

ISO 42001

컴플라이언스체크리 스트



목차

소개	03	부록 A 통제 (확장)	
조항 4 – 조직의 상황	04	A.2 – AI 관련 정책	11
조항 5 – 리더십	05	A.3 – 내부 조직	12
조항 6 – 계획	06	A.4 – AI 시스템을 위한 자원	13
조항 7 – 지원	07	A.5 – AI 시스템의 영향 평가	14
조항 8 – 운영	08	A.6 – AI 시스템 수명 주기	15
조항 9 – 성과 평가	09	A.7 – AI 시스템을 위한 데이터	16
조항 10 – 개선	10	A.8 – 이해관계자를 위한 정보	17
		A.9 – AI 시스템 사용	18
		A.10 – 제3자 및 고객 관계	19
		LRQA의 ISO 42001 서비스	20
		왜 LRQA와 함께 해야할까요?	21

LRQA의 체크리스트를 통해 인증 준비 상태를 사전 점검해보세요



이 ISO 42001 컴플라이언스 체크리스트는 귀사의 경영시스템(AIMS)을 평가하고 인증 또는 전환 심사 전에 주의가 필요한 영역을 식별하는 데 도움이 되는 귀중한 툴입니다. ISO 42001의 핵심 조항을 중심으로 구성된 이 체크리스트는 귀사의 AIMS가 표준 요구사항 및 주요 AI 거버넌스 원칙에 부합하는지 평가하는 데 도움이 됩니다. 다음을 다룹니다:

- 조직의 상황
- 리더십과 거버넌스
- 위험 식별 및 영향 평가
- 운영 및 데이터 관리 통제
- 수명 주기, 투명성 및 제3자 관계

이 체크리스트를 통해 각 요구사항을 검토하고 직접 답변함으로써, 귀사의 현재 상황을 보다 체계적으로 점검할 수 있습니다.

조항 4 - 조직의 상황

조직의 목적, 내부 및 외부 환경, 이해관계자의 기대사항을 명확히 이해하는 것은 효과적인 AIMS을 구축하는 데 있어 핵심적인 단계입니다. 이는 AI 시스템의 범위, 목표, 거버넌스를 설정하는 기반이 됩니다.

- ☐ 귀사의 AI 시스템과 관련된 내부 및 외부 이슈를 식별하셨나요?
- ☐ 이해관계자의 요구와 기대를 파악하셨나요?
- ☐ AIMS의 범위가 명확하게 정의되어 있나요?
- ☐ 귀사의 AIMS는 수립되고, 실행되며, 유지되고, 지속적으로 개선되고 있나요?

의견

조항 5 – 리더십

리더십은 AI 경영시스템의 구축과 운영에 있어 매우 중요한 역할을 합니다. 최고 경영진은 조직의 전략적 방향성과 AIMS를 일치시키고, 이에 대한 명확한 책임을 부여하며 강한 의지를 보여야 합니다.

- ☐
- 최고 경영진이 AIMS에 대한 리더십과 의지를 충분히 보여주었나요?
- ☐
- 조직의 전략적 방향성과 일치하는 AI 정책이 수립되어 있나요?
- ☐
- AI 관리에 대한 역할, 책임, 권한이 명확히 지정되고 구성원들에게 전달되었나요?

의견

조항 6 – 계획

효과적인 계획 수립은 AI 관련 리스크와 기회를 사전에 관리하는 데 핵심적인 역할을 합니다. 여기에는 ISO 42001 요구사항을 충족하기 위한 목표 설정과 실행 방안 수립이 포함됩니다.

☐

AI 관련 리스크와 기회를 해결하기 위한 조치가 수립되어 있나요?

☐

AI 리스크 평가 및 처리 절차가 마련되어 있나요?

☐

AI 시스템에 대한 영향 평가가 수행되고 있나요?

☐

AI 리스크 평가는 AI 정책 및 목표와 일치되어 있나요?

☐

적절한 리스크 처리 방법이 선택되었나요?

☐

AI 관련 목표가 설정되어 있으며, 이를 달성하기 위한 계획이 마련되어 있나요?

의견

조항 7 – 지원

지원 항목은 AIMS를 운영하고 지속적으로 개선하는 데 필요한 자원, 역량,커뮤니케이션 및 문서화를 포함합니다. 팀이 충분한 정보를 갖추고, 적절한 도구와 지원을 받는 것은 일관된 실행을 위해 필수적입니다.

- ☐ AIMS 운영에 필요한 자원이 제공되고 있나요?
- ☐ 교육, 훈련 또는 경력을 기반으로 한 인력의 역량을 확보하기 위한 절차가 마련되어 있나요?
- ☐ 조직의 관리 하에 업무를 수행하는 담당자가 AI 정책과 관련 절차를 인지하고 있나요?
- ☐ 내부 및 외부 커뮤니케이션 방식이 정의되어 있고 실행되고 있나요?
- ☐ AIMS 및 ISO 42001에서 요구하는 문서화된 정보가 적절히 관리되고 있나요?

의견

조항 8 - 운영

운영 계획은 AI 시스템이 정의된 프로세스에 따라 개발되고 활용되도록 보장하는 역할을 합니다. 여기에는 변화 관리, 영향 평가, 그리고 시스템 전체 생애 주기에 걸친 리스크 대응 조치가 포함됩니다.

- ☐ AI 시스템 운영에 필요한 프로세스가 계획되고, 실행되며, 통제되고 있나요?
- ☐ AI 리스크 평가 및 대응 조치가 운영 프로세스에 통합되어 있나요?
- ☐ AI 시스템 영향 평가가 필요에 따라 지속적으로 유지되고 업데이트되고 있나요?

의견

조항 9 – 성과 평가

AIMS의 성과를 평가하는 것은 프로세스가 효과적으로 운영되고 있으며 원하는 결과가 달성되고 있는지를 확인하는 데 도움이 됩니다. 내부 감사와 경영 검토는 지속적인 개선을 추진하는 데 필수적인 도구입니다.

☐

AIMS에 대한 모니터링, 측정, 분석 및 평가가 수행되고 있나요?

☐

내부 감사가 계획된 주기에 따라 수행되고 있나요?

☐

경영진이 조직의 AIMS를 정기적으로 검토하고 있나요?

의견

조항 10 – 개선

부적합이나 사고는 언제든지 발생할 수 있습니다. 중요한 것은 조직이 이를 어떻게 식별하고, 시정하며, 이를 통해 실질적인 조치를 취하는가에 달려있습니다. 견고한 개선 프로세스는 AIMS의 지속적인 신뢰성과 효과성을 보장합니다.

☐

개선 기회를 식별하고 이를 실제로 이행하고 있습니까?

☐

부적합 사항 및 시정조치가 효과적으로 관리되고 있습니까?

의견

Annex A 통제 (확장)

A.2 – AI 관련 정책

조직이 책임 있는 AI 활용을 실현하려면, AI 시스템의 개발, 도입, 운영을 안내하는 명확한 정책을 수립해야 합니다.이 정책은 조직의 비즈니스 목표, 리스크 수용 범위, 법적 의무에 부합해야 하며, 정기적으로 검토 및 갱신되어야 합니다.

☐

공식적인 AI 정책이 문서화되어 있으며, 최고 경영진의 승인을 받았습니까?

☐

정책에는 책임 있는 AI 활용 원칙과 지속적 개선 방안이 포함되어 있습니까?

☐

해당 정책이 정기적으로 검토되어, 적합성과 효과성이 유지되고 있습니까?

☐

AI 정책이 조직의 다른 관련 정책들과 연계되어 있습니까?

의견

A.3 – 내부 조직

AI 경영시스템 전반에 걸쳐 책임성과 명확한 소통을 확보하려면, 조직은 AI 시스템의 전 생애주기에서 책임 있는 활용을 지원할 수 있도록 역할, 책임, 그리고 이슈 보고 및 대응 절차를 명확히 정의하고 구성원들에게 효과적으로 전달해야 합니다.

- ☐ AI 시스템과 관련된 역할과 책임이 명확히 정의되고 할당되어 있습니까?
- ☐ AI의 개발 또는 활용과 관련된 우려 사항을 보고할 수 있는 절차가 마련되어 있습니까?
- ☐ 우려 사항은 비밀리에 보고할 수 있으며, 보복으로부터 보호받을 수 있습니까?
- ☐ 보고 메커니즘에는 적절한 조사 및 해결 절차가 포함되어 있습니까?

의견

A.4 – AI 시스템을 위한 자원

AI 시스템을 효과적으로 운영하고 리스크를 관리하려면, 이를 지원하는 모든 자원에 대한 명확한 이해가 필요합니다. 여기에는 기술 인프라, 데이터 세트, 도구, 인적 역량 등 시스템 생애주기의 각 단계에 필요한 요소들이 포함됩니다.

- ☐ 데이터, 도구, 시스템 및 인력을 포함한 모든 AI 관련 자원의 등록부가 생성되었습니다
- ☐ 도구 및 컴퓨팅 자원이 문서화되고 시스템 요구사항과 일치합니다
- ☐ AI 개발 및 감독에 관련된 인적 자원의 능력과 역량이 평가되고 기록됩니다
- ☐ 해당되는 경우 인프라의 환경적 또는 운영적 영향이 고려됩니다

의견

A.5 – AI 시스템의 영향 평가

조직은 AI 시스템이 개인 및 사회에 미칠 수 있는 잠재적 영향을 평가하고 문서화해야 합니다. 이러한 평가는 시스템 생애주기 전반의 주요 단계에서 수행되어야 하며, 설계 및 리스크 대응 결정에 반영되어야 합니다.

- ☐ AI 시스템이 개인, 집단 또는 사회에 미치는 영향을 평가하기 위한 영향 평가가 수행되고 있습니까?
- ☐ 영향 평가를 수행하는 절차가 문서화되어 있으며 반복 가능합니까?
- ☐ 시스템에 중대한 변경이 발생했거나 계획된 주기가 도래했을 때, 영향 평가가 갱신되고 있습니까?
- ☐ 평가 결과가 시스템 설계, 통제 방안 수립 및 이해관계자 커뮤니케이션에 반영되고 있습니까?

의견

A.6 – AI 시스템 수명 주기

AI 시스템은 설계부터 폐기까지 전 생애주기에 걸쳐 명확하게 정의된 요구사항, 명세, 검증 및 모니터링 절차에 의해 관리되어야 합니다. 이는 시스템의 신뢰성과 의도된 사용 목적과의 정합성을 지속적으로 확보하는 데 도움이 됩니다.

☐

책임 있는 개발을 위한 목표가 정의되고 문서화되어 있습니까?

☐

검증 및 확인 절차가 조직의 목표와 연계되어 명시되어 있습니까?

☐

사용자, 파트너, 규제기관을 위한 기술 문서가 준비되어 있습니까?

☐

시스템 사용 중 발생하는 이벤트 로그가 기록되고 유지되고 있습니까?

의견

A.7 – AI 시스템을 위한 데이터

AI 시스템의 안전성과 효과를 보장하려면, 고품질의 윤리적으로 수집된 데이터가 필요하며, 이 데이터는 적절하게 문서화되어야 합니다. 조직은 AI 생애주기의 모든 단계에서 데이터를 선택·준비·평가하기 위한 기준을 명확히 정의해야 합니다.

- ☐ AI 개발을 위한 데이터 관리 프로세스가 문서화되어 있습니까?
- ☐ 데이터 출처가 명확히 식별되며, 그 출처 및 의도된 사용 목적이 기록되어 있습니까?
- ☐ 데이터 품질에 대한 요구사항이 정의되어 있고, 정기적으로 검토되고 있습니까?
- ☐ 데이터 전처리 방법이 문서화되어 있으며, 그 근거가 명확히 제시되어 있습니까?

의견

A.8 – 이해관계자를 위한 정보

AI 시스템 사용자와 규제기관을 포함한 이해관계자들이 시스템을 이해하고, 활용하며, 평가할 수 있도록 필요한 정보가 제공되어야 합니다. 이는 투명성, 책임성, 신뢰 구축에 기여합니다.

- ☐ 사용자 및 기타 이해관계자에게 필요한 시스템 문서가 제공되고 있습니까?
- ☐ AI 관련 사고를 보고하고 상신할 수 있는 절차가 마련되어 있습니까?
- ☐ 사고 발생 시 커뮤니케이션 계획이 문서화되어 있으며, 정기적으로 검토되고 있습니까?
- ☐ 이해관계자에게 정보를 제공해야 하는 요건이 정의되어 있고, 이를 준수하고 있습니까?

의견

A.9 – AI 시스템 사용

조직은 AI 시스템이 자사의 정책, 목표 및 윤리적 약속에 부합하는 방식으로 사용되도록 관리해야 합니다. 이를 위해 사용 범위, 책임, 기대되는 결과를 명확히 정의해야 합니다.

☐

AI 시스템의 책임 있는 사용을 위한 절차가 정의되어 있습니까?

☐

윤리적이고 적절한 사용을 보장하기 위한 목표가 수립되어 있습니까?

☐

시스템 사용이 의도된 목적 및 문서화된 절차와 일치합니까?

☐

오용 또는 의도하지 않은 결과가 모니터링되고, 필요한 대응이 이루어지고 있습니까?

의견

A.10 – 제3자 및 고객 관계

AI 시스템 생애주기의 어느 단계에서든 제 3자 기관이 참여하는 경우, 지속적인 책임성과 준수를 보장하기 위해 명확한 역할 정의, 공동 책임, 기대치의 연계가 필요합니다.

- ☐ AI 생애주기 전반에 걸친 외부 기관의 책임이 명확히 정의되어 있습니까?
- ☐ AI 시스템에 관여하는 공급업체를 선정하고 관리하는 절차가 마련되어 있습니까?
- ☐ 고객의 기대사항이 시스템 설계 및 운영에 반영되고 있습니까?
- ☐ 제 3자 기관의 역할이 시스템 거버넌스의 일환으로 정기적으로 검토되고 있습니까?

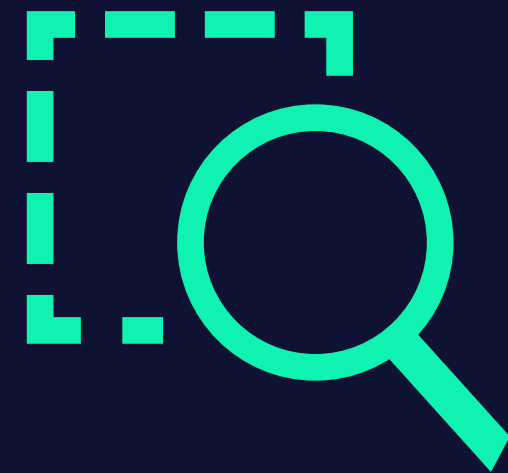
의견

컴플라이언스 ISO 42001 서비스



교육

ISO 42001에 대한 이해를 높이세요. 다양한 경험 수준을 고려한 맞춤형 교육 과정이 준비되어 있으며, 여러 학습 방식으로 제공됩니다.



차이점 분석

인증 전, 당사의 숙련된 심사원이 귀사의 시스템 내 치명적이거나 고위험 또는 취약한 영역을 사전에 식별할 수 있도록 도와드립니다.



인증

ISO 42001 요구사항에 따라 귀사의 AIMS를 평가하며, 특히 Annex A의 통제 항목과 그 영향에 중점을 둡니다.



통합 심사

여러 경영시스템을 함께 운영 중이라면, 통합 심사 및 사후관리 프로그램을 통해 보다 효율적이고 비용 효과적으로 리스크를 관리할 수 있습니다.

왜 LRQA와 함께해야 할까요?

LRQA는 조직이 안전하고 책임감 있으며 효과적으로 AI 및 기술을 도입할 수 있도록 견고하고 미래지향적인 리스크 관리 프로그램을 구축하는데 도움을 드립니다. AI 관련 규제 준수는 물론, 데이터 보안 강화, 거버넌스 모범 사례 내재화까지 신뢰 기반의 혁신을 가능하게 하는 종합적인 보증 서비스를 제공합니다. 기업이 리스크를 사전에 관리하면서 AI와 기술을 조직에 성공적으로 통합할 수 있도록 지원합니다.

현장 전문성

당사의 솔루션은 전 세계의 사이버 보안, 컴플라이언스, 공급망 리스크 관리 분야 전문가들에 의해 제공됩니다. 고객이 AI 관련 리스크를 식별하고, 변화하는 규제 요건을 충족하며, 책임 있는 AI 운영 체계를 조직 내에 통합할 수 있도록 현장에서 직접 지원합니다.

지속적인 보증

AI는 실시간 대응이 필요한 지속적인 리스크 관리가 필수입니다. 당사의 실시간 리스크 대응 접근 방식을 통해 사전적인 이슈 해결을 가능하게 하며, 업무 중단을 최소화하고 조직의 회복탄력성을 강화합니다. 또한, 서로 연결된 리스크 관리 솔루션 포트폴리오를 통해 단순한 규제 준수를 넘어, AI 리스크 관리가 일상 운영에 내재화될 수 있도록 돕습니다.

솔루션 기반 파트너십

LRQA는 단순히 인증만 제공하지 않습니다. 조직의 리스크 및 컴플라이언스 전략에 AI 거버넌스를 효과적으로 통합할 수 있도록 함께합니다. 맞춤형 접근을 통해, AI와 기술이 법적·윤리적 기대에 부응하면서도 지속 가능한 성장을 이끌 수 있도록 지원합니다.

데이터 기반 의사결정

LRQA는 디지털 플랫폼과 분석 도구를 활용해 조직 전반의 AI 리스크에 대한 인사이트를 제공합니다. 데이터 기반 도구로 강화된 전문가의 통찰력은 기업이 취약점을 식별하고, 미래 리스크를 예측하며, 신뢰를 바탕으로 의사결정을 내릴 수 있도록 돕습니다.



LRQA 소개

LRQA는 평가, 어드바이저리, 검사, 사이버 보안 분야에서 수십 년간 축적한 전문성을 바탕으로글로벌 선도 보증 파트너로 자리매김하고 있습니다.데이터 기반 인사이트를 바탕으로 한 솔루션 중심의 파트너십을 통해 고객이 직면한 가장 중요한 비즈니스 과제를 해결할 수 있도록 지원합니다. 150개 이상의 국가에서 5,000명 이상의 전문가가 활동 중이며, LRQA의 수상 경력이 있는 컴플라이언스,공급망, 사이버 보안, ESG 전문가는 사실상 모든 산업 분야에 걸쳐 61,000개 이상의 고객이 리스크를 예측하고, 완화하고, 효과적으로 관리할 수 있도록 돕고 있습니다. LRQA는 모든 활동에서 우리 직원, 고객, 지역사회, 그리고 지구를 위한더 나은 미래를 만들어가는 데 최선을 다하고 있습니다.

문의

더 자세한 정보는홈페이지 lrqa.com/ko-kr 를 방문하거나, 전화(+82 2 736 6231)로 문의주시기 바랍니다.



LRQA Korea
04637)서울특별시
중구 소월로 2길 30
T타워 2층