ISO/IEC 27001:2022 심사 프로세스

고객정보서

개요

이 고객 정보서는 ISO/IEC 27001 정보보안경영시스템 심사 및 인증을 위한 프로세스의 주요 단계를 설명합니다.

심사 프로세스에는 일반적으로 인증을 추천하기 전 두 번의 방문을 포함합니다.
각 단계별 방문은 다음과 같습니다.

- 1단계심사(문서 검토 및 본 심사 계획 수립)
- 2단계심사 (본 심사)

귀사에게 승인된 인증서를 발급한 후에는 귀사의 인증을 유지하기 위해 사후관리심사를 실시할 것입니다.

매 방문마다 심사원은 공개적이고 유용하며 실질적인 접근 방식을 따를 것입니다. 이러한 방식으로 심사 프로세스에 가치를 창출할 것이라 확신합니다.

방문 전 귀사와 심사 일자, 시작 및 종료 시간, 심사 팀 구성원, 심사 기간 및 어떤 사업 영역을 심사할 것 인지에 대해 논의하고 결정할 것입니다.

1단계 심사 – 문서검토 및 본 심사 방문 계획 수립

심사의 목적

- 표준에서 요구하는 경영시스템 프로세스 및 문서가 수립되어 있고 실행에 옮겨지고 있어 의미 있는 2 단계 심사가 진행될 수 있는지를 확인
- 비즈니스 목표와 ISMS간의연계성과 최고 경영진의 의지를 확인
- 2단계심사 일정 및 심사 범위, 심사팀 요구사항에 대해 확인
- 선택한 통제사항이 식별한 리스크 및 기타 요구사항에 적절한지 확인
- 2 단계 심사의 계획 수립을 위하여 귀사의 조직, 프로세스 및 활동에 대한 정보를 수집
- 심사 서비스에 대한 귀사의 질문사항에 답변

심사 수행

1 단계 심사는 시작회의와 함께 시작합니다 (보통 이틀 동안 진행). 심사원은 심사절차에 대해 경영진에게 설명할 것이며, 귀사는 귀사를 소개할 수 있습니다. 심사원은 귀사와 1 단계 심사 프로그램을 협의할 것입니다.

심사 활동은 다음을 포함합니다.

- 최고 경영진과의 면담을 통해 비즈니스 상황, 전략적 방향 그리고 예상되는 결과를 보장하기 위해 경영 시스템의 수립 및 비즈니스 목표 확인
- 리스크 평가 및 처리 프로세스 평가, 범위 외 사항과의 연관성 확인,선택한 통제의 타당성 검토
- 심사표준, 제안된 심사 범위에 적합한 시스템 설계 및 문서화 확인, 및 상위 경영진과의 면담
- 계획한 통제요구사항을 확인하고, 통제 목적에 적합한지 검토
- 가능한 경우 사업장 투어 실시

2단계 심사 수행을 위한 상세 계획 수립

2 단계 최초 심사 방문 전에 주의가 필요한 이슈 및 긍정적인 결과를 모두 설명하는데 초점을 둔 보고서 작성.
2 단계 심사가 끝날 무렵 보고서는 주요한 발견사항으로써 이러한 이슈의 등급을 식별.

심사원은 다음 사항을 검토합니다:

- 비즈니스 상황과 전략방향
- 정보보안방침 및 목표

- ISMS 적용범위
- 리스크 평가 및 보안통제의 선택
- 주요 역할 및 책임
- 의사소통 계획
- 법규, 규제 요구사항
- 리스크 처리계획 및 조치
- 측정 및 분석 계획
- 내부심사 및 경영검토 기록.

종료 회의 시 1 단계 심사 보고서를 발표하고 안전 보건, 보안 및 관리 이슈를 포함한 심사 프로세스의 다음 단계에 합의합니다.

2단계심사 – 본 심사

2 단계 심사에서는 귀사의 경영시스템 이 어떻게 실행되고 있는지에 초점을 맞출 것입니다.

2 단계 심사는 아래의 사항을 확인하는 것을 목표로 합니다:

- 귀사의 방침, 목표, 프로그램 및 절차가 효과적으로 실행되는지 여부
- 적어도 1회의 경영검토와 내부 심사가 전체 적용범위에 대해 실행되었는지 확인
- 효과적인 프로세스 개선을 위해 계획적이고, 체계적인 접근을 기획하는지 확인
- 경영시스템 이 심사 표준의 모든 요구 사항을 충족하는지 여부.

심사 수행

심사는 1 단계 심사 시 준비된 계획에 따릅니다. 심사 팀원들은 발견 사항을 입증하고 원활한 심사를 위해 안내를 맡은 귀사의 직원과 함께 심사를 진행합니다.

2 단계 심사에는 일반적으로 경영 시스템에 대한 전반적인 책임을 지는 최고 경영진과의 면담이 포함됩니다.

심사 팀은 최소한 다음과 관련된 모든 결과를 보고할 것입니다:

- 1 단계 심사 발견사항에 대한 후속 조치
- 심사를 위해 합의된 범위 내에서 정의된 활동, 제품 및 서비스
- 경영시스템이 정보보안 방침 및 목표 달성에 효과적인지,지속적인 개선의 효과 확인
- 관리 프로그램을 통한 목표 달성의 진행
- 경영시스템에서 요하는 시스템 실행 및 적절한 기록 유지
- 경영시스템 성과와 목표 달성 여부를 평가하기 위한 모니터링 및 측정의 이행
- 경영시스템에 대한 최고 경영층의 참여와 의지 표명
- 내부심사, 시정 및 예방조치 및 경영검토의 효과.

심사 팀은 일일 정리 회의를 통해 발견 사항에 대해 논의합니다. 이를 위해 관련 담당자는 발견사항 확인을 위해 회의에 참석해야 합니다.

발견사항을 정의하는 방법은 아래 '보고서' 섹션을 참조하십시오.

심사 종결 시 심사 결과의 등급을 확정합니다

심사는 심사 결과를 요약하고 차기 심사 프로세스를 협의하는 종료 회의로 마무리합니다. 심사원은 완료된 보고서를 경영자 대리인에게 제공합니다.

만약 중부적합 사항이 발견되지 않았고, 경부적합에 대한 제안된 시정조치가 있었다면, 해당 심사원은 심사 표준에 대한 인증을 추천합니다. (LRQA 오피스의 개별적인 기술검토에 의해 달라질 수 있음)

단, 중부적합 사항이 발견되면 인증추천을 지연시키고 후속 심사를 실시하여 시정조치를 검토할 것입니다. 심사팀장은 귀사와 추가 심사일정을 협의할 것입니다.

사후관리심사

심사의 목적

경영시스템 인증을 획득한 후 정기적인 사후관리심사가 수행됩니다. (보통 최소 12 개월 내 1회 심사). 사후관리심사는 승인받은 경영 경영시스템에 대해 다음사항을 확인하기 위해 수행합니다.

- 경영시스템의 유지
- 경영시스템의 운영, 및
- 지속적인 개선 추진.

LRQA는 고객의 불만 및 이슈 제기 사항을 확인합니다.

LRQA 은 또한 시스템 변경의 영향을 고려합니다. 이러한 변화는 귀사의 활동, 제품 또는 서비스의 변경으로 인해 발생 될 수 있습니다.

그 후 귀사가 인증 요구 사항을 지속적으로 충족하는지 여부를 고려합니다.

심사 수행

사후관리심사의 주제는 일반적으로 이전 방문 시 동의합니다. 시작회의 시 자세한 사항을 확인합니다.

- 선택한 주제를 통해 다음 사항을 검토합니다.
- 내부심사, 경영검토 프로세스, 인시던트 보고 (고객불만 포함) 및 관리
- 정보보안 목표 및 성과지표 달성 및 시정조치, 리스크 처리 프로세스
- 시스템의 변경 및 그로인한 리스크 관리에 대한 영향, 적용의 효과성
- 주요 인원의 책임 및 권한과 관련된 변경 사항 관리

LRQA는 심사 발견사항에 대해 검토를 합니다.

심사 중 경부적합 사항이 발견될 경우 시정조치계획을 협의 후 차기심사 방문 시 결과를 확인합니다. 그렇지 않으면 후속 조치에 대한 조정을 가질 것입니다.

심사 중 중부적합 사항이 발견될 경우, 필요한 시정 조치를 확인하기 위해 특별 사후관리심사를 실시합니다. (일반적으로 3 개월 이내).

이는 인증 효력정지 및 철회의 첫 번째 단계입니다.

종료 회의에서 심사원은 심사결과를 보고하고 차기 심사의 주제를 귀사와 합의할 것입니다. 중부적합 사항이 발견될 경우, 심사원은 귀사가 취할 조치에 대한 조정을 할 것입니다

재인증심사

재인증심사 기획

LRQA 은 이전 사후관리심사에서 계획되고 귀사와 합의하여 3 년 주기의 재인증심사를 실시합니다.

재인증심사 기획 프로세스는 다음 3가지 단계를 포함합니다.
: 검토, 사전검토, 계획.

검토

검토 단계에는 다음과 같은 실적에 대한 검토가 포함됩니다:

- 불만사항 및 기타 성과 지표에 대한 경향 정보
- 시스템 문서 개선사항
- 정보보안 목표의 달성
- 심사에서 얻은 교훈
- 심사 발견사항의 경향.

이전 심사 기간의 실적에 대한 이러한 검토를 바탕으로 심사원은 전략과 목표의 성공적인 이행에 관한 현재 경영시스템의 잠재적 위험을 확인합니다.

사전검토

사전검토는 심사활동이 귀사의 전략 및 목표와 제휴할 수 있도록 하는데 있습니다. 심사원은 최고 경영진과의 면담을 통해 비즈니스 및 운영상의 위험, 경쟁적 사안, 내부 및 외부 환경 변화와 같은 장기적인 요구사항을 파악합니다.

심사원은 면담 통해 이러한 기대, 목표 및 전략이 경영시스템 또는 귀사 조직의 이해 관계자에게 영향을 미치는지 여부를 결정합니다.

사전검토 단계는 다가오는 재 인증 심사 방문 및 향후 3 년 주기 동안 사용할 수 있는 추가 테마를 식별 하는데 활용합니다.

계획

다음 단계는 재인증 심사를 계획하는 것입니다. 이 단계에서 심사원은 다음을 수행합니다:

- 사후관리심사 동안 적절하게 다루어지지 않은 시스템 측면을 식별하고 이를 검토하는 방법을 계획
- 검토 및 사전검토 단계에서 얻은 정보를 사용하여 계획 프로세스 지원
- 필요한 경우, 식별된 주제에 관심을 기울일 수 있는 최선의 방법 고려
- 심사 대상 영역, 부서, 프로세스 및 활동 파악
- 위험도에 기반한 각 사하에 대한 심사시간 합의
- 자원의 최적 사용 파악 및 중복 방지
- 보고서 작성, 취합 제공에 필요한 적정 시간을 추가
- 합리적인 방문 계획으로 정보 통합

심사원은 모든 관련 담당자와 논의 및 모든 관련 부서의 기록 검토에 시간을 할애할 것입니다.

재인증심사 수행

재인증 심사 방문은 2 단계 심사와 유사하게 수행합니다. 또한 시스템 문서 검토를 통해 다음과 같은 사항을 확인합니다.

- 귀사의 경영시스템이 적합하게 지속적으로 유지되고 있는지 확인
- 지속적인 개선을 포함하여 인증 요구사항 및 인증 범위를 준수.

인증변경

귀사의 인증승인의 확대 혹은 감소되는 부분이 있을 경우 공식적인 변경 요청을 하십시오. LRQA는 다음 사항을 고려하여 요청을 검토합니다.

- 심사 팀의 역량 요건 추가 또는 변경
- 심사시간의 추가 또는 감소

변경사항은 수정된 계약서에 공지 될 것입니다.

요청된 변경 사항이 문서화된 시스템에 주요 변경 또는 추가를 의미한다면 별도의 문서 검토 방문(1 단계 심사)을 실시합니다

LRQA 은 공식 방문은 계획하지 않지만 2 단계 심사 방문에 대한 프로세스에 따라 인증의 변경을 실시할 것입니다.
문서 검토(1 단계)가 필요하지 않은 경우,
심사 팀 리더가 방문 중 관련 문서를 검토하고 추가 방문 활동 계획에 합의할 시간을 허용합니다.

인증 변경의 방문에 대한 변경은 별도의 방문으로 수행되거나 계획된(사후관리심사 또는 재인증 심사) 방문과 결합될 수 있습니다.

LRQA 은 현 인증서와 동일한 만료일자를 사용하여 수정된 인증서 를 발급합니다

보고

모든 심사에 대한 보고 프로세스는 유사합니다.
심사 결과 기록, 심사 계획에 대한 진행 정도, 긍정적인 코멘트, 그리고 해석이나 명확하게 해야 할 부분을 심사 보고서에 작성합니다.

심사 결과를 발견사항 로그에 기록 하고 중부적합 또는 경부적합사항 으로 식별합니다. 이러한 등급은 다음과 같이 정의됩니다.

중부적합 사항: 하나 이상의 경영시스템 요소가 없거나, 하나 이상의 경영시스템 요소를 구현하고 유지하지 못하거나, 이용 가능한 객관적 증거에 근거하여 경영진이 다음을 달성하는데 있어 상당한 의혹을 제기하는 상황:

- 조직의 정책, 목표 또는 공공책임
- 적용가능한 규제 요건 준수
- 적용가능한 고객 요구 사항의 적합성
- 심사 기준에 대한 적합성.

일반적으로 중부적합 사항은 다음과 같은 시스템 실패를 의미합니다.

- 이미 시스템 효과 또는 결과물에 영향을 미치고 있음
- 경영시스템의 역량에 위험 발생
- 즉각적인 격리가 요구되는 상황
- 즉각적인 근본 원인 분석 및 시정 조치가 필요

LRQA 심사 팀장이 귀사와 후속 조치에 합의할 것입니다.

경부적합 사항: 구현되고 유지되고 있는 시스템의 취약점을 나타내는 발견 사항입니다.
경영시스템의 역할에 큰 영향을 미치지 않거나 시스템 결과물에 위험을 주지 않지만 시스템의 미래 역량을 보장하기 위해 다루어야 합니다.

일반적으로 경부적합 사항은 내부적으로 직면하는 절차나 수순에 있어 취약점이 될 수 있습니다.
합리적으로 고려될 수 있는 어떠한 추가적인 제어의 악화는 시스템을 비효율적으로 만들 수 있습니다.
이는 근본 원인 조사 및 시정 조치가 필요합니다.

이 시정 조치 계획은 귀사의 인증서가 발급되기 전 LRQA에 의한 개별 검토됩니다.
사후관리심사 시 제기된 경우, 심사 후 적절한 시간 내에 시정조치를 취해야 하지만, 일반적으로 다음 방문 전까지 세부 조치 결과를 제공할 필요는 없습니다.

두 경우, 모두 다음 심사에서 귀사가 조치한 시정조치를 검토하고 결과 기록에 기재한 시정조치 검토사항을 심사합니다.

수행된 프로세스 효율성을 향상하는 경영시스템 준수에 대한 개선사항을 다음 중 하나에 기록합니다.

- 전략적 개선 제안을 위한
- 경영진의 요약
- 특정 영역과 관련된 개선제안을 위한 보고서 본문

3 년 동안 모든 심사보고서 사본을 보관해 두십시오. 만일의 경우 이전 보고서의 사본을 요청할 수 있습니다.

이후 방문 시, 부적합 사항 발생을 방지하기 위해 귀사가 해결해야 할 단 하나의 사항이라도 확인한 경우 해당 문제를 보고서의 관련 부분에 기록할 것입니다.

샘플링

활동 영역에서 문제가 식별되지 않을 수 있지만 문제가 없다는 것을 반드시 의미하는 것은 아닙니다.
심사는 샘플링 기법에 기초하기 때문에 통계적으로 항상 심사 중에 문제가 식별되지 않을 가능성이 있습니다.
귀사가 경영시스템 심사 시, 이 점을 유념하십시오.

기밀준수

당사는 귀사의 허가 없이(인정기관에서 요구하는 경우를 제외하고) 귀사의 조직에 대해 수집한정보 (보고서 내용 포함)를 다른 사람이나 조직에 전달하지 않습니다.

추가정보

귀사의 성과를 높이고 위험은 줄일 수 있도록 LRQA가 어떻게 도울 수 있는지에 관한 정보를 더 원하시면 LRQA웹사이트 www.lrqa.com/ko-kr 을 방문하세요.

여기서 귀사가 속한 국가의 LRQA 웹 페이지 또한 방문하실 수 있습니다.

Get in touch

Visit www.lrqa.com/ko-kr for more information.

LRQA Korea Ltd.

2F T Tower 30, Sowol-ro 2-gil,
Jung-gu, Seoul, 04637,
Republic of Korea

YOUR FUTURE. OUR FOCUS.

CIN036 - Version May 2023