ESG PACKAGE

Korea Compliance Initiative

ISO Framework for ESG Management

KCI 한국준법진흥원
KOREA COMPLIANCE INITIATIVE

ISO ESG Framework Package

글로벌 스탠다드(ISO) 경영시스템을 통한 ESG 등급 향상

ESG

목표 UN 지속가능 발전 목표
UN SDGs
2030년까지 17가지 주 목표 이행

E : ISO 14001(환경)
S : ISO 45001(안전보건)
G : ISO 37301(준법)

실행 ESG 관련 대표 글로벌 스탠다드

평가 국내외 평가지표/지수
K-ESG

공개 보고 정보공개 및 보고서 작성 가이드라인
금융위원회 2030년까지 모든
코스피 상장사 ESG 공개 의무화

E **ISO 14001:2015**
Environmental management systems – Requirements with guidance for use

S **ISO 45001:2018**
Occupational health and safety management systems – Requirements with guidance for use

G **ISO 37301:2021**
Compliance management systems – Requirements with guidance for use

E

ISO 14001:2015
Environmental management systems – Requirements with guidance for use

개요

- 환경오염 최소화(안전 및 환경사고 방지), 지속적 환경개선을 달성하기 위하여 조직 각 부분의 책임과 권한을 명확히 하고 업무의 기준을 글로벌 스탠다드로 작성하여 이를 수행하는 경영활동
- 조직이 구축한 환경경영시스템이 글로벌 스탠다드에 적합한지를 제3자 인증기관이 객관적으로 보증하여 주는 인증제도
- 환경사고의 사전 예방 및 최소화, 환경 법규 준수 등 조직의 환경 성과에 중요한 입증 증거자료

환경정책기본법, 환경영향평가법, 대기·수질환경보전법, 자연·토양환경보전법, 폐기물관리법, 유해화학물질관리법, 먹는물관리법, 지하수법, 해양폐기물 및 해양오염퇴적물관리법, 소음 · 진동관리법, 자연의 절약과 재활용촉진에 관한 법률, 환경친화적전환 촉진법, 제품포장방법/재질규격, 자연재해대책법, 오존층보호를 위한 특정물질 제조규제 등에 관한 법률, 폐기물처리시설 설치촉진 및 주변 지역지원 등에 관한법률 등

법률 | 시행령 | 시행규칙 | 행정규칙 | 해석, 지침 | 메뉴얼

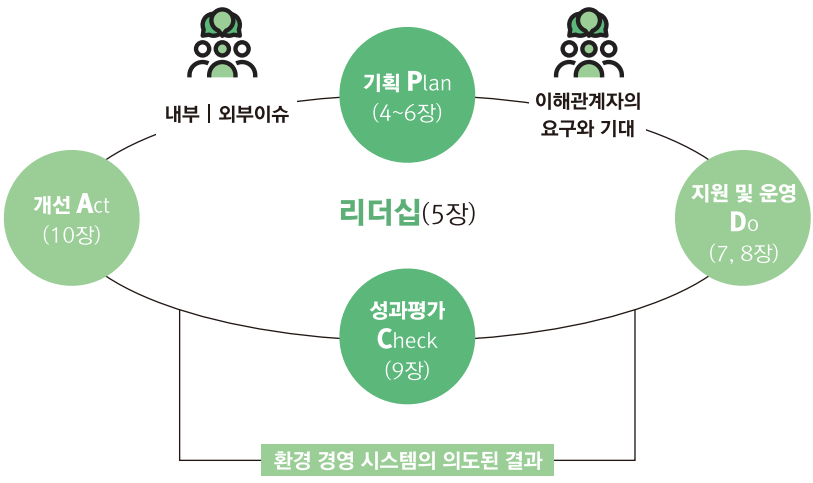
필요성 및 기대효과

- 환경 관련 사고의 리스크 해소
- 강화되는 환경규제에 보다 효과적으로 대응 가능
- 기업 이미지와 제품 및 서비스 이미지 제고를 통해 기업 경영 선진화
- 각종 환경오염 부하 감소 및 에너지 절감 등을 통한 원가절감
- 선진국 수출 시 환경인증 요구 입증
- 환경 관련 법규 제도와 환경영향 파악하여 신속한 의사결정
- 기업 이미지 개선으로 고객 신뢰도 확보
- 이해관계자(환경운동단체 등)와의 커뮤니케이션 활성화

ESG 평가·공시

1. 기후변화 및 탄소배출
   책임있는 구매·조달
   녹색채권
   탄소국경세
2. 친환경제품 개발
   환경 관련법
   화학물질 관련법
   산업발전법

환경 경영 시스템



S

ISO 45001:2018
Occupational health and safety management systems – Requirements with guidance for use

개요

- 사업장에서 발생 가능한 재해 및 사고의 위험성을 예측하여 관리 · 예방하게 하고 지속적인 개선을 통해 인적 재해 및 재산 피해를 사전에 예방함으로써 임직원의 안전보건과 건강을 지킴과 동시에 궁극적으로 기업의 이윤창출과 조직원의 안정을 체계적으로 관리하는 규격
- ISO 45001은 안전보건에 대한 기본 틀을 제공하며, 각종 사고를 예방하기 위해 지켜야 할 최소한의 요구사항을 규정하는 국제표준 규격

2022.1.27 「중대재해처벌법」시행

형벌 주체의 확대 : 사업주, 경영책임자 등 형사책임 | **보호의 대상 확대** : 종사자, 제3자의 종사자, 이용자 등
보호 장소의 확대 : 실질적 지배·운영·관리 개념을 통해 책임 범위 확대 | **책임의 강화** : 형사책임의 강화 및 법인에 대한 징벌적 배상 책임 도입
처벌 주체 확대 : 고용노동부, 경찰, 검찰

필요성 및 기대효과

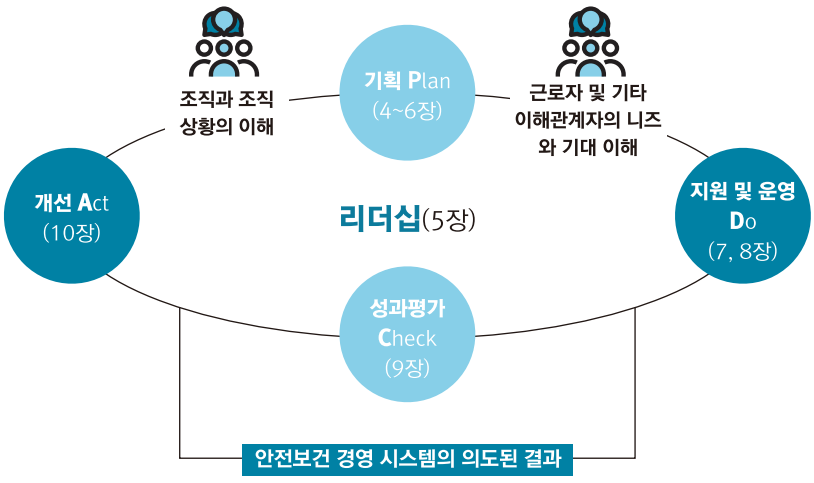
- 법률(중대재해처벌법, 산업안전보건법 등)규정 준수로 사고율 감소
- 임직원의 안전보건에 대한 동기부여와 인식도 향상
- 산업재해에 대한 각종 소송 및 법규, 규제에 대한 대응 가능
- 중대사고 위험성을 단기간 내에 현저히 감소
- 지속적인 안전보건 개선을 위한 측정 및 모니터링 가능
- 글로벌 상거래 시 안전보건에 대한 적격성 요구
- 대내외 평가기간에 대한 안전보건 입증자료로 등급·평가 향상
- 정부 정책에 부응
- 근로자의 불만을 해소하여 노사관계 안정에 기여

ESG 평가·공시

① 안전 보건 추진체계
산업재해율
안전 리스크 관리

② 중대재해처벌법
산업안전보건법
공정거래법

안전보건 경영 시스템



G

ISO 37301:2021
Compliance management systems – Requirements with guidance for use

개요

- 2021년 4월 제정 : 컴플라이언스(준법) 분야에 적용 가능한 요구사항으로 해당 조직에서 정한 컴플라이언스 경영시스템을〈수립, 개발, 실행, 평가, 유지 및 개선〉 운영하고 법령 및 규제, 모범관행, 윤리 및 지역사회의 기대 준수에 대한 조직의 대처를 실증하는 제3자 인증 제도. 즉, 조직의 컴플라이언스 의무(Obligation)와 관련된 관리 프로세스의 결과물들을 심사
- **특징** : 미국 법무부 양형 감경, 기소유예 합의 조건 등으로 Effective Corporate Compliance Program 구축과 운영 의무화(ISO 37301은 국내외 규제/사법기관의 제재 부과시 벤치마크로 활용 가능) 강화 추세

법규준수

자발적으로 관련 법규 등 의무사항을 사전 예방 준수하는 시스템
자발적 컴플라이언스(Compliance)문화 구축
조직의 경영원칙으로써 법과 윤리를 준수하여 지속 가능한 성장

컴플라이언스 문화 만들기 › 컴플라이언스 업무에 대한 투자 › 컴플라이언스 책임자 임명 › 변화하는 규제 환경 따라잡기 › 제3자 검증 (리스크, 모니터링) › 내부고발자 활동장려

필요성 및 기대효과

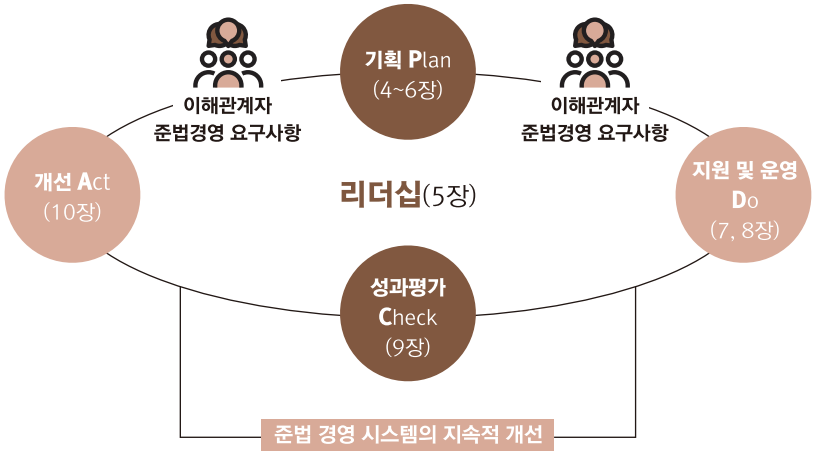
- 국내외 관련 법률의 양형 참작 사유 적용 가능성
- 선진화된 글로벌경영 시스템으로 법률 위반 리스크 사전 예방 및 감소
- 준법(윤리)경영의 실천의지 입증
- 기업의 신뢰성 및 조직가치 향상(외부 투자 유입 등)
- 자체 컴플라이언스 수준 진단, 업무 투명성 제고 등
- 경영불안감 해소(내부통제 강화)
- 컴플라이언스 운영으로 사업활동의 전제조건화 추세 부응
- 임직원의 규정 준수에 대한 동기부여와 인식도 향상
- 입찰참여시 규정준수 요구사항에 적격성 근거자료 충족
- 경쟁사에 대한 비교 우위

ESG 평가·공시

① 기업경영 지배구조
기업윤리 · 부패
임원 도덕성
주주권리

② ESG 전담조직
상법, 자본시장법
청탁금지법
외부감사법

준법 경영 시스템



한국준법진흥원 (Korea Compliance Initiative) 소개

**“고객에게 신뢰할 수 있는 최상의 인증 서비스를 제공하고,
경영시스템의 성과를 달성함으로써 고객의 가치 창출에 기여!”**

Education

실무적 교육 &참관 기회

차별화된 맞춤형 교육(비대면 등),
현장실습과 심사원 참관 기회 제공

Specialty

차별화된 전문 심사자원 보유

젊고 유능한 준법 마인드를 바탕으로
실무적이며 스마트한 심사 자원 보유
(CP, 윤리, 청렴, ESG, CSR, GRC 등 인력풀)

Guard

고객 정보 보호 최우선

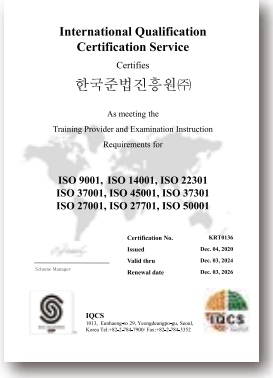
배상책임보험, 보증보험, 계약서,
보안각서, 서버, 심사원 교육 등

미국 IAS 인정기구 최초 등록

ISO 국제표준인증서

IAF 인정서 검색

https://www.iafcertsearch.org/

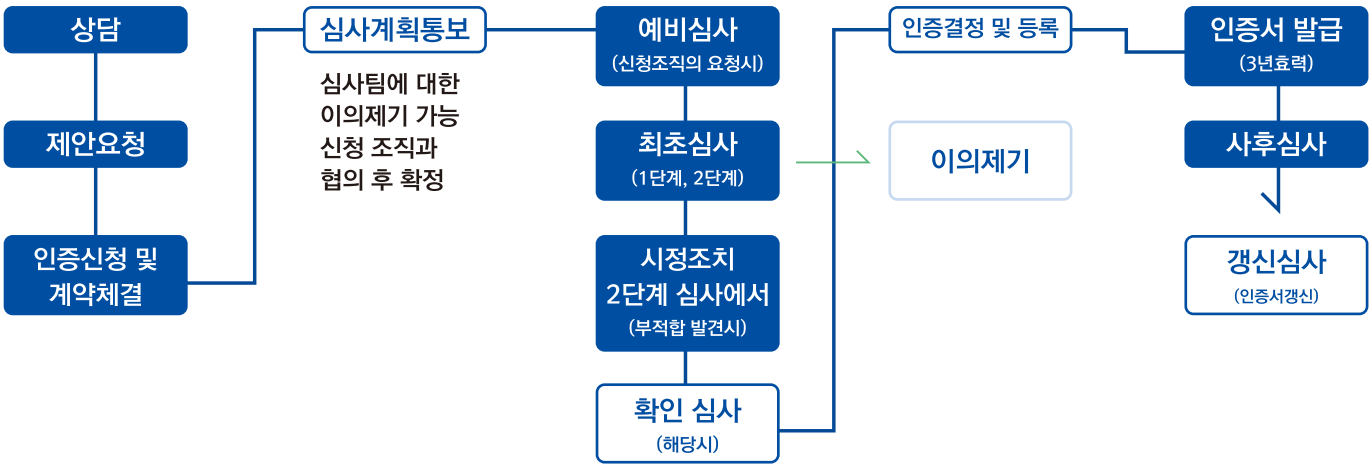


한국준법진흥원 IQCS 연수기관 등록

캐나다 정부 산하기관인 인정기관 SCC(Standard Cound Of Canada)에서 ISO 17024 (개인 자격 국제표준)에 의거 심사원 교육 및 관리기관인 IQCS에 등록된 연수기관입니다. 적격성 방식(Competence)으로 등록된 연수기관 (Training Provider&Examiner Certification Scheme : 이하 TPECS)으로 모듈별로 구분하여 교육하는 방식으로 진행하므로 심사원으로써 적격성을 확보하기에 용이합니다.

형태	온/오프라인 교육(비대면 등)
기타	단체교육 문의 02) 6334-6605
과정	국제 인증심사원 과정, 내부심사원과정, ESG, 공정거래, 기타 방문교육

01 인증 신청 절차

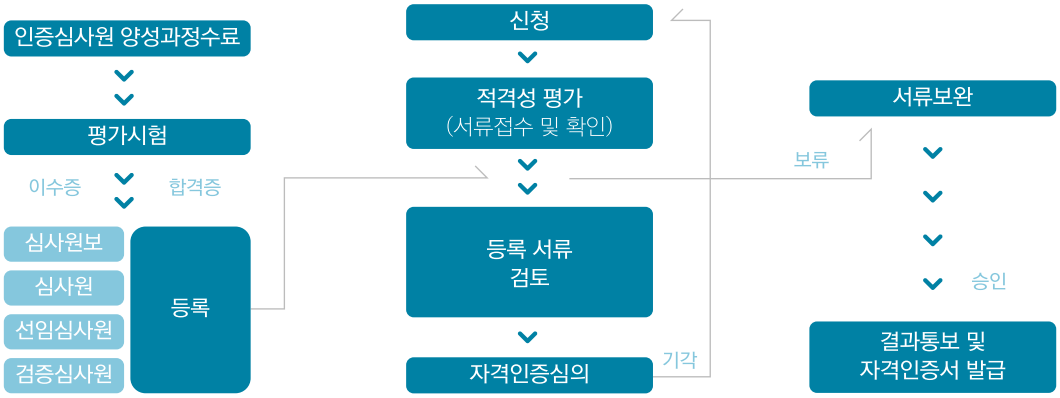


02 교육 신청 절차

교육과정 심사원 과정

한국준법진흥원(KCI : Korea Comliance Initiative)의 ISO 심사원 교육훈련 서비스는 기업 경영에 필요한 요구(Needs)와 기여를 충족하고 실력있는 심사원 배출을 위한 맞춤형 실무 교육과정을 제공합니다.

심사원 등록과정



심사원 활동영역

기업, 연구소, 관공서, 전문 컨설팅 기관 등에 취업 경쟁력 확보 | 소속 조직의 경영 시스템 발전 및 개인의 업무역량 향상 국제 인증(내부)심사원으로 심사업무 수행 | 전문 컨설팅 기관의 창업 | 사회 경험을 활용한 기업체의 경영 지도 및 자문 평생직장 개념이 없어진 기업 환경에서 평생 자격 획득

ISO 9001(품질경영시스템)

Quality Management System

KCI 한국준법진흥원 KOREA COMPLIANCE INSTITUTE

개 요

ISO 9001은 품질경영에 관한 표준으로 조직이 제품 또는 서비스 품질을 지속적으로 개선하여 고객의 요구사항을 충족시킬 수 있는 능력을 보유하고 있음을 국제적으로 인정받기 위해 갖추어야 할 요구사항입니다. 기업 전반에 대한 총제적인 품질 향상을 통하여 경쟁력 우위를 확보하고 고객만족 향상 및 조직 경쟁력 제고를 통해 조직의 장기적인 성장·발전을 추구하는 규격입니다.

필요성

❶ 제품 및 공정품질, 프로세스의 개선으로 생산성 제고
❷ 기업 경쟁력의 제고 및 이미지 개선
❸ 대기업 및 대형유통 납품 우선권 부여
❹ 국제간 무역에서 신뢰감 확보로 시장 진출 확대
❺ 공급자-외주업체간 공급체계 품질시스템 접근
❻ 제조물 책임(PL) 제도 대비

기대효과

❶ 기술축적과 원가절감으로 기업의 매출과 이익 증대
❷ 결함 예방, 낭비적 요소 제거 및 지속적 개선을 통하여 고객만족
❸ 업무 책임과 권한의 명확화 및 효율성 제고
❹ 품질 안정으로 고객만족도 향상 및 시장점유율 제고
❺ 고객감사 및 중복적인 제3자 인증의 경감
❻ 확고한 품질경영시스템의 구축을 통한 회사의 경쟁력 향상과 연계되어 지속적인 개선 활동 기대

품질 요구사항의 구조

4 조직의 상황
4.1 | 조직과 조직상황의 이해
4.2 | 이해관계자의 니즈와 기대 이해
4.3 | 품질경영시스템 적용범위 결정
4.4 | 품질경영시스템과 그 프로세스

5 리더십
5.1 | 리더십과 의지표명
5.2 | 방침
5.3 | 조직의 역할, 책임 및 권한

6 기획
6.1 | 리스크와 기회를 다루는 조치
6.2 | 품질목표와 품질목표 달성 기획
6.3 | 변경의 기획

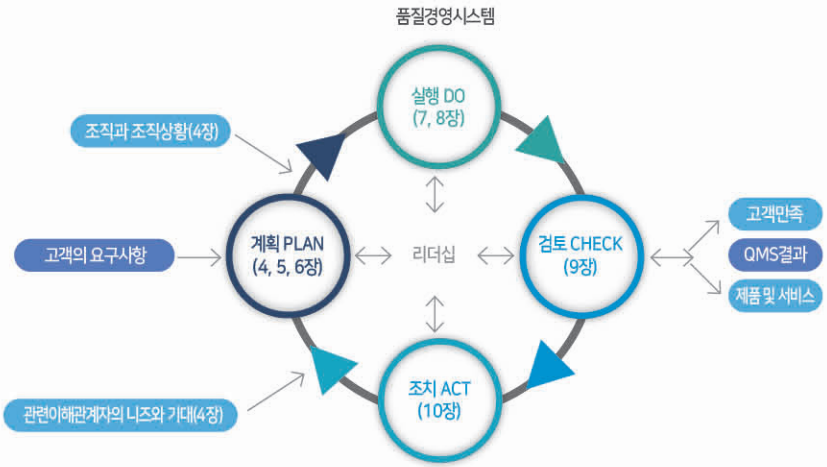
7 지원
7.1 | 자원
7.2 | 역량/적격성
7.3 | 인식
7.4 | 의사소통
7.5 | 문서화된 정보

8 운영
8.1 | 운영 기획 및 관리
8.2 | 제품 및 서비스 요구사항
8.3 | 제품 및 서비스의 설계와 개발
8.4 | 외부에서 제공되는 프로세스, 제품 및 서비스의 관리
8.5 | 생산 및 서비스 제공
8.6 | 제품 및 서비스의 불출/출시(release)
8.7 | 부적합 출력/산출물(output)의 관리

9 성과 평가
9.1 | 모니터링, 측정, 분석 및 평가
9.2 | 내부심사
9.3 | 경영검토/경영평가 (management review)

10 개선
10.1 | 일반사항
10.2 | 부적합 및 시정조치
10.3 | 지속적 개선

기본모델



- **PLAN(계획)** : 고객요구사항 및 조직의 방침에 따라 결과를 도출하는데 필요한 목표 및 프로세스를 수립
- DO(실행) : 프로세스의 실행
- CHECK(검토) : 방침, 목표, 및 제품; 요구사항과 관련되 프로세스 및 제품을 모니터링하고 측정하여 결과를 보고
- ACT(조치) : 프로세스 성과를 지속적으로 개선하기 위하여 조치를 취함

ISO 14001(환경경영시스템)

Environment Management System

개 요

국제표준화기구(ISO)에서 제정한 환경경영과 관련한 국제표준입니다. 환경오염최소화(안전 및 환경 사고 방지), 지속적 환경개선을 달성하기 위하여 조직 각 부분의 책임과 권한을 명확히 하고 업무의 기준을 표준으로 작성하여 이를 수행하는 경영활동 ISO 14000 시리즈와 ISO 14001 규격은 기업활동의 전과정에 걸쳐 지속적 환경성과를 개선하는 일련의 경영활동을 위해 국제표준화기구에서 제정한 환경경영체제에 관한 규격이며, 환경경영체제 인증제도는 조직이 구축한 환경경영시스템이 이 규격에 적합한지를 제 3자 인증기관이 심사하여 객관적으로 보증하여 주는 인증제도입니다.

환경방침(Environmental Policy)을 바탕으로 환경경영시스템의 계획(Planning)에 대한 점검 및 시정조치(Checking and Corrective Action)를 통하여 최종 경영 검토(Management Review)로써 지속적인 환경 개선과 법적 요구사항의 적합성이 ISO 14001의 핵심입니다.

필요성

❶ 환경 리스크 해소
❷ 강화되는 환경 규제에 보다 효과적으로 대응
❸ 기업 이미지와 제품 이미지 제고를 통해 기업경영의 선진화
❹ 각종 환경오염 부하 감소 및 에너지 절감 등을 통한 원가절감
❺ 선진국 수출시 환경 인증 요구

기대효과

❶ 글로벌스탠다드 환경 인증으로 고객 신뢰 확보
❷ 원재료 및 에너지 절감
❸ 환경에 대한 법규제와 환경영향의 파악
❹ 법규제의 준수, 사전점검을 통한 환경 리스크의 경감
❺ 기업이미지 개선, 환경성과의 지속적 개선
❻ 이해관계자와의 커뮤니케이션 활성화

환경 요구사항의 구조

4 조직의 상황
4.1 | 조직과 조직 상황에 대한 이해
4.2 | 이해관계자의 니즈(needs)와 기대의 이해
4.3 | 환경경영시스템의 적용범위 결정
4.4 | 환경경영시스템

5 리더십
5.1 | 리더십과 의지표명
5.2 | 환경방침
5.3 | 조직의 역할, 책임 및 권한

6 기획
6.1 | 리스크와 기회를 다루는 조치
6.1.1 | 일반사항
6.1.2 | 환경측면
6.1.3 | 준수의무사항
6.1.4 | 조치계획
6.2 | 환경목표와 이를 달성하기 위한 기획
6.2.1 | 환경목표
6.2.2 | 환경목표 달성을 위한 조치 기획

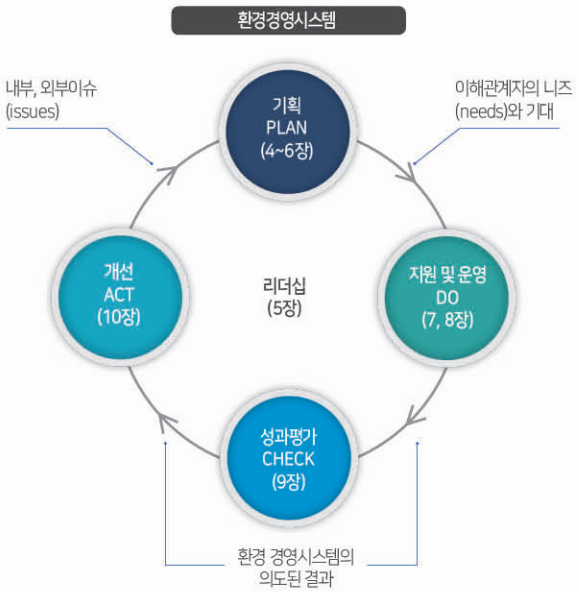
7 지원
7.1 | 자원(resource)
7.2 | 역량(competentce)
7.3 | 인식
7.4 | 의사소통
7.4.1 | 일반사항
7.5.2 | 내부 의사소통
7.6.3 | 외부 의사소통
7.5 | 문서화된 정보
7.5.1 | 일반사항
7.5.2 | 작성(creating) 및 갱신

8 운영
8.1 | 운영 기획 및 관리(control)
8.2 | 비상사태 대비 및 대응

9 성과 평가
9.1 | 모니터링, 측정, 분석 및 평가
9.1.1 | 일반사항
9.1.2 | 준수평가
9.2 | 내부심사
9.2.1 | 일반사항
9.2.2 | 내부심사 프로그램
9.3 | 경영검토

10 개선
10.1 | 일반사항
10.2 | 부적합 및 시정조치
10.3 | 지속적 개선

조직상황



ISO 45001(안전보건경영시스템)

Occupational Health & Safety Management System

KCI 한국준법진흥원 KOREA COMPLIANCE INITIATIVE

개 요

안전보건경영시스템은 사업장에서 발생 가능한 재해 및 사고의 위험성을 예측하여 관리·예방하게 하고 지속적인 개선을 통해 인적 재해 및 재산 피해를 사전에 예방함으로써 조직원의 안전보건과 건강을 지킴과 동시에 궁극적으로 기업의 이윤 창출과 조직원의 안전을 체계적으로 관리하는 규격입니다. OHS(Occupational Health and Safety) 관련 의무 이행에 대한 기본 틀을 제공하며, 안전보건 사고를 예방하기 위해 지켜야 할 최소한의 요구사항을 규정하는 국제표준 규격입니다.

필요성

❶ 법(중대재해기업처벌법, 산업안전보건법) 규정 준수
❷ 임직원의 안전보건에 대한 동기부여와 인식도 향상
❸ 산업재해에 대한 각종 소송 및 법규, 규제에 대한 대응 가능
❹ 중대사고 위험성을 단기간 내에 현저히 감소
❺ 지속적인 안전보건 개선을 위한 측정 및 모니터링
❻ 기업인의 안전보건 의무사항 이행
❼ 글로벌 상거래시 적격성 요구
❽ 정부정책 부응
❾ 국제간 무역에서 신뢰감 확보로 시장 진출 확대

기대효과

❶ 작업장 내의 위험성을 관리, 예방하여 재해사고율 감소
❷ 신뢰성 있는 안전보건경영시스템 구축으로 보험료 절감
❸ 근로자의 보건안전 위험성의 개선을 통한 생산성 향상
❹ 규격에서 요구하는 기준에 적합하게 함으로써 안전부문의 무역장벽을 제거하여 해외시장 진출 용이
❺ 사업주 및 근로자의 안전보건 관리 의식이 선진국 수준으로 발전하여 기업의 자율 안전보건관리 체제가 조속히 정착
❻ 생산제품 및 작업환경에 대해 국제인증을 받음으로써 안전보건에 대한 근로자의 편향된 불만을 해소하여 노사관계 안정에 기여

안전보건 요구사항의 구조

4 조직의 상황
4.1 | 조직과 조직 상황에 대한 이해
4.2 | 이해관계자의 니즈(needs)와 기대의 이해
4.3 | 안전보건경영시스템 적용범위 결정
4.4 | 안전보건경영시스템

5 리더십과 근로자 참여
5.1 | 리더십과 의지표명
5.2 | 안전보건 방침
5.3 | 조직의 역할, 책임 및 권한
5.4 | 근로자 협의 및 참여

6 기획
6.1 | 리스크와 기회를 다루는 조치
6.2 | 안전보건 목표와 목표 달성 기획

7 지원
7.1 | 자원(resource)
7.2 | 역량(competentce)
7.3 | 인식
7.4 | 의사소통
7.5 | 문서화된 정보

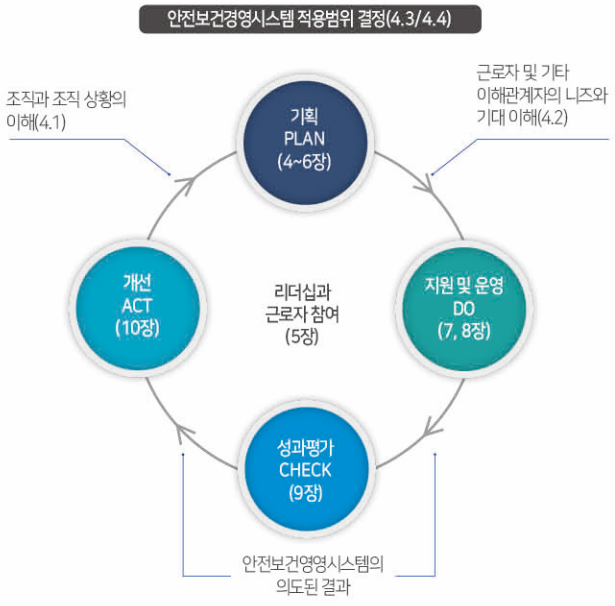
8 운영
8.1 | 운영 기획 및 관리
8.2 | 비상시 대비 및 대응

9 성과 평가
9.1 | 모니터링, 측정, 분석 및 평가
9.2 | 내부심사
9.3 | 경영검토

10 개선
10.1 | 일반사항
10.2 | 부적합 및 시정조치
10.3 | 지속적 개선

부속서 A (참고) 이 표준의 활용을 위한 가이던스
A.1 | 일반사항
A.2 | 인용표준

조직상황



ISO 37001(부패방지경영시스템)

Anti-Bribery Management System

개 요

ISO 37001은 2016년 국제 사회와의 합의를 통해 제정된 국제표준으로 미국의 FCPA를 시작으로 OECD 뇌물방지협약, UN 반부패협약, 영국의 Bribery Act 등 전세계적으로 일어나는 부패방지에 대한 규격입니다. 모든 조직 활동에서 발생할 수 있는 부패방지 분야에 적용 가능한 <요구사항>을 규정하였으며, 조직에서 부패방지경영시스템을 <수립, 실행, 유지, 검토 및 개선>에 대해 인증이 가능한 글로벌 스탠다드 입니다.

특징으로 부패방지에 대한 합리적이고 비례적인 기준 및 통제 시스템이며, 부패를 예방, 탐지, 완화 그리고 대응하기 위한 필요한 모든 관리조치로서 최소한의 도구입니다. 또한, 일반적인 요구사항으로써 국제적 모범사례를 반영하였으며 공공, 민간 또는 비영리 부문에 관계없이 모든 조직(소규모, 중간, 대규모)에 적용 가능한 규격입니다.

필요성

❶ 국내외 반부패관련법「청탁금지법 제24조 양벌규정」대비 (형벌의 양형 또는 과태료 가액 산정 시 반영-입증 증거자료)
❷ 양형위원회(뇌물부분)에 양형 참작사유 적용 가능(정부 반부패 정책과제 5대 추진과제 추진 중)
❸ 입찰 참여시 청렴 준수 요구사항 충족(적격성 근거 자료)
❹ 기업의 글로벌 스탠다드화-투명성 사업 활동의 전제 조건화
❺ 예방차원의 비즈니스 안전(법적, 규제적 요구사항 만족)
❻ 컴플라이언스 수준진단, 업무 투명성 제고, 신고문화 활성화 등

기대효과

❶ <정부 반부패 정책과제>에 따른 요구사항 부응
❷ 이해관계자(임직원, 정부, 고객, 투자자 등)에 대한 신뢰성 및 조직 가치 향상(CSR, 윤리경영 등 실천의지 입증)
❸ 부패 리스크 사전 예방 및 대응 ⇒ 경영 불안감 해소(내부통제 강화)
❹ 경쟁사에 대한 비교 우위
❺ 법 위반 감소로 관련된 비용 및 벌칙 최소화(법과 원칙 준수)
❻ 타 경영시스템(QMS, EMS 등)과 통합 용이
❼ 수출 기업의 무역장벽 제거
❽ 상호 인정을 통한 간접비용 절감

부패방지 요구사항의 구조

4 조직의 상황
4.1 | 조직과 조직 상황에 대한 이해
4.2 | 이해관계자의 니즈 및 기대의 이해
4.3 | 뇌물방지경영시스템 적용범위 결정
4.4 | 뇌물방지경영시스템
4.5 | 반부패 리스크 평가

5 리더십
5.1 | 리더십과 확약
5.1.1 | 이사회
5.1.2 | 최고경영자
5.2 | 뇌물방지 방침
5.3 | 조직의 역할, 책임 및 권한
5.3.1 | 역할 및 책임
5.3.2 | 뇌물 수수 방지 기능
5.3.3 | 위임된 의사 결정

6 기획
6.1 | 리스크와 기회를 다루는 조치
6.2 | 뇌물방지 목표 및 뇌물방지 목표 달성 기획

7 지원
7.1 | 자원
7.2 | 역량/적경성
7.2.1 | 일반사항
7.2.2 | 고용프로세스
7.3 | 인식 및 교육훈련
7.4 | 의사소통
7.5 | 문서화된 정보
7.5.1 | 일반사항
7.5.2 | 작성 및 개정
7.5.3 | 문서화된 정보의 관리

8 운영
8.1 | 운영 기획 및 관리
8.2 | 실사
8.3 | 재정 관리
8.4 | 비재무적인 관리
8.5 | 관리되는 조직과 사업당사자에 의한 뇌물방지 관리의 실행
8.6 | 뇌물 수수 방지 약속
8.7 | 선물, 환대, 기부 및 이와 유사한 혜택
8.8 | 뇌물방지 관리의 부적절한 관리
8.9 | 우려 제기
8.10 | 뇌물 수수 조사 및 처리

9 성과 평가
9.1 | 모니터링, 측정, 분석 및 평가
9.2 | 내부심사
9.3 | 경영검토
9.3.1 | 최고 경영자 검토
9.3.2 | 이사회 검토
9.4 | 뇌물방지 준수 기능 검토

10 개선
10.1 | 부적합 및 시정조치
10.2 | 지속적 개선

ISO 37301(준법경영시스템)

Compliance Management System

KCI 한국준법진흥원 KOREA COMPLIANCE INITIATIVE

개 요

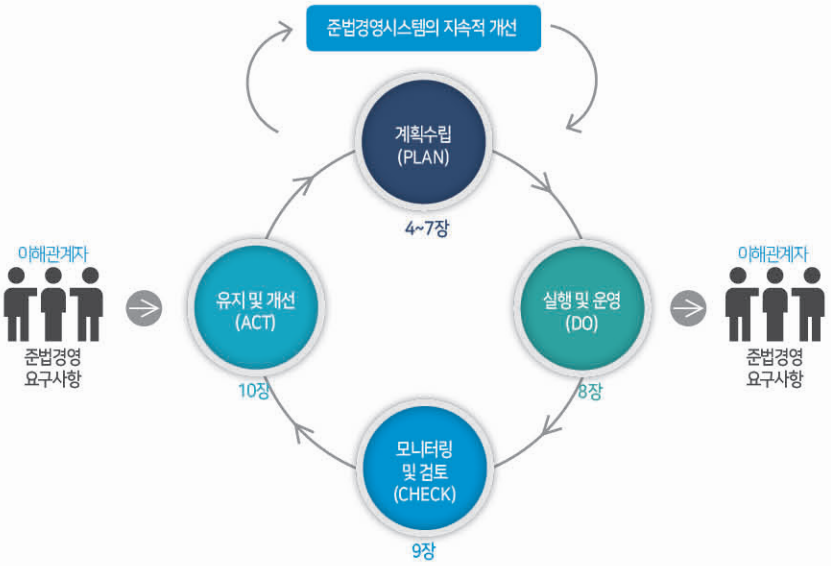
ISO 37301은 2021년 1월 국제표준화기구가 사회적 합의를 통해 모든 조직 활동에서 컴플라이언스(준법 등) 분야에 적용 가능한 요구사항으로 제3자 인증이 가능한 글로벌 스탠다드입니다. 해당 조직에서 정한 컴플라이언스 경영시스템을 <수립, 개발, 실행, 평가, 유지 및 개선> 운영하고 법령 및 규제, 모범관행, 윤리 및 지역사회의 기대 준수에 대한 조직의 대처를 실증하는 제도입니다. 컴플라이언스 의무(Obligation)로써 해당 조직이 정한 법률, 규정, 절차, 행동(윤리)강령 뿐만 아니라 조직 활동, 제품, 서비스 등 관련된 관리 프로세스의 결과물들을 심사하게 됩니다. 특징으로는 미국 법무부 Corporate Compliance Program을 반영하였으며 공공, 민간 또는 비영리 부문에 관계없이 모든 조직에 적용 가능한 규격입니다.

필요성

❶ 임직원의 규정준수에 대한 동기부여와 인식도 향상
❷ 국내·외 관련법들의 양형 참작사유 적용 가능성
❸ 입찰 참여시 규정준수 요구사항 충족(적격성 근거 자료)
❹ 강화되는 규제에 보다 효과적으로 대응
❺ 기업의 글로벌 스탠다드화-투명성 사업 활동의 전제 조건화
❻ 예방차원의 법률 비즈니스 안전장치 마련(준법 건강검진)
❼ 컴플라이언스 수준진단, 업무 투명성 제고, 신고문화 활성화 등
❽ 컴플라이언스 리스크(의무식별) 관리

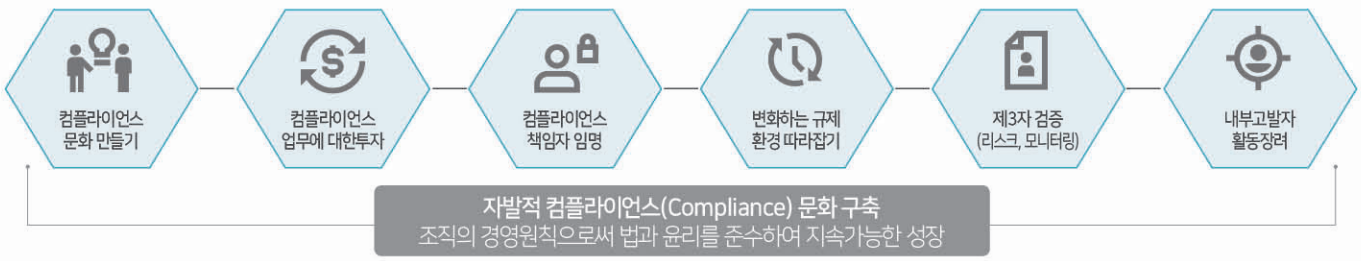
기대효과

❶ 규제기관이나 사법기관에서 조직의 제재 부과시 벤치마크로 활용
❷ 선진화된 시스템으로 법률위반 리스크 사전 예방 및 감소
❸ 이해관계자(임직원, 정부, 고객, 투자자 등)에 대한 신뢰성 및 조직 가치 향상(CSR, 윤리경영 등 실천의지 입증)
❹ 경영 불안감 해소(내부통제 강화)
❺ 경쟁사에 대한 비교 우위
❻ 법 위반 감소로 관련된 비용 및 벌칙 최소화(법과 원칙 준수)
❼ 상호 인정을 통한 간접비용(보험료 등) 절감



법규준수

자발적으로 관련 법규 등 의무사항을 사전 예방 준수하는 시스템



ISO/IEC 27001(정보보안경영시스템)

Information Security Management System

KCI 한국준법진흥원 KOREA COMPLIANCE INITIATIVE

개 요

ISO/IEC 27001은 2005년 11월 제정되어 조직의 소중한 정보 자산 관리와 보호를 지원하는 규격으로 정보보안에 대한 요구사항을 만족함을 제3자 인증이 가능한 글로벌 스탠다드 인증제도 입니다. 정보보호 정책, 통신·운영, 접근통제, 정보보호 사고 대응 등 정보보호 관리 11개 영역, 133개 항목에 대해 얼마나 잘 계획하고 구현하며, 점검하고, 개선하는가를 평가하고 이에 대한 인증을 취득하게 됩니다. 정보보안의 실패는 곧 기업의 위기로 연결되는 시대입니다. 정보보안경영시스템은 비즈니스를 수행하고 이윤을 창출하기위해 생성된 유형·무형 정보들의 기밀성 (Confidentiality), 무결성 (Integrity), 가용성 (Availability) 을 보장하여기업의 리스크를 제거하고 지속적인 생존과 성공을 추구합니다.

국내 인증 : ISMS(Information Security Management System)

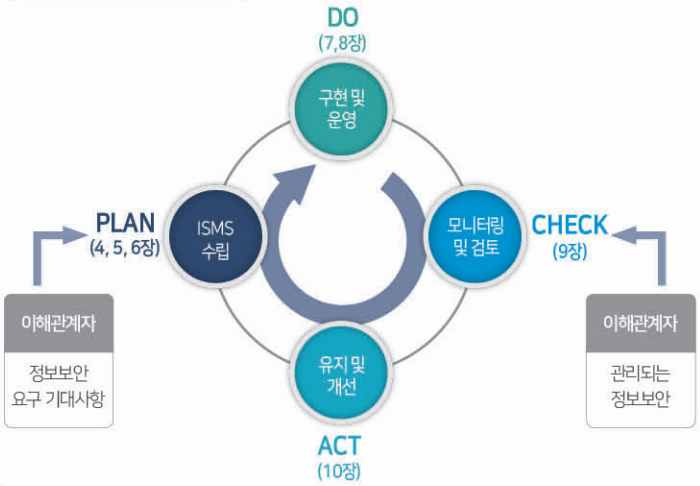
필요성

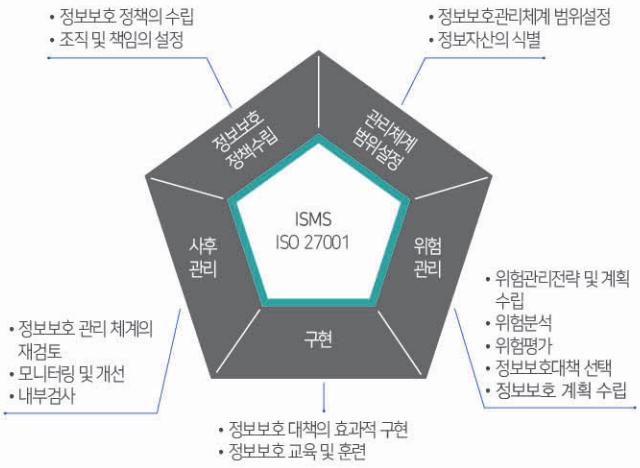
❶ 전 임직원의 정보보안 동기부여와 인식확산
❷ 정보보안 관련 법규 및 규정 준수를 개관적으로 입증 가능
❸ 거래 관계에서 고객 정보보호가 최우선임을 입증
❹ 정보보안 위협과 문제에 대한 대비가능
❺ 정기적인 심사를 통해 성과 및 개선 사항을 지속적으로 모니터링

기대효과

❶ 보안침해 최소화를 통한 비즈니스 연속성 보장
❷ 정보보안 자원 및 활동의 유기적 관리
❸ 정보보안 업무의 실수 및 낭비 제거
❹ 의사결정 지원으로 정보보안 환경조성
❺ 이해관계자에게 정보보안 신뢰도 향상
❻ 제품 및 서비스 관련 보안 책임에 대한 간접 보증

기본모델





표준요구사항의 구조

4 조직의 상황
4.1 | 조직과 상황에 대한 이해
4.2 | 이해당사자의 요구와 기대에 대한 이해
4.3 | 정보보호 경영시스템의 적용범위 결정
4.4 | 정보보호 경영시스템

5 리더십
5.1 | 리더십과 의지
5.2 | 정책
5.3 조직의 역할, 책임, 권한

6 기획
6.1 | 위험과 기회에 따른 조치
6.3 | 정보보호 목표 및 달성 계획

7 지원
7.1 | 자원
7.2 | 적격성
7.3 | 인식
7.4 | 의사소통
7.5 | 문서 정보

8 운영
8.1 | 운용 계획 및 통제
8.2 | 정보보호 위험평가
8.3 정보보호 위험처리

9 성과 평가
9.1 | 모니터링, 측정, 분석 및 평가
9.2 | 내부심사
9.3 | 경영검토

10 개선
10.1 | 부적합 및 시정조치
10.2 | 지속적 개선

부속서 A(규정) 통제 목적과 통제
A.5 | 정보보호 정책
A.6 | 정보보호 조직
A.7 | 인적자원 보안
A.8 | 자산관리
A.9 | 정근통테
A.10 | 암호화
A.11 | 물리적 및 환경적 보안
A.12 | 운영 보안
A.13 | 통신 보안
A.14 | 시스템 도입, 개발, 유지보수
A.15 | 공급자 관계
A.16 | 정보보호 사고 관리
A.17 | 업무연속성 관리의 정보보호 측면
A.18 | 준거성

ISO/IEC 27701(개인정보경영시스템)

Privacy Information Management System

개 요

국제표준인 ISO/IEC 27701은 국제 표준화 기구에서 2019년 8월 제정한 개인정보의 수집과 처리 등 보호에 대한 새로운 글로벌 스탠다드 인증규격입니다.
제3자 인증이 가능한 규격으로 조직이 개인정보보호를 위해 갖추어야 하는 요구사항과 가이드라인을 동시에 제공하고 있으며 조직이 개인식별정보(PII)를 보호하기 위한 프로세스의 정의하며 특히 기술이 아직 유효하지 않은 세계에서 중요한 정보를 제공합니다.
ISO/IEC 27701은 ISO/IEC 27001의 확장판으로 인증을 받기 원하는 조직은 ISO/IEC에 대한 인증을 보유하고 있어야 인증이 가능합니다.

국내 인증 : ISMS-P(Personal Information & Information Security Management System, 구 PIMS)

필요성

❶ GDPR에 명시된 개인정보보호 요건 및 기타 데이터 보호규정 충족
❷ 전 임직원의 개인정보 보호 중요성의 동기부여와 인식확산
❸ 개인정보보호 관련 법규 및 규정 준수를 개관적으로 입증 가능
❹ PII 처리과정이 상호관련이 있는 비즈니스 파트너사와 거래가능
❺ ISO/IEC 27001과 쉽게 통합 가능
❻ 정기적인 심사를 통해 성과 및 개선 사항을 지속적으로 모니터링

기대효과

❶ 개인정보 위반 리스크 감소
❷ 이해관계자에게 개인정보 보호 관리 능력에 대한 신뢰 구축
❸ 조직내 역할과 책임의 명확화
❹ 보안침해 최소화를 통한 비즈니스 연속성 보장
❺ 업무의 실수 및 낭비 제거
❻ 의사결정 지원으로 보안 환경조성
❼ 제품 및 서비스 관련 보안 책임에 대한 간접 보증

ISO 27701

▶ ISO/IEC 27701;
Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information managments
- Requirements and guidelines

▶ ISO/IEC 27001;
Information technology - Security techniques - Information security managments systems - Requirements

▶ ISO/IEC 27002;
Information technology - Security techniques - Code of practice for Information security controls

▶ ISO/IEC 27018;
Information technology - Security techniques - Code of practice for protection of personally identifiable information
(PII) in publice clouds acting as PII processors

▶ ISO/IEC 27017;
Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for clouds services

▶ ISO/IEC 29001;
Information technology - Security techniques - Privacy frammework

KOREA COMPLIANCE INITIATIVE

KCI

한국준법진흥원

"신뢰성 있는 인증 서비스 제공"을 약속드립니다.

서울특별시 금천구 서부샛길 606,B동 2208호

02)6334-6605

kci@grc.or.kr