사이버 보안

ISO/IEC 27001:2022

체크리스트

LRQA

LRQA 체크리스트를 활용하면 인증을 위한 심사 준비를 얼마나 철저히 했는지 사전에 파악해 볼 수 있습니다.

ISO 27001:2022 체크리스트는 현재 사용 중인 정보 보안 경영시스템 (Information Security Management System; ISMS)을 평가하고 인증 또는 전환 심사 이전에 주의가 필요한 영역이나 사안을 정확히 찾아내는 데 도움이 되는 유용한 툴입니다. 해당 체크리스트는 ISO 27001:2022에 명시되어 있는 요구 사항에 따라 구성되었으며, 그 내용은 다음과 같은 핵심 영역을 중점적으로 다룹니다.

- **조직의 주변 환경 및 현황**
- **조각 이해관계자의 니즈와 기대**
- **조경영진과 경영 목표**
- **조리스크와 기회**
- **조리스크 대응**

해당 체크리스트를 활용하면 당면 리스크에 따른 대응 방안을 보다 쉽게 선택하고 각 요구 사항에 필요한 소명 자료나 설명 내용을 준비할 수 있어, 정보 보안 경영시스템을 포괄적으로 이해하는 데 큰 도움이 될 수 있습니다.

LRQA

섹션 01
조직의 주변 환경 및 현황

Annex SL High Level Structure를 따르는 ISO 27001:2022는 정보 보안 경영시스템을 설계하고 구현하기 전에 조직의 주변 환경과 현황에 대한 철저한 분석이 얼마나 중요한지 강조하는 내용을 담고 있습니다. 이 분석은 각 조직이 지닌 고유한 니즈와 요구 사항을 판단하고 궁극적으로는 정보 보안 경영시스템의 효율성을 확보하는 데 매우 중요합니다.

이처럼 주변 환경과 현황을 파악하는 데 충분한 시간을 할애할 경우, 조직이 직면한 리스크와 기회에 보다 효과적으로 대응하는 맞춤식 정보 보안 경영시스템을 구축할 수 있습니다.

인터랙티브 형식의 해당 체크리스트를 사용하면, 이미 완료하거나 요건을 충족한 요구 사항을 기록하고 관련 설명이나 소명 내용을 작성할 수 있습니다.

- [ ] 현재 사용 중인 정보 보안 경영시스템에 영향을 미칠 수 있는 외부 요인과 원하는 목표를 달성하고자 할 때 필요한 역량에 영향을 미칠 수 있는 외부 요인을 모두 식별하였습니다.
- [ ] 현재 사용 중인 정보 보안 경영시스템에 영향을 미칠 수 있는 외부 요인과 원하는 목표를 달성하고자 할 때 필요한 역량에 영향을 미칠 수 있는 외부 요인을 모두 식별하였습니다.
- [ ] 정보 보안 경영시스템의 활용 범위를 정하고 기록할 때, 정보 보안 경영시스템 관련 계획을 수립할 때, 주변 환경과 현황에 영향을 주는 요인(내부 및 외부 요인)을 반영하였습니다.
- [ ] 주변 환경과 현황에 영향을 주는 요인에 변화는 없는지 경영검토 시에 주기적으로 검토하고 있습니다.

섹션 02
각 이해관계자의 니즈와 기대

ISO 27001:2022에 의거, 정보 보안 경영시스템은 이해관계자의 니즈와 기대, 원하는 결과에 미치는 영향을 반영해야 하는데, 이는 정보 보안 경영시스템의 운영 범위와 전략적 역할을 정하고 조직의 운영 목표에 잘 맞게 정보 보안 경영시스템을 조정하는 데 필수적인 부분입니다. 또한, 각 조직은 정보 보안 경영시스템에 대한 소속된 모든 당사자의 이해도와 기대를 파악하고 시스템의 효과적인 운영에 해당 당사자를 참여시켜야 합니다.

- [ ] 기타 이해관계자를 포함해 조직에 소속된 모든 당사자의 니즈와 기대를 파악하였으며, 그 중에서 법적 요구 사항으로 간주될 수 있는 니즈나 기대를 추려 내었습니다.

- [ ] 정보 보안 경영시스템을 계획하고 그 활용 범위를 정하고 기록할 때, 관련 이해관계자의 니즈와 기대를 반영하였습니다.

- [ ] 이해관계자의 니즈와 기대를 반영할 때 조직에 소속된 모든 당사자와 상의를 하였으며, 이러한 니즈와 기대는 경영진이 주기적으로 검토하고 있습니다.

- [ ] 정보 보안 경영시스템과 원하는 목표를 달성하고자 할 때 필요한 역량에 영향을 줄 수 있는 이해관계자와 조직에 소속된 당사자를 모두 식별하였습니다.

섹션 03
경영진과 경영 목표

ISO 27001:2022에는 최고 경영진이 리더십을 발휘하는 방법과 임직원이 정보보안 경영시스템에서 수행해야 하는 역할에 대한 내용이 명시되어 있습니다.

고위 경영진의 경우, 특정 업무를 예하 직원에 할당하더라도 궁극적인 책임은 업무를 할당해 지시한 고위 경영진이 지게 됩니다. 고위 경영진의 적극적이고 능동적인 참여는 회사가 정보 보안 경영시스템의 요구 사항에 맞게 사업 활동을 영위하고, 또한 정보 보안 정책, 사업 목표 및 기업 전략 간의 일관성을 보장하는 데 큰 도움이 됩니다.

- [ ] 고위 경영진은 정보 보안 경영시스템에 따라 조직을 운영하고 지원하는 것의 중요성을 알리는 등 정보 보안 경영시스템의 시행에 직접적으로 참여함으로써 시스템이 그 효과를 발휘할 수 있도록 도와주고 있습니다.

- [ ] 정보 보안 정책에는 정보 보안 요구 사항을 충족하고 정보 보안 경영시스템을 지속적으로 개선하기 위한 책무와 정보 보안 목표(또는 책임이나 목표를 설정하는 데 필요한 프레임워크)가 포함되어 있습니다.

- [ ] 정보 보안 경영시스템에 필요한 관련 역할의 권한과 책임을 정의, 공유 및 기록하였습니다.

섹션 04
리스크와 기회

ISO 27001:2022를 살펴보면, 정보 보안 경영시스템은 그 시스템의 활용 범위 내에서 조직의 상황 및 이해관계자와 관련된 리스크 또는 기회에 모두 효과적으로 대응할 수 있어야 한다고 명시되어 있습니다. 즉, 이는 경영시스템이 원하는 바 목표를 달성할 수 있는지 여부에 따라 리스크와 기회를 평가해야 한다는 뜻이라고 해석해 볼 수 있습니다.

이때, 평가는 정보 보안을 위협하는 리스크나 데이터 보호 관련 규정의 준수를 넘어, 허용될 수 없는 수준의 리스크를 관리하고 평가를 통해 파악된 기회를 활용하기 위한 계획을 수립하는 작업으로 이어져야 하며, 이러한 계획의 효과는 주기적인 점검을 통해 확인해야 합니다.

☐ 정보 보안 경영시스템의 예상 결과와 관련된 리스크와 기회를 모두 파악하였습니다.

☐ 리스크와 기회를 파악할 때, 조직의 전반적인 경영 전략과 목표, 내외부 환경과 현황 요인, 이해관계자의 니즈와 기대, 조직 내부 정보의 수명 주기, 정보 보안 경영시스템의 활용 범위를 두루 고려하였습니다.

☐ 리스크와 기회는 정보 보안 목표 수립, 경영시스템의 계획, 모니터링 및 측정에 대한 니즈 파악, 경영검토 등에 모두 반영되고 있습니다.

섹션 05
리스크 대응

ISO 27001:2022를 도입한 조직의 경우, 리스크 대응 계획을 수립하고 실행해야 하는데, 이때 리스크 대응 계획은 적절한 대응 방법을 선택하고 그 효과를 모니터링하는 데 도움을 줄 수 있는 것이여야 합니다. 특히, 필요한 컨트롤을 올바르게 선택하기 위해서는 ISO 27001:2022 Annex A에 명시된 모범 사례를 통해 제시된 컨트롤과 비교를 해보아야 합니다.

마지막으로 모든 리스크 대응 계획은 파악된 각 리스크의 책임자가 승인하고 수락해야 합니다.

- [ ] 적절한 리스크 대응 방안을 선택하는 프로세스를 마련해 두었습니다.
- [ ] 리스크 대응 방안을 시행하는데 필요한 조직적, 인적, 물리적, 기술적 컨트롤을 결정하기 위한 프로세스를 마련하였습니다.
- [ ] 컨트롤을 Annex A와 비교한 결과, 누락된 컨트롤은 없는 것으로 확인되었습니다.
- [ ] 각 컨트롤의 포함 사유 또는 제외 사유를 기술한 적용성 기술서(Statement of Applicability)를 작성하였습니다.
- [ ] 리스크 대응 계획의 활용을 위해 각 리스크의 책임자로부터 승인을 받았습니다.

LRQA ISO 27001 교육 및 심사 서비스

교육/훈련

LRQA는 ISO 27001을 도입하거나 도입을 고려하고 있는 기관이 관련 지식 기반을 구축할 수 있도록 보안 역량과 보안 시스템을 사용한 경험 등을 활용해 여러 조건에 맞는 교육/훈련 과정을 다양한 방식으로 제공하는 서비스입니다.

관련 과정 조회 →

차이점 분석

당사 전문 심사원을 활용해 ISO 시스템 전환을 위한 심사를 시행하기 이전에 시스템의 핵심 구성 요소와 고위험 요소, 취약점 등을 파악하는 데 도움을 줄 수 있는 서비스(선택형 서비스)입니다.

인증 및 전환 평가

LRQA는 ISO 27001:2022 요구사항에 맞추어 정보보안 경영시스템을 평가합니다. 특히, Annex A에 명시된 컨트롤 방안을 집중 분석하여 경영시스템에 미치는 영향을 평가합니다.

통합 평가

여러 경영시스템을 운용 중인 경우, 더 효율적이고 비용 효과적인 통합 심사 및 모니터링 프로그램을 도입하면 더 큰 시너지를 기대할 수 있습니다.

LRQA를 선택해야 하는 이유

글로벌 역량 및 현지 전문가

고객이 있는 곳이라면, LRQA는 어디든 찾아갑니다. 당사는 전 세계적으로 300여 명의 고도로 숙련된 심사원과 250명의 전담 사이버 보안 전문가를 보유하고 있어, 글로벌 기준에 맞는 서비스를 현지에서 직접 제공할 수 있습니다.

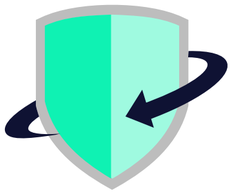
특히, LRQA 직원들은 모두 정보 및 사이버 보안 리스크를 비롯해 사이버 보안 관련 각종 당면 과제, 표준, 규정 및 프레임워크에 대한 방대한 지식을 가진 전문가로 구성되어 있습니다.

유연한 서비스 제공

당사의 모든 ISO 27001 교육 및 인증 서비스는 안전한 보안 기술을 사용하여 대면(현장) 또는 원격으로 제공됩니다. 원격 방식을 선택할 경우, LRQA 글로벌 전문가 네트워크를 통해 대면 방식과 동일한 고품질의 서비스를 고객이 원하는 형태로 유연하고 빠르게 받아볼 수 있습니다.

업계 최초

LRQA는 전 세계적으로 다양한 표준에 대한 인증 서비스를 제공하기 위해 영국 인증국(United Kingdom Accreditation Service, UKAS)의 인증을 받은 최초의 인증 기관입니다. 이처럼 당사는 다양한 부문에 걸쳐 각각의 특정 표준과 프레임워크를 개발하는 데 중요한 역할을 지속적으로 수행하고 있습니다.



단순한 컴플라이언스 이상의 서비스

수상 경력을 자랑하는 LRQA의 사이버 보안 전문가들은 고급 서비스를 통해 정교한 사이버 위협을 한 발 앞서 나갈 수 있도록 고객 여러분을 지원하며, 이러한 서비스는 모든 위협과 취약성에 대한 1차 대응 및 방어선의 역할을 합니다.

고객과의 협업을 통해 완벽한 사이버 보안을 보장하는 LRQA

당사는 어슈어런스 분야에서 쌓은 다양한 경험과 수상 경력에 빛나는 사이버 보안 서비스 및 위협 주도형(threat-led) 인텔리전스를 결합하여, 고객이 직면한 특정 위협에 대한 맞춤형 인사이트와 보호 방안을 제공합니다. LRQA와 함께라면 오늘 뿐만 아니라, 내일 그리고 먼 미래까지 언제나 사이버 보안 리스크에 한 발 앞서 나갈 수 있습니다.

당사는 세계 최고의 국제 표준 및 프로그램을 준수하는 심사, 교육 및 인증 서비스를 제공하며, 고급 사이버 보안 서비스 또한 제공하여 효과를 극대화합니다. 더불어, 당사는 고객과 협력하여 고객이 직면한 특정한 위협을 식별하고 이를 해소, 완화하기 위한 전략을 구축할 수 있도록 지원하며, 고객과 함께 시스템 인증, 취약점 식별을 비롯해 브랜드 무결성, 재정 및 운영에 영향을 미칠 수 있는 공격과 사고를 예방할 수 있도록 최선을 다합니다.

정보 보안

당사의 컴플라이언스 및 인증 서비스는 조직에 반드시 필요한 정보를 보호하고국제적으로 인정받는 모범 사례와 조치를 활용하고 있다는 사실을 입증하는 데 큰 도움이 됩니다.

ISO 27001, ISO 27701, ISO 27017, ISO 27018, CSA STAR

더 자세히 보기 >

운영 리질리언스

당사의 인증, 교육 및 거버넌스, 위험 및 컴플라이언스 서비스를 통해 업무의 중단을 예방하거나 중단에 대응 및 복구하기 위한 준비를 보다 철저히 할 수 있습니다.

ISO 22301, ISO 20000-1, Cyber Essentials

더 자세히 보기 >

사이버 보안 위협에 대한 보호

모든 유형의 사이버 공격에 대한 1차 방어와 대응을 지원하는 맞춤형 솔루션으로 사이버 위협에 한 발 앞서 나갈 수 있습니다.

보안 보증 테스트, 관리형 보안 서비스, 위협 인텔리전스, 인시던트 대응

더 자세히 보기 >

ThreatWatcher 소개

LRQA의 ThreatWatcher 서비스는 고급 정찰 및 분석 기술을 활용하여 사이버 공격에 사용될 수 있는 위협, 기존에 알려지지 않은 위협을 식별하는 관리 평가 체계를 제공합니다.
ThreatWatcher의 보안 인텔리전스 기능은 사용자 교육 프로그램의 약점을 파악하고 과거와는 전혀 다른 방식으로 '디지털 공격 표면'을 식별하는 데 도움을 줄 수 있습니다. 해당 서비스는 고도로 숙련되고 경험이 풍부한 위협 인텔리전스 분석가 팀을 통해 제공됩니다.

ThreatWatcher and ISO 27001:2022

조직을 컨트롤하는 요소 중 하나인 A.5.7 위협 인텔리전스를 구현하기 위해서는 조직이 정보 보안 위협에 관한 위협 인텔리전스를 수집, 분석 및 생산해야 합니다.

해당 컨트롤의 목표는 조직이 현재 및 미래의 사이버 공격에 대한 데이터를 수집, 분석 및 해석하여 사이버 위협에 대한 심층적인 이해를 돕는 것입니다.
이 컨트롤은 또한 해커 등 위협 행위의 주체가 어떻게 해킹할 수 있는지, 어떤 종류의 데이터를 찾고 있는지 파악하는 데 도움을 주도록 설계되었습니다.

ThreatWatcher는 관련 솔루션을 모두 제공하여, 조직이 새로운 위협 인텔리전스 컨트롤에 대한 컴플라이언스를 입증할 수 있도록 지원하는 서비스입니다.

ThreatWatcher 및 ISO 27001:2022에 도입된 요구사항과 컨트롤에 대한 컴플라이언스를 입증하는 데 도움이 되는 기타 LRQA 사이버 보안 서비스에 대해 더 자세히 알고 싶다면 당사 전문가에게 문의해 주시기 바랍니다.

더 자세히 보기 →

LRQA 소개:

LRQA는 평가, 자문, 검사 및 사이버 보안 서비스 분야에서 지난 수십 년 간 독보적인 전문 지식과 경험을 쌓은 세계 최고의 글로벌 어슈어런스 파트너입니다.

당사가 제공하는 솔루션 기반 파트너십은 고객 여러분의 입장에서 가장 중대한 과제를 해결하는 데 도움이 되는 데이터 기반의 인사이트를 지원합니다. 현재 당사는 각종 수상 경력에 빛나는 컴플라이언스, 공급망, 사이버 보안, ESG 분야 전문가 등 5,000여 명의 임직원과 함께 150여 개국, 약 61,000여 곳의 고객사를 대상으로 리스크 예측, 완화 및 관리 서비스를 제공 중이며, 당사는 항상 회사 임직원, 고객, 지역 사회 및 환경을 위한 더 나은 미래를 만들기 위해 최선을 다하고 있습니다.

문의

더 자세한 정보는 홈페이지(www.lrqa.com/ko-kr) 또는 전화(02 736 6231) 로 문의 주시기 바랍니다.

LRQA
2F T Tower 30, Sowol-ro 2gil
Jung-gu, Seoul 04637 South
Korea

LRQA는 제공된 모든 정보가 정확하고 최신 정보인지 확인하기 위해 최선을 다 하고 있습니다. LRQA는 제공된 정보의 오류, 또는 변경에 대한 그 어떤 책임도 지지 않습니다.