KOSHA GUIDE
X - 29 - 2012

안전확보를 위한 정보기술시스템에 관한 리스크 관리지침

2012. 6.

한국산업안전보건공단

안전보건기술지침의 개요

○ 작성자 : 사단법인 한국안전학회 리스크관리 연구위원회
연세대학교 화공생명공학과 박재득

○ 개정자 : 산업안전보건연구원 안전연구실

○ 제·개정 경과

- 2010년 11월 리스크관리분야 제정위원회 심의(제정)
- 2012년 4월 리스크관리분야 제정위원회 심의(개정, 법규개정조항 등 반영)

○ 관련규격 및 자료

- Risk Management Guide for Information Technology Systems: NIST, 2002

○ 기술지침의 적용 및 문의

이 기술지침에 대한 의견 또는 문의는 한국산업안전보건공단 홈 페이지 안전보건 기술지침 소관 분야별 문의처 안내를 참고하시기 바랍니다.

공표일자 : 2012년 6월 20일
제 정 자 : 한국산업안전보건공단 이사장

KOSHA GUIDE
X - 29 - 2012

안전확보를 위한 정보기술시스템에 관한 리스크 관리 지침

1. 목 적

이 지침은 정보기술시스템을 이용하는 사업장에 대하여 효과적인 리스크 관리의 토대를 제공하고, 리스크 평가와 관련된 방안을 제공하는데 목적이 있다.

2. 적용범위

이 지침은 사업장의 생산현장 자동화 설비, 공정 제어설비, 자산・인력관리 등에 활용하는 정보기술시스템에 관련된 리스크를 평가하는 업무에 적용된다.

3. 용어의 정의

(1) 이 지침에서 사용되는 용어의 정의는 다음과 같다.

(가) “자원(Resource)”이라 함은 컴퓨터 프로그램을 작동시키기 위한 모든 기능과 기구의 총칭. 주기억 장치, 중앙 처리 장치, 입출력 장치, 데이터, 파일, 프로그램 등을 말한다.

(나) “정보기술시스템(Information technology system)”이라 함은 사업장의 생산현장 자동화 설비, 공정 제어설비, 자산・인력관리 등에 활용하는 전산체계를 말한다.

(2) 그 밖에 이 지침에서 사용하는 용어의 정의는 이 지침에 특별한 규정이 있는 경우를 제외하고 산업안전보건법, 같은 법 시행령, 같은 법 시행규칙, 산업안전보건기준에 관한 규칙 및 KOSHA GUIDE X-1-2011(리스크 관리의 용어 정의에 관한 지침)에서 정하는 바에 의한다.

4. 역할에 따른 주요임무

리스크 관리와 관련된 업무를 담당하는 주요 직원의 역할은 다음과 같다.

4.1 고위경영진 (Senior management)

(1) 고위경영진은 업무를 위해 필요한 역량을 개발하기 위하여 사·내외의 자원을 효과적으로 이용할 수 있도록 한다.

(2) 고위경영진은 의사결정 단계에 리스크 평가 활동의 결과를 포함하여 평가한다.

(3) 고위경영진은 정보기술과 관련된 리스크를 평가하거나 처리하는 리스크 관리 절차에 참여한다.

4.2 최고정보책임자 (Chief Information Officer, CIO)

(1) 최고정보책임자는 정보기술 계획, 예산, 실행, 보안정보 등의 업무를 관장한다.

(2) 최고정보책임자는 효과적인 리스크 관리 결과를 참고하여 의사결정을 한다.

4.3 시스템 및 정보 관리자

(1) 시스템 및 정보관리자는 정보기술시스템과 관련 자료를 적절하게 통제한다.

(2) 시스템 및 정보관리자는 정보기술시스템의 변경에 대한 업무를 수행한다.

(3) 시스템 및 정보관리자는 시스템의 개선, 소프트웨어 및 하드웨어의 주요한 변경 등에 대하여 의견을 제시한다.

(4) 시스템 및 정보관리자는 리스크 관리 절차에 참여한다.

4.4 정보기술시스템의 사용부서 등 관리자

(1) 사업의 운영 또는 정보기술시스템의 조달과정 등에 책임있는 관리자는 리스크 관리 절차에 참여한다.

(2) 관리자는 필요한 개선 방안을 결정한다.

(3) 관리자가 리스크 관리 절차에 참여함으로써 정보기술시스템이 최소의 비용으로 최대의 효과를 낼 수 있도록 한다.

4.5 정보시스템 보안 책임자 (Information system security officer, ISSO)

(1) 정보시스템 보안 책임자는 사업장의 보안 프로그램, 리스크 등을 관리한다.

(2) 정보시스템 보안 책임자는 사업장의 업무를 지원하는 정보기술시스템의 리스크를 확인, 평가, 최소화하는 구조화된 방법론 제시를 위한 선도적인 역할을 한다.

(3) 정보시스템 보안 책임자는 고위경영진의 업무가 지속적으로 잘 이루어질 수 있도록 지원한다.

4.6 정보기술 보안 담당자

(1) 정보기술 보안 담당자는 정보기술시스템의 필수적인 보안사항을 적절하게 실행한다.

(2) 네트워크 연결 확장, 기반시설의 변화, 새로운 기술의 도입 등 정보기술시스템 환경의 변화에 따라 정보기술 보안 담당자는 새로운 잠재적인 리스크를 통제하기 위하여 리스크 관리 절차를 이용한다.

(3) 사업장의 정보기술시스템의 상황을 정확하게 알아야 하며, 정기적인 취약요인 평가를 실시하고 적절한 조치를 취한다.

(4) 공용 네트워크상에서는 업무에 중요한 데이터가 노출될 위험이 있는 경우 외부의 접근을 방지하기 위해 암호화한다.

(5) 비밀번호 시스템 등의 적절한 인증 시스템을 사용하여 관계자외의 접근을 막기 위한 기술적인 방안을 강구하고 적용한다.

5. 리스크 평가

5.1 일반사항

(1) 정보기술시스템의 리스크에 대한 잠재적인 취약요인 및 가동 중인 정보기술시스템의 통제에 대하여 분석한다.

(2) 리스크의 영향은 정보기술시스템 구성 및 데이터 등 정보기술 자산에 영향을 미치는 자원에 따라 다르게 분석된다.

(3) 리스크 평가는 다음과 같이 9단계로 나눌 수 있다.

(가) 단계 1 : 시스템 특성화

(나) 단계 2 : 리스크 확인

(다) 단계 3 : 취약요인 확인

(라) 단계 4 : 통제 분석

(마) 단계 5 : 가능성 결정

(바) 단계 6 : 영향 분석

(사) 단계 7 : 리스크 결정

(아) 단계 8 : 리스크 처리

(자) 단계 9 : 결과 문서화

5.2 1 단계 : 시스템 특성화

5.2.1 일반사항

(1) 정보기술시스템에 대한 리스크 평가를 위하여 활동범위를 결정한다.

(2) 정보기술시스템의 범위는 시스템을 구성하는 자원 및 정보를 통해 확인할 수 있다.

(3) 정보기술시스템의 특성화는 리스크 평가의 활동범위와 리스크 정의를 위해 필수적인 하드웨어, 소프트웨어, 시스템 등에 대한 정보를 제공할 수 있도록 한다.

(4) 시스템 관련 정보는 정보기술시스템과 운영환경을 특성화하는데 사용된다.

5.2.2 시스템 관련 정보

(1) 리스크 평가를 수행하는 담당자는 시스템의 처리환경을 이해하여야 하므로 시스템과 관련된 다음의 정보를 수집한다.

(가) 하드웨어

(나) 소프트웨어

(다) 시스템 인터페이스

(라) 데이터 및 정보

(마) 정보기술시스템을 지원하거나 사용하는 담당자

(바) 시스템의 역할

(사) 시스템 및 데이터의 리스크 상태

(아) 시스템 및 데이터의 민감성

(2) 정보기술시스템의 운전환경과 관련된 추가적인 정보는 다음 내용을 포함할 수 있다.

(가) 정보기술시스템의 기능적 요구사항

(나) 시스템 이용자

(다) 정보기술시스템 관리를 위한 시스템 보안 정책 및 구성

(라) 네트워크 기술

(마) 보호 장치 시스템

(바) 정보기술시스템에서의 정보 흐름

(사) 암호 등의 기술적 통제

(아) 시스템 유지보수 등의 관리

(자) 시설 안전, 데이터 정책 등의 물리적 환경

(차) 습도, 전원, 온도 등

(3) 시설 안전과 관련된 기술적인 내용은 KOSHA CODE D-28-2006(제어실의 위치선정 및 설계에 관한 기술지침)을 참고한다.

5.3 2 단계 : 리스크 확인

5.3.1 일반사항

(1) 취약요인은 우연한 계기로 나타날 수 있고, 의도적으로 활용될 수도 있다.

(2) 취약요인이 없는 경우 리스크의 근원은 존재하지 않는다.

5.3.2 리스크 근원 확인

(1) 이 단계는 정보기술시스템이 평가될 때 적용할 수 있는 리스크의 근원을 확인하는 것이다.

(2) 일반적인 리스크의 근원은 자연적, 인간적, 환경적인 것으로 구분할 수 있다.

(3) 리스크의 근원을 확인하기 위하여 정보기술시스템의 처리환경에서 손상을 유발하는 모든 리스크의 근원을 고려한다.

5.4 3 단계 : 취약요인 확인

5.4.1 일반사항

(1) 정보기술시스템에 대한 리스크 분석은 시스템 환경과 관련 있는 취약요인 분석을 포함한다.

(2) 이 단계는 리스크 근원에 의해 시스템의 취약요인에 대한 목록을 개발하는 것이다.

5.4.2 안전성 확인 체크리스트 개발

(1) 리스크 평가 직원은 정보기술시스템에 규정될 필수 안전사항을 결정한다.

(2) 안전성 확인 체크리스트는 정보기술시스템과 관련된 자산, 정보전달, 절차 등의 취약요인을 체계적으로 평가 및 확인 하는데 이용될 수 있는 다음의 기본적인 안전 기준을 포함 한다.

(가) 관리

(나) 운영

(다) 기술

(3) 안전 영역별 정보기술시스템의 취약요인을 식별하는데 <표 1>를 참고할 수 있다.

<표 1> 안전 기준

안전 영역	안전 기준
관리	• 책임 부여

	• 지원의 연속성 • 사고대응 기능 • 보안 관리의 정기적인 검토 • 직원 배경 조사 • 리스크 평가 • 보안 및 기술 훈련 • 직무 분리 • 시스템 인증 및 재인가 • 시스템 또는 보안 계획
운영	• 공기 오염물질 통제 (예: 연기, 먼지, 화학물질 등) • 전력공급의 품질을 보장하기 위한 통제 • 데이터 미디어 접근 및 폐기 • 외부 데이터 분배 및 등급 표시 • 시설 보호 (예: 자동화 생산현장, 전산실, 데이터 센터, 사무실 등) • 습도 통제 • 온도 통제 • 탁상용 컴퓨터, 노트북
기술	• 의사소통 (예: 직통전화, 시스템 연결) • 암호화 • 임의의 접근 제한 • 확인 및 인증 • 침입 탐지 • 시스템 감사

5.5 4 단계 : 통제 분석

(1) 이 단계는 시스템의 취약요인으로 인한 리스크의 가능성을 최소화하거나 제거하기 위한 통제를 분석하는 것이다.

(2) 리스크 환경과 관련된 잠재적인 취약요인의 전체적인 가능성을 확인하기 위하여 현재 또는 계획된 통제의 성취 정도를 확인한다.

5.6 5 단계 : 가능성 결정

(1) 리스크 환경과 관련된 구조 내에서 잠재적인 취약요인이 확인될 가능성을 도출하기 위하여 다음의 요소를 고려한다.

(가) 리스크 근원 유도 및 가능성

(나) 취약요인의 특성

(다) 통제 효과

(2) 잠재적인 취약요인이 리스크의 근원으로 작용할 수 있는 가능성은 높음, 중간, 낮음으로 <표 2>와 같이 구분할 수 있다.

<표 2> 가능성 구분

가능성 등급	가능성 구분
높음	리스크 근원의 동기 및 발생 가능성이 매우 높으며, 취약요인을 예방하기 위한 통제가 효과적이지 못하다.
중간	리스크 근원의 동기 및 발생 가능성이 높지만 통제를 통해 취약요인을 예방할 수 있다.
낮음	리스크 근원의 동기 및 발생 가능성이 낮으며 통제 및 최소한의 조치를 통해 취약성을 예방할 수 있다.

5.7 6 단계 : 영향분석

(1) 영향분석은 취약요인으로 인한 부정적인 영향을 결정할 수 있다.

(2) 영향분석을 시작하기 전에 다음의 정보를 수집한다.

(가) 시스템 임무

(나) 시스템 및 데이터의 리스크 상태

(다) 시스템 및 데이터의 민감성

5.8 7 단계 : 리스크 결정

(1) 이 단계는 정보기술시스템의 리스크 수준을 판정하는 것이다.

(2) 특정한 리스크 및 취약요인에 대한 리스크의 결정은 다음 사항을 참고한다.

(가) 리스크 근원의 가능성

(나) 취약요인에 미치는 영향의 크기

(다) 리스크를 감소 또는 제거시키기 위한 기존 조치의 타당성

(3) 리스크 결정을 위하여 리스크 측정, 리스크 규모, 리스크 수준 매트릭스 등을 개발하여 활용한다.

5.9 8 단계 : 리스크 처리

(1) 리스크 처리 단계에서는 확인된 리스크를 감소·제거할 수 있는 방안을 제시한다.

(2) 리스크 처리 단계의 목표는 정보기술시스템에서 리스크를 허용한계까지 낮추는 것이다.

(3) 리스크를 최소화하거나 제거하기 위하여 다음과 같은 요소를 고려한다.

(가) 시스템의 호환 가능성 등 효율성

(나) 법률 및 규정

(다) 조직의 정책

(라) 운영의 영향

(마) 안전성 및 신뢰성

(4) <부록>의 <별표 1>은 리스크 수준 매트릭스, <별표 2>는 리스크 수준별 필요 조치사항에 대한 예를 나타낸다.

5.10 9 단계 : 결과 문서화

(1) 리스크 평가 결과는 보고서로 문서화한다.

(2) 리스크 평가 보고서는 관리자 및 운영자, 정책, 절차, 예산, 시스템 운영 등의 결정에 활용한다.

(3) 리스크 평가 보고서는 리스크에 대한 체계적이고 분석적인 접근 방법을 통해 잠재적 손실을 줄일 수 있도록 구성한다.

6. 관련 시스템의 오경보

6.1 오경보의 발생 원인

(1) 장비 사용자나 종사원의 잘못된 기기사용

(2) 설치회사의 잘못된 설치와 유지 보수

(3) 경보기기의 자체 결함

(4) 일반전화선을 이용하는 등의 통신회로의 문제

(5) 자연현상에 대한 기기의 그릇된 감지

(6) 실제 사고 발생, 관계자외의 진입 등 이상상황시 경보가 작동하지 않는 상태

(7) 원인을 알 수 없는 기타 장애

6.2 오경보 시 안전사고 예방을 위한 주의 사항

(1) 설정된 안전장치 등을 임의로 해지하고 위험지역 출입

(2) 혼자서 위험지역의 경보시스템을 점검

(3) 위험지역 출입관련 안전절차 미준수

(4) 담당자가 아닌 기기의 임의조작

6.3 오경보 발생 시 대응

(1) 문제의 정의

(2) 문제의 분해

(3) 중요하지 않는 내용의 제거

(4) 작업계획 수립

(5) 분석 수행

(6) 결과 종합

6.4 비상상황

6.4.1 비상상황 발생 시 대응

(1) 비상상황 대응을 위한 조직 구성 및 계획 수립

(2) 비상상황에 대한 판단

(3) 비상상황 선언 및 보고

(4) 비상상황 대응 조직 운영 및 복구

6.4.2 비상상황 선언 시 참고 요소

(1) 비상상황 선언 시 참고 자료

(가) 1차 담당자 보고자료

(나) 2차 경영진 보고자료

(다) 장애 등급 및 비상 계획서

(2) 비상상황 선언권자

(가) 장애의 규모와 피해 정도에 따라 사전에 계획된 등급에 따라 결정

(3) 비상상황 선언 목표시간

(가) 대형 장애 시 최초 경영진 보고 후 권고시간 이내

(4) 비상상황 선언 방법

(가) 유무선 전화

(나) 대내외 메일

(다) 대내외 공지

(5) 비상상황 선언 내용

비상상황 선언 시에는 장애 등급과 관련된 기본적인 내용 선언

(6) 비상상황 선언 직후 상황실에서 할 일

비상상황 위원회 소집과 주요 의사결정 수행

<부록>

<별표 1> 리스크 수준 매트릭스

리스크 가능성	영향		
	낮음 (10)	중간 (50)	높음 (100)
높음 (1.0)	낮음 10 × 1.0 = 10	중간 50 × 1.0 = 50	높음 100 × 1.0 = 100
중간 (0.5)	낮음 10 × 0.5 = 5	중간 50 × 0.5 = 25	중간 100 × 0.5 = 50
낮음 (0.1)	낮음 10 × 0.1 = 1	중간 50 × 0.1 = 5	낮음 100 × 0.1 = 10

※ <별표 1>의 자료는 NIST "Risk Management Guide for Information Technology Systems" 자료의 25쪽 내용을 참조한 내용으로 실제 사업장과 맞지 않을 수 있다.

<별표 2> 리스크 수준별 필요 조치사항

리스크 수준	필요 조치사항
높음	리스크가 높을 경우 강도 높은 시정조치가 필요하다. 기존 시스템에 대하여 시정조치계획을 가능한 조속히 수립하고 이행한다.
중간	리스크가 중간일 경우에도 시정조치가 필요하다. 합리적으로 설정한 기간 내에 시정조치를 위한 계획을 수립하고 이행한다.
낮음	리스크가 낮을 경우 시스템 관리자는 리스크의 수용여부, 시정조치의 필요여부를 결정한다.