KOSHA GUIDE
X - 67 - 2015

조직의 위험관리에 관한 지침

2015. 11

한국산업안전보건공단

안전보건기술지침의 개요

○ 작성자 : 주식회사 류앤컴퍼니 류보혁

○ 제·개정 경과
- 2015년 11월 리스크관리분야 제정위원회 심의(제정)

○ 관련규격 및 자료
- KS A ISO/IEC Guide 73, 리스크관리-용어-규격에 사용하기 위한 지침, 2002
- ISO 31000, Risk management - Principles and guidelines, 2009
- HB 203, Environmental risk management - Principles and process, 2006
- HB 205, OHS Risk management handbook, 2004
- HB 327, Communicating and consulting about risk, 2010
- HB 4360, Risk management guidelines - Companion to AS/NZS 4360, 2004

○ 기술지침의 적용 및 문의
- 이 기술지침에 대한 의견 또는 문의는 한국산업안전보건공단 홈페이지(www..kosha.or.kr)의 안전보건기술지침 소관분야별 문의처 안내를 참고하시기 바랍니다.
- 동 지침 내에서 인용된 관련규격 및 자료, 법규 등에 관하여 최근 개정본이 있을 경우에는 해당 개정본의 내용을 참고하시기 바랍니다.

공표일자 : 2015년 12월 7일

제 정 자 : 한국산업안전보건공단 이사장

KOSHA GUIDE
X - 67 - 2015

조직의 위험관리에 관한 지침 제안개요

I. 제정이유

이 지침은 조직의 활동 범위, 전략, 의사결정, 운영, 절차, 기능, 제품, 서비스 및 자산 등에서의 위험관리를 하고자 하는 경우, 필요한 사항에 대하여 규정함을 목적으로 함

II. 제정(안)의 주요내용

1. 이 기술지침은 다음의 기존 기술지침을 통합한 제정(안)임
   - X-2-2014 리스크관리 절차에 관한 지침
   - X-3-2012 리스크평가 절차에 관한 지침
   - X-4-2012 리스크 평가기법 선정에 관한 지침
   - X-17-2012 리스크 관리절차의 문서화에 관한 지침
   - X-16-2012 리스크관리를 위한 환경조건설정에 관한 지침
   - X-18-2012 리스크 정보교환 및 상담에 관한 지침

2. 이 기술지침의 주요 내용은 다음과 같음
   - 위험관리의 기본 원칙
   - 위험관리의 구조
   - 위험관리 절차

3. 주요 수정, 변경 내용은 다음과 같음
   - 목적 및 적용범위 등을 통합하고 수정함
   - 기술지침에서 사용되는 용어에 대해 정리하고 이를 보완함

KOSHA GUIDE
X - 67 - 2015

조직의 위험관리에 관한 지침

1. 목 적

이 지침은 조직의 활동 범위, 전략, 의사결정, 운영, 절차, 기능, 제품, 서비스 및 자산 등에서의 위험관리를 하고자 하는 경우, 필요한 사항에 대하여 규정함을 목적으로 한다.

2. 적용범위

이 지침은 공기관, 기업, 협회, 단체 또는 개인 등의 모든 조직의 위험관리에 적용한다.

3. 용어의 정의

(1) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

(가) “위험(Risk)”이라 함은 목적(Objective)에 대한 불확실(Uncertainty)한 결과(Effect)를 말한다.

주 1) 위험은 사건의 발생 확률과 사건(환경 변화) 결과의 조합으로 나타낸다.

2) 목적은 다양한 관점(재무, 안전보건, 환경 목적 등)과 다양한 수준(전략, 조직, 프로젝트, 제품 및 절차)이 될 수 있다.

3) 결과는 긍정적 및/또는 부정적으로 예측된 것으로부터 이탈된 것이다.

4) 불확실은 사건, 그 결과나 확률에 관한 지식이나 이해에 관련된 정보가 결핍된 상태이다.

(나) “위험관리(Risk management)”라 함은 위험과 관련되는 조직을 직접 또는 제어하기 위한 관련 활동을 말한다.

(다) “위험관리 구조(Risk management framework)”라 함은 조직 전체를 통하여 위험관리의 설계, 실행, 모니터링, 검토 및 지속적인 증진을 위한 기반(Foundations) 및 조직구성 부분을 말한다.

주 1) 기반은 위험을 관리하기 위한 정책(Policy), 목적, 규정(Mandate) 및 실행(Commitment)을 포함한다.

2) 조직구성은 계획, 관계, 책임(Accountabilities), 자원, 절차(Processes) 및 활동을 포함한다.

(라) “위험관리자”라 함은 위험을 관리할 책임과 권한이 있는 개인 또는 단체를 말한다.

(마) “위험관리 절차(Risk management process)”라 함은 위험에 대한 관리정책, 정보교환 절차 및 실행, 상담, 환경조건 설정, 파악, 분석, 평가, 처리, 모니터링 및 검토 등을 체계적으로 관리하는 절차를 말한다.

(바) “환경조건 설정(Establishing the context)”이라 함은 위험을 관리할 때 고려하여야 하는 내외부 파라미터를 수립하고 위험관리 정책을 수립하기 위한 범위 및 위험관리 기준을 설정하는 것을 말한다.

(사) “의사소통(Communication and consultation)”이라 함은 조직이 위험관리와 관련하여 정보를 얻거나 전달하고 이해관계자와 의사소통을 하는 등 지속적이고 반복적인 절차를 말한다.

(아) “이해관계자”라 함은 어떠한 결정이나 활동에 의해 영향을 받거나 줄 수 있는 사람 또는 조직을 말한다.

(자) “위험성평가(Risk assessment)”라 함은 위험의 파악, 분석, 수준결정 등의 절차를 말한다.

(차) “위험수준 결정(Risk evaluation)”이라 함은 위험성 및/또는 그 크기가 수용가능한지 여부를 결정하기 위하여 위험관리 기준을 갖고 위험분석 결과를 분석하는 절차를 말한다.

(카) “위험기준(Risk criteria)”이라 함은 위험의 강도에 대한 기준을 정하는 용어를 말한다.

(타) “위험수준(Risk level)”이라 함은 위험의 빈도와 강도의 조합으로 표현하는 위험성의 크기를 말한다.

(파) “개선조치”라 함은 위험원의 제거, 발생 확률의 변경, 사고결과의 변경 등을 통하여 위험을 감소시키는 절차를 말한다.

(하) “모니터링”이라 함은 요구 또는 기대되는 성과수준의 변화를 파악하기 위하여 상태의 지속적인 점검, 감독, 관찰 또는 판정하는 것을 말한다.

(2) 그밖에 용어의 정의는 이 지침에서 특별히 규정하는 경우를 제외하고는 산업안전보건법, 같은 법 시행령, 같은 법 시행규칙 및 산업안전보건기준에 관한 규칙에서 정하는 바에 따른다.

4. 위험관리의 기본원칙

모든 조직은 효과적인 위험관리를 위하여 다음 원칙을 지켜야 한다.

(1) 위험관리는 근로자의 건강·안전보건·보안·법규 및 규정 준수·환경보호·품질·프로젝트 관리·운영의 효율성 등 조직의 목적 달성 및 증진에 기여한다.

(2) 위험관리는 조직의 주요활동 및 절차에서 분리된 별도의 활동이 아니고, 조직의 전략계획·프로젝트 및 경영절차를 포함한 모든 조직의 업무와 책임 등을 포함해야 한다.

(3) 위험관리는 필요한 정보제공으로 여러 대안을 검토하여 우선순위를 정하는 데 도움을 준다.

(4) 위험관리는 불확실성을 명확히 해결해 준다.

(5) 위험관리는 체계적이고 시의 적절하여야하며 효율성·지속성·신뢰성이 있는 결과의 산출에 기여한다.

(6) 위험관리 절차의 입력은 과거 데이터·경험·이해관계자의 의견·관찰·예측 및 전문가의 결정 등과 같은 정보를 기반으로 한다.

(7) 위험관리는 조직 내외부 환경 및 위험 조건에 적합하여야 한다.

(8) 위험관리는 조직의 목적 달성을 촉진하거나 저해할 수 있는 내외부 사람들의 능력, 인지 및 의도 등을 고려한다.

(9) 위험관리는 조직의 모든 수준에서, 특히 경영자는 시의 적절하게 이해관계자의 참여하에 위험관리를 지속적으로 보완함을 보장한다.

(10) 위험관리는 변화를 지속적으로 감지하고 이에 반응해야 하며, 내외부 사건은 환경조건과 지식의 변화, 위험의 모니터링과 검토, 새로운 위험의 발생 또는 변경, 기타 소멸 등으로 나타날 수 있다.

(11) 위험관리는 조직의 지속적인 개선 증진을 위한 전략을 개발하고 실행한다.

5. 위험관리의 구조

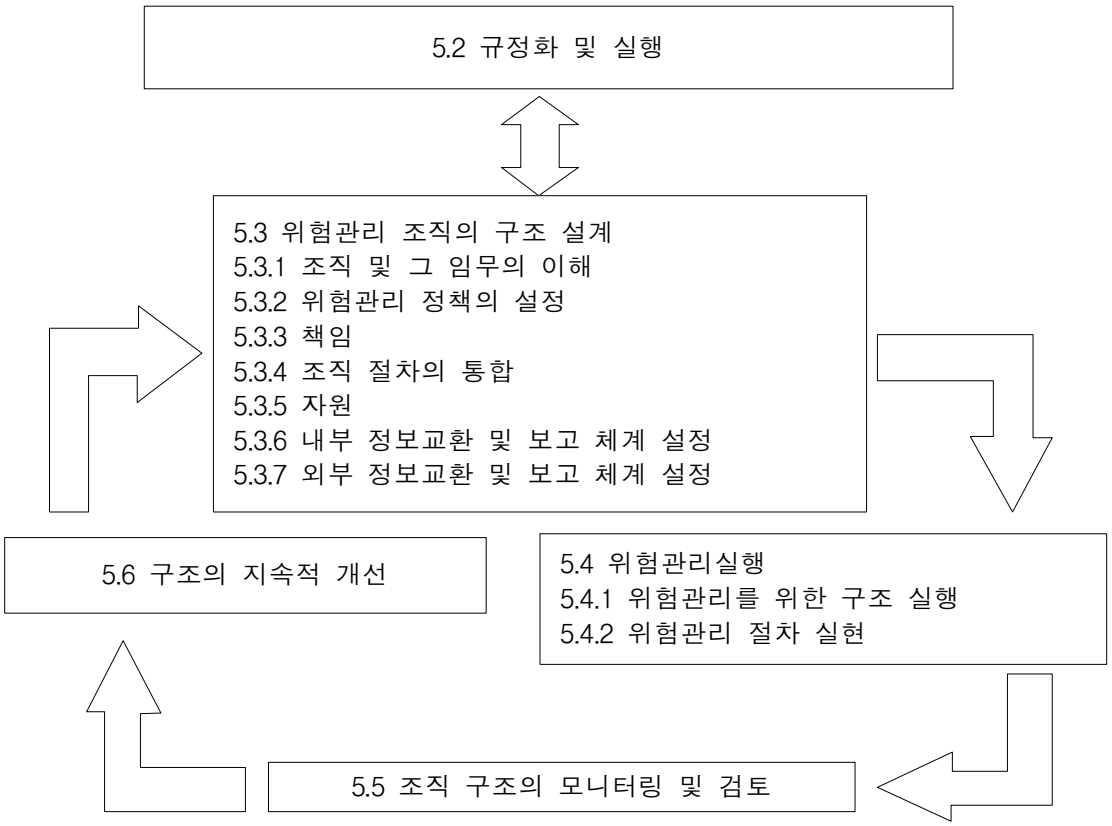
5.1 일반사항

(1) 위험관리의 성공은 효율적인 조직의 구성 여부에 달려있다.

(2) 위험관리의 구조는 변화하는 환경조건 내에서 위험관리 절차의 적용을 통한 효과적인 위험관리를 지원하도록 구성한다(6절 참조).

(3) 위험관리의 구조는 도출된 위험정보가 모든 조직의 각 계층에 충분히 보고되고, 이에 따라 의사결정을 하고 책임을 갖고 수행하도록 한다.

(4) 이 절에서는 위험관리 구조의 구성요소에 대하여 기술하며, 이를 요약하면 <그림 1>과 같다.



<그림 1> 위험관리구조의 구성 요소 사이의 관계

5.2 규정화 및 실행

위험관리의 도입과 지속적인 효과보장을 위하여 다음과 같은 전략과 계획이 필요하다.

(1) 위험관리 정책의 수립 및 승인

(2) 조직의 문화와 위험관리 정책의 부합 확인

(3) 조직의 성과지표에 부합하는 위험관리 성과지표 결정

(4) 조직의 목적과 전략에 부합하는 위험관리 목적

(5) 법률 및 규정 준수 보장

(6) 조직 내에서 적절한 수준의 책임을 부여

(7) 필요한 자원이 위험관리에 배정되는지를 보장

(8) 모든 이해관계자들에게 위험관리의 장점을 홍보

(9) 위험관리를 위한 조직구조의 지속적인 유지를 보장

5.3 위험관리 조직의 구조 설계

5.3.1 조직 및 환경조건의 이해

(1) 위험관리 조직의 구조를 설계하고 실행하기 전에 조직에 중대한 영향을 미치는 내외부의 환경조건에 대한 평가와 이해가 중요하다.

(2) 조직 외부환경조건 평가에서는 다음을 포함하나 이에 한정하지 않는다.

(가) 국제, 국내 또는 지역 여부에 관계없이, 사회적, 문화적, 정치적, 법적, 규정, 재정, 기술, 경제, 자연 및 경쟁 환경 등
(나) 조직의 목적에 영향을 주는 핵심요인과 경향
(다) 외부 이해관계자와의 관계, 인식 및 가치

(3) 조직 내부환경조건 평가에서는 다음을 포함하나 이에 한정하지 않는다.

(가) 지배구조, 조직구조, 책임
(나) 정책, 목적 및 전략을 달성하기 위한 적재적소 환경조건
(다) 자원 및 지식에 관한 이해(즉, 자본, 시간, 사람, 절차, 시스템 및 기술 등)
(라) 정보시스템, 정보흐름(공식 및 비공식) 및 결정 절차
(마) 내부 이해관계자와의 관계, 인식 및 가치
(바) 조직문화
(사) 조직에서 채택하고 있는 표준, 지침 및 모델
(아) 관계자 등과의 계약 형태와 범위 등

5.3.2 위험관리 정책의 설정

(1) 위험관리 정책은 다음과 같이 조직의 목적을 명확히 기술하고 실행한다.

(가) 위험관리 조직의 기반
(나) 조직의 목적과 위험관리 정책의 연계
(다) 위험관리를 위한 재정능력 및 책임
(라) 상충되는 이해관계자를 다루는 방법
(마) 위험관리를 위한 재정능력 및 책임을 다하기 위하여 필요한 가용자원을 지원
(바) 위험관리 성과를 측정하고 보고하기 위한 방법
(사) 사건이나 주변 환경변화에 따른 위험관리 정책 및 구조를 검토하고 개선을 위한 실행방법

(2) 위험관리 정책을 수립할 때에는 관련정보를 적절히 교환한다.

5.3.3 책임

조직은 위험관리의 실행 및 유지, 개선조치의 적절성·효율성·효과성 등을 포함하여 위험을 관리하는 데 필요한 재정, 권한 및 적합한 능력 등을 보장하되, 다음에 따라 이를 실행하도록 한다.

(1) 위험을 관리하기 위한 책임과 권한을 보유하고 있는 위험관리자의 파악

(2) 위험관리를 위한 개발, 실행, 정비 등의 책임자의 파악

(3) 위험관리 조직에서의 모든 계층에 있는 사람들의 책임을 파악

(4) 성과측정, 내외부 보고 및 절차의 향상 방안을 수립

5.3.4 조직절차의 구성

(1) 조직의 모든 절차에 위험관리를 효과적이고 효율적으로 포함시킨다.

(2) 정책개발, 사업과 전략의 계획 및 검토, 변경관리 절차에 위험관리 절차를 포함시키도록 한다.

(3) 위험관리 계획은 전략계획과 같은 조직의 다른 계획에 포함시키도록 한다.

5.3.5 자원

조직은 위험관리를 위해 적절한 자원을 할당하되, 고려해야 할 사항은 다음과 같다.

(1) 사람, 기술, 경험과 능력

(2) 위험관리 절차의 각 단계에서 필요한 자원

(3) 위험관리에 사용되는 조직의 절차, 방법 및 도구

(4) 문서화된 절차

(5) 정보와 지식경영시스템

(6) 교육훈련프로그램

5.3.6 내부 의사소통 체계 설정

(1) 조직은 재정 및 위험관리자를 지원하고 격려하기 위한 내부 의사소통 체계를 구축하되, 이러한 체계는 다음을 통하여 실행을 보장한다.

(가) 위험관리 구조의 핵심요소, 변경 등의 적절한 정보교환
(나) 위험관리 구조에 대한 내부보고, 효과 및 출력 등
(다) 위험관리의 적용에 의해 도출된 적절한 수준과 횟수에 관한 정보
(라) 내부 이해관계자와의 상담절차

(2) 이러한 체계에는 다양한 계통으로부터의 위험정보를 통합하는 절차를 포함하되 정보의 민감성을 고려할 필요가 있다.

5.3.7 외부 정보교환 및 보고체계의 설정

(1) 조직은 외부 이해관계자와 의사소통을 위하여 다음과 같은 계획을 수립한다.

(가) 적합한 외부 이해관계자의 참여와 정보의 효과적인 교환을 보장
(나) 법률, 규제 및 정부 요구사항 등 외부보고의 충족
(다) 의사소통의 피드백 및 보고계통을 구비
(라) 조직의 신뢰구축을 위한 정보교환
(마) 위기 또는 우발사고 발생의 경우, 이해관계자와의 의사소통 관계 등

(2) 이러한 체계는 다양한 계통으로부터의 위험정보를 통합하는 절차를 포함하되 정보의 민감성을 고려할 필요가 있다.

5.4 위험관리 실행

5.4.1 위험관리를 위한 구조 실행

조직구조는 위험관리를 실행하기 위하여 다음에 따르도록 한다.

(1) 조직구조 실행을 위한 적합한 시기 및 정책에 대한 수립

(2) 조직절차에 대한 위험관리 정책 및 절차의 적용

(3) 법적 및 규제 요구사항의 준수

(4) 위험관리절차의 출력에 부합하는 목적의 개발 및 설정을 포함한 의사결정 보장

(5) 위험관리 구조가 적절히 유지됨을 보장하기 위한 이해관계자와의 의사소통

5.4.2 위험관리 절차 실행

위험관리는 5절에서 규정하는 위험관리 절차의 실행과 조직절차의 일환으로 적절한 수준 및 기능에서 위험관리 계획에 따라 보장하고 이를 실행하도록 한다.

5.5 조직구조의 모니터링 및 검토

조직은 위험관리가 효과적이고 지속적으로 관리하고 있음을 보장하기 위하여 다음과 같이 조직구조를 모니터링하고 검토하도록 한다.

(1) 위험관리 성과측정 지표의 적합성에 대한 주기적인 검토

(2) 위험관리 계획의 편차를 포함하는 측정 환경조건에 대한 주기적인 검토

(3) 조직의 내외부 환경조건에 따른 위험관리 구조, 정책 및 계획이 적절하게 유지되는 지를 주기적으로 검토

(4) 위험관리 계획의 환경조건과 위험관리 정책과의 부합하는 지를 기록

(5) 위험관리 구조의 효과성 검토

5.6 조직구조의 지속적 개선

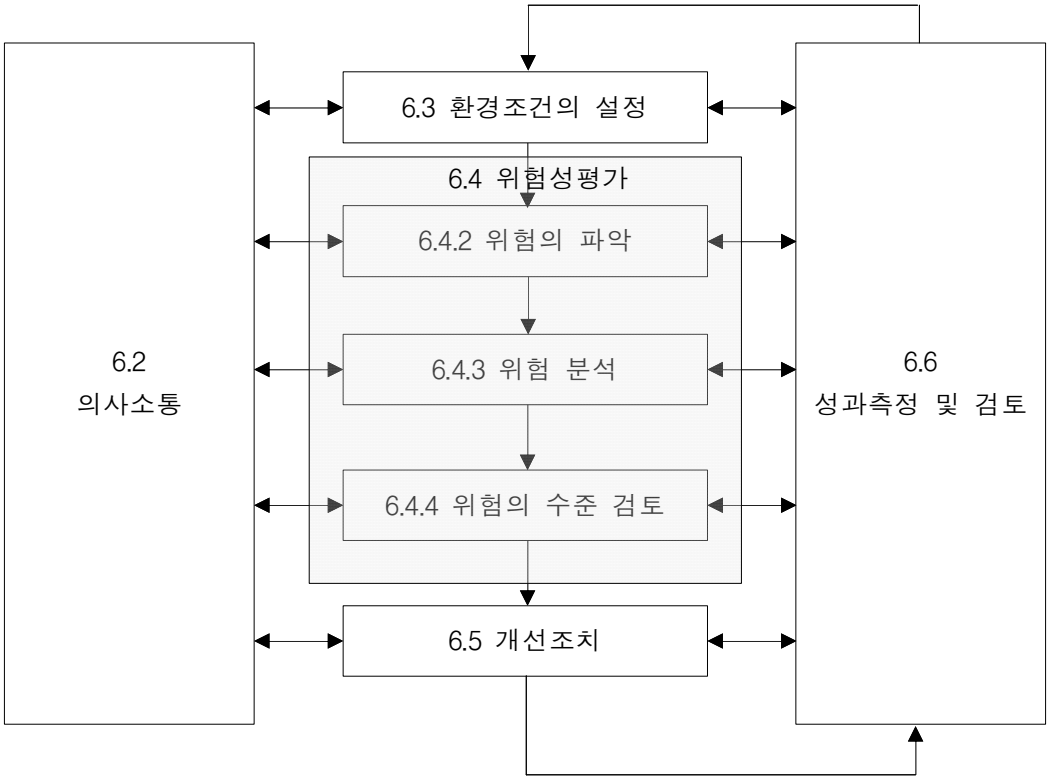
(1) 조직구조의 모니터링 및 검토 내용을 바탕으로, 위험관리의 구조·정책 및 계획을 개선할 수 있는 방법을 결정한다.

(2) 이러한 결정은 위험관리의 조직과 문화의 개선으로 이어지도록 한다.

6. 위험관리 절차

6.1 일반 사항

위험관리의 절차는 관리의 통합, 조직문화와 실행에 포함시키고 조직의 사업절차에 맞도록 하되, 6.2 ~ 6.6에 규정된 활동을 포함하도록 한다(<그림 2> 참조),



<그림 2> 위험관리 절차

6.2 의사소통

(1) 내외부 이해관계자와의 의사소통은 위험관리 절차의 모든 단계에서 이루어져야 하며, 이를 위한 계획은 초기단계에서 개발하도록 한다.

(2) 도출된 위험과 그 결과가 알려진 경우라면, 위험에 관련된 사항들은 의사소통에서 다루도록 한다.

(3) 효과적인 내외부의 의사소통은 위험관리의 시행책임이 있는 사람과 이해관계자에게 각종 행위의 이유와 그 결정 내용의 이해를 보장하고자 하는 것이다.

(4) 의사소통은 다음과 같은 방법으로 접근하도록 한다.

(가) 환경조건을 적절히 설정하는 데 지원
(나) 이해관계자의 이익을 이해하고 고려
(다) 위험의 적절한 파악
(라) 위험분석을 함께 할 다양한 전문가 확보
(마) 위험관리 기준을 정할 경우, 다양한 의견을 존중
(바) 개선조치 계획에 대한 적절한 지원
(사) 위험관리 절차에서 적절한 변경 관리
(아) 내외부 의사소통 계획의 수립 등

(5) 이해관계자와의 의사소통은 위험의 인식을 바탕으로 한 위험을 결정하는 것이므로 중요하다.

6.3 환경조건의 설정

6.3.1 일반사항

(1) 위험관리 환경조건을 설정하고 고려하여야 할 내외부 파라미터를 설정하고 절차에 대한 범위와 기준을 정한다.

(2) 파라미터는 위험관리 구조(5.3.1 참조)를 설계할 때 고려하는 것과 유사하다.

6.3.2 외부환경조건 설정

(1) 외부환경조건은 조직이 목적을 달성하기 위하여 추구하는 대외적인 환경조건을 말하며, 이는 위험관리 기준을 설정할 때 외부 이해관계자와의 관계를 고려해야 하기 때문에 중요한다.

(2) 외부환경조건 설정은 위험관리절차의 범위를 특정화하기 위하여 법적, 규정 요구사항, 이해관계자의 인식 및 기타 위험과 관련하여 구체적으로 규정한다.

(3) 외부환경조건은 다음과 같은 사항을 포함하되, 이에 한정하지 않는다.

(가) 사회적, 문화적, 정치적, 법적, 재정, 기술, 경제, 자연 및 경쟁환경, 국제적 또는 국내적, 지역적 또는 지방적 인지 여부 등
(나) 조직목적에 영향을 미칠 수 있는 핵심요소와 동향
(다) 외부 이해관계자의 인식과 가치와의 관계 등

6.3.3 내부환경조건 설정

(1) 내부환경조건은 조직이 달성하기 위하여 추구하는 내부환경조건을 말한다.

(2) 위험관리 절차는 조직의 지배구조, 구성 및 전략에 적합하여야하며, 내부환경조건은 조직이 위험을 관리하는데 영향을 미칠 수 있는 조직 내부의 모든 것을 포함하며, 다음에 의하여 확립된다.

(가) 위험관리는 조직목적, 환경조건에서 발생하는 것을 고려
(나) 특정 사업, 절차 또는 활동의 목적과 기준은 조직전체의 목적을 고려
(다) 일부조직에서 전략, 프로젝트 또는 사업목적을 달성할 수 있는 기회인식 실패로 조직의 신뢰와 가치에 미치는 영향을 고려

(3) 다음은 내부환경조건을 이해하기 위해 필요하나 이에 한정하지 않는다.

(가) 지배구조, 조직구조, 역할과 책무.
(나) 정책, 목적 및 전략을 달성하기 위한 적재적소 배치
(다) 자원과 역량(자본, 시간, 인력, 절차, 시스템 및 기술)관점에서의 능력 및 이해
(라) 내부 이해관계자의 인식 및 가치
(마) 조직문화
(바) 정보시스템, 정보흐름(공식 및 비공식 포함) 및 의사결정 과정
(사) 조직에서 채택한 표준, 지침 및 모델
(아) 계약관계의 형태와 범위

6.3.4 위험관리 환경조건 설정

(1) 위험관리가 적용되는 조직의 활동 목적, 전략, 범위 및 파라미터를 설정한다.

(2) 위험관리는 이를 수행하는데 사용되는 자원의 필요성에 대하여 충분히 고려하여 수행한다.

(3) 필요한 자원, 책임 및 권한 그리고 기록을 유지한다.

(4) 위험관리 절차의 환경조건은 조직의 필요에 따라 달라지며, 여기에는 다음을 포함하나 이에 한정하지 않는다.

(가) 위험관리 활동의 목적
(나) 위험관리 절차 내에서의 책임
(다) 위험관리 활동(포함 또는 배제할지까지)의 크기와 범위
(라) 시간과 장소 측면에서의 활동, 절차, 기능, 프로젝트, 제품, 서비스 또는 자산
(마) 특정 프로젝트의 절차 또는 활동과 기타 프로젝트의 절차 또는 활동 사이의 관계
(바) 위험성평가 기법
(사) 위험관리의 성과 및 효과를 평가하는 방법
(아) 의사결정에 대한 파악

(5) 선정된 위험관리 기법이 조직의 목적 달성에 영향을 미치는 주위환경 위험 등에 도움이 될 수 있도록 (4)항 및 기타요소의 영향을 고려한다.

6.3.5 위험관리 기준의 수립

(1) 위험의 수준을 결정하기 위하여 조직의 가치, 목적과 자원 등을 고려하여 위험관리 기준을 정해야 한다.

(2) 위험관리 기준 중 일부는 규정 또는 조직이 승인한 사항일 수 있다.

(3) 위험관리 기준은 조직의 위험관리 정책(5.3.2 참조)을 충족하되, 위험관리 초기 단계에서 수립하고 지속적으로 검토한다.

(4) 위험관리 기준을 수립할 때, 고려해야 할 요소는 다음과 같다.

(가) 발생할 수 있는 원인과 결과의 특성(측정 방법 포함)
(나) 발생 가능성에 대한 수립 방법
(다) 위험의 가능성 및 결과의 기간(시기)
(라) 위험수준의 결정 방법
(마) 이해관계자의 관점(견해)
(바) 허용 또는 허용 가능한 위험수준
(사) 다양한 위험의 조합이 필요할 경우, 이를 고려

6.4 위험성평가

6.4.1 일반사항

위험성평가는 위험을 파악하고 분석하고 수준을 결정하는 전체적인 과정이다.

6.4.2 위험파악(Risk identification)

(1) 조직은 위험원, 영향의 범위, 사건(환경 변화 포함), 잠재적인 원인 및 결과 등을 파악하여, 목적달성의 생성, 강화, 예방, 저하, 가속 또는 지연시킬 수 있는 사건을 바탕으로 포괄적인 위험목록을 만든다. 이는 어떠한 기회를 찾고자 하는 것이 아니고 관련된 위험을 파악하고자 하는 것이다.

(2) 이 단계에서 파악되지 않은 위험은 더 이상 분석되지 않기 때문에 이 파악은 매우 중요하다.

(3) 위험파악은 그 위험원이나 원인이 명백하지 않더라도 조직의 통제 여부에 관계없이 모든 위험을 포함한다.

(4) 위험파악은 특정결과의 종속 및 누적효과를 포함한 연쇄효과에 의한 시험을 포함한다.

(5) 위험원이나 원인이 분명하지 않을 경우라도 결과의 폭넓은 범위를 고려한다.

(6) 발생할 사건의 파악뿐만 아니라, 발생할 수 있는 원인과 시나리오를 고려할 필요가 있고, 모든 중요한 원인과 결과를 고려한다.

(7) 조직은 그 목적과 능력 및 직면한 위험에 적합한 위험파악 도구와 기술을 적용한다.

(8) 적절한 최신정보는 위험파악에 중요하며, 여기에는 발생할 수 있는 적절한 배경정보를 포함해야한다.

(9) 적절한 지식을 가진 사람들이 위험파악에 참여한다.

6.4.3 위험분석(Risk analysis)

(1) 위험분석은 위험의 이해를 포함하며, 위험수준을 검토하여 이를 처리해야 할지를 결정하여 입력하고 가장 적합한 개선조치 정책 및 방법을 제공한다.

(2) 위험분석은 다양한 형태와 수준의 위험을 포함하는 방법의 의사결정에 의하여 선정되고 입력할 수 있어야한다.

(3) 위험분석은 위험요인과 위험원, 결과(긍정적 및 부정적인), 발생할 수 있는 강도의 확률 등을 고려하고, 그 빈도와 강도에 영향을 미치는 요소를 확인한다.

(4) 위험은 결정된 빈도와 강도 그리고 위험의 기타요인에 의하여 분석된다.

(5) 사건은 복수의 결과를 가져올 수도 있고, 복수의 목적에 영향을 미칠 수 있으므로, 기존의 조치와 효과 및 효율성도 고려한다.

(6) 위험성평가 결과는 위험수준을 결정하기 위한 빈도와 강도의 조합이다.

(7) 이들 모두는 위험관리 기준과 부합해야하며, 다양한 위험과 위험원의 상호 의존성을 고려하는 것 또한 중요하다.

(8) 경영자는 가능하다면, 위험을 분석 할 때 이해관계자와의 효과적인 정보교환으로 사전조치 및 위험수준 및 그 민감도 등을 결정하도록 한다.

(9) 전문가들 사이에서 의견의 차이, 정보의 불확실성, 가용성, 품질, 수량 및 적합성 또는 모델링의 제한 등과 같은 요소들에 대해 기술하고 이를 강조한다.

(10) 위험분석은 위험의 분석 목적, 정보, 데이터, 가용 가능한 자원에 의존되는 세부적인 변화의 정도 등을 고려하여, 환경조건에 따라 정량적, 반정량적 또는 이들의 조합으로 한다.

6.4.4 위험수준 결정(Risk evaluation)

(1) 위험성평가의 목적은 위험분석 결과를 바탕으로 개선조치의 우선순위를 정하는 의사결정을 지원하기 위함이다.

(2) 위험수준 검토는 환경조건을 고려할 때 설정된 위험관리 기준분석 절차에서 발견된 위험수준을 비교하는 것으로, 이를 바탕으로 개선조치에 대한 필요성을 고려한다.

(3) 판단은 보다 넓은 위험 환경조건을 고려하고 위험으로부터 혜택을 받는 조직 이외의 집단이 부담하는 위험의 허용오차를 포함한다.

(4) 판단은 법적, 규제 및 기타 요구사항에 따라야 하며, 일부 환경조건에서는 위험평가가 추가적인 분석에 의한 결정으로 이어질 수 있다.

(5) 판단은 기존의 조치를 유지하는 것 이외의 방법으로 위험을 처리하지 않을 수 있고, 이러한 판단은 위험상태 및 위험관리 기준에 의하여 영향을 받을 수 있다.

6.5 개선조치(Risk treatment)

6.5.1 일반

(1) 개선조치는 위험의 크기를 보완하기 위하여 다음 중 하나 이상의 방법을 선정하고 실행한다. 개선조치는 다음의 순환 절차에 따른다.

(가) 개선조치의 평가
(나) 잔존위험 수준의 허용가능 여부를 결정
(다) 허용가능 하지 않을 경우, 새로운 개선조치 방안 강구
(라) 개선조치의 효과를 평가

(3) 개선조치 방법은 모든 환경조건에서 다음중 하나 이상을 포함한다.

(가) 위험회피
(나) 위험의 수용 또는 증가
(다) 위험원의 제거
(라) 확률의 변경
(마) 결과의 변경
(바) 다른 조직(계약 및 보험 포함)과의 위험 분담
(사) 위험유지

6.5.2 개선조치 방법의 선정

(1) 가장 적절한 개선조치 선택방법은 사회적 책임, 자연환경의 보호, 법률, 규정 및 기타 요구사항에 대하여 비용과 효과를 고려한다.

(2) 개선조치 방법은 개별 또는 조합하여 적용할 수 있다.

(3) 개선조치 방법을 선택할 때, 이해관계자의 인식과 가치, 적절한 정보교환 방법을 고려하며, 개선조치 방법이 조직 또는 이해관계자들에게 다른 위험을 줄 수 있는가를 고려한다.

(4) 동일한 효과라 하더라도 일부의 개선조치는 일부 이해관계자들에게 더 필요할 수도 있으므로, 개선조치 계획은 개별 개선조치의 우선순위를 정할 수 있도록 분명히 구분한다.

(5) 중대한 위험은 개선조치의 실패나 무효가 발생할 수 있으므로, 개선조치 방법의 유효성을 보장하기 위한 모니터링 계획을 수립한다.

(가) 개선조치는 평가, 처리, 모니터링 및 검토를 필요로 하는 2차 위험을 유발할 수 있다.
(나) 2차 위험은 최초위험의 처리계획에 포함시켜 관리하나, 새로운 위험으로 간주하지는 않는다.

6.5.3 개선조치 계획의 준비 및 실행

(1) 개선조치 계획은 선택된 실행방법을 문서화하기 위함으로 처리계획에서 제공되는 정보에는 다음을 포함한다.

(가) 실행방법을 선택한 근거
(나) 계획을 승인하고 실행할 책임자
(다) 제안된 활동
(라) 예비비를 포함한 자원
(마) 성과측정 및 제약조건
(바) 보고, 모니터링 및 추진 일정 등

(2) 개선조치 계획은 관련 이해관계자와 논의한다.

(3) 경영자와 기타 이해관계자들은 개선조치 후 잔존위험의 특성과 크기를 알아야 하며, 잔존위험을 문서화하고 모니터링 및 검토하여 필요할 경우 조치한다.

6.6 모니터링 및 검토

(1) 모니터링 및 검토는 위험관리 절차계획의 일부로써 정기적으로 점검 또는 사후관리하여야 하며, 필요한 경우 수시 또는 특별히 실시할 수 있다.

(2) 모니터링 및 검토 절차는 다음사항을 고려한다.

(가) 책임자 지정
(나) 개선조치는 설계 및 운영 모두에서 효과적이고 효율적임을 보장
(다) 위험성평가를 개선하기 위한 추가 정보
(라) 사건(아차사고 포함), 변경, 추이, 성공 및 실패로부터의 분석 및 학습 절차
(마) 내외부 환경조건 변화를 확인
(바) 추가 위험의 파악

(3) 개선조치 결과는 성과측정하고 조직의 전체 성과관리, 측정 및 내외부 보고활동에 포함될 수 있다.

(4) 모니터링 및 검토 결과는 기록하며, 내외부에 적절히 보고하고, 조직구조의 모니터링 및 검토(5.5 참조)에서 피드백 자료로 사용한다.

6.7 위험관리 과정의 기록

(1) 위험관리 활동은 추적 가능하여야 하고, 위험관리 절차에서, 기록은 전반적인 절차뿐 만아니라 해당방법과 도구의 개선을 위한 기초자료로 제공된다.

(2) 기록물을 작성하는 경우에는 다음을 고려한다.

(가) 지속적인 학습을 위한 조직의 요구사항
(나) 위험관리 목적을 위한 재사용 정보의 편익
(다) 기록을 생성하고 유지하는 데 소요되는 비용 및 노력
(라) 기록에 대한 법적, 규정과 운영의 필요성
(마) 검색 및 저장 매체의 접근방법과 용이성
(바) 보존기간
(사) 정보의 민감도 등