 클라이언트가 컴퓨터를 기반으로 한 도구를 사용하고 있다면 심사원에게 이러한 사항을 알려야 하며, 이것은 클라이언트(또는 그들의 하청업체)에 의해 실행된 평가결과를 지원하는데 사용될 수 있다.	ISO/IEC 27001:2022 부속서 A의 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.	- 내용 명확화 - 시스템시험 → 시스템검사로 용어 변경
기술적 통제검토를 위한 두 개의 범주는 다음과 같다.	표 E.1의 “시스템시험” 영역은 기술적 통제검토를 위한 지침을 제공한다.	- 영문표현 변경에 따른 번역 수정
<신 설>	- 공란 : ISMS 심사에서 보통 적용이 불가능하거나 필요하지 않은 시스템시험	- 표 해석법 명확화

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
	을 의미	
- 가능 : 시스템검사 통제실행을 위한 평가에 적절하나 통상적으로 ISMS 심사에 필요한 것은 아님	- 가능 : 시스템시험 통제구현을 위한 평가에 보통 적절하나 통상적으로 ISMS 심사에 필요한 것은 아님	- 번역 수정
- 권고 : 시스템검사가 통상적으로 ISMS 심사에 필요함	- (현행과 같음)	
비고 다른 설명이 제시되지 않는 한 본 부속서에서 “시스템”은 “정보시스템”을 의미한다.	<삭 제>	- 비고 삭제
D.2.4 “육안검사” 영역	E.2.3 “육안검사” 영역	- 조항번호 변경
“육안검사”란 이러한 통제항목의 효과성 평가 시 통상적으로 해당 위치에서의 육안검사가 필요함을 의미한다. 즉 관련 문서에 대한 검토나 인터뷰만으로는 충분치 않음을 의미한다. 심사원은 통제가 실행되는 장소에서 검증해야 할 필요가 있다.	ISO/IEC 27001:2022 부속서 A의 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.	- 영문표현 변경에 따른 번역 수정 - 번역 수정
<신 설>	비고 현장에서의 육안검사는 또한 원격 검사 기술(예: 현장에서 인원이 실시간 비디오를 심사원에게 제공)을 활용하여 수행될 수도 있다.	- 표 해석 방법 명확화
<신 설>	표 E.1의 “육안검사” 영역은 통제항목의 물리적 증거를 검토하는 지침을 제공한다.	- 표 해석 방법 명확화
<신 설>	- 공란 : ISMS 심사에서 보통 적용이 불가능하거나 필요하지 않은 육안검사를 의미	- 표 해석 방법 명확화
<신 설>	- 가능 : 육안검사가 통제구현을 위한 평가에 보통 적절하나 통상적으로 ISMS 심사에 필요한 것은 아님	- 표 해석 방법 명확화
<신 설>	- 권고 : 육안검사가 통상적으로 ISMS 심사에 필요함	
D.2.5 “심사검토지침” 영역	<삭 제>	
<신 설>	E.2.4 통제항목의 설계 및 구현에 대한 가능한 증거	- 통제항목 설계 및 시행 관련 증거에 대한 지침 신설
“심사검토 지침” 영역은 심사원을 위한 추가 지침으로 통제 평가를 위한 중점	<삭 제>	- 통제항목 설계 및 시행 관련 증거에

현행(Issue No.2, 2020.12.03.)	개정(안) (Issue No.3, 2024.06.20.)	개정 사유
<p>분야를 제공한다.</p> <p><신 설></p>	<p>“통제항목의 설계 및 구현에 대한 가능한 증거” 영역은 심사원이 ISO/IEC 27001:202 8.3(리스크 처리 계획에 필요한 요구사항 및 그렇게 함으로써 필요한 통제항목)에 대한 적합성을 평가하도록 지원할 수 있는 증거에 대한 지침을 제공한다.</p> <p>이 영역의 많은 다양한 요점들은 요구사항이 아니며, 전체 목록을 구성하는 것도 아니다.</p> <p>ISO/IEC 27001:2022 부속서 A의 통제항목 문구에서 도출된 것으로 조직이 필요한 통제항목에 반드시 적합한 것은 아니다.</p> <p>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 A에서 제외된 모든 통제항목에 대한 정당성을 포함한다.</p>	<p>대한 지침 신설</p>
<u>표 D.1 통제항목의 분류</u>	<u>표 E.1 통제항목의 평가</u>	- 표 번호 및 제목 변경
(표 생략)	(표 생략)	- 표의 현행/개정(안)은 [별표 3] 참조

[별표 1]

현행(Issue No.2, 2020.12.03.)				개정(안) (Issue No.3, 2024.XX.XX.)			
표 A.1 ISMS 심사 및 인증을 위한 지식				표 A.1 ISMS 심사 및 인증을 위한 지식 및 스킬			
지식	인증업무기능			지식 및 스킬	인증업무기능		
	신청서 검토 수행 (요구되는 심사팀 적격성 결정, 심사팀 구성원 선정, 심사시간 결정을 위한 신청서 검토 수행)	심사 보고서 검토 및 인증결정	심사 및 심사팀 통솔		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		7.1.2.4.2	7.1.2.1.2	정보보안경영 용어, 원칙, 관행 및 기술		○ (7.1.3.3.2 참조)	○ (7.1.3.1.2 참조)
정 보 보 안 경 영 시 스 템 표준/참조문서	7.1.2.3.1	7.1.2.4.3	7.1.2.1.3	정 보 보 안 경 영 시 스 템 표준/참조문서			○ (7.1.3.1.3 참조)
비즈니스경영 관행			7.1.2.1.4	비즈니스경영 관행			○ (7.1.3.1.4 참조)
클라이언트의 비즈니스 분야	7.1.2.3.2	7.1.2.4.4	7.1.2.1.5	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	7.1.2.3.3	7.1.2.4.5	7.1.2.1.6	클라이언트의 제품, 프로세스 및 조직	○ (7.1.3.2.2 참조)	○ (7.1.3.3.4 참조)	○ (7.1.3.1.6 참조)

[별표 2]

현행(Issue No.2, 2020.12.03.)				개정(안) (Issue No.3, 2024.XX.XX.)			
표 C.1 심사시간 계산 요인의 분류				표 D.1 심사시간 계산 요인의 분류			
요인 (B.3.4 참조)	심사수행에 미치는 영향			요인 (C.3.5 참조)	심사수행에 미치는 영향		
	심사수행 감소	일반적인 심사수행	심사수행 증가		심사수행 감소	일반적인 심사수행	심사수행 증가
a) (생략)	(생략)	(생략)	<ul style="list-style-type: none">더 높은 규모의 민감 또는 기밀 정보(예: 건강, 개인 신원 정보, 보험, 은행) 또는 높은 가용성 요구사항다수의 중요 자산다수의 인터페이스 및 비즈니스 유닛이 포함된 두 개 이상의 복합적 절차	a) (생략)	(생략)	(생략)	<ul style="list-style-type: none">더 높은 규모의 민감 또는 기밀 정보(예: 건강, 개인 신원 정보, 보험, 은행) 또는 높은 가용성 요구사항다수의 중요 자산다수의 인터페이스 및 비즈니스 유닛이 포함된 세 개 이상의 복합적 절차
(생략)				(생략)			
g) (생략)	(생략)	(생략)	<ul style="list-style-type: none">요구사항 가용성이 높음(예: 24시간)다수의 대체 DR 사업장다수의 데이터 센터	g) (생략)	(생략)	(생략)	<ul style="list-style-type: none">요구사항 가용성이 높음(예: 24시간)다수의 DR 사업장다수의 데이터 센터
<신 설>							
h) 사후관리 및 갱신 짐사에 대해: KAB-R-MSCB, 8.5.3 따라 ISMS와 관련된 변경사항 규모와 범위	(생략)	(생략)	<ul style="list-style-type: none">ISMS 범주 또는 사후 관리에서의 주요 변화. 예를 들어, 새로운 프로세스, 새로운 비즈니스 단위, 지역, 리스크 평가 관리 방법, 정책, 문서, 리스크관리상기 언급된 사항에서의 주요 변화	h) 통제항목의 수 및 복잡성	<ul style="list-style-type: none">포함되지 않은 일부 공통 통제항목 영역을 포함하여, 통제항목의 수가 통상적인 것보다 적음	<ul style="list-style-type: none">통제항목의 대표적인 수와 복잡성	<ul style="list-style-type: none">자세하고 복잡한 통제항목의 수가 통상적인 것보다 많음. 예: 네트워킹 프로토콜 또는 암호 해독에 관련된 다수의 통제항목
				i) 사후관리 및 갱신 짐사에 대해: KAB-R-MSCB, 8.5.3 따라 ISMS와 관련된 변경사항 규모와 범위	(생략)	(생략)	<ul style="list-style-type: none">ISMS 범주 또는 사후 관리에서의 주요 변화. 예를 들어, 새로운 프로세스, 새로운 비즈니스 단위, 지역, 리스크 평가 관리 방법, 정책, 문서, 리스크 처리

				<ul style="list-style-type: none"> • 상기 언급된 사항에서의 주요 변화
--	--	--	--	--

[별표 3]

현행(Issue No.2, 2020.12.03.)								개정(안) (Issue No.3, 2024.XX.XX.)				
표 D.1 통제항목의 분류								표 E.1 통제항목의 평가				
ISO/IEC 27001:2013, 부속서A에서의 통제항목	조직 제	직 통 제	기 적 제	술 통	시스템 사	스 견	육안 검사	심사검토 지침	ISO/IEC 27001:2022, 부속서A ^a 에서의 통제항목	시스템 시험	육안 검사	통제항목의 설계 및 구현에 대한 가능한 증거
A.5 보안 방침									5 조직적 통제항목			
A.5.1 정보보안 관리 지침									5.1 정보보안 방침			- 정보보안 방침 - 조직에 의해 필요하다고 판단된 경우, 정보보안 특정 주제에 대한 방침 - 관련 인원 및 이해관계자에게 방침 배포
A.5.1.1 정보보안 방침	○								5.2 정보보안 역할 및 책임			- 정보보안의 실행, 운영 및 관리를 위하여 분배된 역할 및 책임
A.5.1.2 정보보안 방침 검토	○								5.3 의무의 구분			- 상충되는 의무 또는 책임을 식별하고 상충하는 분리 규칙 식별
A.6 정보보안 조직									5.4 경영책임			- 정보보안 목표, 방침, 절차 등에 대한 경영기술 및 지원 - 인원의 정보보안에 책임을 지는 개인에 대한 모니터링
A.6.1 내부 조직									5.5 권한에 대한 접근			- 관련 권한에 대한 규정된 연락망 - 사건 보고 규칙 - 관련 권한 간의 정보흐름의 내용
A.6.1.1 정보보안 역할 및 책임	○								5.6 특정 목적 집단과의 접촉			- 특정 목적 집단, 기타 포럼 또는 연합체에 대한 멤버십 또는 연락망 (예: 컴퓨터 비상사태 대응 팀(CERTs), 사이버보안 업체) - 이러한 조직 내에서 논의될 수 있는 사항에 대한 규칙 - 이러한 조직 간의 정보흐름의 내용
A.6.1.2 의무의 구분	○								5.7 위협 인텔리전스			- 관련된 위협 인텔리전스 수집에 대한 접근법 - 조직과 관련된 위협 인텔리전스 분석 및 분석 내용을 적절한 집단에 배포
A.6.1.3 권한에 대한 접근	○								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
A.6.1.4 특정 목적 집단과의 접촉	○								5.9 인벤토리 및 기타 관련 자산			- ISMS에 의해 보유되는 정보 및 기타 관련 자산의 인벤토리 - 인벤토리 목록 내에서 보유하고 있는 소유권
A.6.1.5 프로젝트 관리에서의 정보보안	○											
A.6.2 모바일 장치 및 재택근무												
A.6.2.1 모바일 장비 정책	○		○		가능			적용 가능한 방침의 이행을 점검				
A.6.2.2 재택근무	○		○		가능			적용 가능한 방침의 이행을 점검				
A.7 인적 자원 보안												
A.7.1 고용 전												
A.7.1.1 선발	○											
A.7.1.2 고용 기간 및 조건	○											
A.7.2 고용												
A.7.2.1 경영자 책임	○											
A.7.2.2 정보보안 인식, 교육, 훈련	○							직원의 정보보안 인식에 대한 질문				
A.7.2.3 훈련 프로세스	○											
A.7.3 고용 종료 및 변경												
A.7.3.1 고용 책임 종료 및 변경	○											

A.8 자산 관리					
A.8.1 자산에 대한 책임					
A.8.1.1 자산 목록	○				자산 식별
A.8.1.2 자산 소유권	○				
A.8.1.3 허용 가능한 자산 사용	○				
A.8.1.4 자산 반환	○				
A.8.2 정보 분류					
A.8.2.1 정보의 분류	○				적용 가능한 방침의 이행을 점검
A.8.2.2 정보의 표시	○				이름 붙이기: 디렉토리, 파일, 인쇄된 보고서, 기록 미디어 (예: 테이프, 디스크, CD), 전자 메시지 및 파일 이동
A.8.2.3 자산 처리	○				
A.8.3 미디어 처리					
A.8.3.1 제거 가능한 미디어 관리	○	○	가능		
A.8.3.2 미디어 제거	○			○	처분 프로세스
A.8.3.3 물리적 미디어 이동	○				처분 프로세스
A.9 접근 통제					
A.9.1 접근 통제를 위한 업무 요구사항					
A.9.1.1 접근 통제 정책	○				적용 가능한 방침의 이행을 점검
A.9.1.2 네트워크 및 네트워크 서비스 접근	○				적용 가능한 방침의 이행을 점검
A.9.2 사용자 접근 관리					
A.9.2.1 사용자 등록 및 등록 해제	○				
A.9.2.2 사용자 접근권한설정	○	○	가능		모든 시스템 접근 권한에 대한 조직의 관리 하에 업무를 수행하는 개인/ 계약자를 샘플링함
A.9.2.3 특권 관리	○	○	가능		직원의 내부 이동
A.9.2.4 사용자 비밀 인증 정보 관리	○				
A.9.2.5 사용자 접근권한 검토	○				

				- 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 식별된 정보 전환 및 그에 상응하는 규칙, 절차 또는 협약 유즈 케이스에 대한 정의 - 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

A.9.2.6 접근권한 제거 및 조정	○				
A.9.3 사용자 책임					
A.9.3.1 비밀 인증 정보 사용	○				등록된 사용자의 지 침/정책 검증
A.9.4 시스템 및 어플리케이션 접근 통제					
A.9.4.1 정보 접근 제한	○	○	권고		
A.9.4.2 보안 로그인 절차	○	○	권고		
A.9.4.3 패스워드 경영시스템	○	○	권고		
A.9.4.4 특권 유틸리티 사용	○	○	권고		
A.9.4.5 프로그램 보안 코드 접근 통제	○	○	권고		
A.10 암호 해독					
A.10.1 암호 해독 통제					
A.10.1.1 암호 해독 통제 사용 정책	○				적용 가능한 방침의 이행을 점검
A.10.1.2 키 관리	○	○	권고		적용 가능한 방침의 이행을 점검
A.11 물리적, 환경적 보안					
A.11.1 보안 영역					
A.11.1.1 물리적 보안 경계	○				
A.11.1.2 물리적 출입 통제	○	○	가능	○	접근 기록의 보관소
A.11.1.3 보호되는 사무실, 방 및 시설	○			○	
A.11.1.4 외부 및 환경적 리스크에 대한 보호	○			○	
A.11.1.5 안전 구역에서의 업무	○			○	
A.11.1.6 이주 및 정착 지역	○			○	
A.11.2 장비					
A.11.2.1 장비 계획 및 보호	○			○	
A.11.2.2 유틸리티 지원	○	○	가능	○	
A.11.2.3 케이블링 보안	○			○	
A.11.2.4 장비 유지	○				
A.11.2.5 자산의 폐기	○				접근 기록의 보관소
A.11.2.6 장비의 안전 및 오프 장비 보안	○	○	가능		이동 장치 암호화
A.11.2.7 장비의 안전한 처분 또는	○	○	가능	○	디스크 삭제, 디스크

			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 정보 및 커뮤니케이션 기술 공급망 관리			- CT 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 클라우드 서비스 사용 관련 방침에서) 클라우드 서비스에서의 정보보안 리스크 관리 규칙 - 조직에서 사용하는 클라우드 서비스의 목록 - 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			- 정보보안사고를 다루기 위한 프로세스,

재사용					암호화
A.11.2.8 보호되지 않은 사용자 장비	○				등록된 사용자의 지침/정책 검증
A.11.2.9 데스크 및 스크린 정비 방침	○			○	적용 가능한 방침의 이행을 점검
A.12 운영 보안					
A.12.1 운영 과정 및 책임					
A.12.1.1 문서화된 운영 과정	○				
A.12.1.2 관리 변경	○	○	권고		
A.12.1.3 자격 관리	○	○	가능		
A.12.1.4 개발, 테스트, 운영 시설의 분리	○	○	가능		
A.12.2 악성코드에 대한 보호					
A.12.2.1 악성코드에 대한 통제	○	○	권고		악성코드 통제 소프트웨어의 설치 및 완전성
A.12.3 백업					
A.12.3.1 정보 백업	○	○	권고		검토 정책, 복구 테스트
A.12.4 로깅 및 모니터링					
A.12.4.1 이벤트 로깅	○	○	가능		로그 이벤트의 리스크 기반 선택
A.12.4.2 로그 정보의 보호	○	○	가능		
A.12.4.3 관리자 및 운영자 로그	○	○	가능		
A.12.4.4 시간 동기화		○	가능		
A.12.5 운영 소프트웨어 통제					
A.12.5.1 운영 시스템 소프트웨어 설치	○	○	가능		
A.12.6 기술적 취약성 관리					
A.12.6.1 기술적 취약성 관리	○	○	권고		리스크 기반 패치 관리 및 운영 시스템, 데이터베이스, 어플리케이션 강화
A.12.6.2 소프트웨어 설치 제한	○	○	가능		
A.12.7 정보시스템 심사 고려사항					
A.12.7. 정보시스템 심사 통제	○				
A.13 커뮤니케이션 보안					
A.13.1 네트워크 보안 관리					

및 대비					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, 통관리 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)을 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 영향

A.13.1.1 네트워크 통제	○	○	가능		네트워크 관리			을 미칠 수 있는, 조직이 사업을 수행하는 또는 제품 및 서비스를 사용하는 관련 국가의 목록
A.13.1.2 네트워크 서비스 보안	○	○	권고		SLA, 네트워크 서비스의 정보보안 제공 (예: 네트워크 라우팅 및 연결 조정, 네트워크 장치 설정)			- 개인 정보의 프라이버시 및 보호에 대한 법적, 규제적 또는 계약 요구사항을 포함하여 식별된 외부 요구사항
A.13.1.3 네트워크 분리	○	○	가능		네트워크 다이어그램, 네트워크 구획 (예: DMZ) 및 분리 (예: VLAN)			- 적절한 기술적 및 조직적 조치를 통해 요구사항이 충족됨을 보여주는 개인 정보를 다루는 데 책임이 있는 집단이 수행한 분석
A.13.2 정보 이전								
A.13.2.1 정보 이전 정책 및 절차	○				적용 가능한 방침의 이행을 점검			- 정보보안의 독립적 검토 수행 계획
A.13.2.2 정보 이전 협의	○							- 독립적 검토 결과(샘플)를 최고 경영자에게 보고
A.13.2.3 전자 메시징	○	○	가능		샘플링된 메시지 확인방침 및 절차 확인			- 조직의 정보보안 관리 접근법이 부적절하다고 발견된 경우에 취해진 시정조치
A.13.2.4 기밀 또는 유출 방지 협약	○				계약검토			- 이러한 검토(샘플)의 결과 및 취해진 시정조치
A.14 시스템 획득, 개발 및 유지								- 정보보안과 관련된, 정보처리 시설에 대한 운영 절차
A.14.1 보안 요구사항 및 정보시스템								
A.14.1.1 정보보안 요구사항 분석 및 명세화	○							
A.14.1.2 공동 네트워크에서의 어플리케이션 서비스 보안	○	○	권고		어플리케이션 서비스의 리스크 기반 디자인			- 정보보안 정책, 특정 주제에 대한 방침, 규칙 및 표준에 대한 조직의 준수를 검토하는 계획
A.14.1.3 어플리케이션 서비스 이동 보안	○	○	권고		기밀성, 통합성, 부인 방지			- 이러한 검토(샘플)의 결과 및 취해진 시정조치
A.14.2 개발 및 지원 프로세스 보안								
A.14.2.1 보안 개발 정책	○				적용 가능한 방침의 이행을 점검			- 정보보안과 관련된, 정보처리 시설에 대한 운영 절차
A.14.2.2 시스템 변화 통제 절차	○	○	권고					
A.14.2.3 운영 플랫폼 변경 이후 어플리케이션의 기술적 검토	○							
A.14.2.4 소프트웨어 패키지 변경 제한	○							
A.14.2.5 보안 시스템 엔지니어링 원리	○							
A.14.2.6 보안 개발 환경	○	○	가능					

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

A.14.2.7 개발 아웃소싱	○				
A.14.2.8 시스템 보안 테스트	○				
A.14.2.9 시스템 수용 테스트	○	○	가능		
A.14.3 테스트 데이터					
A.14.3.1 테스트 데이터 보호	○	○	가능	○	
A.15 공급자 관계					
A.15.1 공급자 관계 정보보안					
A.15.1.1 공급자 관계 정보보안 정책	○			적용 가능한 방침의 이행을 점검	
A.15.1.2 공급자와 협약 시 보안 언급	○			일부 계약 조건에 대해 시험	
A.15.1.3 정보 및 커뮤니케이션 공급망	○			일부 계약 조건에 대해 시험	
A.15.2 공급자 서비스 전달 관리					
A.15.2.1 공급자 서비스 모니터링 및 검토	○				
A.15.2.2 공급자 서비스 변경 관리	○				
A.16 정보보안사고 관리					
A.16.1 정보보안사고 및 개선 관리					
A.16.1.1 책임 및 절차	○				
A.16.1.2 정보보안 이벤트 보고	○				
A.16.1.3 정보보안 약점 보고	○				
A.16.1.4 정보보안 이벤트에 대한 평가 및 결정	○				
A.16.1.5 정보보안사고에 대한 반응	○				
A.16.1.6 정보보안사고에 대한 시사점	○				
A.16.1.7 증거 수집	○				
A.17 비즈니스연속성 관리의 정보보안 측면					
A.17.1 정보보안 지속성				경영자 검토 회의록	
A.17.1.1 정보보안 지속성 계획	○				
A.17.1.2 정보보안 지속성 수행	○				
A.17.1.3 정보보안 지속성 검증, 검토 및 평가	○				
A.17.2 중복사항					

의 책임			효한 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 - 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 대

A.17.2.1 정보 프로세싱 설비 이용 가능성	○	○	가능					한 불시(임의) 점검
A.18 준수성								7.8 장비위치 및 보호
A.18.1 법적 요구사항에 대한 준거								가능 - 장비 위치 및 보호에 대한 규칙 - 장비 위치 및 보호에 대한 불시(임의) 점검
A.18.1.1 적용가능한 법적 및 계약상 요구사항 식별	○		권고					7.9 사업장 외 자산의 보안
A.18.1.2 지적재산권	○							- 조직 사업장 밖 자산 활용에 대한 규칙 (예: “개인 기기 지참” 가이드라인) - 조직 사업장 밖 자산을 활용하는 인원에게 수행한 인터뷰 또는 설문조사 결과
A.18.1.3 기록물 보호	○	○	권고					7.10 저장 매체
A.18.1.4 개인 정보의 프라이버시 및 보호	○					적용 가능한 방침의 이행을 점검		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
A.18.1.5 암호화 통제 규제사항	○							7.11 보조 유틸리티
A.18.2 정보보안 검토								권고 - 특히, 데이터 센터에서, 설치된 유틸리티 보호 조치(예: 온도, 전기 공급, 물) - 전기, 물, 가스 또는 기타 유틸리티를 차단하는 비상사태 조항
A.18.2.1 정보보안의 독립적 검토	○					보고서 참조		7.12 케이블류 보안
A.18.2.2 보안 정책 및 표준의 준거	○							가능 - 케이블류의 물리적 라우팅 및 보호
A.18.2.3 기술적 준거 검토	○	○						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 - 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 모니터링에 대한 규칙 - 특권 관리를 위한 승인 및 검토 프로세스
								8.3 정보 접근 제한
								권고 - (예를 들어, 특정 주제에 대한 방침에서)

			<p>정보 및 기타 관련 재산에 대한 접근 제한 규칙</p> <ul style="list-style-type: none"> - 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		<ul style="list-style-type: none"> - 소스코드, 개발도구 및 소프트웨어 라이브러리에 대한 읽기 및 쓰기 접근(엑세스) 관리 절차
8.5 보안 인증	권고		<ul style="list-style-type: none"> - (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		<ul style="list-style-type: none"> - 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		<ul style="list-style-type: none"> - 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		<ul style="list-style-type: none"> - 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 애플리케이션 업데이트의 설치 보장
8.9 형상 관리	권고		<ul style="list-style-type: none"> - 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			<ul style="list-style-type: none"> - (예를 들어, 특정 주제와 관련된 데이터 보존 방침에 따라) 정보 시스템, 기기 또는

			<p>기타 저장 수단에 저장된 정보의 시기적절한 삭제에 대한 규칙</p> <ul style="list-style-type: none"> - 시스템, 어플리케이션 및 서비스 상의 민감 정보를 안전하게 삭제하는 절차 - 제 3자가 조직의 정보를 저장하는 경우, 정보 삭제에 대한 조항을 포함한 제 3자 계약
8.11 데이터 마스킹			<ul style="list-style-type: none"> - (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		<ul style="list-style-type: none"> - 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		<ul style="list-style-type: none"> - (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			<ul style="list-style-type: none"> - 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		<ul style="list-style-type: none"> - (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		<ul style="list-style-type: none"> - 이상행위에 대한 네트워크, 시스템 및 어플리케이션(응용 프로그램) 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 클럭 동기화	가능		<ul style="list-style-type: none"> - 조직이 사용하는 기준 시간 출처의 목록 - 클럭 동기화 방법 및 시차 처리
	8.18 특권을 가진 유틸리티 프로그램의 사용	가능		<ul style="list-style-type: none"> - 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		<ul style="list-style-type: none"> - 버전과 함께, 설치된 소프트웨어 인벤토리를 포함하여 운영 시스템 상의 소프트웨어 설치를 관리하는데 사용되는 절차 및 조치 - 사용자가 설치할 수 있는 소프트웨어 종류에 대한 규칙 - 교육을 받은 관리자 이외의 인원이 소프트웨어를 설치하기 위한 제한사항
	8.20 네트워크 보안	권고		<ul style="list-style-type: none"> - 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			<ul style="list-style-type: none"> - 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			<ul style="list-style-type: none"> - 네트워크 도메인 분리에 관한 규칙(예 : 신뢰수준, 중요도 및 민감도)과 액세스 제어에 대한 특정 주제별 정책에 따른 규칙

				<ul style="list-style-type: none"> - 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		<ul style="list-style-type: none"> - 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		<ul style="list-style-type: none"> - (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		<ul style="list-style-type: none"> - 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			<ul style="list-style-type: none"> - 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
	8.27 보안 시스템 구성 및 공학 원칙			<ul style="list-style-type: none"> - 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

				<ul style="list-style-type: none"> - 적용 가능한 경우, 외주처리된 개발에 대한 계약서 상에 삽입된 안전한 공학 원칙
8.28 보안 코딩	가능			<ul style="list-style-type: none"> - 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			<ul style="list-style-type: none"> - 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				<ul style="list-style-type: none"> - 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			<ul style="list-style-type: none"> - 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: 민감한 생산 정보가 활용되지 않음을 보장하면서, 접근 제한, 네트워크 분리)
8.32 변경 관리	권고			<ul style="list-style-type: none"> - 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			<ul style="list-style-type: none"> - 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.			