KOSHA GUIDE
Z - 51 - 2022

컴플라이언스 경영시스템에 관한 지침

2022. 12.

한국산업안전보건공단

안전보건기술지침의 개요

○ 작성자 : 한국안전문화진흥원

○ 제·개정 경과

- 2022년 12월 리스크관리분야 표준제정위원회(제정)

○ 관련규격 및 자료

- 안전보건경영시스템

○ 기술지침의 적용 및 문의

- 이 기술지침에 대한 의견 또는 문의는 한국산업안전보건공단 홈 페이지 안전보건기술지침 소관 분야별 문의처 안내를 참고하시기 바랍니다.
- 동 지침 내에서 인용된 관련규격 및 자료 등에 관하여 최근 개정 본이 있을 경우 해당 최근 개정 본을 참고하시기 바랍니다.

공표일자 : 2022년 12월 31일
제 정 자 : 한국산업안전보건공단 이사장

KOSHA GUIDE
Z - 51 - 2022

컴플라이언스 경영시스템에 관한 지침

1. 목 적

이 가이드라인의 목적은 컴플라이언스 관련 위험에 대하여 효과적이고 건전한 경영이 여러 이점으로 인해 추구하고 취할 수 있는 기회로 간주되어야한다는 점을 고려하여 조직이 긍정적인 컴플라이언스 문화를 개발하고 확산 되도록 지원하는 것이다. 여러 이점은 비즈니스 기회 및 지속 가능성 개선, 조직의 평판과 신뢰성 보호 및 향상, 이해 관계자의 기대 고려, 컴플라이언스 리스크를 효과적이고 효율적으로 관리하는 조직의 의지 표명, 지속적인 성공을 달성하기 위한 조직의 역량에 대한 제 3자의 신뢰도 향상, 수반되는 비용 및 평판 손상으로 발생하는 위반 위험 최소화 등을 포함한다.

2. 적용 범위

이 가이드라인은 조직 내에서 효과적인 컴플라이언스 경영시스템을 수립, 개발, 실행, 평가, 유지, 개선하기 위한 지침(안내서)을 제공하고, 요구사항을 규정하고 있다. 활동의 유형, 규모 및 성격에 관계없이 모든 유형의 조직에 적용되며 조직이 공공, 민간 또는 비영리 부문인지 여부에 관계없이 적용된다. 이 가이드라인에 명시된 모든 요구 사항은 조직이 별도의 기능으로 지배기구를 가지고 있지 않은 경우 최고 경영진에게 적용된다.

3. 용어의 정의

3.1 조직: 조직의 목표를 달성하기 위한 책임, 권한 및 관계를 가지고 있는 기능을 자체적으로 보유한 사람 또는 그룹

[비고 1] 조직의 개념은 개인사업자, 회사, 법인, 상사, 기업, 당국, 파트너십, 자선단체, 협회 또는 이들의 부분 또는 조합으로, 민간 또는 공공부문을 포함하나 이에 국한하지 않는다.

[비고 2] 조직이 더 큰 조직의 일부인 경우 "조직"이라는 용어는 컴플라이언스 경영 시스템의 범위 내에 있는 더 큰 조직의 일부만 언급한다.

3.2 이해관계자: 의사결정 또는 활동에 영향을 줄 수 있거나 또는 영향을 받을 수 있거나 또는 그들 자신이 영향을 받는다는 인식을 할 수 있는 사람 또는 조직

3.3 최고경영자: 최고 계층에서 조직을 지휘하고 관리하는 사람 또는 그룹

[비고 1] 최고경영자는 조직 내에서 권한을 위임하고 자원을 제공하는 권한을 가진다.

[비고 2] 경영시스템의 적용범위가 단지 조직의 일부만을 포함하는 경우, 조직의 그 일부분을 지휘하고 관리하는 사람들을 최고경영자라고 한다.

[비고 3] 이 가이드라인의 목적을 위하여 최고경영자라는 용어는 최고경영진을 의미한다.

3.4 경영시스템: 방침과 목표를 수립하고 그 목표를 달성하기 위한 프로세스를 수립하기 위한, 상호 관련되는 또는 상호 작용하는 조직 요소의 집합

[비고 1] 경영시스템은 단일 또는 다수 분야를 다룰 수 있다.

[비고 2] 경영시스템 요소는 조직의 구조, 역할과 책임, 기획 및 운영을 포함한다.

3.5 방침: 최고 경영자에 의해 공식적으로 표명된 조직의 의도 및 방향

3.6 목표: 달성되어야 할 결과

[비고 1] 목표는 전략적, 전술적, 또는 운영적일 수 있다.

[비고 2] 목표는(예: 재무, 안전보건, 그리고 환경목표) 다른 분야와 관련될 수 있고, 상이한 계층[예: 전략적, 조직 - 전반, 프로젝트, 제품, 그리고 프로세스에 적용될 수 있다.

[비고 3] 목표는 다른 방식, 예를 들면, 컴플라이언스 목표로서 의도된 결과, 목적, 운영기준으로, 또는 비슷한 의미를 갖는 다른 용어[예: 목표(aim), 목표(goal), 세부목표(target)]의 사용에 의해 표현될 수 있다.

[비고 4] 조직은 컴플라이언스 경영시스템의 맥락에서 특정 결과를 달성하기 위해서는 컴플라이언스 목표는 조직에 의해서 수립되고, 컴플라이언스 방침과 일관성이 있다.

3.7 리스크: 불확실성의 영향

[비고 1] 영향은 긍정적 또는 부정적 예상으로부터 벗어나는 것이다.

[비고 2] 불확실성은 사건, 그 결과 또는 가능성에 대한 이해 또는 지식과 관련된 정보가 부족하거나 부분적으로 부족한 상태이다.

[비고 3] 리스크는 흔히 잠재적인 “사건”(KS A ISO Guide 73:2009, 3.5.1.3)과

"결과"(KS A ISO Guide 73:2009, 3.6.1.3), 또는 이들의 조합을 특징으로 한다.

[비고 4] 리스크는 흔히(주변 환경의 변화를 포함하는) 사건의 결과와 연관된 발생"가능성"(KS A ISO Guide 73:2009, 3.6.1.1)의 조합으로 표현된다.

3.8 프로세스: 결과를 제공하기 위해 입력(input)을 사용하거나 변형하는 상호관련 되거나 상호 작용하는 활동의 집합

[비고 1] 프로세스의 결과를 출력, 제품 또는 서비스라고 하는지 여부는 참조의 문맥에 따라 다르다.

3.9 역량/적격성: 의도된 결과를 달성하기 위해 지식 및 스킬을 적용하는 능력

3.10 문서화된 정보: 조직에 의해 관리되고 유지되도록 요구되는 정보 및 정보가 포함되어 있는 매체

[비고 1] 문서화된 정보는 특정 형태 및 매체일 수 있으며 특정 출처로부터 올 수 있다.

[비고 2] 문서화된 정보는 관련 프로세스들(3.8)를 포함하는 경영시스템, 조직에서 운용하기 위해 작성한 정보(문서화), 달성된 결과의 증거(기록)이다.

3.11 성과: 측정 가능한 결과

[비고 1] 성과는 정량적 또는 정성적 발견 사항과 관련될 수 있다.

[비고 2] 성과는 활동, 프로세스, 제품(서비스 포함), 시스템의 관리 또는 조직의 경영에 관련될 수 있다.

3.12 지속적 개선: 성과를 향상시키기 위하여 반복하는 활동

3.13 효과성: 계획된 활동이 실현되고 계획된 결과가 달성되는 정도

3.14 요구사항: 일반적으로 묵시적 또는 의무적이라고 언급된 '니즈' 또는 '기대'

[비고 1] 일반적으로 묵시적"이라 함은 조직 및 이해관계자에 대한 관습과 일반적 관행이 고려되는 상황에서 요구 및 기대가 암시됨을 의미한다.

[비고 2] 규정된 요구사항은 명시된 것으로, 문서화된 정보가 이에 해당한다.

3.15 적합: 요구사항의 충족

3.16 부적합: 요구사항의 불충족

[비고 1] 부적합이 반드시 비준수라는 것은 아니다.

3.17 시정조치: 부적합의 원인을 제거하고 재발을 방지하기 위한 조치

3.18 심사: 심사기준이 충족되는 정도를 결정하기 위해 증거를 확보하고 객관적으로 평가하기 위한 체계적이고 독립적인 프로세스

[비고 1] 심사는 내부심사(1자심사), 또는 외부심사(2자 또는 3자)가 있으며, 결합심사(둘 이상의 분야가 결합된 형태)가 있을 수 있다.

[비고 2] 내부심사는 조직이 자체적으로 수행하거나 또는 조직을 대신하는 외부 인원에 의해 수행된다.

[비고 3] “심사 증거” 또는 “심사 기준”은 ISO19011에 정의되어 있다.

[비고 4] 독립성은 심사되고 있는 활동에 대한 책임으로부터의 자유, 또는 편견과 이해의 충돌로부터의 자유에 의해 실증되어야 한다(객관성, 공정성).

3.19 측정: 값을 결정하는 프로세스

3.20 모니터링: 시스템, 프로세스 또는 활동의 상태를 결정 하는 것

[비고 1] 상태를 결정하기 위해서는 확인, 감독 또는 심도 있는 관찰이 필요할 수 있다.

3.21 지배기구(이사회): 조직의 활동, 지배구조(governance) 및 방침에 대한 최종 책임과 권한을 소유하며, 최고 경영자로부터 보고를 받고 최고경영자에게 책임을 부여하는 개인 또는 그룹

[비고 1] 모든 조직, 특히 소규모 조직이 최고경영진과 별도로 구분된 지배기구를 갖추어야 하는 것은 아니다.

[비고 2] 지배기구에는 이사회, 위원회, 감독위원회, 수탁자 및 감독관을 포함할 수 있으나 이에 국한 되지는 않는다.

3.22 인원 : 국내법 및 관행상 고용관계로 인식되는 관계 또는 조직의 활동에 의존하는 계약 속에 있는 개인들

3.23 컴플라이언스 책임자: 컴플라이언스 경영시스템에 관한 책임을 가지고 있는 사람 또는 그룹

[비고 1] 가급적이면 한 개인에게 컴플라이언스 경영에 대한 전반적인 책임이

할당되어질 것이다.

3.24 컴플라이언스 리스크: 조직의 컴플라이언스 목표에 대한 비준수에 따른 발생 가능성 및 결과

3.25 컴플라이언스 의무: 조직이 의무적으로 준수해야하는 요구 사항 뿐만 아니라 자발적으로 준수하기로 선택한 요구 사항

3.26 컴플라이언스: 조직의 모든 컴플라이언스 의무 충족

3.27 비준수: 컴플라이언스 의무의 불충족

3.28 컴플라이언스 문화: 가치, 윤리, 신념 및 행동은 조직 전체에 존재하며 조직의 구조 및 제어 시스템과 상호 작용하여 컴플라이언스에 도움이 되는 행동 규범을 생성

3.29 행동: 고객, 직원, 공급 업체, 시장 및 지역사회의 결과에 영향을 미치는 조직의 행동 및 관행

3.30 3자: 조직과 독립적인 인원 또는 인정기구
[비고 1] 모든 비즈니스 관계자는 제 3자이지만 모든 제 3자가 비즈니스 관계자는 아니다.

3.31 절차: 활동 또는 프로세스를 수행하기 위한 구체적인 방법

3.32 갈등: 갈등이란 개인 및 집단 사이의 목표나 이해관계의 차이로 서로 적대시하거나 충돌하는 것이라 정의된다. 사업장에서 갈등은 필요 불가결한 것이며, 예방도 필요하지만 어떻게 해소하는지가 더 중요하다. 갈등을 통해 개인 및 사업장의 문제점을 드러내어 통합 및 발전의 계기가 될 수 있고, 침체된 사업장 분위기에 활력을 불어 넣어주는 순기능도 있다.

3.33 협상: 협상이란 갈등을 관리하고 상호 간에 만족스러운 결과를 도출해내기 위한 갈등 해소의 기술로서 오늘날 모든 관리자에게 중요한 직무 관련 역량이다.

4. 조직 상황

4.1 조직과 조직상황의 이해

4.1.1 조직은 조직의 목적과 관련이 있으며 컴플라이언스 경영시스템의 의도 된 결과를 달성하는 능력에 영향을 미치는 외부 및 내부 이슈를 결정해야 한다. 이를 위해 조직은 다음 사항에 국한되지 않는 광범위한 이슈를 고려해야 한다.

(1) 전략, 성격, 규모 및 규모의 복잡성과 조직 활동 및 운영의 지속 가능성을 포함한 비즈니스 모델

(2) 제 3자와의 비즈니스 관계의 성격 및 범위

(3) 법적 및 규제적 상황

(4) 경제 상황

(5) 사회적, 문화적, 환경적 상황

(6) 기술을 포함한 내부 구조, 방침, 프로세스, 절차 및 자원

(7) 컴플라이언스 문화

4.2 이해관계자들의 니즈와 기대의 이해

4.2.1 조직은 다음 사항을 정하여야 한다.

(1) 컴플라이언스 경영시스템에 관련된 이해관계자

(2) 이러한 이해관계자와 관련되는 요구사항

4.2.2 이러한 요구 사항은 컴플라이언스 경영시스템을 통해 관리 될 것이다.

4.3 컴플라이언스 경영시스템의 적용 범위 결정

4.3.1 조직은 컴플라이언스 경영시스템의 적용범위를 설정하기 위해 컴플라이언스 경영시스템의 경계와 적용 가능성을 결정하여야 한다.

[비고] 컴플라이언스 경영시스템의 범위는 특히 조직이 거대조직의 일부일 경우 조직이 직면하고 있는 주요 컴플라이언스 리스크와 컴플라이언스 경영시스템이 적용 될 지리적 또는 조직적 범주를 명확히 하여야 한다.

4.3.2 적용범위를 정할 때, 조직은 다음 사항을 고려하여야 한다.

(1) 4.1에 언급된 외부와 내부 이슈

(2) 4.2, 4.4 및 4.5에 언급된 요구사항

4.3.3 이 적용범위는 문서화된 정보로 이용 가능하여야 한다.

4.4 컴플라이언스 경영시스템

4.4.1 조직은 이 가이드라인의 요구사항에 따라 필요한 프로세스들과 그 프로세스들의 상호 작용을 포함하는 컴플라이언스 경영시스템을 수립, 개발, 실행, 평가, 유지 및 지속적으로 개선하여야 한다.

4.4.2 컴플라이언스 경영시스템은 조직의 상황을 고려하여 조직의 가치, 목표, 전략 및 컴플라이언스 리스크를 반영하여야 한다.

4.5 컴플라이언스 의무

4.5.1 조직은 활동, 제품 및 서비스로부터 기인한 컴플라이언스 의무를 체계적으로 식별하고 운영에 영향을 미치는 영향을 평가해야 한다. 조직은 다음을 위한 프로세스를 갖추어야 한다.

(1) 지속적인 컴플라이언스를 보장하기 위하여 신규 및 변경된 컴플라이언스 의무 식별

(2) 식별된 변경의 영향을 평가하고 컴플라이언스 의무 경영에 필요한 변경의 실현

4.5.2 조직은 컴플라이언스 의무에 대한 문서화된 정보를 유지해야 한다.

4.6 컴플라이언스 리스크 평가

4.6.1 조직은 컴플라이언스 리스크 평가에 근거한 조직의 컴플라이언스 리스크를 식별, 분석 및 평가 하여야 한다.

4.6.2 조직은 컴플라이언스 의무를 활동, 제품, 서비스 및 운용 관련 측면에 관련시킴으로써 컴플라이언스 리스크를 식별하여야 한다.

4.6.3 조직은 아웃소싱 및 제3자 프로세스와 관련된 컴플라이언스 리스크를 평가해야 한다.

4.6.4 컴플라이언스 리스크는 정기적으로 그리고 환경 또는 조직의 상황에 중대한 변화가 있을 때마다 평가해야 한다.

4.6.5 조직은 컴플라이언스 리스크 평가 및 컴플라이언스 리스크를 해결하기 위한 조치에 대한 문서화된 정보를 유지하여야 한다.

5. 리더십

5.1 리더십과 의지표명

5.1.1 지배구조 및 최고경영자

(1) 지배기구와 최고경영자는 다음과 같은 방법으로 컴플라이언스 경영시스템에 대한 리더십과 의지를 보장하여야 한다.

(가) 컴플라이언스의 방침 및 컴플라이언스 목표가 수립되고 조직의 전략적 방향과 일치되는지 확인

(나) 컴플라이언스 경영시스템 요구사항이 조직의 비즈니스 프로세스에 통합

(다) 컴플라이언스 경영시스템에 필요한 자원의 사용 가능여부 확인

(라) 효과적인 컴플라이언스경영 및 컴플라이언스 경영시스템 요구사항 준수의 중요성 전달

(마) 컴플라이언스 경영시스템이 의도한 결과를 달성하도록 보장

(바) 컴플라이언스 경영시스템의 효율성에 기여하도록 인원들을 지도 및 지원

(사) 책임영역에 적용되는 리더십을 입증하기 위해 기타관련 경영역할 지원

[비 고] 이 가이드라인에서 "비즈니스"에 대한 언급은 조직의 존재 목적에 핵심적인 활동을 의미하는 것으로 광범위하게 해석 될 수 있다.

(2) 지배기구와 최고경영자는 아래와 같아야 한다.

(가) 조직의 가치를 확립하고 유지

(나) 컴플라이언스 목표를 달성하기 위한 방침, 절차 및 프로세의 개발 및 실행

(다) 비준수 사례를 포함하여 컴플라이언스 문제에 대해 적시에 알리고 적절한 조치가 취해 졌는지 확인

(라) 컴플라이언스에 대한 의지가 유지되고 비준수 및 비준수에 대한 행동이 적절하게 처리 되는지 확인

(마) 준수책임이 직무분장에 적절하게 포함

(바) 준수기능에 대한 지정 및 지명

(사) 8.3에 따라 문제를 제기하고 해결하기 위한 시스템이 확립되었는지 확인

5.1.2 컴플라이언스 문화(Compliance culture)

(1) 조직은 조직 내 모든 계층 내에서 컴플라이언스 문화를 개발, 유지 및 장려 하여야 한다.

(2) 지배기구, 최고경영진 및 경영자는 조직 전체에 요구되는 행동 및 공표된 행동기준에 대한 적극적이고 가시적이며 일관된 지속적인 의지를 보여야 한다.

5.1.3 컴플라이언스 거버넌스

(1) 지배기구와 최고경영진은 다음 원칙을 보장하여야 한다.

(가) 컴플라이언스 감시기구에 대한 지배기구의 직접접근

(나) 컴플라이언스 감시기구의 독립성

(다) 컴플라이언스 감시기구에 대한 적절한 권한과 역량

[비고 1] 직접적인 접근은 다음을 포함 할 수 있다: 지배기구에 대한 직접적인 보고 체계, 지배기구에 대한 정기적인 보고서 제출 및 회의 참여
[비고 2] 독립성은 컴플라이언스 감시기구 운영시 어떠한 간섭 및/ 또는 압력이 없음을 의미한다.

5.2 컴플라이언스 방침

5.2.1 지배기구와 최고경영자는 컴플라이언스 방침을 수립 하여야 한다.

(1) 조직의 목적에 적합

(2) 컴플라이언스 목표를 확립하기 위한 프레임워크(구조)를 제공

(3) 적용 가능한 요구사항들을 충족하기 위한 의지를 포함

(4) 컴플라이언스 경영시스템의 지속적인 개선에 대한 의지를 포함

5.2.2 컴플라이언스 방침은 아래와 같아야 한다.

(1) 조직의 가치, 목표 및 전략과 일치

(2) 조직의 컴플라이언스 의무 준수를 요구

(3) 5.1.3항에 따른 컴플라이언스 거버넌스 원칙을 지원

(4) 컴플라이언스 기능을 참조하고 설명

(5) 방침, 절차 및 지침과 함께 조직의 준수 의무를 준수하지 않을 경우의 결과를 설명

(6) 보복에 대한 두려움 없이 우려 제기를 촉진

(7) 모든 직원이 원칙과 의도를 쉽게 이해 할 수 있도록 일반적인 언어로 작성

(8) 적절하게 실행되고 적용 됨

(9) 문서화된 정보로서 이용 가능

(10) 조직 내에서 전달 되어야함

(11) 이해관계자들이 적절하게 이용 가능하여야 함

5.3 역할, 책임 및 권한

5.3.1 지배기구 및 최고경영자

(1) 지배기구와 최고경영자는 관련 책임과 권한에 대하여 조직내에서 할당되고 전달되어야 한다. 지배기구와 최고경영자는 다음에 대한 책임과 권한을 할당해야 한다.

(가) 컴플라이언스 경영시스템이 이 가이드라인의 요구사항을 준수함을 보장

(나) 컴플라이언스 경영시스템의 성과를 지배기구와 최고경영자에게 보고

(2) 지배기구

(가) 최고경영진이 컴플라이언스 목표의 달성에 관련되어 측정 하도록 보장하여야 한다.

(나) 컴플라이언스 경영시스템의 운영에 관해 최고경영진에 대한 감시를 수행하여야 한다.

(3) 최고경영진

(가) 컴플라이언스 경영시스템을 수립, 개발, 이행, 평가, 유지 및 개선하기 위한 적절하고 적합한 자원을 할당

(나) 컴플라이언스 성과에 대해 적시에 보고하는 효과적인 시스템이 마련되어 있는지 확인

(다) 전략 및 운영 목표와 컴플라이언스 의무 간의 일치를 보장

(라) 징계 조치 및 결과를 포함한 책임 매커니즘을 수립하고 유지

(마) 컴플라이언스 성과가 직원의 성과 평가에 통합됨을 보장

5.3.2 컴플라이언스 책임자(준수 기능)

(1) 컴플라이언스 책임자(준수 기능)는 다음을 포함한 컴플라이언스 경영시스템의 운영에 대한 책임이 있다

(가) 컴플라이언스 의무의 식별을 용이하게 함

(나) 컴플라이언스 리스크평가 문서화

(다) 컴플라이언스 경영시스템을 컴플라이언스 목표와 통합

(라) 컴플라이언스 성과 모니터링 및 측정

(마) 시정조치의 필요성을 식별하기 위해 컴플라이언스 경영시스템의 성과를 분석 및 평가

(바) 컴플라이언스 보고 및 문서화 시스템 구축

(사) 컴플라이언스 경영시스템이 주기적으로 검토 되도록 보장

(아) 우려 사항을 제기하고 우려 사항을 해결하기 위한 시스템 구축

(2) 컴플라이언스 책임자(준수 기능)는 다음사항을 감독하여야 한다.

(가) 식별된 컴플라이언스 의무를 달성하기 위한 책임이 조직 전체에 적절하게 할당

(나) 컴플라이언스 의무가 방침, 프로세스 및 절차에 통합

(다) 모든 관련인원을 필요에 따라 교육을 받음

(라) 컴플라이언스 성과 지표 설정

(3) 컴플라이언스 책임자(준수기능)는 다음을 제공해야 한다.

(가) 컴플라이언스 방침, 프로세스 및 절차에 대한 자원에 접근할 수 있는 인원

(나) 컴플라이언스와 관련한 문제에 대하여 조직에게 조언을 제공

[비고] 컴플라이언스 책임자의 구체적인 의무는 컴플라이언스에 대한 조직의 책임의 가진 다른 인원들의 책임을 완화시킬 수 없다.

(4) 조직은 컴플라이언스 책임자(준수기능)에 다음에 대한 접근 권한을 부여해야 한다.

(가) 고위 의사 결정자 및 의사 결정 과정 초기에 기여할 수 있는 기회

(나) 조직의 모든 계층

(다) 필요한 모든 직원, 문서화 된 정보 및 데이터

(라) 관련 법률, 규정, 규칙 및 조직 표준에 대한 전문가의 조언

5.3.3 경영진

(1) 경영진은 책임 범위 내에서 컴플라이언스에 대한 책임이 존재 한다.

(가) 컴플라이언스 책임자(준수 기능)에게 협력하고 지원하며, 인원들도 동일하게 실행 하도록 독려

(나) 관리되는 모든직원이 조직의 컴플라이언스 의무, 방침, 프로세스 및 절차를 준수하는지 확인

(다) 운영상의 컴플라이언스 리스크를 식별하고 의사소통

(라) 책임범위 내에서 기존의 경영 관행 및 절차에 컴플라이언스 의무를 통합

(마) 컴플라이언스 교육 활동에 참여 및 지원

(바) 컴플라이언스 의무에 대한 인원들의 인식을 발전시키고 교육훈련 및 역량 요구사항을 충족 하도록 지도

(사) 필요에 따라 컴플라이언스 관련 사건 및 이슈의 관리 및 해결에 적극적으로 참여

(아) 일단 시정조치의 필요성이 식별되면 적절한 시정조치를 권장하고 실행

5.3.4 인원들

(1) 조직의 컴플라이언스 의무, 방침 및 절차 및 프로세스를 준수

(2) 컴플라이언스 우려, 이슈 및 실패를 보고

(3) 필요에 따라 교육에 참여

6. 기획

6.1 리스크와 기회를 다루는 조치

6.1.1 컴플라이언스 경영시스템을 기획시, 조직은 4.1에서 언급된 이슈와 4.2에서 언급한 요구사항을 고려하고 다음사항을 다뤄야 하는 리스크와 기회를 결정하여야 한다.

(1) 컴플라이언스 경영시스템이 의도한 성과를 달성할 수 있다는 것을 보증

(2) 바람직하지 않은 영향(효과)을 예방, 발견, 감소

(3) 지속적 개선을 달성

6.1.2 컴플라이언스 경영시스템을 기획시, 조직은 다음 사항을 고려해야 한다.

(1) 컴플라이언스 목표

(2) 식별된 컴플라이언스 의무

(3) 컴플라이언스 리스크 평가의 결과

6.2 컴플라이언스 목표와 목표 달성 기획

6.2.1 조직은 관련 기능과 계층에서 컴플라이언스 목표를 수립하여야 한다. 컴플라이언스 목표는 다음과 같아야 한다.

(1) 컴플라이언스 방침과 일관성이 있어야 함

(2) (가능한 경우) 측정 가능해야 함

(3) 적용 가능한 요구사항들을 고려해야 함

(4) 모니터링 되어야 함

(5) 의사소통되어야 함

(6) 적절하게 업데이트 되어야 함

(7) 문서화된 정보를 보유하여야 함

6.2.2 컴플라이언스 목표 달성 방법을 기획할 때, 조직은 다음사항을 결정하여야 한다.

(1) 무엇을 할 것인가

(2) 필요 자원

(3) 누가 책임을 질것인가

(4) 완료시기

(5) 결과에 대한 평가방법

6.3 변경 계획

6.3.1 조직이 컴플라이언스 경영시스템의 변경 필요성을 판단하면 계획된 방식으로 변경을 수행해야 한다.

7. 지원

7.1 자원

7.1.1 조직은 조직의 규모, 복잡성, 구조와 운용에 적절한 컴플라이언스 경영시스템을 수립, 실행, 평가, 유지 및 지속적으로 개선하기 위하여 필요한 자원들을 정하고 제공하여야 한다.

7.2 역량

7.2.1 (조직) 일반

(1) 조직의 관리 하에 컴플라이언스 경영시스템 성과에 영향을 주는 업무를 수행하는 인원들의 필요한 역량 결정

(2) 적절한 학력, 교육훈련 또는 경험을 근거로 이러한 인원들이 적격하다는 것을 보장

(3) 적용 가능한 경우, 필요한 역량을 갖추기 위한 조치를 취하고 그 조치의 효과성을 평가

(4) 역량의 증거로 적절한 문서화된 정보를 보유 하여야 함

[비 고] 적용할 수 있는 조치에는 예를 들면, 현재 고용된 인원에 대한 교육훈련 제공, 멘토링 또는 재배치가 포함 되며, 이들에 대한 고용 또는 계약을 포함할 수 있다.

7.2.2 고용 프로세스

(1) 조직의 모든 인원과 관련하여, 조직은 다음과 같은 프로세스를 개발, 수립, 실행 및 유지해야 한다.

(가) 고용 조건으로 컴플라이언스 의무, 방침과 프로세스 및 절차를 준수할 것을 인원들에게 요구

(나) 고용이 시작된 이후 적절한 기간 내 인원에 대해 해당 방침과 관련된 컴플라이언스 방침 및 교육 교재를 받거나 이에 대한 접근 권한을 제공

(다) 조직의 컴플라이언스 의무, 방침, 프로세스 및 절차를 위반한 인원에 대하여 적절한 징계 조치를 취함

(2) 고용 프로세스 내에 조직은 직무 및 인원들이 제기한 컴플라이언스 리스크를 고려하고 채용 및 승진 전에 필요한 실사(due diligence) 절차를 적용 하여야 한다.

(3) 조직은 비준수를 방지하기 위한 적절한 조치가 있음을 입증하기 위해 성과목표, 성과보너스 및 기타 인센티브를 주기적으로 검토할 수 있는 프로세스를 실행하여야 한다.

7.2.3 교육(훈련)

(1) 조직은 고용 시작 시점부터 조직이 결정한 계획된 간격으로 관련 직원에게 주기적인 교육을 제공 하여야 한다. 교육은 다음과 같다.

(가) 인원의 역할 및 노출될 수 있는 컴플라이언스 리스크에 적절

(나) 효과성에 대한 평가

(다) 정기적으로 검토

(2) 식별 된 컴플라이언스 리스크를 고려하여 조직은 조직에 컴플라이언스 리스크를 초래할 수 있는 제 3자에 대한 컴플라이언스 인식 및 교육을 관리하기 위한 절차를 실행해야 한다.

(3) 교육 기록은 문서화된 정보로 유지되어야 한다.

7.3 인식

7.3.1 조직의 관리 하에 업무를 수행하는 인원들은 다음 사항을 인식하여야 한다.

(1) 컴플라이언스 방침

(2) 개선된 컴플라이언스 성과의 이점을 포함한 컴플라이언스 경영시스템의 효율성에 대한 그들의 기여

(3) 컴플라이언스 경영시스템의 요구사항에 준수하지 않는다는 것의 의미

(4) 컴플라이언스 문제를 제기하기 위한 수단 및 절차

(5) 컴플라이언스 방침 및 역할과 관련된 컴플라이언스 의무의 관계

(6) 컴플라이언스 문화 지원의 중요성

7.4 의사소통

7.4.1 조직은 다음 사항을 포함하는 컴플라이언스 경영시스템에 관련된 내부 및 외부 의사소통을 결정하여야 한다.

(1) 의사소통 내용

(2) 의사소통 시기

(3) 의사소통 대상

(4) 의사소통 방법

7.4.2 조직

(1) 의사소통 요구를 고려할 때 다양한 측면과 잠재적인 장벽을 고려

(2) 프로세스를 수립하는데 이해관계자의 관점을 고려

(3) 의소소통 프로세스를 수립할 때 컴플라이언스 문화, 목적 및 의무에 대한 의사소통 포함

(4) 의사소통되는 컴플라이언스 정보는 컴플라이언스 경영시스템 내에서 생성된 정보와 일치하고 신뢰할 수 있음을 보장

(5) 컴플라이언스 경영시스템에 관련 있는 의사소통에 대응

(6) 적절하다면 의사소통의 증거로 문서화된 정보를 유지

(7) 적절하다면 컴플라이언스 경영 시스템의 변경을 포함한 조직의 다양한 계층 및 기능 간에 컴플라이언스 경영시스템과 관련된 정보를 내부적으로 의사소통

(8) 의사소통 프로세스가 인원들이 컴플라이언스 경영시스템의 지속적인 향상에 기여할 수 있도록 보장

(9) 의사소통 프로세스가 인원들이 우려 사항을 제기 할 수 있도록 보장

(10) 수립된 의사소통 프로세스에 의해 컴플라이언스 문화, 목표 및 의무에 대한 의사소통을 포함한 컴플라이언스 경영시스템과 관련된 정보를 외부에 전달

7.5 문서화된 정보

7.5.1 일반 사항

(1) 조직의 컴플라이언스 경영시스템은 다음을 포함하여야 한다.

(가) 이 가이드라인에서 요구하는 문서화된 정보

(나) 컴플라이언스 경영시스템의 효율성을 위해 필요한 것으로 조직이 결정한 문서화된 정보

[비 고] 컴플라이언스 경영시스템을 위한 문서화된 정보의 범위는 다음과 같은 이유로 조직마다 다를 수 있다.

- 조직의 규모, 활동, 프로세스, 제품 및 서비스의 유형

- 프로세스의 복잡성과 그 상호 작용
- 인원들의 역량

7.5.2 생성 및 갱신

(1) 문서화된 정보를 생성하거나 갱신할 경우, 조직은 다음 사항의 적절함을 보장하여야 한다.

(가) 식별 및 내용(예: 제목, 날짜, 작성자 또는 참고 또는 문서번호)

(나) 형식(예: 언어, 소프트웨어 버전, 그래픽)과 매체(예: 종이, 전자)

(다) 적합성 및 적절성에 대한 검토 및 승인.

7.5.3 문서화된 정보의 관리

(1) 컴플라이언스 경영시스템과 이 가이드라인에서 요구하는 문서화된 정보는, 다음 사항을 보장하기 위하여 관리되어야 한다.

(가) 필요한 장소 및 시기에 사용 할 수 있고, 접근할 수 있고, 사용하기에 적절함

(나) (예를 들어 기밀성 상실, 부적절한 이용, 또는 무결성 손실) 적절하게 보호됨

(2) 문서화된 정보의 관리를 위해 조직은 해당되는 경우 다음의 활동을 적용 하여야 한다.

(가) 배포, 접근, 검색 및 사용

(나) 가독성 보존을 포함한 보관 및 보존

(다) 변경 관리(예: 버전 관리)

(라) 보유 및 폐기

(3) 컴플라이언스 경영시스템의 기획과 운용을 위해 필요하다고 조직이 결정한 외부 출처의 문서화된 정보는 적절하게 식별되고 관리되어야 한다.

[비 고] 접근(access)이란 문서화된 정보를 검토하는 것만 허용하거나, 문서화된 정보를 변경 할 수 있는 허용 권한에 관한 결정을 의미할 수 있다.

8. 운용

8.1 운용기획 및 관리

8.1.1 조직은 요구사항을 충족시키고 6항에서 결정된 조치를 실행하기 위해 필요한 프로세스를 계획, 실행 및 관리하여야 한다.

(1) 프로세스의 기준 설정

(2) 기준에 따라 프로세스 관리의 실행

8.1.2 기준에 따라 프로세스가 계획대로 실행되었다는 것을 확신하기 위해 필요한 정도의 문서화된 정보를 보유해야 한다.

8.1.3 조직은 계획된 변경을 관리하고, 의도하지 않은 변경의 결과를 검토 하며, 필요에 따라 악영향을 완화하기 위한 조치를 취하여야 한다.

8.1.4 조직은 컴플라이언스 경영시스템과 관련된 외주처리 프로세스, 제품 또는 서비스가 관리됨을 보장하여야 한다.

[비 고] 조직의 운영을 아웃소싱 한다고 해서 조직의 법적 책임이나 컴플라이언스 의무가 완화되는 것은 아니다. 조직은 제 자 프로세스가 관리되고 모니터링 되도록 해야한다.

8.2 관리와 절차의 수립

8.2.1 조직은 컴플라이언스 의무 및 관련된 컴플라이언스 리스크를 처리하기 위한 관리를 실행하여야 한다. 이러한 관리는 지속적인 효과를 보장하기 위해 유지 되고 주기적으로 검토 및 테스트 되어야 한다.

[비 고] 관리 테스트는 의도한 것을 수행하는지 또는 우회 할수 없지는 또는 리

스크의 영향 또는 가능성을 줄이는데 실제적으로 효과적인지를 확인하기 위해 설계된 연습을 수행하는 것을 의미 한다.

8.3 우려 제기

8.3.1 조직은 컴플라이언스 방침 또는 컴플라이언스 의무에 대한 위반 시도, 의심 또는 실제 위반에 대한 보고 (정보가 사실이라고 믿을 수 있는 합리적인 근거가 있는 경우)를 장려하고 활성화하는 프로세스를 수립, 실행 및 유지해야 한다.

8.3.2 이 프로세스는 다음과 같아야 한다.

(1) 조직 전체에서 확인 할 수 있고 접근 할 수 있어야 한다.

(2) 보고서를 기밀로 취급

(3) 익명의 신고를 허용

(4) 신고 인원을 보복으로부터 보호

(5) 인원이 조언을 받을 수 있도록 할 것

8.3.3 조직은 모든 인원이 신고 절차, 자신의 권리 및 보호를 인식하고, 이를 이용할 수 있도록 하여야 한다.

8.4 조사 프로세스

8.4.1 조직은 미준수 의심 또는 실제 사례가 있는 신고들을 접근하고 평가, 조사 및 종료할 수 있는 프로세스를 수립하여야 한다.

8.4.2 이러한 프로세스들은 공정하고 공정한 의사결정을 보장 해야한다.

8.4.3 조사 프로세스는 독립적으로 역량 있는 인원에 의해 이해충돌 없이 수행되어야 한다.

8.4.4 조직은 컴플라이언스 경영시스템의 개선을 위해 조사 결과를 적절하게 이용하여야 한다.

8.4.5 조직은 조사의 수와 결과를 지배기구 또는 최고 경영진에게 주기적으로 보고해야 한다.

8.4.6 조직은 조사에 대한 문서화된 정보를 유지하여야 한다.

9. 성과평가

9.1 모니터링, 측정, 분석 및 평가

9.1.1 일반 사항

(1) 조직은 컴플라이언스 목표가 달성 되었는지 확인하기 위하여 컴플라이언스 경영시스템을 모니터링 하여야 한다.

(2) 조직은 다음 사항을 결정하여야 한다.

(가) 모니터링 및 측정해야 할 사항

(나) 유효한 결과를 보장하기 위한, 모니터링, 측정, 분석 및 평가 방법(해당되는 경우)

(다) 모니터링 및 측정이 수행되어야 하는 시기

(라) 모니터링 및 측정 결과를 분석하고 평가해야 하는 경우

(3) 결과에 대한 증거로서 문서화된 정보를 보유하여야 한다.

(4) 조직은 컴플라이언스 성과와 컴플라이언스 경영시스템의 효과성을 평가하여야 한다.

9.1.2 컴플라이언스 성과에 대한 피드백의 출처

(1) 조직은 다양한 범위로부터 컴플라이언스 성과에 대한 피드백을 구하고 받기 위한 프로세스를 수립, 실행, 평가 및 유지하여야 한다.

(2) 정보는 비준수에 대한 근본 원인을 식별하고 취해진 조치가 적절했는지를 확인하며 4.5에서 요구되는 주기적 리스크평가에 이 정보를 반영하기 위해 분석되고 비판적으로

평가되어야 한다.

9.1.3 지표 개발

(1) 조직은 조직이 컴플라이언스 목표 달성을 평가하고, 컴플라이언스 성과를 평가하는데 도움이 되는 적절한 지표를 개발, 실행 및 유지해야 한다.

9.1.4 컴플라이언스 보고

(1) 조직은 다음을 보장하기 위해 컴플라이언스 보고 프로세스를 수립, 실행 및 유지해야 한다.

(가) 보고에 대한 기준을 설정할 것

(나) 정기보고를 위한 일정 수립 할 것

(다) 임시보고를 용이하게 하는 예외보고 시스템의 시행

(라) 정보의 정확성과 완전성을 보장하기 위한 시스템과 프로세스의 시행

(마) 예방, 시정 및 구제조치를 취하기 위하여, 정확하고 완전한 정보가 조직의 올바른 기능 또는 영역에 제공

(2) 컴플라이언스 기능이 지배기구 또는 최고경영진에게 발행한 모든 보고서는 변경으로부터 적절히 보호되어야 한다.

9.1.5 기록 관리

(1) 조직은 모니터링 및 검토 프로세스를 지원하기 위하여 컴플라이언스 활동들에 대한 정확한 최신의 기록을 유지 하여야 하며, 컴플라이언스 경영시스템의 적합성을 증명 하여야 한다.

9.2 내부 심사

9.2.1 조직은 컴플라이언스 경영시스템의 다음 사항에 대한 정보를 제공하기 위해, 계획된 주

기로 내부 심사를 수행하여 한다.

(1) 다음 사항을 준수함(적합성)

(가) 컴플라이언스 경영시스템에 대한 조직 자체의 요구사항

(나) 이 가이드라인의 요구사항

(2) 효과적으로 실행되고 유지되는지 여부

9.2.2 내부심사 프로그램

(1) 조직은 주기, 방법, 책임, 요구사항의 기획 및 보고를 포함하는, 심사 프로그램을 계획, 수립, 실행 및 유지하여야 한다.

(2) 내부심사 프로그램을 수립할 때 조직은 관련 프로세스의 중요성과 이전의 심사 결과를 고려되어야 한다.

(3) 조직의 역할

(가) 각 심사에 대한 심사 목표, 기준 및 범위를 정의

(나) 심사 프로세스의 객관성 및 공평성을 보장하기 위한 심사원의 선정 및 심사 수행

(다) 심사 결과가 관련 관리자와 경영진에게 보고되었음을 보장

[비고1] 관련 관리에는 컴플라이언스 기능, 최고경영진 및 지배기구가 포함될 수 있다.
[비고2] 내부심사를 수행하기 위한 가이드는 ISO19011에서 찾을 수 있다.

9.3 경영 검토

9.3.1 일반사항

(1) 지배기구 및 최고 경영자는 조직의 지속적인 적합성, 적절성 및 효과성을 보장하기 위

하여 계획된 주기대로 조직의 컴플라이언스 경영시스템을 검토해야 한다.

9.3.2 경영검토 입력사항

(1) 경영검토는 다음이 포함되어야 한다.

(가) 이전 경영 검토에 따른 조치의 상태

(나) 컴플라이언스 경영시스템과 관련된 외부 및 내부 이슈의 변경

(다) 컴플라이언스 경영시스템과 관련된 이해관계자의 요구 및 기대 변화

(라) 다음경향을 포함한 컴플라이언스 성과에 대한 정보
- 부적합, 비준수 및 시정조치
- 모니터링 및 측정결과
- 심사 결과

(마) 지속적 개선을 위한 기회

(2) 경영검토는 다음 사항을 고려해야 한다.

(가) 컴플라이언스 방침의 타당성(적절성)

(나) 컴플라이언스 목표가 충족된 정도

(다) 자원의 적절성

(라) 기존 통제 및 성과 지표의 효과성

(마) 피드백 및 불만을 포함하여 우려를 제기하는 인원, 이해관계자들로부터의 의사소통

(바) 조사

(사) 보고 시스템의 효율성

9.3.3 경영검토 출력

(1) 경영 검토 결과는 지속적 개선을 위한 기회 및 컴플라이언스 경영시스템에 대한 변경의 필요성에 관한 결정을 포함하여야 한다.

(2) 조직은 검토결과의 증거로써 문서화된 정보를 보유하여야 한다.

10. 개선

10.1 지속적 개선

10.1.1 조직은 컴플라이언스 경영시스템의 적합성, 적절성 및 효과성을 지속적으로 개선하여야 한다.

10.1.2 조직이 컴플라이언스 경영시스템의 변경 필요성이 판단되며 계획된 방식으로 변경은 계획된 방식으로 수행하여야 한다.

10.1.3 조직은 다음 사항을 고려하여야 한다.

(1) 변경의 목적 및 잠재적인 결과

(2) 컴플라이언스 경영시스템의 설계 및 운영 효율성

(3) 적절한 자원의 가용성

(4) 책임과 권한의 할당 및 재할당

10.2 부적합 및 시정조치

10.2.1 부적합 또는 비준수 발생시, 조직은 다음 사항을 실행하여야 한다.

(1) 부적합 및 비준수에 즉시 조치하고, 적용 가능한 경우

(2) 부적합 및 비준수에 대응하고 해당되는 경우

(가) 관리 및 시정조치를 취함

(나) 결과 처리

(3) 부적합 또는 비준수 또는 둘 다가 재발하거나 다른 곳에서 발생하지 않도록 부적합 및 비준수 또는 둘 다의 원인(들)을 제거하기 위한 조치의 필요성을 평가

(가) 부적합 및/또는 비준수 또는 둘 다를 검토

(나) 부적합 또는 비준수 또는 둘 다의 원인을 결정

(다) 유사한 부적합 또는 비준수 또는 둘 다가 존재하거나 잠재적으로 발생할 수 있는지에 대하여 결정

(4) 필요한 조치를 실행

(5) 취해진 시정조치의 효과성 검토

(6) 필요한 경우 컴플라이언스 경영시스템을 변경

10.2.2 시정조치는 부적합 또는 비준수 또는 둘 다의 영향에 적절하여야 한다.

10.2.3 문서화된 정보는 다음의 증거로 사용할 수 있어야 한다.

(1) 부적합 또는 비준수 또는 둘 다의 성격 및 취해진 후속조치

(2) 시정조치의 결과