

KOSHA GUIDE

X - 1 - 2014

리스크 관리의 용어 정의에 관한 지침

2014. 11.

한국산업안전보건공단

안전보건기술지침의 개요

○ 작성자 : 사단법인 한국안전학회 리스크관리 연구위원회
서울과학기술대학교 안전공학과 박달재

○ 개정자 : 한국산업안전보건공단 전문기술총괄실

○ 제·개정 경과

- 2010년 8월 위험관리분야 제정위원회 심의(제정)
- 2011년 6월 리스크관리분야 제정위원회 심의(개정)
- 2014년 11월 리스크관리분야 제정위원회 심의(개정)

○ 관련규격 및 자료

- ISO GUIDE 73, Risk management-vocabulary, 2009
- ISO/IEC 73, Risk management-vocabulary-Guidelines for use in standards, 2002
- ISO/IEC GUIDE 51, Safety aspects-Guidelines for their inclusion in standards, 1999
- KOSHA GUIDE G-13-2011(프로젝트 위험관리에 관한 안전가이드)
- KS A ISO/IEC GUIDE 73:2002(리스크 관리-용어-규격에 사용하기 위한 지침)
- KOSHA GUIDE X-14-2014(4M 리스크 평가 기법에 관한 기술지침)

○ 기술지침의 적용 및 문의

- 이 기술지침에 대한 의견 또는 문의는 한국산업안전보건공단 홈페이지 안전보건 기술지침 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 : 2014년 11월 24일

제 정 자 : 한국산업안전보건공단 이사장

리스크 관리의 용어 정의에 관한 지침

1. 목 적

이 지침은 특정 조직, 단체 또는 개인 등이 리스크 관리에서 사용되는 용어의 의미를 올바르게 해석하고 이해하는데 그 목적이 있다.

2. 적용범위

이 지침은 특정 조직, 단체 또는 개인 등이 리스크 관리를 수행하는 사업장에 적용한다.

3. 용어의 정의

3.1. 리스크 관리(Risk management)와 관련된 용어

(1) “리스크(Risk)”라 함은 특정 목적에 영향을 주는 긍정 또는 부정적인 상황의 발생 기회에 대한 불확실성을 말한다.

(가) 리스크는 사상(Event)의 발생 가능성(Likelihood)과 그 결과(Consequence)의 조합으로 표현될 수 있다.

(나) 리스크는 안전·보건 측면에서 일반적으로 부정적인 결과가 발생할 가능성이 있을 경우 사용된다.

(다) 여기서 사용되는 리스크는 적용 분야별 또는 의미상으로 위험, 위험성, 유해성, 위험도 및 유해도 등으로 표현될 수 있다.

(2) “리스크 관리(Risk management)”라 함은 리스크와 직·간접적으로 관련된 모든 활동으로서 리스크 평가(Risk assessment), 리스크 처리(Risk treatment), 리스크 정보

교환 및 상담(Communication & consultation) 등의 세부절차를 통하여 특정 조직 또는 단체의 리스크를 총괄적으로 관리하는 것을 포함한다.

- (3) “리스크 관리 시스템(Risk management system)”이라 함은 특정 조직 또는 단체의 리스크를 지속적으로 관리하기 위한 조직화된 체계를 말한다. 이 시스템에는 전략계획, 의사결정, 조직의 문화 등을 포함한다.
- (4) “리스크 관리 정책(Risk management policy)”이라 함은 리스크 관리와 관련된 특정 조직의 방침과 전체 목적에 대한 설명을 의미한다.
- (5) “리스크 관리 계획(Risk management plan)”이라 함은 리스크 관리에 적용되는 관리 구성요소 및 수단, 접근방식을 구체화하기 위해 리스크 관리 시스템에 포함되는 계획을 말한다.

(가) 관리 구성요소는 절차, 실행, 책임자 지정, 활동 시기 및 순서를 포함한다.

(나) 리스크 관리 계획은 제품, 공정 및 프로젝트, 조직 전체 또는 일부에 적용될 수 있다.

3.2. 리스크 관리 절차(Risk management process)와 관련된 용어

“리스크 관리 절차(Risk management process)”라 함은 특정 조직 또는 단체에 대한 환경조건 설정을 시작으로 리스크를 확인, 분석, 평가하고 그 리스크를 어떻게 처리할 것인지에 대한 리스크 처리 방법, 리스크 검토 및 모니터링, 내부 및 외부와의 리스크 정보교환 및 상담 등 세부적인 단계의 적용을 말한다.

3.2.1 환경조건(Context)

“환경조건(Context)”이라 함은 리스크를 관리할 때 그리고 리스크 기준 및 범위를 설정할 때 고려해야 할 외부 또는 내부의 변수를 말한다.

- (1) “외부 환경조건(External context)”이라 함은 특정 조직 또는 단체가 목적을 달성하고자 추구하는 외부 환경조건을 말한다. 외부 환경조건은 다음과 같은 항목을 포함한다.

(가) 국외, 국내, 지방 또는 지역의 문화, 사회, 정치, 법률, 규정, 재정, 기술, 경제 및 경쟁 환경조건

(나) 조직의 목적에 영향을 미치는 핵심 원동력

(다) 외부 관계자의 평가와 인식 및 외부 관계자와의 관계

(2) “내부 환경조건(Internal context)”이라 함은 특정 조직 또는 단체가 목적을 달성하고자 추구하는 내부 환경조건을 말한다. 내부 환경조건은 다음과 같은 항목을 포함한다.

(가) 조직의 지배구조, 조직 구성, 규칙 및 책임

(나) 목적 달성을 위한 정책, 전략

(다) 조직의 자원 및 역량(자본, 시간, 인력, 공정, 시스템 및 기술)

(라) 정보 시스템, 정보 흐름, 의사결정 과정(공식 및 비공식 포함)

(마) 내부 관계자의 평가와 인식 및 내부 관계자와의 관계

(바) 조직 문화

(사) 조직에서 채택한 규칙, 지침과 모델

(아) 계약 관계의 형태 및 범위

(3) “리스크 기준(Risk criteria)”이라 함은 리스크의 유의성(Significance)을 판단하기 위한 기준 항목을 말한다.

(가) 리스크 기준은 조직의 목적, 외부 또는 내부 환경조건을 바탕으로 한다.

(나) 리스크 기준에는 관련 비용 및 이익, 법적 요건, 사회·경제·환경적 측면, 당사자

의 관심사, 우선순위, 평가에 대한 기타 고려사항을 포함한다.

3.2.2 리스크 평가(Risk assessment)

“리스크 평가(Risk assessment)”라 함은 리스크 확인(Risk identification), 리스크 분석(Risk analysis), 리스크 수준 판정(Risk evaluation)에 대한 전체적인 과정을 말한다.

(1) “리스크 확인(Risk identification)”이라 함은 리스크 근원을 찾아 인지하고 기술하는 과정을 말한다. 리스크 확인은 리스크 근원, 사상, 리스크 근원과 사상의 원인 및 잠재적인 결과의 확인을 포함한다. 리스크 확인은 과거 자료, 이론적 분석, 정보화된 견해 또는 전문가의 의견, 관계자의 요구를 포함한다.

(가) “리스크 설명(Risk description)”이라 함은 리스크의 근원, 사상, 원인 및 결과를 포함하는 리스크에 대한 체계적인 서술을 의미한다.

(나) “리스크 근원(Risk source)”이라 함은 리스크를 발생시키는 단일 또는 복수의 요인을 말한다. 리스크 근원은 보이거나 보이지 않을 수 있으며, 유해위험요인(Hazard)과 동일한 의미로 해석될 수 있다.

(다) “사상(Event)”이라 함은 특정한 단위 상황의 발생 또는 변화를 말한다.

① 사상은 확실하거나 불확실할 수 있다.

② 사상은 하나 또는 여러 개의 사상으로 이루어질 수 있다.

③ 사상은 결과를 초래하거나 초래하지 않을 수 있다.

(라) “사고(Accident)”라 함은 유해위험요인(Hazard)을 근원적으로 제거하지 못함으로써 위험에 노출되어 사망, 상해, 질병 및 기타 경제적 손실 등 원하지 않는 결과를 초래하는 비고의적인 사상을 말한다.

(마) “사건(Incident)”이라 함은 유해위험요인으로 인한 사고(Accident), 앗차사고(Near miss), 고의성이 전제되는 범죄(Crime)를 포함하는 사상을 말한다.

(바) “유해위험요인(Hazard)”이라 함은 위해의 잠재적 근원을 말한다. 유해위험요인은 리스크 근원(Risk source)이 될 수 있다.

(사) “위해(Harm)”라 함은 신체적 상해, 사람의 건강에 대한 손상 또는 재산이나 환경에 대한 손실을 말한다.

(아) “리스크 책임자(Risk owner)”라 함은 리스크를 관리하는 책임과 권한을 가진 사람을 말한다.

(2) “리스크 분석(Risk analysis)”이라 함은 리스크 수준(Risk level)을 결정하고, 리스크의 특성을 이해하기 위한 과정을 말한다. 리스크 평가와 리스크 처리에 대한 결정은 리스크 분석의 결과를 바탕으로 이루어진다.

(가) “가능성(Likelihood)”이라 함은 사상의 발생 가능한 정도를 말한다.

① 가능성은 확률(Probability) 또는 빈도(Frequency)로 표현할 수 있다.

② “확률(Probability)”이라 함은 일정한 조건 아래에서 특정 사건이나 사상이 일어날 가능성을 의미하며, 분율(0~1) 또는 퍼센트(0~100 %)로 표시한다.

③ “빈도(Frequency)”라 함은 특정한 시간 내에 특정 사건이나 사상이 일어날 가능성을 의미한다.

(나) “결과(Consequence)”라 함은 특정 목적에 영향을 미치는 사상의 산출물(Output)을 말한다.

① 결과는 단일 사상에서 단일 또는 복수의 산출물이 발생할 수 있다.

② 결과는 긍정적이거나 부정적일 수 있다.

③ 결과는 정성적 또는 정량적으로 표현할 수 있다.

(다) “노출(Exposure)”이라 함은 특정 조직 또는 관계자가 사상에 관련되는 정도를 말한다.

(라) “리스크 매트릭스(Risk matrix)”이라 함은 가능성과 결과에 대한 범위를 구분하여 리스크 등급을 표시하고, 리스크 우선순위를 정하기 위한 도구를 말한다.

(마) “리스크 수준(Risk level)”이라 함은 가능성과 결과가 조합되어 표현된 단일 또는 복수의 리스크에 대한 크기를 말한다.

(3) “리스크 수준 판정(Risk evaluation)”이라 함은 리스크 또는 리스크 경감이 수용할만한 수준인지 결정하기 위하여 주어진 리스크 기준과 리스크 분석의 결과를 비교하는 과정을 말한다. 리스크 수준 판정은 리스크 처리 결정을 위해 보조적으로 활용된다.

(가) “리스크 태도(Risk attitude)”라 함은 특정 조직 또는 단체가 리스크를 회피 또는 수용, 보유, 추구, 평가에 대하는 태도를 말한다.

(나) “리스크 선호(Risk appetite)”라 함은 특정 조직 또는 단체가 리스크를 추구하거나 보유할 의지가 있는 리스크의 유형과 정도를 말한다.

(다) “리스크 기피(Risk aversion)”라 함은 리스크를 피하려는 성향을 말한다.

(라) “리스크 통합(Risk aggregation)”라 함은 전체 리스크 수준을 이해하기 위해 다수의 리스크를 하나의 리스크로 통합시키는 것을 말한다.

(마) “리스크 허용한계(Risk tolerance)”라 함은 특정 조직 또는 관계자가 목적을 달성하기 위하여 리스크 처리(Risk treatment) 이후의 리스크를 허용할 수 있는 한계를 말한다.

(바) “리스크 수용(Risk acceptance)”이라 함은 특정 리스크를 수용하는 것을 말한다. 리스크 수용은 리스크 처리(Risk treatment) 없이 또는 처리 과정 중에 발생할 수 있다. 수용된 리스크는 모니터링(Monitoring)과 검토(Review)의 대상이 된다.

3.2.3 리스크 처리(Risk treatment)

“리스크 처리(Risk treatment)”라 함은 리스크를 처리하기 위한 방안을 선택하고 집행하는 과정을 말한다. 리스크 처리에는 리스크 회피, 리스크 감소 및 제거, 리스크 분담,

리스크 보유 등의 방법이 있다. 리스크 처리는 새로운 리스크를 발생시킬 있거나 현재의 리스크를 변화시킬 수 있다.

- (1) “리스크 통제(Risk control)”라 함은 리스크를 통제하기 위한 조치를 말한다. 리스크 통제는 리스크를 통제하는 과정, 정책, 실행 및 그 이외의 활동을 포함한다.
- (2) “리스크 회피(Risk avoidance)”라 함은 특정 리스크에 노출되지 않기 위한 활동 또는 개입되지 않기 위한 결정을 말한다. 리스크 회피에 대한 결정은 리스크 수준 판정의 결과를 바탕으로 한다.
- (3) “리스크 분담(Risk sharing)”라 함은 다른 관계자와 동의하여 리스크를 서로 공유하는 것을 말한다.
 - ① 리스크 분담은 보험 또는 다른 형태의 계약을 통해 수행되어 질 수 있다.
 - ② 리스크 분담 정도는 분담 약정의 명확성 및 신뢰성에 의존한다.
 - ③ 리스크 전가는 리스크 분담 방법 중의 하나이다.
- (4) “리스크 재무(Risk financing)”라 함은 리스크 처리에 대한 실행 비용과 관련 비용을 충당할 자금의 준비를 말한다.
- (5) “리스크 보유(Risk retention)”라 함은 특정 리스크로부터 발생하는 손실부담 또는 잠재적 이익에 대한 수용을 말한다. 리스크 보유는 잔존 리스크(Residual risk)를 포함하며, 보유한 리스크 수준은 리스크 기준에 따라 달라질 수 있다.
- (6) “잔존 리스크(Residual risk)”라 함은 리스크 처리 후에도 남아 있는 리스크를 말한다. 잔존 리스크는 확인되지 않은 리스크도 포함한다.

3.2.4 리스크 정보교환 및 상담(Risk communication and consultation).

“리스크 정보교환 및 상담(Risk communication and consultation)”이라 함은 특정 조직 또는 단체가 관계자(Stakeholders)와 협의하여 리스크 관리에 대한 정보를 제공, 공유 또는 얻기 위해 수행하는 연속적이면서 반복적인 과정을 말한다.

- (1) “관계자(Stakeholders)”라 함은 리스크 관리 활동 또는 결정에 의해 영향을 주고 받거나, 주고 받을 것으로 예상되는 특정 조직, 단체 또는 개인을 말하며 의사결정자도 관계자가 될 수 있다.
- (2) 정보는 리스크의 존재, 특징, 형태, 가능성, 중대성, 평가, 수용, 처리와 관련된다.
- (3) “리스크 인식(Risk perception)”이라 함은 관계자가 특정(관심대상) 리스크에 대해 바라보는 관점을 말한다. 리스크 인식은 관계자의 요구, 현안, 지식, 믿음, 가치관을 반영한다.

3.2.5 리스크 모니터링 및 검토(Risk monitoring and review)

“리스크 모니터링(Risk monitoring)”이라 함은 요구되거나 예상된 성능 수준으로부터의 변화를 확인하기 위하여 상태를 지속적으로 점검, 감독, 관찰하는 것을 말한다. 모니터링은 리스크 관리 시스템, 리스크 관리 절차, 리스크 또는 통제에 적용될 수 있다. “검토(Review)”라 함은 설정된 목적을 달성하기 위하여 주제의 적합성, 타당성, 효과를 결정하기 위해 착수된 활동을 말한다.

- (1) “리스크 보고(Risk reporting)”라 함은 내부 또는 외부 관계자에게 리스크와 리스크 관리에 대한 현재 상태의 정보를 제공하는 것을 말하여, 의사소통에 대한 하나의 형태이다.
- (2) “리스크 등록(Risk register)”이라 함은 확인된 리스크에 대한 정보를 등록하는 것을 말한다.
- (3) “리스크 프로파일(Risk profile)”이라 함은 조직 또는 단체에서 관리 대상이 되는 리스크의 우선순위 및 그에 관한 설명을 말한다.
- (4) “리스크 관리 감사(Risk management audit)”라 함은 리스크 관리 체계를 객관적으로 평가하고, 입증하기 위한 체계적이고 문서화된 과정을 말한다.